

Contents

Microsoft 365 admin center help

Get started

[Sign up](#)

[Try or buy Microsoft 365](#)

[Plan your setup](#)

[Plan for Windows 365 Business](#)

[Get started with Windows 365 Business and Cloud PCs](#)

[Windows 365 Business sizing options](#)

[Set up your organization with the guided setup](#)

[Microsoft 365 Business Basic](#)

[Microsoft 365 Business Standard](#)

[Microsoft 365 Business Premium](#)

[Microsoft 365 Apps for business](#)

[Explore the Setup page and wizard](#)

[Secure Windows 10 computers](#)

[Download software and product keys](#)

[Install Office apps](#)

[Set up windows devices](#)

[Set up mobile devices](#)

[Migrate your data to Microsoft 365](#)

[Roll out Teams](#)

[App training for everyone](#)

[What subscription do I have?](#)

[Customize Sign-in page](#)

[Customize your organization theme](#)

[Learn about Office 365 Germany](#)

[Access on-premises users and resources](#)

[Synchronize domain users to Microsoft 365](#)

[Enable domain-joined Windows 10 devices to be managed](#)

[Access resources from an Azure AD-joined device](#)

[Overview of the Microsoft 365 admin center](#)

[Admin center overview](#)

[About admin roles](#)

[Admin mobile app](#)

[What's new in the admin center](#)

[Search in the Microsoft 365 admin center](#)

[Stay on top of changes](#)

[Manage multiple tenants](#)

[Office 365 operated by 21Vianet](#)

[About Office 365 operated by 21Vianet](#)

[Download the Office app for Android for Office 365 operated by 21Vianet](#)

[Download the Office app for iOS for Office 365 operated by 21Vianet](#)

[Apply for a Fapiao](#)

[Azure Information Protection support](#)

[Manage users, groups, and passwords](#)

[Users](#)

[Add users](#)

[Add a new employee](#)

[Assign licenses to users](#)

[Assign admin roles](#)

[Unassign licenses from users](#)

[Guest users](#)

[Add guest users to a Microsoft 365 group](#)

[Change a user name and email address](#)

[Restore a user](#)

[Create template to add users](#)

[Upgrade users to the latest apps](#)

[Remove a former employee](#)

[Overview](#)

[Step 1. Prevent an employee from logging in and block access to Microsoft 365 services](#)

[Step 2. Save the contents of a former employee's mailbox](#)

Step 3. Forward a former employee's email to another employee or convert to a shared mailbox

Step 4. Give another employee access to OneDrive and Outlook data

Step 5. Wipe and block a former employee's mobile device

Step 6. Remove the Microsoft 365 license from a former employee

Step 7. Delete a former employee's user account

Groups

Groups overview

Compare groups

Create a group

Explain groups

Manage groups

Add or remove group members

Restore a deleted group

Manage guest access to groups

Passwords

Reset passwords

Let users reset passwords

Set passwords to never expire

Resend user passwords

Turn off strong passwords

Set the password expiration policy

Manage email and calendars

About user email settings

Add another email alias for a user

Use your custom domain

Migrate email and contacts to Microsoft 365

Create signatures and disclaimers

Create, edit, or delete a security group

Set up email forwarding

Shared mailboxes

About shared mailboxes

Create a shared mailbox

[Configure shared mailbox settings](#)

[Convert a user mailbox to a shared mailbox](#)

[Remove a license from a shared mailbox](#)

[Resolve issues with shared mailboxes](#)

[Set up Focused Inbox](#)

[Add user or contact to distribution group](#)

[Manage clutter for your organization](#)

[Manage domains](#)

[Add a domain](#)

[Buy a domain](#)

[Remove a domain](#)

[Transfer a domain from Microsoft 365 to another host](#)

[Pilot Microsoft 365 from my custom domain](#)

[Domains FAQ](#)

[DNS instructions](#)

[Change nameservers at any DNS host](#)

[Create DNS records at any DNS host](#)

[Troubleshoot domain issues](#)

[Manage your data and services](#)

[Monitor Microsoft 365 activity by using reports](#)

[Microsoft Productivity Score - overview](#)

[Content collaboration](#)

[Communication](#)

[Mobility](#)

[Teamwork](#)

[Meetings](#)

[Microsoft 365 Apps health](#)

[Endpoint Analytics](#)

[Change your organization contact info](#)

[Update your admin contact info](#)

[Customize the app launcher](#)

[Pin apps to users' app launcher](#)

[Upgrade users to the latest apps](#)

[Integrated apps](#)

[Centralized deployment of add-ins](#)

[Requirements for centralized deployment of add-ins](#)

[Deploy add-ins in the admin center](#)

[Manage add-ins in the admin center](#)

[Centralized Deployment FAQ](#)

[Manage industry news](#)

[Manage Office Scripts settings](#)

[Find a partner or a re-seller](#)

[Manage Microsoft feedback for your organization](#)

[Set up release options](#)

[Show or hide new features](#)

[Power BI usage analytics](#)

[About usage analytics](#)

[Enable usage analytics](#)

[Get the latest version of usage analytics](#)

[Navigate and use reports](#)

[About active users in usage reports](#)

[Customize reports](#)

[Usage analytics with Microsoft 365 GCC](#)

[About the usage analytics data model](#)

[Troubleshoot usage analytics errors](#)

[Manage subscriptions and billing](#)

[Secure your organization](#)

[Top 10 ways to secure your data](#)

[Multi-factor authentication for Microsoft 365](#)

[Set up multi-factor authentication](#)

[Manage and monitor priority accounts](#)

[Enable Modern Authentication for Office 2013](#)

[Secure Microsoft 365 Business Premium](#)

[Pre-requisites for data protection](#)

Security features

Increase threat protection

Threats detected by Microsoft Defender Antivirus

Review detected threats and take action

Set up compliance features

Secure score

A guide to GDPR compliance

Manage devices and app data

Device and app data protection methods

Microsoft Intune documentation

Microsoft 365 Business Premium

View and edit policies and devices

Remove company data

Reset devices to factory settings

Map protection features to Intune settings

Device states

App protection settings for Windows 10 PCs

Set app protection settings for Android and iOS

Validate settings on Android or iOS

Edit or create device protection settings for Windows 10 PCs

Validate settings on Windows 10 PCs

Autopilot

Add Autopilot devices and profile

Create and edit AutoPilot profiles

Create and edit AutoPilot devices

AutoPilot Profile settings

Microsoft 365 for enterprise documentation

Basic Mobility and Security

Overview of Basic Mobility and Security

Compare Basic Mobility and Security and Intune

Capabilities of Basic Mobility and Security

Set up Basic Mobility and Security

- Create device security policies
- Create an APNs certificate for iOS devices
- Manage device access settings
- Get details about managed devices
- Manage enrolled devices
- Enroll your mobile device
- Privacy and security
- Frequently asked questions
- Wipe mobile devices
- Turn off Basic Mobility and Security
- Troubleshoot

Work with customers

- Share sites and files with guest users
- Share calendars with guest users
- Create a Team with guest users
- Schedule a Teams meeting with guest users
- Join a Teams meeting with guest users

Troubleshoot

Contact support

Navigation guide

How to sign up - Admin Help

7/12/2021 • 3 minutes to read • [Edit Online](#)

Sign up for Microsoft 365 for business so that your team can begin using the latest versions of Word, Excel, PowerPoint, and other Office programs.

If you're in China, Office 365 operated by 21Vianet is designed to meet the needs for secure, reliable, and scalable cloud services in China. This service is powered by technology that Microsoft has licensed to 21Vianet. Microsoft does not operate the service itself. 21Vianet operates, provides, and manages delivery of the service. 21Vianet is the largest carrier-neutral Internet data center services provider in China, providing hosting, managed network services, and cloud computing infrastructure services. By licensing Microsoft technologies, 21Vianet operates local Microsoft datacenters to provide you the ability to use Microsoft services while keeping your data within China. 21Vianet also provides your subscription and billing services, as well as support.

NOTE

These services are subject to Chinese laws.

Sign up for Office 365 operated by 21Vianet so that your team can begin using the latest versions of Word, Excel, PowerPoint, and other Office programs.

Ready to sign up? [Select a Plan](#).

Choose a plan

Before you buy, put some thought into the plan you sign up for. This will help prevent growing pains later.

Watch: Choose a Microsoft 365 subscription

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

Need help with choosing a plan? Sales consultants are available to answer your questions. Go to [Compare all products](#) and choose one of the contact support options listed at the left side of the page.

Choose a plan

Before you buy, put some thought into the plan you sign up for. This will help prevent growing pains later.

Need help with choosing a plan? Sales consultants are available to answer your questions. Just go to [Compare all products](#) and choose one of the contact support options listed at the left side of the page.

Ready to sign up for a free trial or buy a subscription?

Go to [Compare all products](#) to choose the plan you want to buy and to start the sign-up wizard.

If you start with a free trial, you can [buy it later](#). All your users and data from the trial will still be there.

You don't need to cancel your trial. If you don't buy the trial subscription, it automatically expires at the end of the trial period, and all the information is permanently deleted.

Watch: Set up Microsoft 365 Business Premium

Ready to sign up for a free trial or buy a subscription?

Go to [Compare all products](#) to choose the plan you want to buy and to start the sign-up wizard.

If you start with a free trial, you can [buy it later](#). All your users and data from the trial will still be there.

You don't need to cancel your trial. If you don't buy the trial subscription, it automatically expires at the end of the trial period, and all the information is permanently deleted.

You'll be asked for the following information when you sign up

- **The address and contact information for your subscription:**
 - **Country** where the services will be used. You **won't** be able to change the country later, even during the sign up process; you'll have to restart the sign up wizard.
 - **Email and phone number** so we can contact you if needed about your subscription. For example, if you forget your password, we would use this information to send you a temporary one. We also send your billing information to the email address you specify.

NOTE

The email address you enter here is different from your Microsoft 365 email address (your logon name, below). Because this is where we also send your billing information, we recommend you use an e-mail address that's appropriate for receiving business email.

- **A sign-in name (user ID):** This user ID becomes your initial Microsoft 365 email address, just to get you started quickly.

This user ID is the email address that you use to sign in. For example, if your business name is Fourth Coffee, you might choose rob@fourthcoffee.onmicrosoft.com for your user ID.

Most people add their own custom domain shortly after they sign up so they can start getting email to it. For example, if you have a custom domain named fourthcoffee.com, you can set up your email address as rob@fourthcoffee.com.

- **Payment information:**

You can pay for your subscription with a credit card. If the cost reaches a certain amount, you may also have the option to pay by invoice.

IMPORTANT

When you sign up, be sure to choose the best payment option for your organization. Changing payment options involves calling billing support.

Related content

[Microsoft 365 for business training videos](#) (link page)

Try or buy a Microsoft 365 for business subscription

7/12/2021 • 6 minutes to read • [Edit Online](#)

Microsoft 365 for business is a subscription service that lets you run your organization in the cloud while Microsoft takes care of the IT for you. Microsoft manages devices, protects against real-world threats, and provides your organization with the latest in business software. You can sign up for a free trial subscription for Microsoft 365 Business Standard, Microsoft 365 Business Premium, or Microsoft 365 Apps for business and try it out for 30 days.

NOTE

You must use a credit card when you sign up for a free trial. At the end of your free trial period, your trial subscription is automatically converted to a paid subscription. Your credit card isn't billed until the end of the trial period.

IMPORTANT

Payment options for Office 365 operated by 21Vianet in China International credit cards are not accepted. You can pay for your subscription by:

- Invoice
- Online payment using Alipay or China UnionPay Proof of payment will be provided in the form of Fapiao. You can submit your Fapiao request to our [Fapiao system](#) about three (3) days after you have paid. For more information, see [Apply for a Fapiao for Office 365 operated by 21Vianet](#).

Before you begin

You don't need an existing Microsoft account to sign up for a free trial. For all other procedures in this article, you must be a Global or Billing admin for your organization. For more information, see [About admin roles](#).

Try a free trial subscription

Are you a new customer, and you don't already have an account with Microsoft? Use these steps to create an account and sign up for a free trial subscription of Microsoft 365 Business Standard, Microsoft 365 Business Premium, or Microsoft 365 Apps for business.

1. Go to the [Microsoft 365 Products site](#).
2. Select the plan that you want to sign up for, such as **Microsoft 365 Business Standard**, scroll down the page, and select **Try free for 1 month**.
3. On the next page, follow the steps to set up your account.
4. The sign up process may take several minutes to complete. After it's complete, you're ready to start the setup wizard for your subscription. For more information about setting up your subscription, see [Next steps](#).

Buy a subscription from your free trial

At the end of your free trial period, your trial subscription automatically converts to a paid subscription. The paid subscription defaults to the plan you currently have. You can buy a different plan by following the steps in [Buy a different subscription](#).

If you want to buy your subscription before your trial is over, use these steps:

1. In the Microsoft 365 admin center, go to the **Billing** > [Your products](#) page.
2. On the **Your products** page, find the subscription that you want to buy.
3. In the **Licenses** section, select **Purchase subscription**.
4. Choose either a monthly or annual commitment for your subscription, then select **Checkout**.
5. On the next page, verify the subscription, and select **Checkout**.
6. On the next page, verify the **Sold to** address, the **Billed to** information, and **Items in this order**. If you need to make any changes, select **Change** next to the applicable section.
7. When you're finished, select **Accept agreement & place order**.

Extend your trial

Do you need more time to try out the features of Microsoft 365 for business before buying? If your trial subscription is within 15 days of expiring and the trial hasn't been extended before then you can extend your trial for another 30 day period. You can only do this one time.

1. In the admin center, go to the **Billing** > [Your products](#) page.
2. On the **Products** tab, select the trial subscription that you want to extend.
3. On the subscription details page, in the **Subscriptions and payment settings** section, select **Extend end date**.
4. In the **Extend end date** pane, review the extension information, and if necessary, select a payment method. When you're finished, select **Extend trial**.

When you're ready to buy, see [Buy your trial version](#).

Cancel your free trial subscription

If you decide to cancel your trial subscription before the free trial period ends, go to the Microsoft 365 admin center and [turn off Recurring billing](#). The trial will automatically expire when your month ends, and your credit card won't be charged.

Try a different subscription

If you already have a Microsoft 365 for business subscription, you can use the Microsoft 365 admin center to try a different subscription.

When you add a subscription through the Microsoft 365 admin center, the new subscription is associated with the same organization (domain namespace) as your existing subscription. This association makes it easier to move users in your organization between subscriptions, or to assign them a license for the additional products they need.

1. In the admin center, go to the **Billing** > [Purchase services](#) page.
2. On the **Purchase services** page, you see the plans that are available to your organization. Choose the Microsoft 365 plan that you want to try.
3. On the next page, select **Get free trial**. The trial gives you 25 user licenses for a one-month term.
4. Choose to receive a text or a call, enter your phone number, then choose **Text me** or **Call me**.
5. Enter the verification code, then select **Start your free trial**.
6. On the **Check out** page, select **Try now**.
7. On the **order receipt** page, select **Continue**.

Buy a different subscription

If you already have a Microsoft 365 for business subscription, you can go through the Microsoft 365 admin center to buy a different subscription for your organization.

When you buy another subscription through the admin center, the new subscription is associated with the same organization (domain name space) as your existing subscription. This makes it easier to move users in your organization between subscriptions or assign them a license for the additional subscription they need.

1. In the admin center, go to the **Billing** > [Purchase services](#) page.
2. On the **Purchase services** page, select the plan that you want to buy, select **Details**, then select **Buy**.
3. Enter the number of licenses that you need and choose whether to pay each month or for the whole year. Choose whether you want to automatically assign licenses to everyone who does not currently have a license. Then select **Check out now**.
4. Review the pricing information and select **Next**.
5. Provide your payment information, and then select **Place order** > **Go to Admin Home**.

NOTE

You must move users from your free trial subscription to the new subscription before your 90-day grace period ends after your trial subscription expires. By doing this, you keep your data, accounts, and configuration. Otherwise, that information is deleted.

Payment options

You can pay for your subscription by:

- Invoice
- Online payment using Alipay or China UnionPay

Proof of payment will be provided in the form of Fapiaos. You can submit your Fapiao request to our [Fapiao system](#) about three (3) days after you have paid. For more information, see [Apply for a Fapiao for Office 365 operated by 21Vianet](#).

NOTE

International credit cards are not accepted.

Next steps

If you have a new account and are setting up your first subscription, you can use the guided setup articles to help you get started.

- [Set up Microsoft 365 Business Basic](#)
- [Set up Microsoft 365 Business Standard](#)
- [Set up Microsoft 365 Business Premium](#)
- [Set up Microsoft 365 Apps for business](#)

If you already have a subscription and are adding a new subscription, you can move users to it. To learn how, see [Move users to a different subscription](#).

Related content

[Microsoft 365 for business training videos](#) (video)

[Add users and assign licenses at the same time](#) (article)

[Assign licenses to users](#) (article)

[Upgrade to a different plan](#) (article)

[Buy or edit an add-on for Microsoft 365 for business](#) (article)

[Add storage space for your subscription](#) (article)

Plan your setup of Microsoft 365 for business

5/7/2021 • 7 minutes to read • [Edit Online](#)

This article is for people who have subscribed to a Microsoft 365 for business plan.

Before moving your organization to Microsoft 365, there are requirements you need to meet, info you need to have on hand, and decisions you have to make.

Info to have on hand before you run the setup wizard

When you're ready to run the setup wizard and move your domain to Microsoft 365, here's the info you'll need to have on hand:

- List of people you want to add to Microsoft 365. Even if you've already added them to Microsoft 365, if you're updating your domain information, you need to enter their names here.
- How you're going to notify your employees of their user ID and password so they can sign in. Are you going to call them with the info? Or send it to their personal email address? They won't have access to their email, so you can't use that.
- If you have a domain name for your organization (such as contoso.com) **and** you plan on using Microsoft email, you'll need to know where your domain is registered and have sign-in information.

What happens when you run the Microsoft 365 setup wizard

The setup wizard walks you through installing the Microsoft 365 apps on your computer, adding and verifying your domain, adding users and assigning licenses to them, and connecting your domain.

NOTE

If you need to [Assign admin roles in Microsoft 365 for business](#) to the users you add in the wizard, you can do that later on the [Users](#) page.

If you don't complete the setup wizard, you can complete setup tasks at any time from [admin center](#) > **Setup**. From here you can migrate email and contacts from another email service, change the domain of your admin account, manage your billing information, add or remove users, reset passwords, and do other business functions. For more information about the differences between the setup wizard and the **Setup** page, see [Differences between the Microsoft 365 setup wizard and the Setup page](#).

If you get stuck at any point, call us. [We're here to help!](#)

When not to use the setup wizard: Active Directory synchronization and hybrid environments

There are a couple of scenarios that include either migrating data or users from on-premises environments or setting up a hybrid system that includes directory synchronization. If you're in either category, follow the instructions in these articles:

- To set up directory synchronization with your on-premises Active Directory, see [Set up directory synchronization for Microsoft 365](#), and to understand the different identity models in Microsoft 365, read [Understanding Microsoft 365 identity and Azure Active Directory](#).

- To set-up an Exchange hybrid, the full set of instructions that guide you through all the different ways of setting up a hybrid exchange (including setting up DNS records) can be found here: [Exchange Server Deployment Assistant](#)
- To set up a SharePoint hybrid, particularly hybrid search and site features, see [Hybrid Search in SharePoint](#).

Move to Microsoft 365 all at once or in stages

- **Do you want to move your organization to Microsoft 365 all at once?** If so, then plan to move your domain to Microsoft 365 right away. Start by running the Microsoft 365 setup wizard; it will prompt you to set up your domain.
- **Do you want to move to Microsoft 365 gradually?** If you want to move to Microsoft 365 in stages, then skip running the Microsoft 365 setup wizard and consider adopting Microsoft 365 features in the following order:
 1. [Add your employees to Microsoft 365](#) so they can download and install the Office apps.
 2. [Download and install the Office apps](#) to use Word, Excel, and PowerPoint on your computer and devices.
 3. [Set up Microsoft Teams](#) to use for your meetings.
 4. [Move your content to Microsoft 365 cloud storage](#) (OneDrive or SharePoint team sites).
 5. When you're ready, in the [admin center](#), select **Setup** in the left navigation pane, and use the **Setup** page to [move your domain and email](#).

Check that your devices meet system requirements

Each person in your organization can install the Office 2016 suite of apps (Word, Excel, PowerPoint, and so on) on up to five PCs and Macs. See the operating system and computer requirements for installing [Office 2016 suites](#) for business.

Mobile apps can be installed on iOS, Android, and Windows devices. You can find information on mobile device and browser support in [System requirements for Office](#).

Plan for email

If you're planning to move from an existing email service to Microsoft 365, it usually takes two days to make the switch.

Plan for email downtime

If you're going to use Microsoft 365 for your email:

- To move your business email address (such as *rob@contoso.com*) from another email service to Microsoft 365, you need to direct your mail to be delivered to your new Microsoft 365 mailbox. You do this by selecting **Migrate your users' data** on the **Setup** page, where we guide you through the updates you need to make at your domain host, step by step.
- After you update your domain host, the changes typically take effect in just an hour or two. But be aware that it can sometimes take up to 72 hours for the changes to update across the internet.
- Because you might have email downtime, we recommend you plan to switch to Microsoft email during an evening or weekend when you receive fewer emails.

Plan to move your existing email, contacts, and calendar

If you're going to use Microsoft 365 for your email account, you can bring your existing email, contacts, and calendar with you. The **Setup** page helps you move your existing email and contacts for most scenarios. We also have step-by-step guides to move one or many mailboxes.

HOW MANY MAILBOXES?	RECOMMENDATION
Just a few	If you don't want to use the Setup page to migrate the mailboxes, you can let mailbox owners migrate their own email and contacts. See Migrate email and contacts to Microsoft 365 for business .
Several	If you're migrating from Gmail, see Migrate G Suite mailboxes to Microsoft 365 . If you're migrating from another email provider, including Exchange, see Ways to migrate multiple email accounts to Microsoft 365 .

Plan for file storage and migration

Microsoft 365 provides cloud storage for individuals, small organizations, and enterprises. For guidance about what to store where, see [Where you can store documents in Microsoft 365](#).

- **You can move hundreds of files** to [OneDrive](#) or to a [SharePoint team site](#). You can upload 100 files at a time. Avoid uploading files larger than 2GB, which is the maximum file size by default.
- **If you want to move several thousand files** to Microsoft 365 storage, review the [SharePoint Online Limits](#). We recommend that you use a migration tool or consider hiring a [partner](#) to help you with the migration. For information about how to migrate a large number of files, see [SharePoint Online and OneDrive Migration User Guide](#).

Plan for Teams

You can use Microsoft Teams to make calls to other people in your organization who are on your subscription. For example, if your organization has 10 people, you can call and IM each other using Teams without any special setup. For more information, see [Get started with Microsoft Teams](#).

For larger organizations or if you're starting from Skype for Business, on-premises, or hybrid deployments, see [How to roll out Microsoft Teams](#).

Plan for integration with Active Directory or other software

- **Do you want to integrate with your on-premises Active Directory?** You can integrate your on-premises Active Directory with Microsoft 365 by using Azure Active Directory Connect. For instructions, see [Set up directory synchronization for Microsoft 365](#).
- **Do you want to integrate Microsoft 365 with software made by other companies?** If you need to integrate Microsoft 365 with other software in your organization, we recommend you consider [hiring a partner](#) to help you with your deployment.

Do you want someone to help you set up Microsoft 365?

- **If you have fewer than 50 employees:**
 - **Ask for help and we'll call you.** After you buy Microsoft 365, you can access the admin center (you don't need to run setup to get to it). At the bottom of the admin center, select **Need help?** Describe your problem, and we'll call you.

- Call [Microsoft 365 for Business Support](#) with your questions. We're here to help!
- Consider hiring a [Microsoft partner](#). If you're short on time, or have advanced requirements (like moving thousands of files to Microsoft 365 cloud storage or integrating with other software), an experienced partner can be a big help.
- If you have more than 50 employees, the [FastTrack Onboarding Center](#) is available to help you with your deployment.

Get started with Windows 365 Business and Cloud PCs

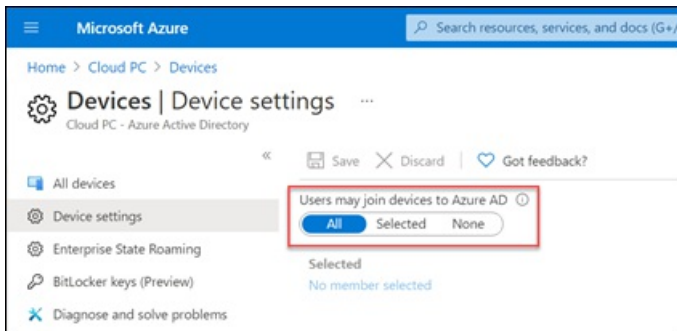
8/5/2021 • 6 minutes to read • [Edit Online](#)

This article is for people who plan to buy and set up Windows 365 Business for their organization.

[Windows 365 Business](#) is a version of Windows 365 that is made specifically for use in smaller companies (up to 300 seats). It gives organizations an easy, streamlined way of providing Cloud PCs to their users. With Windows 365 Cloud PCs, you can stream your apps, data, content, settings, and storage from the Microsoft cloud.

NOTE

Before starting, make sure that your [Azure AD device settings](#) for **Users may join devices to Azure AD** are set to **All**.



Prerequisites

There are no prerequisites to set up Windows 365 Business.

Buy subscriptions

There are two different ways in which you can buy Windows 365 Business subscriptions for your users:

- The [Windows 365 products site](#)
- Microsoft 365 admin center

After you buy a subscription, you can use the Microsoft 365 admin center to assign licenses to users in your organization.

Buy subscriptions through the Windows 365 products site

If you don't already have a Microsoft 365 subscription, you can buy your Windows 365 Business subscriptions on the [Windows 365 products site](#). Use the following steps to buy a Windows 365 Business subscription through the Windows 365 products page.

1. On the [Windows 365 Business](#) page, select **See plans and pricing**.
2. On the next page, select the subscription you want to purchase, and then select **Buy now**.
3. On the **Thank you for choosing Windows 365 Business** page, follow the steps to set up your account.
4. In **step 5 - Confirmation details**, if you are ready to assign licenses to users, select **Get started** to go to your Windows 365 home page at <https://windows365.microsoft.com>.
5. On the Windows 365 home page, in the **Quick actions** section, select **Manage your organization**. This takes you to the Microsoft 365 admin center where you can assign licenses to users.

Buy a subscription through the Microsoft admin center

If you already have a Microsoft 365 tenant and are a Global or Billing admin, you can use the Microsoft 365 admin center to buy a Windows 365 Business subscription for your organization.

1. In the Microsoft admin center, go to the **Billing > Purchase services** page.
2. On the **Purchase services** page, search for **Windows 365 Business**. When you find it, select **Details**.
3. On the **Windows 365 Business** page, in the **Processor/Ram/Storage Options** section, use the **Select a subscription** menu to select a subscription for your users based on their CPU, RAM, and storage needs. See [Windows 365 Business sizing options](#) for guidance on selecting the subscription that best fits your users' needs.
4. On the **Checkout** page, enter the number of subscriptions you want to buy, as well as your payment information. Then select **Place Order**.
5. The **You're all set!** page appears confirming your purchase.

Assign licenses to users

Whether you purchased your subscriptions through the Windows 365 products site, or through the Microsoft 365 admin center, you can [assign licenses to users](#) through the **Billing** page in the Microsoft 365 admin center.

You can assign different Windows 365 Business license types to a user, based on the user's business need. See [Windows 365 Business sizing options](#) for guidance on which license type might be suitable for your users.

IMPORTANT

The first time a Windows 365 license is assigned on your tenant, a system account called "CloudPCBPRT" is automatically created in Azure Active Directory. Do not delete this account. If the system account is deleted, the setup might fail. This system account ensures a smooth set up process, and doesn't have any write capabilities or access to your tenant beyond the scoped service capabilities of Windows 365 Business. If you delete this user, file a ticket through Support Central.

Get your users started with Cloud PC

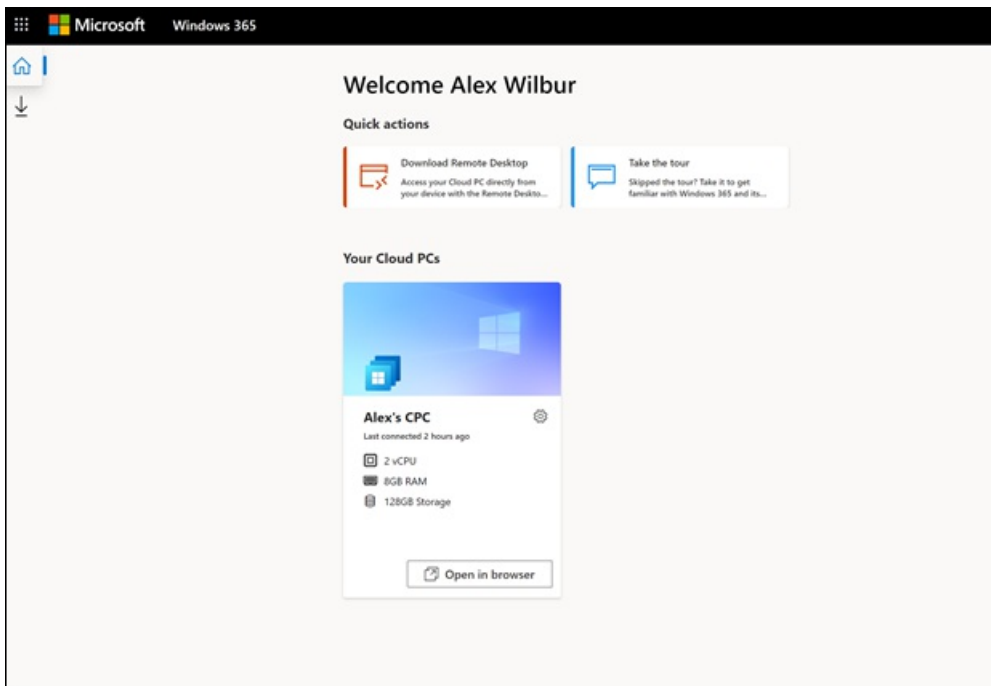
After licenses are assigned, let your users know that there are two different ways in which they can access their Cloud PCs:

- Via the Windows 365 home page (<https://windows365.microsoft.com>)
- By using a Microsoft Remote Desktop client

Windows 365 home page

Users can navigate to <https://windows365.microsoft.com> to access their Cloud PCs.

On their Windows 365 home page, users see the Cloud PCs they have access to in the **Your Cloud PCs** section.



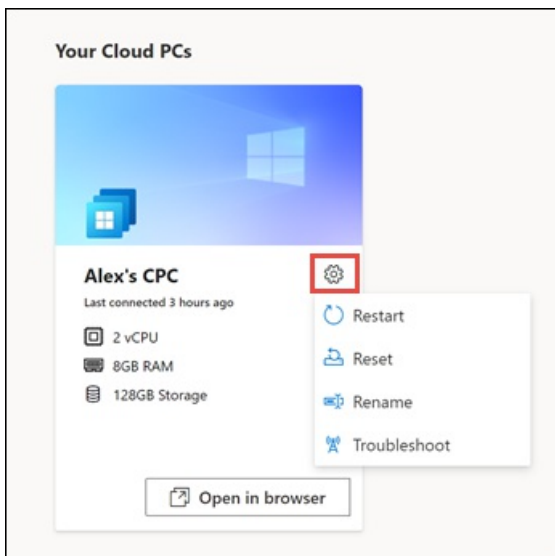
Users can select **Open in browser** to open their Cloud PC.

NOTE

Mobile devices aren't currently supported.

User actions

While on the Windows 365 home page, users can perform actions on their Cloud PCs by selecting the gear icon on a Cloud PC card.



- **Restart:** Restarts the Cloud PC.
- **Reset:** Reset does the following:
 - Reinstalls Windows 10.
 - Removes your personal files.
 - Removes any changes you made to settings.
 - Removes your apps.

IMPORTANT

Before resetting your Cloud PC, make sure to back up any important files you need to keep to a cloud storage service or external storage. Resetting your Cloud PC will delete these files.

- **Rename:** Changes the name of the Cloud PC shown to the user on the Windows 365 home page.
- **Troubleshoot:** Troubleshoot and attempt to fix any issues that may be keeping a user from connecting to their Cloud PC. The following table describes the statuses that can result from the checks.

STATUS	DESCRIPTION
No issues detected	None of the checks ran discovered an issue with the Cloud PC.
Issues resolved	An issue was detected and fixed.
Can't connect to Cloud PC. We're working to fix it, try again later.	A Microsoft service required for connectivity is unavailable. Try connecting again later.
We couldn't fix issues with your Cloud PC. Contact your administrator.	An issue was detected but it was unable to be fixed. This could be due to an ongoing Windows update or another issue. If this error persists for an extended period of time the Cloud PC may need to be reset.

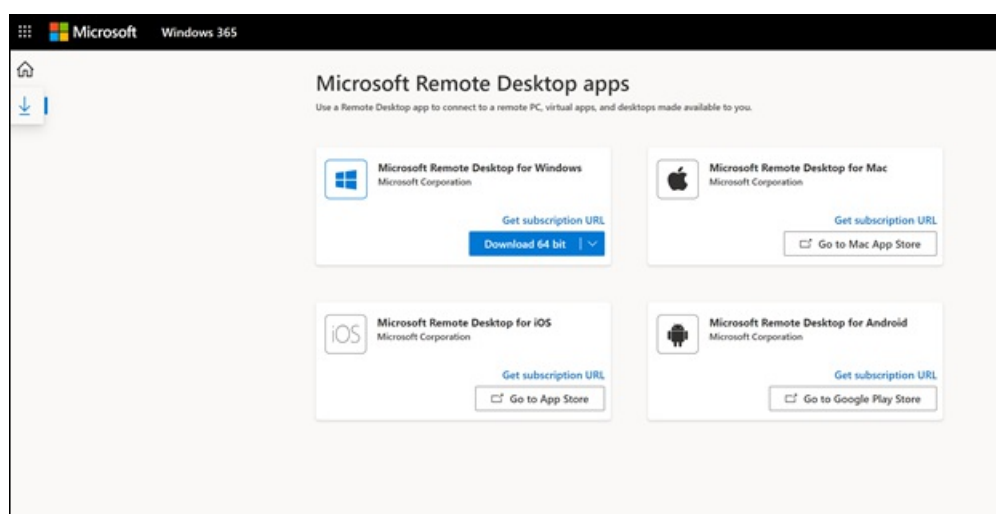
Remote Desktop

The Microsoft Remote Desktop app lets users access and control a remote PC, including a Cloud PC. Windows 365 users can download and install the Remote Desktop client they need from the Windows 365 home page.

Install the Microsoft Remote Desktop app

To set up their Remote Desktop client, users follow these steps:

1. On the **Windows 365 home page**, select the **Microsoft Remote Desktop apps** icon (under the home icon).
2. On the **Microsoft Remote Desktop apps** page, download and install the Remote Desktop app you need.



For a list of clients by operating system, see [Remote Desktop clients](#).

Installing apps

Users can install apps on their Cloud PC as they would normally in Windows by either downloading them from the application's website or by downloading them from the Microsoft Store.

All Windows 365 Business users have local administrator privileges on their Cloud PC, so they should have the permissions required to install apps to their workspaces.

IMPORTANT

If a user tries to use a Microsoft 365 Business Standard license on their Cloud PC, they might see the following error: "Account Issue: The products we found in your account cannot be used to activate Office in shared computer scenarios." In this scenario, the user must uninstall the version of Office installed on their Cloud PC and install a new copy from Office.com.

Management through Intune

Windows 365 Business does not enroll Cloud PCs to [Intune](#) as part of the provisioning process. If the organization and users are properly licensed, Cloud PCs can be enrolled to Intune using the same procedure for [enrolling Windows 10 machines to Intune](#).

Sending outbound email messages using port 25 is not supported

Sending outbound email messages directly on port 25 from a Windows 365 Business Cloud PC is not supported. Communication over port TCP/25 is blocked at the Windows 365 Business network layer for security reasons. If your email service uses Simple Mail Transfer Protocol (SMTP) for your email client application, you can use their web interface, if available. Or you can ask your email service provider for help to configure their email client app to use secure SMTP over Transport Layer Security (TLS), which uses a different port.

How to get help

If you need to get help while setting up Windows 365 Business in the Microsoft 365 admin center, see [Get help or support](#).

Related content

[Windows 365 Business](#)

[Windows 365 Business sizing options](#)

[Windows 365 Business plan comparison](#)

[Remote Desktop client app comparison](#)

[Set up Microsoft Teams in your small business](#)

Windows 365 Business sizing options

8/2/2021 • 2 minutes to read • [Edit Online](#)

Windows 365 Business offers fixed-price licensing (through Microsoft 365) for different Cloud PC sizes. When you assign a license to a user, you need to select one of several size options. Each has a different number of CPUs, RAM, and storage, and is intended to support different usage scenarios. Assess your business requirements to determine which sizes make sense for your users.

This table shows examples of the different sizes available for a Cloud PC.

NOTE

If Microsoft 365 Apps and Microsoft Teams are included in the **Supported apps** column, they are pre-installed for those Cloud PC options.

CPUS, RAM, AND STORAGE	EXAMPLE SCENARIOS	SUPPORTED APPS
1vCPU/2GB/64GB	Firstline workers, call centers, education/training/CRM access.	Office light (web-based), Microsoft Edge, OneDrive, lightweight line-of-business app (call center application – web-apps), Defender support.
2vCPU/4GB/256GB 2vCPU/4GB/128GB 2vCPU/4GB/64GB	Mergers and acquisition, short-term and seasonal, customer services	Microsoft 365 Apps, Microsoft Teams light (Chat and Audio only), OneDrive, Adobe Reader, Microsoft Edge, line-of-business apps, Defender support.
2vCPU/8GB/256GB 2vCPU/8GB/128GB	Bring-your-own-PC, work from home, market researchers, government, consultants.	Microsoft 365 Apps, Microsoft Teams, Outlook, Excel, Access, PowerPoint, OneDrive, Adobe Reader, Microsoft Edge, line-of-business apps, Defender support.
4vCPU/16GB/512GB 4vCPU/16GB/256GB 4vCPU/16GB/128GB	Finance, government, consultants, healthcare services, bring-your-own-PC, work-from-home.	Microsoft 365 Apps, Microsoft Teams, Outlook, Excel, Access, PowerPoint, Power BI, Dynamics 365, OneDrive, Adobe Reader, Microsoft Edge, line-of-business apps, Defender support.
8vCPU/32GB/512GB 8vCPU/32GB/256GB 8vCPU/32GB/128GB	Software developers, engineers, content creators, design, and engineering workstations.	Microsoft 365 Apps, Microsoft Teams, Outlook, Access, OneDrive, Adobe Reader, Microsoft Edge, Power BI, Visual Studio Code, line-of-business apps, Defender support.

Related content

[Get started with Windows 365 Business](#)

[Windows 365 Business plan comparison](#)

[Windows 365 Business](#)

Set up Microsoft 365 Business Basic

7/12/2021 • 3 minutes to read • [Edit Online](#)

Watch: Set up Microsoft 365 Business Basic

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

Add your domain to personalize sign-in

When you purchase Microsoft 365 Business Basic, you have the option of using a domain you own, or buying one during the sign-up.

- If you purchased a new domain when you signed up, your domain is all set up and you can move to [Add users and assign licenses](#).
1. Go to the admin center at <https://admin.microsoft.com>.
 1. Go to the admin center at <https://portal.office.de>.
 1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
 2. Choose **Go to setup** to start the wizard.
 3. In the **Add domain** step, enter the domain name you want to use (like contoso.com).

IMPORTANT

If you purchased a domain during the sign-up, you will not see **Add a domain** step here. Go to [Add users](#) instead.

4. Follow the steps in the wizard to [Create DNS records at any DNS hosting provider for Office 365](#) that verifies you own the domain. If you know your domain host, see also [Add a domain to Microsoft 365](#).

If your hosting provider is GoDaddy or another host enabled with [domain connect](#), the process is easy and you'll be automatically asked to sign in and let Microsoft authenticate on your behalf.



Add users and assign licenses

You can add users in the wizard, but you can also [add users later](#) in the admin center. Additionally, if you have a local domain controller, you can add users with [Azure AD Connect](#).

Add users in the wizard

Any users you add in the wizard get automatically assigned a Microsoft 365 Business Basic license.

1. If your Microsoft 365 Business Basic subscription has existing users (for example, if you used Azure AD Connect), you get an option to assign licenses to them now. Go ahead and add licenses to them as well.
2. After you've added the users, you'll also get an option to share credentials with the new users you added. You can choose to print them out, email them, or download them.

Connect your domain

NOTE

If you chose to use the .onmicrosoft domain, or used Azure AD Connect to set up users, you will not see this step.

To set up services, you have to update some records at your DNS host or domain registrar.

1. The setup wizard typically detects your registrar and gives you a link to step-by-step instructions for updating your NS records at the registrar website. If it doesn't, [Change nameservers to set up Office 365 with any domain registrar](#).
 - If you have existing DNS records, for example an existing web site, but your DNS host is enabled for [domain connect](#), choose **Add records for me**. On the **Choose your online services** page, accept all the defaults, and choose **Next**, and choose **Authorize** on your DNS host's page.
 - If you have existing DNS records with other DNS hosts (not enabled for domain connect), you'll want to manage your own DNS records to make sure the existing services stay connected. See [domain](#)

[basics](#) for more info.

2. Follow the steps in the wizard and email and other services will be set up for you.

When the signup process is complete, you'll be directed to the admin center, where you can add users, and assign licenses. After you complete the initial setup, you can use the **Setup** page in the admin center to continue setting up and configuring the services that come with your subscriptions.

For more information about the setup wizard and the admin center **Setup** page, see [Difference between the setup wizard and the Setup page](#).

Set up Microsoft Business Standard

7/12/2021 • 4 minutes to read • [Edit Online](#)

Add your domain to personalize sign-in

When you purchase Microsoft 365 Business Standard, you have the option of using a domain you own, or buying one during the sign-up.

- If you purchased a new domain when you signed up, your domain is all set up and you can move to [Add users and assign licenses](#).
1. Sign in to [Microsoft 365 admin center](#) by using your global admin credentials.
 2. Choose **Go to setup** to start the wizard.
 3. On the **Install your Office apps** page, you can optionally install the apps on your own computer.
 4. In the **Add domain** step, enter the domain name you want to use (like contoso.com).

IMPORTANT

If you purchased a domain during the sign-up, you will not see **Add a domain** step here. Go to [Add users](#) instead.

5. Follow the steps in the wizard to [Create DNS records at any DNS hosting provider for Office 365](#) that verifies you own the domain. If you know your domain host, see also [Add a domain to Microsoft 365](#).

If your hosting provider is GoDaddy or another host enabled with [domain connect](#), the process is easy and you'll be automatically asked to sign in and let Microsoft authenticate on your behalf.



Add users and assign licenses

You can add users in the wizard, but you can also [add users later](#) in the admin center. Additionally, if you have a local domain controller, you can add users with [Azure AD Connect](#).

Add users in the wizard

Any users you add in the wizard get automatically assigned a Microsoft 365 Business Standard license.

1. If your Microsoft 365 Business Standard subscription has existing users (for example, if you used Azure AD Connect), you get an option to assign licenses to them now. Go ahead and add licenses to them as well.
2. After you've added the users, you'll also get an option to share credentials with the new users you added. You can choose to print them out, email them, or download them.

Connect your domain

NOTE

If you chose to use the .onmicrosoft domain, or used Azure AD Connect to set up users, you will not see this step.

To set up services, you have to update some records at your DNS host or domain registrar.

1. The setup wizard typically detects your registrar and gives you a link to step-by-step instructions for updating your NS records at the registrar website. If it doesn't, [Change nameservers to set up Office 365 with any domain registrar](#).
 - If you have existing DNS records, for example an existing web site, but your DNS host is enabled for [domain connect](#), choose **Add records for me**. On the **Choose your online services** page, accept all the defaults, and choose **Next**, and choose **Authorize** on your DNS host's page.
 - If you have existing DNS records with other DNS hosts (not enabled for domain connect), you'll want to manage your own DNS records to make sure the existing services stay connected. See [domain basics](#) for more info.
2. Follow the steps in the wizard and email and other services will be set up for you.

When the signup process is complete, you'll be directed to the admin center, where you'll follow a wizard to install Office apps, add your domain, add users, and assign licenses. After you complete the initial setup, you can use the **Setup** page in the admin center to continue setting up and configuring the services that come with your subscriptions.

For more information about the setup wizard and the admin center **Setup** page, see [Difference between the setup wizard and the Setup page](#).

Finish setting up

Set up Outlook for email

1. On the Windows Start menu, search for Outlook, and select it.

(If you're using a Mac, open Outlook from the toolbar or locate it using the Finder.)

If you've just installed Outlook, on the Welcome page, select **Next**.

2. Choose **File > Info > Add Account**.
3. Enter your Microsoft email address and select **Connect**.

Watch: Set up Outlook for email

More at [Set up Outlook for email](#).

Import email

If you were using Outlook with another email account, you can import your previous email, calendar, and contacts into your new Microsoft account.

1. Export your old email

In Outlook, choose **File > Open & Export > Import/Export**.

Select **Export to a File** and then follow the steps to export your Outlook Data File (.pst) and any subfolders.

2. Import your old email

In Outlook, choose **File > Open & Export > Import/Export** again.

This time, select **Import from another program or file** and follow the steps to import the backup file you created when you exported your old email.

Watch: Import and redirect email

More at [Import email with Outlook](#).

You can also use Exchange admin center to import everyone's email. For more information, see [migrate multiple email accounts](#).

Use a public website

Microsoft 365 doesn't include a public website for your business. If you want to set one up, consider using a Microsoft partner, such as GoDaddy or WIX.

1. From the admin center, go to **Resources**, and then select **Public website**.
2. Select **Learn more** under one of the options, and then sign up with a website partner and use their tools to set up and design your site.

Watch: Create your business website

Related content

[Create a website](#) (video)

[Microsoft 365 for your business](#) (link page)

Set up Microsoft 365 Business Premium in the setup wizard

6/30/2021 • 3 minutes to read • [Edit Online](#)

Watch: Overview of Microsoft 365 setup

Watch this video for an overview of Microsoft 365 Business Premium setup.

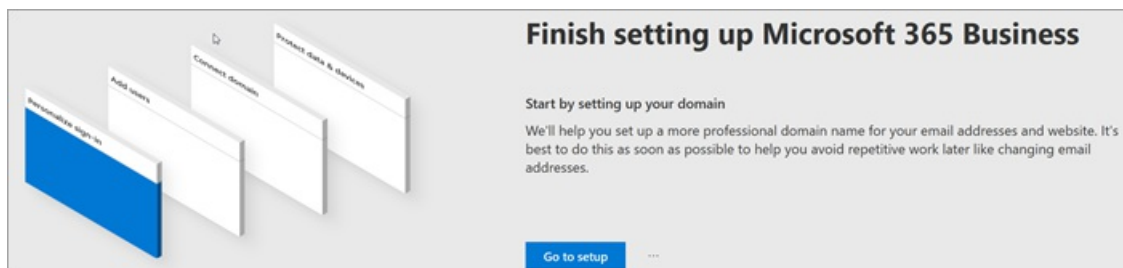
Add your domain, users, and set up policies

When you purchase Microsoft 365 Business Premium, you have the option of using a domain you own, or buying one during the [sign-up](#).

- If you purchased a new domain when you signed up, your domain is all set up and you can move to [Add users and assign licenses](#).

Add your domain to personalize sign-in

1. Sign in to [Microsoft 365 admin center](#) by using your global admin credentials.
2. Choose **Go to setup** to start the wizard.



3. On the **Install your Office apps** page, you can optionally install the apps on your own computer.
4. In the **Add domain** step, enter the domain name you want to use (like contoso.com).

IMPORTANT

If you purchased a domain during the sign-up, you will not see **Add a domain** step here. Go to [Add users](#) instead.



5. Follow the steps in the wizard to [Create DNS records at any DNS hosting provider for Microsoft 365](#) that verifies you own the domain. If you know your domain host, see also [Add a domain to Microsoft 365](#).

If your hosting provider is GoDaddy or another host enabled with [domain connect](#), the process is easy and you'll be automatically asked to sign in and let Microsoft authenticate on your behalf.

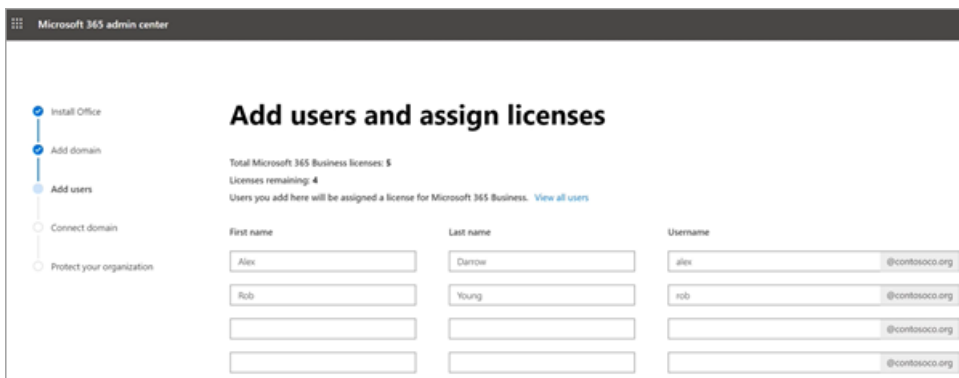


Add users and assign licenses

You can add users in the wizard, but you can also [add users later](#) in the admin center. Additionally, if you have a local domain controller, you can add users with [Azure AD Connect](#).

Add users in the wizard

Any users you add in the wizard get automatically assigned a Microsoft 365 Business Premium license.



1. If your Microsoft 365 Business Premium subscription has existing users (for example, if you used Azure AD Connect), you get an option to assign licenses to them now. Go ahead and add licenses to them as well.
2. After you've added the users, you'll also get an option to share credentials with the new users you added. You can choose to print them out, email them, or download them.

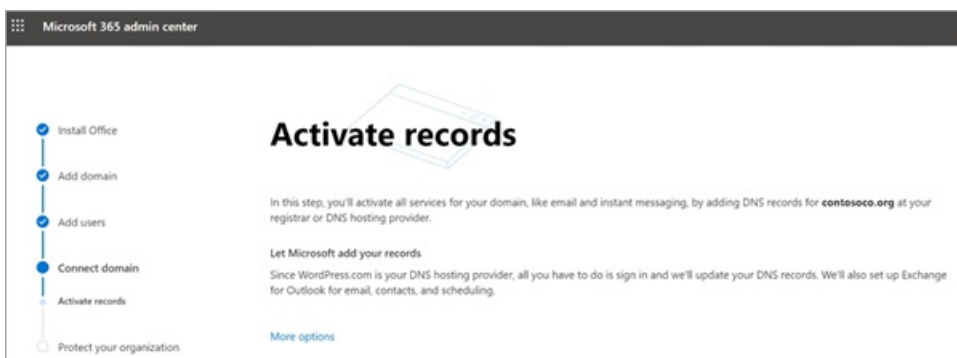
Connect your domain

NOTE

If you chose to use the .onmicrosoft domain, or used Azure AD Connect to set up users, you will not see this step.

To set up services, you have to update some records at your DNS host or domain registrar.

1. The setup wizard typically detects your registrar and gives you a link to step-by-step instructions for updating your NS records at the registrar website. If it doesn't, [Change nameservers to set up Microsoft 365 with any domain registrar](#).
 - If you have existing DNS records, for example an existing web site, but your DNS host is enabled for [domain connect](#), choose **Add records for me**. On the **Choose your online services** page, accept all the defaults, and choose **Next**, and choose **Authorize** on your DNS host's page.
 - If you have existing DNS records with other DNS hosts (not enabled for domain connect), you'll want to manage your own DNS records to make sure the existing services stay connected. See [domain basics](#) for more info.

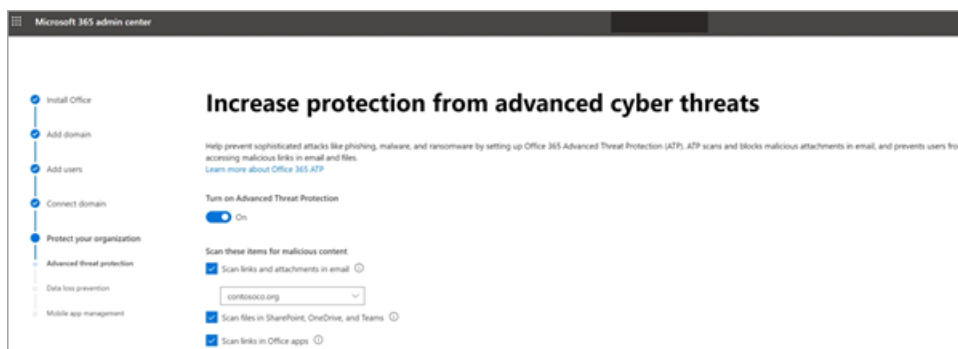


2. Follow the steps in the wizard and email and other services will be set up for you.

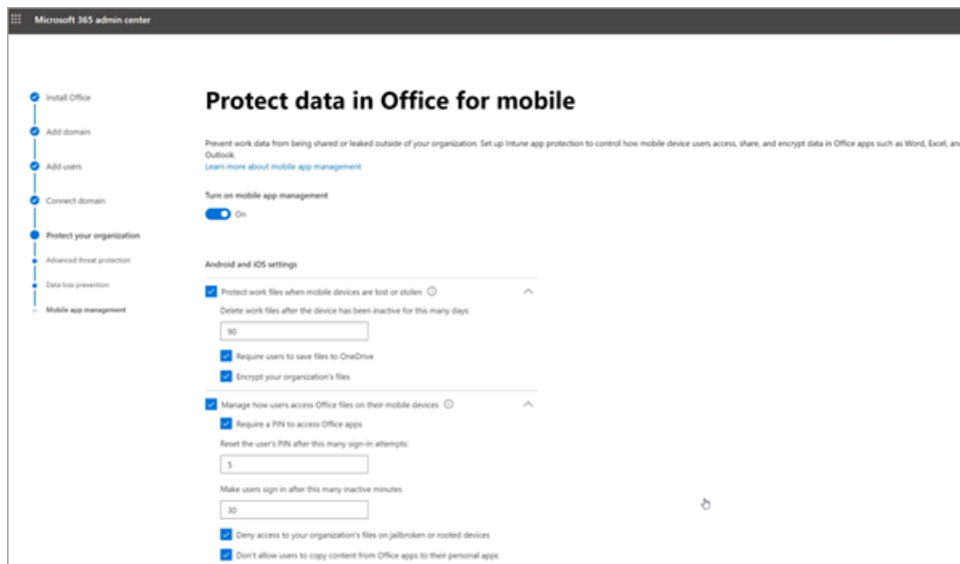
Protect your organization

The policies you set up in the wizard are applied automatically to a [Security group](#) called *All Users*. You can also create additional groups to assign policies to in the admin center.

1. On the **Increase protection from advanced cyber threats**, it is recommended that you accept the defaults to let [Office 365 Advance Threat Protection](#) scan files and links in Office apps.



2. On the **Prevent leaks of sensitive data** page, accept the defaults to turn on Office 365 Data Loss Prevention (DLP) to track sensitive data in Office apps and prevent the accidental sharing of these outside your organization.
3. On the **Protect data in Office for mobile** page, leave mobile app management on, expand the settings and review them, and then select **Create mobile app management policy**.



Secure Windows 10 PCs

On the left nav, select **Setup** and then, under **Sign-in and security**, choose **Secure your Windows 10 computers**. Choose **View** to get started. See [secure your Windows 10 computers](#) for complete instructions.

Deploy Office 365 client apps

If you chose to automatically install Office apps during setup, the apps will install on the Windows 10 devices once the users have signed in to Azure AD from their Windows devices, using their work credentials.

To install Office on mobile iOS or Android devices, see [Set up mobile devices for Microsoft 365 Business Premium users](#).

You can also install Office individually. See [install Office on a PC or Mac](#) for instructions.

Related content

[Microsoft 365 for business training videos](#) (link page)

Set up Microsoft 365 Apps for business

5/13/2021 • 2 minutes to read • [Edit Online](#)

Add users and assign licenses

You can add users in the wizard, but you can also [add users later](#) in the admin center.

1. Go to the admin center at <https://admin.microsoft.com>.
1. Go to the admin center at <https://portal.office.de>.
1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Choose **Go to setup** to start the wizard.
3. On the first page you will get the option to install Office apps on your computer. You can also do this later.
4. On the next page you can add users and they will automatically get assigned the Microsoft Apps for business license. After you've added the users, you'll also get an option to share credentials with the new users you added. You can choose to print them out, email them, or download them.

When the sign-up process is complete, you'll be directed to the admin center, where you can add users, and assign licenses.

Install Office

Once you've created accounts for other people in your business, you and your team members will be able to install the full desktop version of Office (Word, Excel, Outlook, etc.). Each person can install Office on up to 5 PCs or Macs.

Go to <https://admin.microsoft.com/OLS/MySoftware.aspx>.

If you're using Office 365 Germany, go to <https://portal.office.de/OLS/MySoftware.aspx>.

If you're using Office 365 operated by 21Vianet, go to <https://portal.partner.microsoftonline.cn/OLS/MySoftware.aspx>.

1. Sign in with your work or school account.
2. Select **Install**.

Need more detailed steps or want to install the 64-bit version of Office? See [Step-by-step installation instructions](#).

Set up mobile

Install Office on your mobile device, and set up Outlook to work with your new Microsoft mailbox. Everyone on your team will need to do this step. Each person can install the Office mobile apps on up to 5 phones and 5 tablets.

Get the steps for your device: [Android](#) | [iOS](#) | [Windows Phone](#)

Store files online

Microsoft makes online file storage easy. To learn which storage locations are best for your business, see [Where](#)

[you can store files in Office 365.](#)

Everyone gets a **OneDrive** cloud storage location automatically when you create Microsoft accounts for them. With OneDrive, you can access files across your computers, phones, and tablets.

1. On your computer, use File Explorer to open OneDrive. Or, from [Office 365](#), open **OneDrive** from the app launcher.
2. View and upload personal files, or share documents or folders by selecting **Share** and then either inviting others to view the documents or sending them a link. To learn more, see [Share OneDrive files and folders](#).

More at [Upload files to a library](#).

Get started using Office

To take a tour of Microsoft 365 and learn how to use all the Office mobile apps, see [Get started](#).

Add a custom domain

During the sign-up you chose an .onmicrosoft domain. You can also add a custom domain, like *contoso.com*, to your account to personalize the emails. For more information, see [add a domain](#).

Difference between the setup wizard and the Setup page

4/3/2021 • 2 minutes to read • [Edit Online](#)

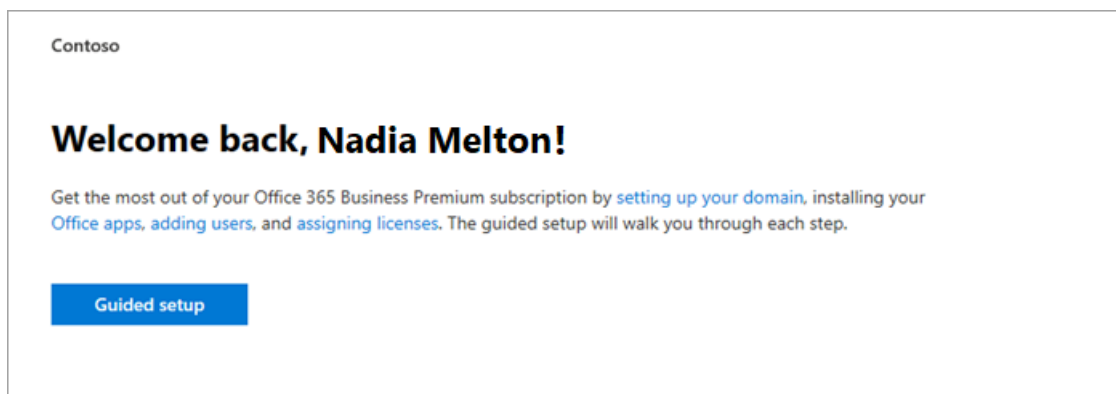
Microsoft 365 provides two setup experiences:

- Initial setup using the setup wizard
- Ongoing and advanced setup using the **Setup** page

The setup wizard provides a guided walkthrough for setting up the basic Microsoft 365 configuration. After you complete the initial setup, you can go to the **Setup** page to finish setting up and configuring the services that come with your subscriptions.

Use the setup wizard to complete initial setup tasks

To set up your account, go to the [admin center](#), select **Setup** in the left navigation pane, and then select **Guided setup** on the **Setup** page.



The setup wizard guides you through the following steps:

1. Install the Microsoft 365 apps on your computer.
2. Choose and verify your domain, such as contoso.com.
3. Add new users and assign licenses to them so that they can download and install Microsoft 365 apps.
4. Connect your domain.

Use the Setup page to complete and manage your configuration

To access the **Setup** page in the [admin center](#), select **Setup** in the navigation pane. Based on products you've purchased, features you've set up, and your admin role, tasks and related information from across Microsoft 365 are surfaced here.

You'll see the complete list of setup tasks arranged in logical categories, including those that you completed in the setup wizard.

Contoso The new admin center

Welcome back, Nadia Melton!

Discover, learn about, and set up services, solutions, and add-ins included with your subscription.

Sign-in and security

Increase security for sign-in, links, and more

- Turn on multi-factor authentication (MFA)**
Strengthen sign-in security by requiring an alternative method of authentication to verify users' identity whe...
[View](#)
- Get your custom domain set up**
Connecting a domain will allow users in your organization to send and receive email from a custom...
[View](#)
- Customize your sign-in pages**
Present users with a branded look-and-feel when they sign in to your organization's web-based Office apps.
[View](#)
- Set passwords to never expire**
Setting passwords to never expire is more secure and leads to fewer work stoppages.
[View](#)
- Let users reset their own passwords**
Reduce support costs by allowing users to register for self-service password reset.
[View](#)
- Give admins only the access they need**
Limit risk to your organization by reassigning some global admins to more limited admin roles, removing...
[View](#)
- Increase protection from advanced threats**
Prevent users from accessing malicious content by scanning attachments, links, and files by setting up...
[View](#) Add-on service
- Add users and decide how they sign in**
Add your users right the first time and choose cloud or hybrid authentication.
[View](#)

Data migration

Bring over email and data from a previous solution

- Migrate G Suite users to Microsoft 365**
Move their Gmail mailboxes, contacts, and calendar info from G Suite to Exchange Online.
[View](#)
- Migrate your users' data**
Bring email and data over from another service so you can manage it all in one place with Microsoft 365 app...
[View](#)

Apps and updates

Deploy Office and other Microsoft apps

- Help users install their Office apps**
Make sure users in your organization have installed and activated all the Office apps they're licensed for.
[View](#)
- Get feature updates for Office every month**
Give your users new and improved features every month.
[View](#)
- Deploy Office to your users**
Use the Office Deployment Tool to customize your Office app deployment and deploy it from the Office...
[View](#)

Choose **View** for any task to get at-a-glance information, such as task description, user impact, prerequisites, effort to implement, and security and adoption statistics to help you understand consequences and impact before proceeding.

You'll also see the status of the task (**Started**, **Not started yet**, or **Completed**). If you're multi-tasking, working on tasks over several days, or if there are multiple admins working on tasks, you can track completion by seeing at a glance which tasks have been completed and which ones still require attention.

For access to comprehensive articles about the features you're setting up, select any of the **Learn more** links. The collection of tasks is always here, so you can return to the **Setup** page at any time to explore resources further.

When you're ready to complete a task, select **Get started** to walk through the configuration process. Once you complete a task, the **Get started** button changes to a **Manage** button, allowing you to manage the task, as needed.

Turn on multi-factor authentication (MFA)

If usernames and passwords are compromised, your organization is exposed to serious risks. MFA adds a second level of sign-in security and users must verify their identity. Even if an attacker manages to steal the user's password, the password is useless without knowing the second authentication method.

Not started yet

[Get started](#)

At a glance

Protects against: Password cracking, account breach

Compliance: Recommended with GDPR

Secure score increase: 50 points

User impact

ⓘ After setting up multi-factor authentication (MFA), people who use the built-in email apps on Android or iOS devices may need to add their email account again on those devices.

When you turn on MFA, you'll assign it to specific users. Those users will be guided to set it up the next time they try to sign in.

We recommend that you require all global admins to use MFA. Since global admins have permission to do everything, you should definitely verify their identity.

For your users

[Set up 2-step verification](#)

About multi-factor authentication (MFA)

Multi-factor authentication (MFA) requires users to sign in with a second method to verify their identity with a phone call or with an authenticator app.

Learn more

[Plan for multi-factor authentication](#)

[Set up multi-factor authentication](#)

[Top 10 ways to secure your organization](#)

Secure Windows 10 computers

4/3/2021 • 2 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

After you have [set up](#) Microsoft 365 Business Premium, it is time to protect the Windows 10 computers in your org from theft, and malicious threats like viruses and malware.

To secure your Windows 10 computers

1. Sign in to [Microsoft 365 admin center](#) by using your global admin credentials.
2. On the left nav, select **Setup** and then, under **Sign-in and security**, choose **Secure your Windows 10 computers**. Choose **View** to get started.
3. On the **Secure your Windows 10 computers** page, read all the information to understand what you are turning on, and what the user impact is.

On the top of the page, choose **Get started**.

4. On the **Secure your Windows 10 computers** pane, select the options you want to turn on. For more information about the settings, see [Secure Windows 10 devices](#).

For most organizations, the options here offer a good level of security, however, if your organization has more complex security needs, you can also use pre-defined security baselines to secure your Windows 10 devices. For more information, see [security baselines for Windows 10 devices](#).

5. Choose **Apply settings**.

These settings will apply to all users in your organization. To set up different policies for different security groups, see [Set device protection settings for Windows 10 PCs](#).

Download perpetual software and product license keys

5/11/2021 • 2 minutes to read • [Edit Online](#)

This article explains how to download software and product license keys for perpetual software bought through the Cloud Solution Provider (CSP) program.

Before you begin

You must be a Global admin to do the steps in this article. For more information, see [About admin roles](#).

Download software and product license keys

1. In the Microsoft 365 admin center, go to the **Billing** > [Your products](#) page.
2. On the **Products** tab, in the **Software** section, select the software that you want to download.
3. On the subscription details page, in the **Downloads & keys** section, choose the **Product version**, **Language**, and **CPU & file type**, then select **Download**.
4. To download the key, select **Copy key to clipboard**.
5. In the right pane, select **Copy**, then close the pane.
6. Paste the key in a file in a secure location and then enter it as instructed during the software installation. The key is needed to activate the downloaded software.

Install Office applications

7/12/2021 • 2 minutes to read • [Edit Online](#)

Now that you've set up Microsoft 365, you can install individual Office applications on your Mac, PC, or mobile devices.

Follow these links for information on how to:

- Install Office applications: [Install Office on your PC or Mac](#)
- Install other apps: [Project](#), [Visio](#), or [Skype for Business](#)
- Set up mobile devices: [Microsoft 365 mobile setup - Help](#)
- Set up email in Outlook: [Windows](#) or [Mac](#)
- [Upgrade users to the latest apps](#)

If you purchased Azure Active Directory Premium (AADP) Plan 1 or Plan 2, you're eligible for Microsoft Identity Manager (MIM). To download MIM, go to the [Download Center](#).

Related content

[Troubleshoot installing Office and Microsoft 365](#) (article)

Set up Windows devices for Microsoft 365 Business Premium users

7/12/2021 • 3 minutes to read • [Edit Online](#)

Before you begin

Before you can set up Windows devices for Microsoft 365 Business Premium users, make sure all the Windows devices are running Windows 10 Pro, version 1703 (Creators Update). Windows 10 Pro is a prerequisite for deploying Windows 10 Business, which is a set of cloud services and device management capabilities that complement Windows 10 Pro and enable the centralized management and security controls of Microsoft 365 Business Premium.

If you have Windows devices running Windows 7 Pro, Windows 8 Pro, or Windows 8.1 Pro, your Microsoft 365 Business Premium subscription entitles you to a Windows 10 upgrade.

For more information on how to upgrade Windows devices to Windows 10 Pro Creators Update, follow the steps in this topic: [Upgrade Windows devices to Windows Pro Creators Update](#).

See [Verify the device is connected to Azure AD](#) to verify you have the upgrade, or to make sure the upgrade worked.

Watch: Connect your PC to Microsoft 365 Business

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

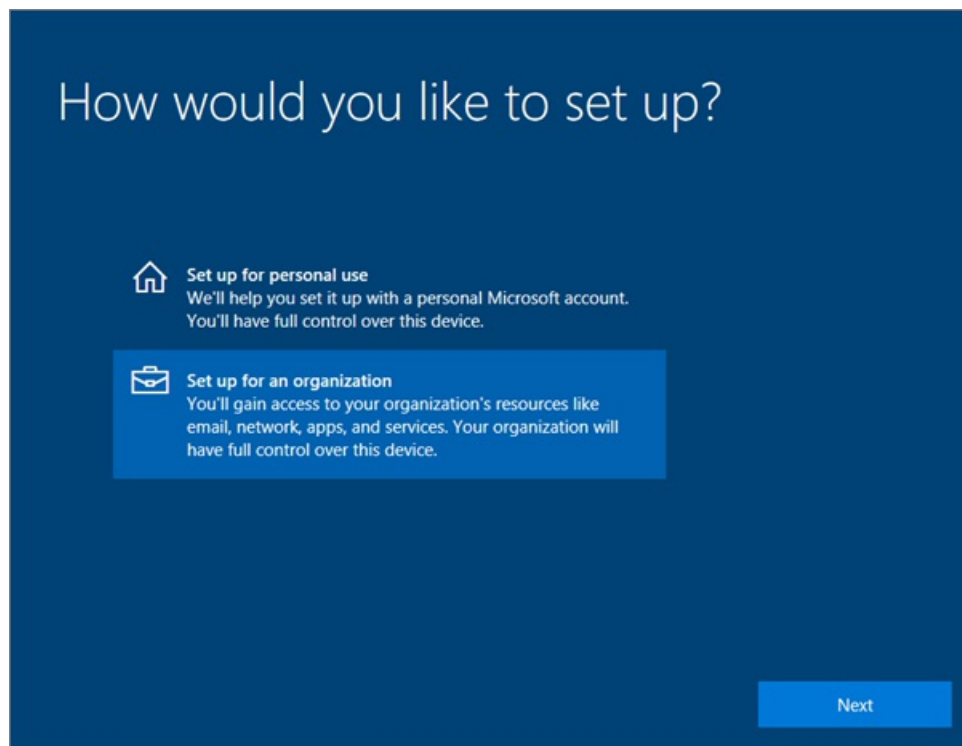
Join Windows 10 devices to your organization's Azure AD

When all Windows devices in your organization have either been upgraded to Windows 10 Pro Creators Update or are already running Windows 10 Pro Creators Update, you can join these devices to your organization's Azure Active Directory. Once the devices are joined, they'll be automatically upgraded to Windows 10 Business, which is part of your Microsoft 365 Business Premium subscription.

For a brand new, or newly upgraded, Windows 10 Pro device

For a brand new device running Windows 10 Pro Creators Update, or for a device that was upgraded to Windows 10 Pro Creators Update but has not gone through Windows 10 device setup, follow these steps.

1. Go through Windows 10 device setup until you get to the **How would you like to set up?** page.



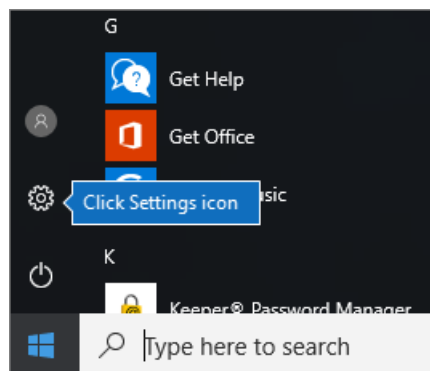
2. Here, choose **Set up for an organization** and then enter your username and password for Microsoft 365 Business Premium.
3. Finish Windows 10 device setup.

Once you're done, the user will be connected to your organization's Azure AD. See [Verify the device is connected to Azure AD](#) to make sure.

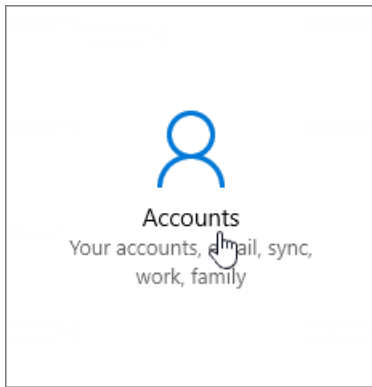
For a device already set up and running Windows 10 Pro

Connect users to Azure AD:

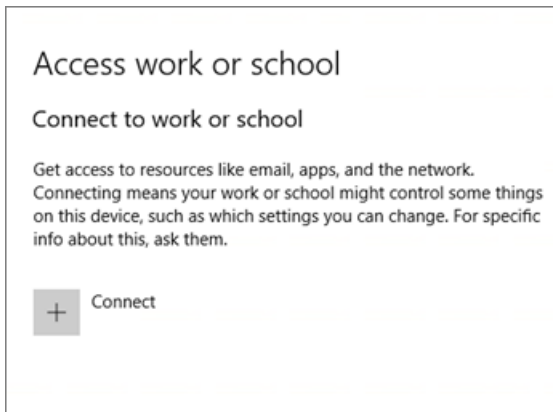
1. In your user's Windows PC, that is running Windows 10 Pro, version 1703 (Creators Update) (see [pre-requisites](#)), click the Windows logo, and then the Settings icon.



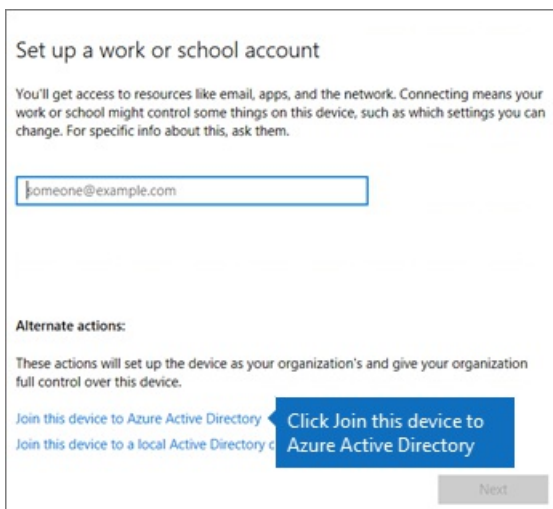
2. In Settings, go to Accounts.



3. On **Your info** page, click **Access work or school** > **Connect**.

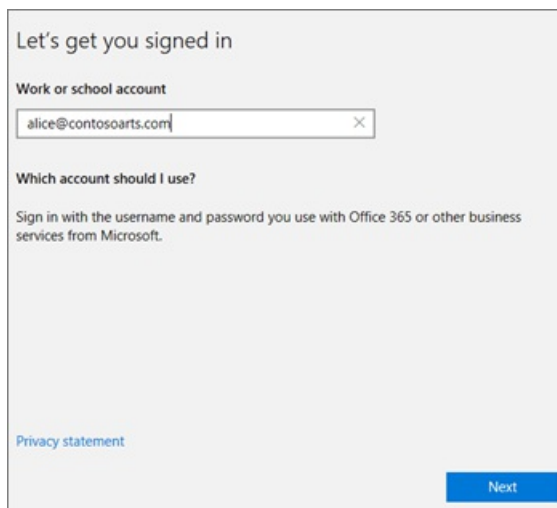


4. On the **Set up a work or school account** dialog, under **Alternate actions**, choose **Join this device to Azure Active Directory**.



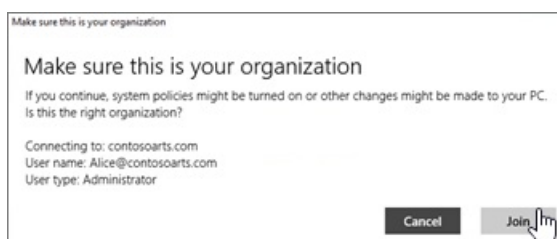
5. On the **Let's get you signed in** page, enter your work or school account > **Next**.

On the **Enter password** page, enter your password > **Sign in**.



6. On the **Make sure this is your organization** page, verify that the information is correct, and choose **Join**.

On the **You're all set!** page, choose **Done**.



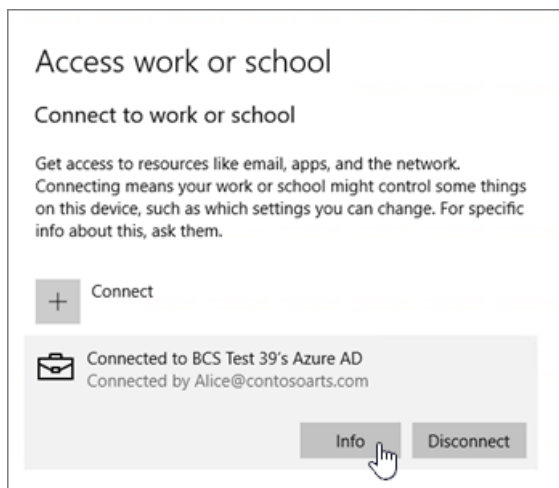
If you uploaded files to OneDrive for Business, sync them back down. If you used a third-party tool to migrate profile and files, also sync those to the new profile.

Verify the device is connected to Azure AD

To verify your sync status, on the **Access work or school** page in **Settings**, select the **Connected to <organization name>** area to expose the buttons **Info** and **Disconnect**. Choose **Info** to get your synchronization status.

On the **Sync status** page, choose **Sync** to get the latest mobile device management policies onto the PC.

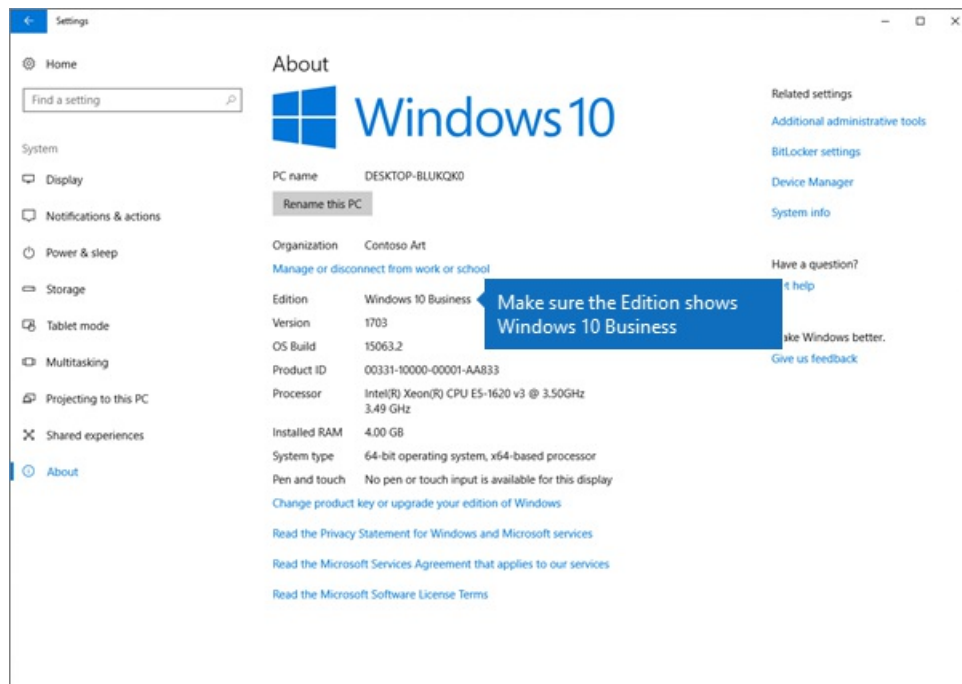
To start using the Microsoft 365 Business Premium account, go to the Windows **Start** button, right-click your current account picture, and then **Switch account**. Sign in by using your organization email and password.



Verify the PC is upgraded to Windows 10 Business

Verify that your Azure AD joined Windows 10 devices are upgraded to Windows 10 Business as part of your Microsoft 365 Business Premium subscription.

1. Go to **Settings > System > About**.
2. Confirm that the **Edition** shows **Windows 10 Business**.



Next steps

To set up your mobile devices, see [Set up mobile devices for Microsoft 365 Business Premium users](#), To set device protection or app protection policies, see [Manage Microsoft 365 for business](#).

Related content

[Microsoft 365 for business training videos](#) (link page)

Set up mobile devices for Microsoft 365 for business users

7/12/2021 • 2 minutes to read • [Edit Online](#)

Follow the instructions in the tabs to install Office on an iPhone or an Android phone. After you follow these steps, your work files created in Office apps will be protected by Microsoft 365 for business.

The example is for Outlook, but applies for any other Office apps you want to install also.

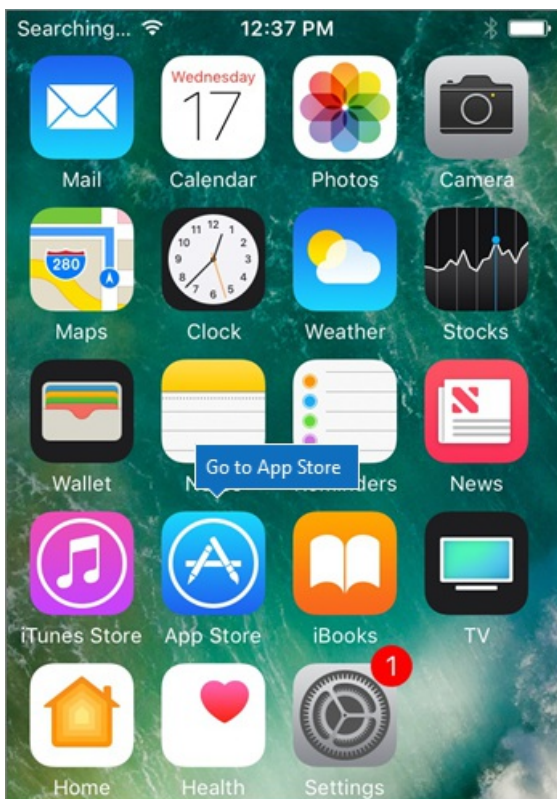
Set up mobile devices

- [iPhone](#)
- [Android](#)

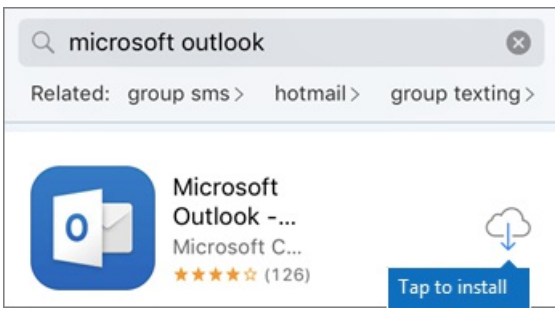
Watch a short video on how to set up Office apps on iOS devices with Microsoft 365 for business.

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

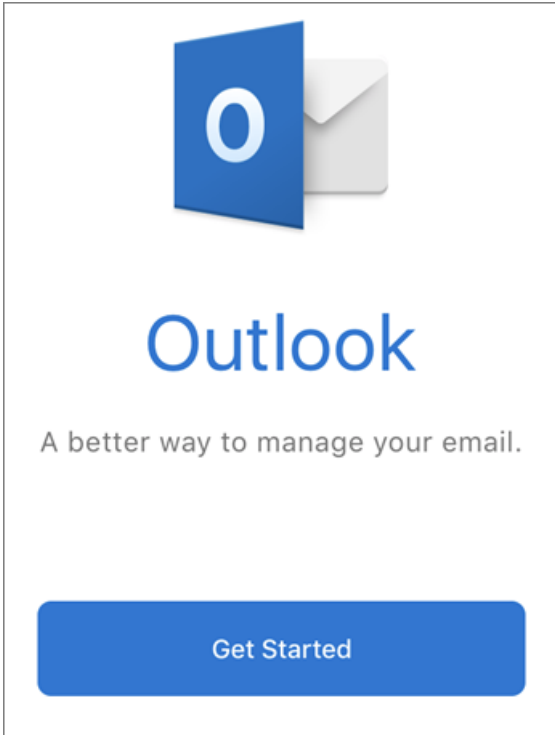
Go to **App store**, and in the search field type in Microsoft Outlook.



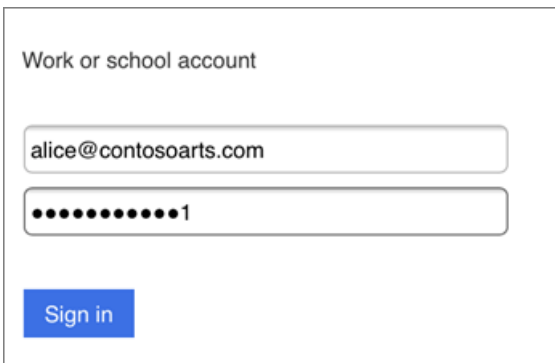
Tap the cloud icon to install Outlook.



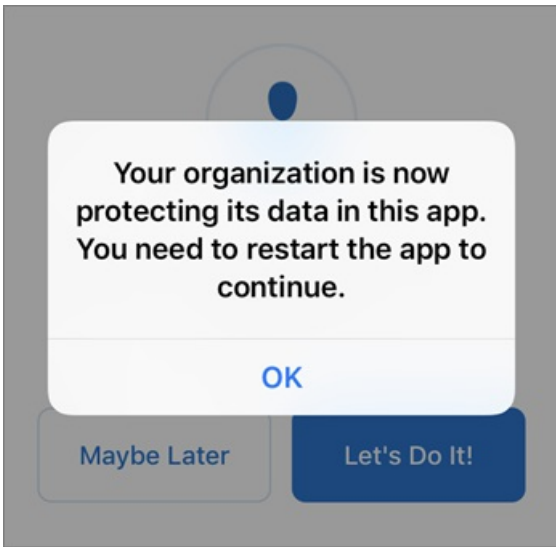
When the installation is done, tap the **Open** button to open Outlook and then tap **Get Started**.



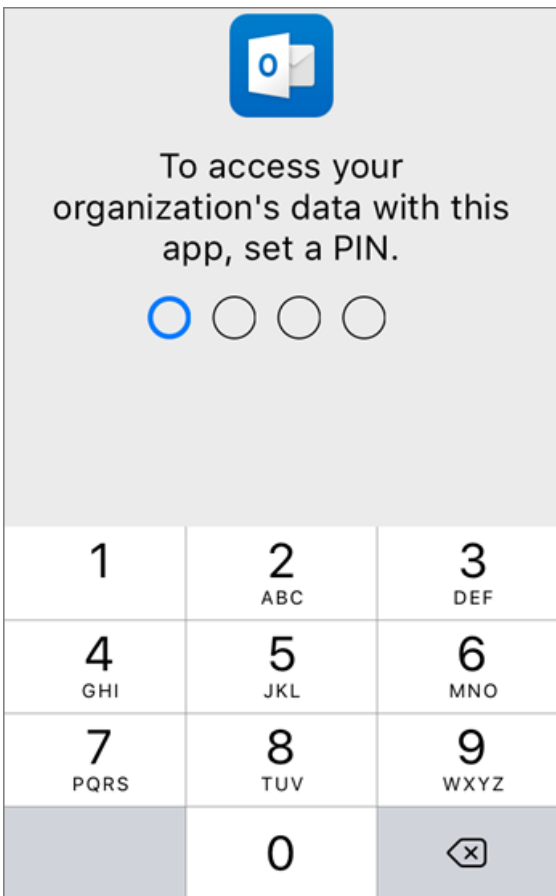
Enter your work email address on the **Add Email Account** screen > **Add Account**, and then enter your Microsoft 365 for business credentials > **Sign in**.



If your organization is protecting files in apps, you'll see a dialog stating that your organization is now protecting the data in the app and you need to restart the app to continue to use it. Tap **OK** and close Outlook.



Locate Outlook on the iPhone, and restart it. When prompted, enter a PIN and verify it. Outlook on your iPhone is now ready to be used.



Migrate email and contacts to Microsoft 365

7/12/2021 • 2 minutes to read • [Edit Online](#)

Import or migrate email from Gmail or another email provider to Microsoft 365.

Want help with this? [Contact Microsoft 365 for business support](#) .

You need to use a version of Outlook that is installed on your desktop for this task. Outlook is included in most Microsoft 365 [plans](#).

Migrate Gmail to Microsoft 365

Follow these steps to import or migrate email, contacts, and calendar from Gmail into Outlook with Microsoft 365:

- [Import Gmail to Outlook](#)
- [Import contacts to Outlook](#)
- [Import Google Calendar](#)

Watch: Import calendars

Import Outlook pst files to Microsoft 365 (desktop)

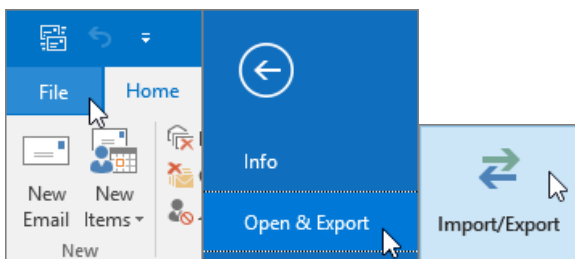
Follow these steps to export email, contacts and calendars from Outlook to a .pst file, and then import that file to Outlook with Microsoft 365:

1. [Export email, contacts, and calendar](#)
2. [Import mail, contacts, and calendar](#)

If you just want contacts, follow these steps:

1. [Export contacts from Outlook](#)
2. [Import contacts to Outlook](#)

To start the process, open Outlook and choose **File > Open & Export > Import/Export**.



See other email accounts in Outlook

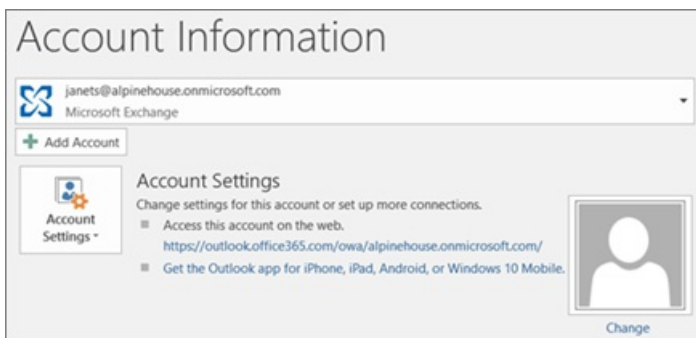
Just want to see your email from another provider (like Gmail, Yahoo, or Live.com) in Outlook? No need to import or migrate. You can set up Outlook or Outlook Web App so you can access your other accounts from the same place as your Microsoft 365 mailbox and send, receive, and read email sent to those accounts.

Outlook (desktop)

Add an account, such as your private Gmail account, to Outlook.

- Open Outlook, then go to **File > Add account**.

Need more detailed steps? See [Add an account](#).



Multiple mailboxes: Admins can bulk import email, contacts, and calendars to Microsoft 365

Depending on your source email system, you can choose from several bulk migration methods. Read [Ways to migrate multiple email accounts to Microsoft 365](#) to decide which method works for you.

Related content

[Plan your setup of Microsoft 365 for business](#) (article)

[Install Office applications](#) (link page)

[Overview of the Microsoft 365 admin center](#) (video)

What subscription do I have?

7/12/2021 • 2 minutes to read • [Edit Online](#)

If you're an admin, you can verify which subscriptions your organization has by going to the admin center.

Not an admin? See [What Microsoft 365 for business product or license do I have?](#)

1. In the admin center, go to the **Billing** > **Your products** page.
2. On the **Products** tab, you see all your subscriptions. Each subscription line includes information about licenses, subscription status, and billing.
3. If you want to change the columns that appear in the list, select **Choose columns**. Change the selection of columns, then select **Save**.
4. To see more details for a single subscription, select that subscription.

Related content

[Subscriptions and billing](#) (link page)

[View your bill or invoice](#) (article)

[Paying for your subscription](#) (article)

[Change your billing addresses](#) (article)

Add your company branding to the Sign In page

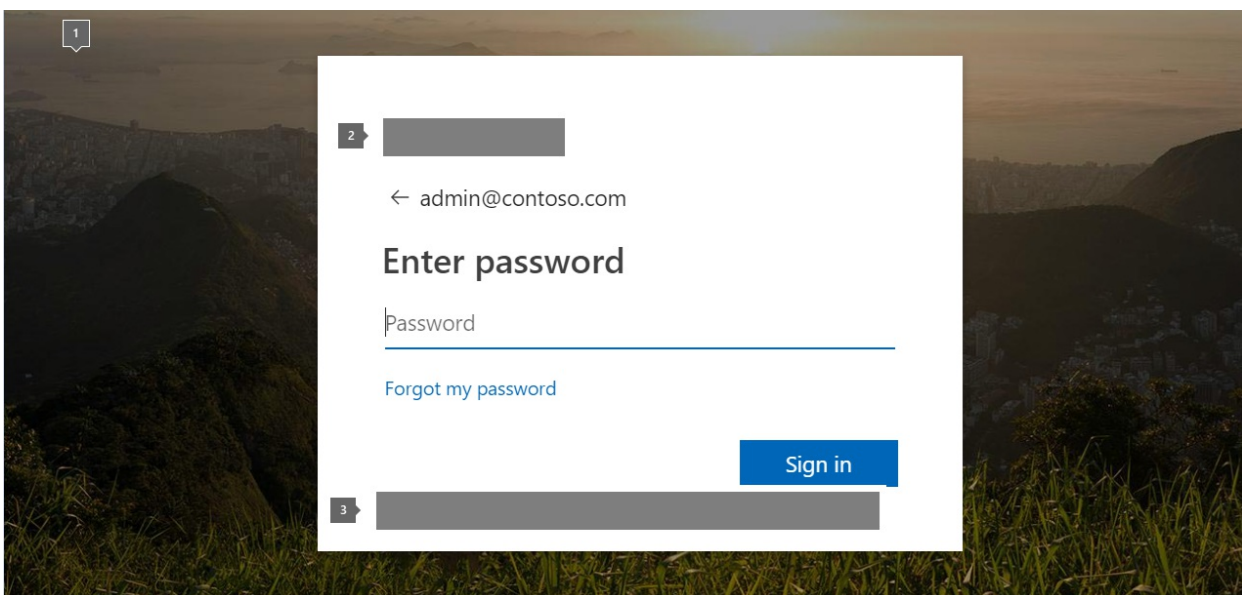
7/12/2021 • 2 minutes to read • [Edit Online](#)

You can now use the Azure Active Directory (AD) subscription that is included with your Microsoft 365 subscription to customize the sign-in page your users see.

Add company branding to your sign in page and Access Panel pages

If you have a paid subscription to Microsoft 365 for business, Microsoft Dynamics CRM Online, Enterprise Mobility Suite, or other Microsoft services, you have a free subscription to Azure Active Directory. You can use Azure Active Directory to create and manage user and group accounts, and add company branding to your pages. To activate this subscription and access the Microsoft Azure Management Portal, you have to complete a one-time registration process. Afterward, you can access Azure Active Directory from your Microsoft service that uses it. For instructions on how to register your Microsoft 365 subscription see [Register your free Azure Active Directory subscription](#), and see [Manage the directory for your Microsoft 365 subscription in Azure](#) for general management instructions.

The following figure shows which parts of the sign-in page can be modified in Azure.



1. The large illustration and/or its background color
2. The banner logo
3. You can also add text to this area

In addition to the sign-in page, you can customize the Access Panel page in Azure.

Next steps

If you are ready to add branding, explore the customization options in the Azure content set: [Add company branding to your Sign-in and Access Panel pages](#).

Related content

[Customize the Microsoft 365 theme for your organization](#) (article)

[Difference between the setup wizard and the Setup page](#) (article)

[Set up mobile devices for Microsoft 365 for business users \(video\)](#)

Customize the Microsoft 365 theme for your organization

7/12/2021 • 5 minutes to read • [Edit Online](#)

As the admin of your organization, you can create multiple themes for the people in your organization, and select which themes apply to different members of your organization. The organization theme is what appears in the top navigation bar for people in your organization.

You can add or update a default theme that applies to everyone within your org. You can also create up to four additional group themes that can be assigned to multiple Microsoft 365 groups.

Add or update your organization's theme

1. In the admin center, go to the **Settings > Org Settings** page, and then choose the **Organization profile** tab.
2. On the **Organization profile** tab, select **Custom themes**.

All organization themes can be customized using the following tabs.

TAB	WHAT CAN YOU DO?
General	Modify a theme name and assign to up to five groups (if applicable).
Logos	Add your organization logo, including alternate logo for dark theme.
Colors	Customize a color scheme by specifying navigation bar, accent, text and icon colors.

General: Modify a theme

Your experience on the General tab depends on whether you're adding or modifying the default theme or a group theme.

Update the default theme

The default theme is the first theme displayed.

1. If you previously customized a theme for your organization, select **Default Theme** and use one of your saved customizations, or, select **Add theme**.
2. On the **General** page, you can prevent users from overriding their theme and show the user's display name.
3. Select **Save** to save your changes.

IMPORTANT

The default theme is unique, it can't be renamed and applies to everyone within your organization. To delete the default theme, you have to delete all other themes first.

Default theme

General Logos Colors

Name

Default theme

- Prevent users from overriding their theme.**
High-contrast themes, which enhance usability and make items easier to see, aren't affected by this setting.
- Show the user's display name**
Name appears on top navigation bar when user is signed in. Long names may be shortened.

Create a group theme

You can create up to four additional group themes.

1. On the **General** page, enter a name for your new theme.
2. Under **Groups**, you can select up to 5 Microsoft 365 Groups that can see your group theme, instead of using the default theme. You can also prevent users from overriding their theme and show the user's display name.
3. Select **Save**.

Contoso

General Logos Colors


Name

Contoso

Groups

Choose up to five Microsoft 365 groups. Users in these groups will see this custom theme instead of the 'Organizational Theme'.

Select up to 5 groups

 Contoso marketing ×

- Prevent users from overriding their theme.**
High-contrast themes, which enhance usability and make items easier to see, aren't affected by this setting.
- Show the user's display name**
Name appears on top navigation bar when user is signed in. Long names may be shortened.

Logos: Specify your theme logos

On the **Logos** page, you can add your logos, and specify the URL where users will navigate to, when they select the logo.

- **Default logo:** Add a URL location that points to your logo. Make sure that the URL uses HTTPS. Add a HTTPS image url that allows anonymous access and doesn't require authentication. For default theme, you also have an option to upload a logo image that is less than 10kb. Your default logo can be in the JPG, PNG, GIF, or SVG format. For SVG images, they will be resized to fit 24 pixels vertically. JPG, PNG, GIF images will be scaled to

fit 200 x 48 pixels. Logo aspect ratio will always be preserved.

- **Alternate logo:** Add a URL location that points to your logo. Your alternate logo should be optimized for use in Office dark themes. Same requirements as the default logo.
- **On-click link:** Add a URL location that points to your logo. You can use your logo as a link to any company resource, for example, your company's website. If you don't select a URL location for your logo, it'll default to the Office home page.

Select **Save** to save your changes.

Default theme

General **Logos** Colors

Default Logo

Add a logo image for your organization. For information on setting up your logo, see [Logos](#).

Upload



Browse



Contoso Electronics

Remove

Alternate Logo

Should be optimized for use in Office dark themes and darker brand color palettes. Same requirements as the default logo.

https://



Remove

On-click link

When users click the logo, they'll go to the URL you provide here, for example, a company home page. If no URL is specified, URL will be defaulted to Office homepage.

You can remove your logos at any time. Just return to the **Logos** page and select **Remove**.

Colors: Choose theme colors

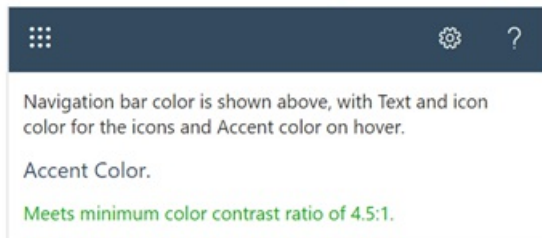
On the **Colors** page, you can set the default colors and choose which logo should be used.

- **Navigation bar color:** Select a color to use for the background of the navigation bar. The navigation bar appears at the top on every page.
- **Text and icon color:** Select a color to use for the text and icons on the top navigation bar.
- **Accent color:** Pick one that shows up well on a white or light background. The accent color is used to color some links and buttons that show up on a white or light background. For example, the accent color is used to color elements in a user's inbox and on their Office.com portal page.
- **Reset color:** Select this link to reset colors to the default colors.

Default theme

General Logos Colors

Set the default colors and logo for all Microsoft apps and services in standard mode. Dark mode will override them. [See our guidance for creating accessible color schemes.](#)



Navigation bar color

Background color of the top navigation bar.



#334A5F



Text and icon color

Affects text and icons on the navigation bar.



#F7FFF4



Accent color

Accent buttons, links and other elements.



#334A5F



[Reset Colors](#)

Frequently asked questions

My organization already has a theme for all employees. How will this change?

The default theme will continue to be shown to all employees. Adding a new group theme will only be made available to the Microsoft 365 groups associated with that theme.

Why don't I see group themes in the Admin Center?

Only global admins can customize company themes. Global readers have read-only access.

How many different themes can I set up for my organization?

Up to five themes can be created. A default theme and four group themes.

Can I use security groups or distribution groups instead of Microsoft 365 Groups?

No, new group themes must be mapped to one or more Microsoft 365 groups and not security groups or distribution groups.

NOTE

You can convert [distribution groups to Microsoft 365 groups](#) in Outlook.

Can I manually assign a theme independent of Microsoft 365 Groups?

No, new group themes must be mapped to one or more Microsoft 365 groups. Users who are members of the Microsoft 365 group will get the theme applied to their group. You can [create and add new members to a Microsoft 365 Group](#) by going to the **Settings > Groups** in the admin center.

What happens if a user is assigned to multiple group themes?

Users who are assigned to multiple group themes will be shown the default theme.

Why can't I delete the default theme?

The default theme can only be deleted once all group themes are deleted. Make sure you delete all group themes before you try to delete the group theme.

Why am I receiving an error message every time I upload a logo URL.

Make sure the logo you're using is specified as a publicly addressable URL. Follow these steps for [uploading logos to Azure Blob Storage](#) or the [Office 365 Content Delivery Network with SharePoint Online](#).

Why am I receiving the message "Doesn't meet minimum color contrast ratio of 4.5:1"?

The recommended contrast ratio between text, icon or button color and background color is 4.5:1. You can override this recommendation and still save your theme as this is not a requirement.

If I define a theme, which places in Microsoft 365 will this be used?

Any theme appears in the top navigation bar for everyone in the organization as part of the Microsoft 365 suite header.

Related content

[Add custom tiles to the My apps page and app launcher](#) (article)

[Overview of Microsoft 365 Groups for administrators](#) (article)

Learn about Office 365 Germany

5/7/2021 • 3 minutes to read • [Edit Online](#)

NOTE

Office 365 Germany is no longer accepting new customers or deploying new services. The new cloud regions in Germany, available in the first quarter of 2020 for Microsoft 365 and Office 365, will provide both core customer data residency within Germany, as well as full connectivity to the Microsoft global cloud network.

Office 365 Germany was a differentiated option to the Office 365 services available across Europe. It helped to address the needs of the most regulated customers in Germany, the European Union (EU), and the European Free Trade Association (EFTA) by delivering our industry-leading productivity services for digital work, from German datacenters, with data residency in Germany, and strict data access and control measures via a unique data trustee model governed by German law.

The data trustee, T-Systems International, an independent German company and subsidiary of Deutsche Telekom, controls physical and logical access to customer data. Customer data can't be accessed without approval from or supervision by the data trustee, which is governed by German law.

Customers needs have shifted, and the isolation of Office 365 Germany imposed limits on its ability to address the flexibility and consistency that customers want. Since August 2018, we're no longer accepting new customers or deploying any new services from the currently available Microsoft Cloud Germany. For more information, see this blog post: [Microsoft to deliver cloud services from new datacentres in Germany in 2019 to meet evolving customer needs](#).

Which Microsoft online services are available in Office 365 Germany?

Office 365 Germany plan offerings are aligned with global offers as much as possible in this isolated environment. Exclusions include Yammer-related plans, plans that are nearing their end-of-life, and plans available by way of non-profit programs. Office 365 E5, SPE, and other services will be available after general availability of Office 365 Germany.

The following services and features are available in some [Office 365 Germany subscription plans](#). Additionally, see the [Online Services Terms](#).

- Microsoft 365 Apps for enterprise, Office 2016, and Office 2013¹. Note that Office 2013 requires [using Office 365 modern authentication with Office clients](#).
- Exchange Online
- SharePoint Online
- OneDrive for Business
- Skype for Business
- Exchange Online Protection
- Office apps for the web
- Microsoft 365 Video
- Project for the web

- Visio for the web
- Groups
- Security & Compliance Center
- Customer Lockbox
- Advanced eDiscovery
- Microsoft Defender for Office 365
- Office 365 Threat Intelligence
- Office 365 Advanced Data Governance
- Audit Log Search
- Power BI Pro
- Delve

¹Office 365 Germany plans include client software applications that are installed and run on an end-user's device ("client software applications"), such as Microsoft 365 Apps for enterprise, Office 2013, and Office 2016. Client software applications do not operate exclusively in German data centers and may enable an end-user to access online services that are not [German Online Services](#). For purposes of your agreement with Microsoft, client software applications are not [German Online Services](#). German data residency commitments and access control by German data trustee apply only to the [German Online Services](#).

General information

ITEM	INFORMATION
Sign in portal	https://portal.office.de
Subscriptions, billing, and technical support	Germany-based support available in German and English For details, see Contact support for business products - Admin Help .
IP Addresses and URLs	See Office 365 Germany endpoints .
Yammer	Not available.
Versions of Office older than Office 2013 or Microsoft 365 Apps for enterprise ¹	Not supported.
Office Lens	Not available.
Ability to buy a domain from within Microsoft 365	Not available.

ITEM	INFORMATION
SharePoint Store	<p>Each app that is available in a Microsoft app store is provided by either Microsoft or a third-party app publisher and is subject to a separate privacy statement and terms and conditions. Data provided through the use of a Microsoft app store and any app may be accessible to Microsoft or the third-party app publisher, as applicable, and transferred to, stored, and processed in the United States or any other country where Microsoft or the app publisher and their affiliates or service providers maintain facilities. Please work with the app publisher to make sure it meets requirements for your Office 365 Germany deployment.</p>

For a more detailed look at services available for each Microsoft 365 plan, see the [Microsoft 365 Service Description](#).

Synchronize domain users to Microsoft 365

4/3/2021 • 2 minutes to read • [Edit Online](#)

1. Prepare for Directory Synchronization

Before you synchronize your users and computers from the local Active Directory Domain, review [Prepare for directory synchronization to Microsoft 365](#). In particular:

- Make sure that no duplicates exist in your directory for the following attributes: **mail**, **proxyAddresses**, and **userPrincipalName**. These values must be unique and any duplicates must be removed.
- We recommend that you configure the **userPrincipalName** (UPN) attribute for each local user account to match the primary email address that corresponds to the licensed Microsoft 365 user. For example: *mary.shelley@contoso.com* rather than *mary@contoso.local*
- If the Active Directory domain ends in a non-routable suffix like *.local* or *.lan*, instead of an internet routable suffix such as *.com* or *.org*, adjust the UPN suffix of the local user accounts first as described in [Prepare a non-routable domain for directory synchronization](#).

The **Run IdFix** in step four (4) below, will also make sure your on-premises Active Directory is ready for directory synchronization.

2. Install and configure Azure AD Connect

To synchronize your users, groups, and contacts from the local Active Directory into Azure Active Directory, install Azure Active Directory Connect and set up directory synchronization.

1. In the [admin center](#), select **Setup** in the left nav.
2. Under **Sign-in and security**, choose **View** under **Sync users from your org's directory**.
3. On the **Sync users from your org's directory** page, choose **Get started**.
4. In the first step run IdFix tool to prepare for Directory sync.
5. Follow the wizard steps to download Azure AD Connect and use it to synchronize your domain-controlled users to Microsoft 365.

See [Set up directory synchronization for Microsoft 365](#) to learn more.

As you configure your options for Azure AD Connect, we recommend that you enable **Password Synchronization**, **Seamless Single Sign-On**, and the **password writeback** feature, which is also supported in Microsoft 365 for business.

NOTE

There are some additional steps for password writeback beyond the check box in Azure AD Connect. For more information, see [How-to: configure password writeback](#).

If you also want to manage domain-joined Windows 10 devices, see [Enable domain-joined Windows 10 devices to be managed by Microsoft 365 Business Premium](#) to set up a hybrid Azure AD Join.

Enable domain-joined Windows 10 devices to be managed by Microsoft 365 Business Premium

7/12/2021 • 4 minutes to read • [Edit Online](#)

If your organization uses Windows Server Active Directory on-premises, you can set up Microsoft 365 Business Premium to protect your Windows 10 devices, while still maintaining access to on-premises resources that require local authentication. To set up this protection, you can implement **Hybrid Azure AD joined devices**. These devices are joined to both your on-premises Active Directory and your Azure Active Directory.

Watch: Configure Hybrid Azure Active Directory join

This video describes the steps for how to set this up for the most common scenario, which is also detailed in the steps that follow.

Before you begin

- Synchronize users to Azure AD with Azure AD Connect.
- Complete Azure AD Connect Organizational Unit (OU) sync.
- Make sure all the domain users you sync have licenses to Microsoft 365 Business Premium.

See [Synchronize domain users to Microsoft](#) for the steps.

1. Verify MDM Authority in Intune

Go to [Endpoint Manager](#) and on the Microsoft Intune page, select **Device enrollment**, then on the **Overview** page, make sure **MDM authority** is **Intune**.

- If **MDM authority** is **None**, click the **MDM authority** to set it to **Intune**.
- If **MDM authority** is **Microsoft Office 365**, go to **Devices > Enroll devices** and use the **Add MDM authority** dialog on the right to add **Intune MDM authority** (the **Add MDM Authority** dialog is only available if the **MDM Authority** is set to **Microsoft Office 365**).

2. Verify Azure AD is enabled for joining computers

- Go to the admin center at <https://admin.microsoft.com> and select **Azure Active Directory** (select **Show all** if **Azure Active Directory** is not visible) in the **Admin centers** list.
- In the **Azure Active Directory** admin center, go to **Azure Active Directory**, choose **Devices** and then **Device settings**.
- **VerifyUsers may join devices to Azure AD** is enabled
 1. To enable all users, set to **All**.
 2. To enable specific users, set to **Selected** to enable a specific group of users.
 - Add the desired domain users synced in Azure AD to a [security group](#).
 - Choose **Select groups** to enable MDM user scope for that security group.

3. Verify Azure AD is enabled for MDM

- Go to the admin center at <https://admin.microsoft.com> and select **Endpoint Management** (select

Show all if Endpoint Manager is not visible)

- In the **Microsoft Endpoint Manager admin center**, go to **Devices > Windows > Windows Enrollment > Automatic Enrollment**.
- Verify MDM user scope is enabled.
 1. To enroll all computers, set to **All** to automatically enroll all user computers that are joined to Azure AD and new computers when the users add a work account to Windows.
 2. Set to **Some** to enroll the computers of a specific group of users.
 - Add the desired domain users synced in Azure AD to a [security group](#).
 - Choose **Select groups** to enable MDM user scope for that security group.

4. Create the required resources

Performing the required tasks to [configure hybrid Azure AD join](#) has been simplified through the use of the [Initialize-SecMgmtHybirdDeviceEnrollment](#) cmdlet found in the [SecMgmt](#) PowerShell module. When you invoke this cmdlet it will create and configure the required service connection point and group policy.

You can install this module by invoking the following from an instance of PowerShell:

```
Install-Module SecMgmt
```

IMPORTANT

It is recommended that you install this module on the Windows Server running Azure AD Connect.

To create the required service connection point and group policy, you will invoke the [Initialize-SecMgmtHybirdDeviceEnrollment](#) cmdlet. You will need your Microsoft 365 Business Premium global admin credentials when performing this task. When you are ready to create the resources, invoke the following:

```
PS C:\> Connect-SecMgmtAccount  
PS C:\> Initialize-SecMgmtHybirdDeviceEnrollment -GroupPolicyDisplayName 'Device Management'
```

The first command will establish a connection with the Microsoft cloud, and when you are prompted, specify your Microsoft 365 Business Premium global admin credentials.

5. Link the Group Policy

1. In the Group Policy Management Console (GPMC), right-click on the location where you want to link the policy and select *Link an existing GPO...* from the context menu.
2. Select the policy created in the above step, then click **OK**.

Get the latest Administrative Templates

If you do not see the policy **Enable automatic MDM enrollment using default Azure AD credentials**, it may be because you don't have the ADMX installed for Windows 10, version 1803, or later. To fix the issue, follow these steps (Note: the latest MDM.admx is backwards compatible):

1. Download: [Administrative Templates \(.admx\) for Windows 10 October 2020 Update \(20H2\)](#).
2. Install the package on a Domain Controller.
3. Navigate, depending on the Administrative Templates version to the folder: **C:\Program Files (x86)\Microsoft Group Policy\Windows 10 October 2020 Update (20H2)**.

4. Rename the **Policy Definitions** folder in the above path to **PolicyDefinitions**.
5. Copy the **PolicyDefinitions** folder to your SYSVOL share, by default located at **C:\Windows\SYSVOL\domain\Policies**.
 - If you plan to use a central policy store for your entire domain, add the contents of PolicyDefinitions there.
6. In case you have several Domain Controllers, wait for SYSVOL to replicate for the policies to be available. This procedure will work for any future version of the Administrative Templates as well.

At this point you should be able to see the policy **Enable automatic MDM enrollment using default Azure AD credentials** available.

Related content

[Synchronize domain users to Microsoft 365](#) (article)

[Create a group in the admin center](#) (article)

[Tutorial: Configure hybrid Azure Active Directory join for managed domains](#) (article)

Access on-premises resources from an Azure AD-joined device in Microsoft 365 Business Premium

7/12/2021 • 2 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

Any Windows 10 device that is Azure Active Directory joined has access to all cloud-based resources, such as your Microsoft 365 apps, and can be protected by Microsoft 365 Business Premium. You can also allow access to on-premises resources like line of business (LOB) apps, file shares, and printers. To allow access, use [Azure AD Connect](#) to synchronize your on-premises Active Directory with Azure Active Directory.

To learn more, see [Introduction to device management in Azure Active Directory](#). The steps are also summarized in the following sections.

Run Azure AD Connect

Complete the following steps to enable your organization's Azure AD joined devices to access on-premises resources.

1. To synchronize your users, groups, and contacts from local Active Directory into Azure Active Directory, run the Directory synchronization wizard and Azure AD Connect as described in [Set up directory synchronization for Office 365](#).
2. After the directory synchronization is complete, make sure your organization's Windows 10 devices are Azure AD joined. This step is done individually on each Windows 10 device. See [Set up Windows devices for Microsoft 365 Business Premium users](#) for details.
3. Once the Windows 10 devices are Azure AD joined, each user must reboot their devices and sign in with their Microsoft 365 Business Premium credentials. All devices now have access to on-premises resources as well.

No additional steps are required to get access to on-premises resources for Azure AD joined devices. This functionality is built into Windows 10.

If you have plans to login to the AADJ device other than password method Like PIN/Bio-metric via WHFB credential login and then access on-premise resources (shares, printers, etc.), please follow [this article](#).

If your organization isn't ready to deploy in the Azure AD joined device configuration described above, consider setting up [Hybrid Azure AD Joined device configuration](#).

Considerations when you join Windows devices to Azure AD

If the Windows device that you Azure-AD joined was previously domain-joined or in a workgroup, consider the following limitations:

- When a device Azure AD joins, it creates a new user without referencing an existing profile. Profiles must be manually migrated. A user profile contains information like favorites, local files, browser settings, and Start menu settings. A best approach is to find a third-party tool to map existing files and settings to the new profile.
- If the device is using Group Policy Objects (GPO), some GPOs may not have a comparable [Configuration Service Provider](#) (CSP) in Intune. Run the [MMAT tool](#) to find comparable CSPs for existing GPOs.
- Users might not be able to authenticate to applications that depend on Active Directory authentication.

Evaluate the legacy app and consider updating to an app that uses modern Auth, if possible.

- Active Directory printer discovery won't work. You can provide direct printer paths for all users or use [Universal Print](#).

Related Articles

[Prerequisites for Azure AD Connect](#)

Overview of the Microsoft 365 admin center

6/30/2021 • 7 minutes to read • [Edit Online](#)

- [The admin center in simplified view](#)
- [The admin center in dashboard view](#)

The Microsoft 365 admin center has two views: simplified view helps smaller organizations manage their most common tasks. Dashboard view includes more complex settings and tasks. You can switch between them from a button at the top of the admin center.

Watch: The admin center in simplified view

With the Microsoft 365 admin center, you can reset passwords, view your invoice, add or remove users, and much more all in one place.

Sign in to Office.com with your work account, and select the app launcher.

If you have permission to access the admin center, you'll see **Admin** in the list. Select it.

At the top of the admin center, review the top actions for you. You may see different actions depending on what you've already set up, such as creating new accounts, using Teams, setting up email, and installing Office apps.

Under **Your organization** on the **Users** tab is a list of people who can access apps and services, add new users, reset passwords, or use the three dots (more actions) menu. Select a person to view or edit their information and settings.

On the **Teams** tab, create a new team or manage existing teams. You can manage the members of a team or select the three dots (more actions) to change other Teams settings.

On the **Subscriptions** tab, add more products, add licenses, or use the three dots (more actions) menu to modify licenses or payment method.

On the **Learn** tab, browse videos and articles about the admin center and other Microsoft 365 features. To explore more advanced features of the admin center, open the navigation menu and expand the headings to see more. Select **Show all** to see everything in the navigation menu or use the search bar to quickly find what you're looking for.

If you need assistance, select **Help & support**. Search for topic you want help with and view the recommended solution or select the headset to contact support, and then enter your question and contact information.

Watch: The admin center in dashboard view

The Microsoft 365 admin center is where you manage your business in the cloud. You can complete such tasks as adding and removing users, changing licenses, and resetting passwords.

Specialist workspaces, like Security or Device management, allow for more granular control. For more information about how the admin centers work together, see [What about the specific types of IT roles and other workspaces like Security, Device Management, or Exchange?](#) in this article.

To get to the Microsoft 365 admin center, go to admin.microsoft.com or, if you're already signed in, select the app launcher, and choose **Admin**.

On the home page, you can create cards for tasks that you perform frequently. To add a new card, select **Add card**, then select the plus sign next to the card you want to add. When you are finished, close the window. You can rearrange the cards by selecting and then dragging them to where you want. To remove a card, select the three dots (more actions), and then choose **Remove**.

To view more admin tasks, expand the navigation menu. You'll find advanced configuration settings in the additional admin centers at the bottom.

One common task that you might perform in the admin center is adding a user. To do this, select **Users, Active users**, and then select **Add a user**. Enter the user's name and other information, and then select **Next**. Follow the prompts to finish adding the user. When you are done, select **Finish adding**, and then select **Close**.

You can sort your active users by columns, such as **Display name** or **Licenses**. To add more columns, select **Choose columns**, select the columns you want to add, and then select **Save**.

Select a user to see more options, such as managing their product licenses.

To enable more features that come with your subscription, select **Setup**. Here you can turn on sign-in security, mobile app protection, DLP, and other features included with your subscription.

If you need support at any time, choose **Need help**. Enter your question, then check out the links that appear. If you don't get your answer here, choose **Contact support** to open a service request.

For more information on managing billing, passwords, users, and admins, see the other lessons in this course.

Who is an admin?

By default, the person who signs up for and buys an Microsoft 365 for business subscription gets admin permissions. That person can assign admin permissions to other people to help them manage Microsoft 365 for their organization.

If you get the message "**You don't have permission to access this page or perform this action**," you aren't an admin.

Who has admin permissions in my business?

When looking for your admin to reset your password, delete an account, or do other tasks, here's who you should contact:

- **Universities and schools:** Contact your technical support team. Usually you can find a link on your university site. At smaller schools, there may be just a few individuals who have admin permissions.
- **Large businesses:** Contact your internal help desk / technical support.
- **Small businesses:** Contact the business owner / co-owner. Often they give admin permissions to their IT consultant who does all the computer maintenance work for their business.

If you have no idea who to contact at your work or school for help, try asking the person who gave you your user account and password.

NOTE

Targeted release admins have first access to new features. New features later roll out to all admins. This means that you might not see the admin center, or it might look different than what is described in help articles. To be among the first to see new features, see [Participate in the admin center](#), below.

Turn on Targeted release

1. Sign in at admin.microsoft.com, go to the navigation pane and select **Settings > Organization profile**.
2. Go to the **Release preferences** card, and then select **Edit**.
3. Select either **Targeted release for everyone** or **Targeted release for selected users**. If you choose **Targeted release for selected users**, make sure that you add your admin account (and any other admins in your org who want to participate) to the list of selected users.

Admin center feedback

While in the admin center, you can give Microsoft feedback about your experience by selecting **Give feedback** right next to the **Need help?** button at the bottom of every page. Tell us what you like and what we could do better. In addition, you may get pop-up surveys from time-to-time asking about your overall impressions or a particular experience that's newly released. You can also give feedback at the end of this article by selecting **Was this information helpful?**

Frequently asked questions

Don't see your questions answered here? Go to the **Feedback** section at the bottom of this page and ask your question.

Which Microsoft 365 plans are available to trial or buy?

Microsoft 365 is a complete, intelligent solution that includes Office 365, Windows 10, and Enterprise Mobility + Security that empowers everyone to be creative and work together, securely. The following Microsoft 365 subscriptions are available in the admin center for you to try or buy now:

- Microsoft 365 for business
- Microsoft 365 Enterprise E3
- Microsoft 365 Enterprise E5

For more information, see [Try or buy a Microsoft 365 subscription](#).

I found a bug or I want to request a feature enhancement. How do I let Microsoft know?

We love to hear from you! Reporting bugs and sharing feedback helps us make the Microsoft 365 admin center better. To give feedback, select the **Feedback** button on the bottom of the page and use the form to send us your thoughts. Select the checkbox and confirm your email address if you want someone from the Microsoft 365 admin center team to follow up on your comments. We can't promise to follow up on every piece of feedback, but we're going to try!

You can also give feedback from outside of the admin center on our UserVoice forum. You can use this page to make feature suggestions that can be voted on by other forum users: [UserVoice forum for the new admin center](#).

What about the specific types of IT roles and other workspaces like Security, Device Management, or Exchange?

The Microsoft 365 admin center is the common entry point for all teams and roles managing Microsoft 365. The experience, information, and controls are tailored and customizable for each admin and role. Additionally, specialist workspaces allow for deep, granular control. These specialist workspaces include SharePoint, Teams & Skype, Exchange, Security, Compliance, Device Management, and Azure Active Directory. You can find the specialist workspaces from the navigation pane in the Microsoft 365 admin center at <https://admin.microsoft.com>.

What language options are available the Admin Center?

The Microsoft 365 admin center is fully localized in 40 languages.

LANGUAGE	LOCALE
Arabic	ar
Bulgarian	bg
Catalan	ca
Czech	cs
Danish	da
German	de
Greek	el
Spanish	es
English	en
Estonian	et
Basque	eu
Finnish	fi
French	fr
Galician	gl
Hebrew	he
Croatian	hr
Hungarian	hu
Indonesian	id
Italian	it
Japanese	ja
Korean	ko
Lithuanian	lt
Latvian	lv
Dutch	nl
Norwegian	no

LANGUAGE	LOCALE
Polish	pl
Portuguese (Brazil)	pt
Portuguese (Portugal)	pt-pt
Romanian	ro
Russian	ru
Slovak	sk
Slovenian	sl
Serbian (Cyrillic)	sr-cyrl
Serbian Latin	sr
Swedish	sv
Thai	th
Turkish	tr
Ukrainian	uk
Vietnamese	vi
Chinese Simplified	zh-hans
Chinese Traditional	zh-hant

Related content

[What is a Microsoft 365 admin? \(video\)](#)

[Add an admin \(video\)](#)

[Customize the Microsoft 365 theme for your organization \(article\)](#)

About admin roles

8/13/2021 • 8 minutes to read • [Edit Online](#)

Microsoft 365 or Office 365 subscription comes with a set of admin roles that you can assign to users in your organization using the [Microsoft 365 admin center](#). Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers.

The [Microsoft 365 admin center](#) lets you manage Azure AD roles and Microsoft Intune roles. However, these roles are a subset of the roles available in the Azure AD portal and the Intune admin center.

Before you begin

Looking for the full list of detailed Azure AD role descriptions you can manage in the [Microsoft 365 admin center](#)? Check out Administrator role permissions in Azure Active Directory. [Administrator role permissions in Azure Active Directory](#).

Looking for the full list of detailed Intune role descriptions you can manage in the [Microsoft 365 admin center](#)? Check out [Role-based access control \(RBAC\) with Microsoft Intune](#).

For more information on assigning roles in the [Microsoft 365 admin center](#), see [Assign admin roles](#).

Watch: What is an admin?

Security guidelines for assigning roles

Because admins have access to sensitive data and files, we recommend that you follow these guidelines to keep your organization's data more secure.

RECOMMENDATION	WHY IS THIS IMPORTANT?
Have 2 to 4 global admins	Because only another global admin can reset a global admin's password, we recommend that you have at least 2 global admins in your organization in case of account lockout. But the global admin has almost unlimited access to your org's settings and most of the data, so we also recommend that you don't have more than 4 global admins because that's a security threat.
Assign the <i>least permissive</i> role	Assigning the <i>least permissive</i> role means giving admins only the access they need to get the job done. For example, if you want someone to reset employee passwords you shouldn't assign the unlimited global admin role, you should assign a limited admin role, like Password admin or Helpdesk admin. This will help keep your data secure.

RECOMMENDATION	WHY IS THIS IMPORTANT?
Require multi-factor authentication for admins	<p>It's actually a good idea to require MFA for all of your users, but admins should definitely be required to use MFA to sign in. MFA makes users enter a second method of identification to verify they are who they say they are. Admins can have access to a lot of customer and employee data and if you require MFA, even if the admin's password gets compromised, the password is useless without the second form of identification.</p> <p>When you turn on MFA, the next time the user signs in, they'll need to provide an alternate email address and phone number for account recovery.</p> <p>Set up multi-factor authentication</p>

If you get a message in the admin center telling you that you don't have permissions to edit a setting or page, it's because you are assigned a role that doesn't have that permission.

Commonly used Microsoft 365 admin center roles

In the Microsoft 365 admin center, you can go to [Role assignments](#), and then select any role to open its detail pane. Select the **Permissions** tab to view the detailed list of what admins assigned that role have permissions to do. Select the **Assigned** or **Assigned admins** tab to add users to roles.

You'll probably only need to assign the following roles in your organization. By default, we first show roles that most organizations use. If you can't find a role, go to the bottom of the list and select **Show all by Category**. (For detailed information, including the cmdlets associated with a role, see [Administrator role permissions in Azure Active Directory](#).)

ADMIN ROLE	WHO SHOULD BE ASSIGNED THIS ROLE?
Billing admin	<p>Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.</p> <p>Billing admins also can:</p> <ul style="list-style-type: none"> - Manage all aspects of billing - Create and manage support tickets in the Azure portal
Exchange admin	<p>Assign the Exchange admin role to users who need to view and manage your user's email mailboxes, Microsoft 365 groups, and Exchange Online.</p> <p>Exchange admins can also:</p> <ul style="list-style-type: none"> - Recover deleted items in a user's mailbox - Set up "Send As" and "Send on behalf" delegates

ADMIN ROLE	WHO SHOULD BE ASSIGNED THIS ROLE?
Global admin	<p>Assign the Global admin role to users who need global access to most management features and data across Microsoft online services.</p> <p>Giving too many users global access is a security risk and we recommend that you have between 2 and 4 Global admins.</p> <p>Only global admins can:</p> <ul style="list-style-type: none"> - Reset passwords for all users - Add and manage domains <p>Note: The person who signed up for Microsoft online services automatically becomes a Global admin.</p>
Global reader	<p>Assign the global reader role to users who need to view admin features and settings in admin centers that the global admin can view. The global reader admin can't edit any settings.</p>
Groups admin	<p>Assign the groups admin role to users who need to manage all groups settings across admin centers, including the Microsoft 365 admin center and Azure Active Directory portal.</p> <p>Groups admins can:</p> <ul style="list-style-type: none"> - Create, edit, delete, and restore Microsoft 365 groups - Create and update group creation, expiration, and naming policies - Create, edit, delete, and restore Azure Active Directory security groups
Helpdesk admin	<p>Assign the Helpdesk admin role to users who need to do the following:</p> <ul style="list-style-type: none"> - Reset passwords - Force users to sign out - Manage service requests - Monitor service health <p>Note: The Helpdesk admin can only help non-admin users and users assigned these roles: Directory reader, Guest inviter, Helpdesk admin, Message center reader, and Reports reader.</p>
License admin	<p>Assign the License admin role to users who need to assign and remove licenses from users and edit their usage location.</p> <p>License admins also can:</p> <ul style="list-style-type: none"> - Reprocess license assignments for group-based licensing - Assign product licenses to groups for group-based licensing

ADMIN ROLE	WHO SHOULD BE ASSIGNED THIS ROLE?
Office Apps admin	<p>Assign the Office Apps admin role to users who need to do the following:</p> <ul style="list-style-type: none"> - Use the Office cloud policy service to create and manage cloud-based policies for Office - Create and manage service requests - Manage the What's New content that users see in their Office apps - Monitor service health
Password admin	<p>Assign the Password admin role to a user who needs to reset passwords for non-administrators and Password Administrators.</p>
Message center reader	<p>Assign the Message center reader role to users who need to do the following:</p> <ul style="list-style-type: none"> - Monitor message center notifications - Get weekly email digests of message center posts and updates - Share message center posts - Have read-only access to Azure AD services, such as users and groups
Power Platform admin	<p>Assign the Power Platform admin role to users who need to do the following:</p> <ul style="list-style-type: none"> - Manage all admin features for Power Apps, Power Automate, and data loss prevention - Create and manage service requests - Monitor service health
Reports reader	<p>Assign the Reports reader role to users who need to do the following:</p> <ul style="list-style-type: none"> - View usage data and the activity reports in the Microsoft 365 admin center - Get access to the Power BI adoption content pack - Get access to sign-in reports and activity in Azure AD - View data returned by Microsoft Graph reporting API
Service Support admin	<p>Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:</p> <ul style="list-style-type: none"> - Open and manage service requests - View and share message center posts - Monitor service health
SharePoint admin	<p>Assign the SharePoint admin role to users who need to access and manage the SharePoint Online admin center.</p> <p>SharePoint admins can also:</p> <ul style="list-style-type: none"> - Create and delete sites - Manage site collections and global SharePoint settings

ADMIN ROLE	WHO SHOULD BE ASSIGNED THIS ROLE?
Teams service admin	<p>Assign the Teams service admin role to users who need to access and manage the Teams admin center.</p> <p>Teams service admins can also:</p> <ul style="list-style-type: none"> - Manage meetings - Manage conference bridges - Manage all org-wide settings, including federation, teams upgrade, and teams client settings
User admin	<p>Assign the User admin role to users who need to do the following for all users:</p> <ul style="list-style-type: none"> - Add users and groups - Assign licenses - Manage most users properties - Create and manage user views - Update password expiration policies - Manage service requests - Monitor service health <p>The user admin can also do the following actions for users who aren't admins and for users assigned the following roles: Directory reader, Guest inviter, Helpdesk admin, Message center reader, Reports reader:</p> <ul style="list-style-type: none"> - Manage usernames - Delete and restore users - Reset passwords - Force users to sign out - Update (FIDO) device keys

Delegated administration for Microsoft Partners

If you're working with a Microsoft partner, you can assign them admin roles. They, in turn, can assign users in your company, or their company, admin roles. You might want them to do this, for example, if they are setting up and managing your online organization for you.

A partner can assign these roles:

- **Admin Agent** Privileges equivalent to a global admin, with the exception of managing multi-factor authentication through the Partner Center.
- **Helpdesk Agent** Privileges equivalent to a helpdesk admin.

Before the partner can assign these roles to users, you must add the partner as a delegated admin to your account. This process is initiated by an authorized partner. The partner sends you an email to ask you if you want to give them permission to act as a delegated admin. For instructions, see [Authorize or remove partner relationships](#).

Related content

[Assign admin roles](#) (article)

[Azure AD roles in the Microsoft 365 admin center](#) (article)

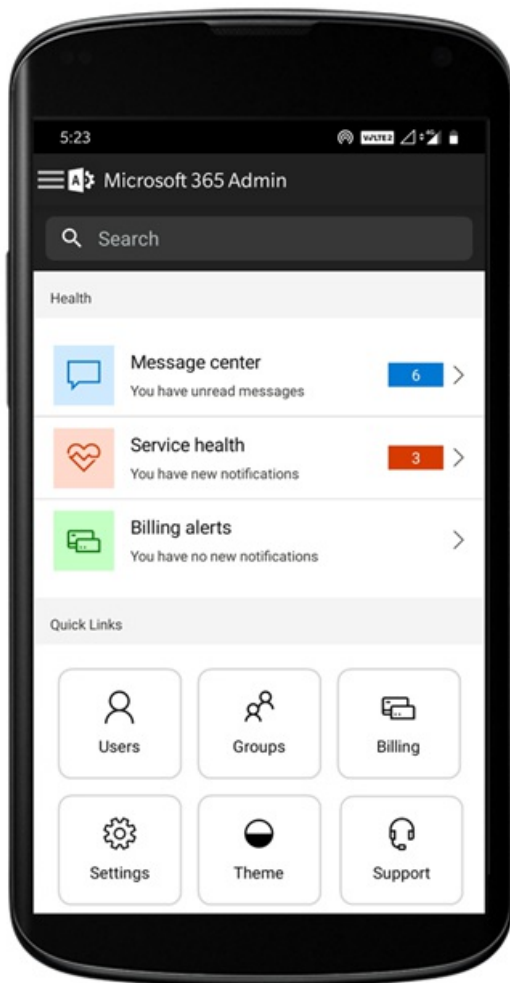
[Activity reports in the Microsoft 365 admin center](#) (article)

[Exchange Online admin role](#) (article)

About the Microsoft 365 admin mobile app

5/26/2021 • 4 minutes to read • [Edit Online](#)

Are you an admin who's usually on the go? Even if you aren't, there may be times when you need to manage Microsoft 365 from your phone or tablet. Check out the free [Microsoft 365 Admin app](#), the perfect companion to the web-based Microsoft 365 admin center. You can download the app from the [Apple App Store](#), and from the [Google Play Store](#).



The admin app has a lot of capabilities which will enable you to manage Microsoft 365 from your mobile or tablet device, when you can't get to a computer. Here's a list of a few of the tasks you can do from the app:

- **Manage users and devices** Add or edit a user, reset a user's password, assign a role, block user, delete user, manage alias, assign licenses, wipe device data and more.
- **Manage groups** Add a group, add or remove users from groups.
- **License management and billing** View a list of purchased and assigned licenses, assign licenses to users, purchase or remove licenses and view and download invoices.
- **Support** Create a new service request and keep track of all the updates related to the service requests while you are on the go.
- **Message Center** Stay on top of all the upcoming changes, planned maintenance, or other important announcements related to Microsoft 365
- **Service Health** Monitor the health of all the services by viewing the current status of the service and details about service disruption and outages.

- **Notifications** Stay on top of all the important information and updates related to message center posts, service health and billing through push notifications. You can even customize what you want to be notified of.

If you're an admin and you're responsible for more than one Microsoft 365 organization, you can sign in to multiple organizations and quickly switch between them. The app supports dark theme and is available in 39 languages.

IMPORTANT

If you're having issues using the Admin mobile app on iOS or Android, email us at feedback365@microsoft.com to let us know.

Before you begin

You must be an administrator in a Microsoft 365 organization to use the admin mobile app.

Download the admin mobile app

[Apple App Store](#)

[Google Play Store](#).

Watch: Install the admin mobile app

Frequently asked questions

Below are answers to frequently asked questions.

What do I need to do to be able to use the app?

To use the app you need to have admin permissions and a valid subscription to one of the following Microsoft 365 subscriptions:

- Microsoft 365 Apps for Enterprise
- Microsoft 365 Apps for Business
- Microsoft 365 Business Premium
- Microsoft 365 Business Standard
- Microsoft 365 Business Basic
- Microsoft 365 E3/E5
- Office 365: E1, E3/E5
- Exchange Online plan
- OneDrive for business plan

Can I use the app with my Microsoft 365 Family subscription?

No, the app doesn't work with Microsoft 365 Family or Microsoft 365 Personal subscriptions.

Will the app work if my organization has directory synchronization enabled?

Yes, but with reduced functionality. You'll be able to sign in and view service information, but most of the user management functions will be read-only. You won't be able to add, edit, or delete users. However, you'll be able to assign licenses to users in your organization and get notifications.

What languages are supported by the app?

The app supports all 39 languages that the web-based Microsoft 365 admin center supports. To change the

language, from the left navigation menu in the admin center, go to **Settings > Language** or select the **Language** icon in **Quick Links** section of the admin mobile app home page.

How can I share the Service Incidents and Messages with the rest of my organization?

If you select a specific service incident or a message, the share option will be in the top right corner.

Can I use this app with multiple accounts or tenants?

Yes, you can setup multiple accounts or organizations.

I'm unable to login or my app is acting funny. What can I do to troubleshoot or fix the issue?

You can try some common mobile app troubleshooting steps:

1. Close and reopen the app.
2. Uninstall and reinstall the app. Ensure that you are on the latest version of the app.
3. If you have Microsoft Authenticator or Company portal app installed on your device, try reinstalling it or updating to the latest version.
4. If that doesn't work, you can email us at feedback365@microsoft.com to let us know.

How do I manage notifications in the app?

From the left navigation menu, go to **Settings > Notifications**. You can manage service health, message center and billing notifications here.

What do I do if my question isn't answered?

Email feedback365@microsoft.com to report an issue with the app. Or you can give feedback at the bottom of this article.

Next steps

Once you've downloaded the admin mobile, you can add users to get you started.

Related content

[Microsoft 365 for business training videos](#)

What's new in the Microsoft 365 admin center

8/13/2021 • 24 minutes to read • [Edit Online](#)

NOTE

Some of the information in this article might not apply to Office 365 operated by 21Vianet.

We're continuously adding new features to [the Microsoft 365 admin center](#), fixing issues we learn about, and making changes based on your feedback. Take a look below to see what's available for you today. Some features get rolled out at different speeds to our customers. If you aren't seeing a feature yet, [try adding yourself to targeted release](#).

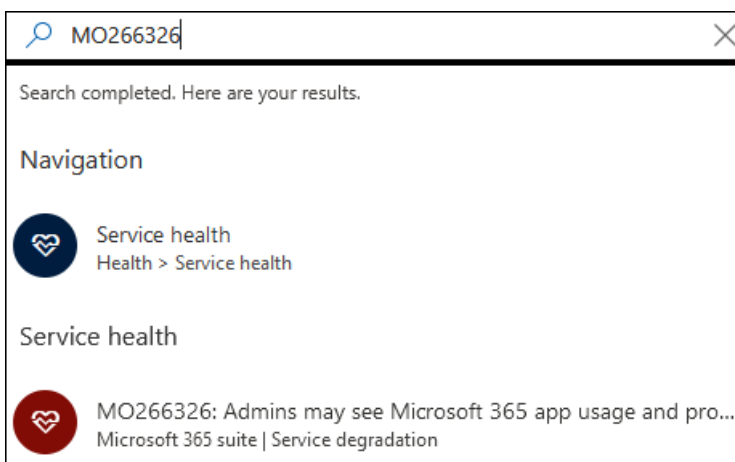
And if you'd like to know what's new with other Microsoft cloud services:

- [What's new in Azure Active Directory](#)
- [What's new in the Exchange admin center](#)
- [What's new in Microsoft Intune](#)
- [What's new in the Microsoft 365 compliance center](#)
- [What's new in Microsoft 365 Defender](#)
- [What's new in the SharePoint admin center](#)
- [Office updates](#)
- [How to check Windows release health](#)

July 2021

Microsoft 365 admin center search

You can now search for incident IDs in the [Microsoft 365 admin center](#). You may learn about current incidents through social media, industry publications or from other admins. You can now go to the admin center to look up more details about the incident and to understand the impact to your organization. Just search for the incident ID in the admin center.



Support ticket insight for Premier organizations

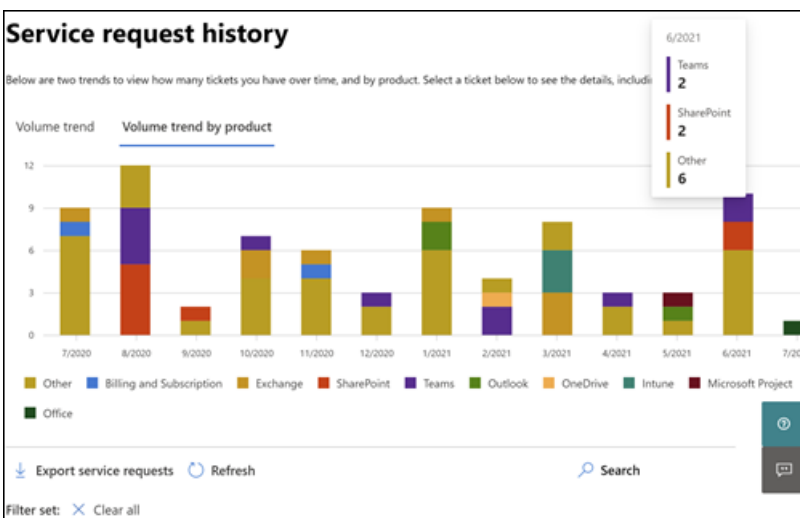
We've added 2 graphs called **Volume trend** and **Volume trend by product** to give you visual insights about your support volume.

The liner graph under **Volume trend** tab highlights the trend if support cases are increasing or decreasing for

your organization month over month. You can hover on the graph to check the number of support cases created in each month.



The **Volume trend by product** graph shows the top 3 products of each month with the highest support cases. We've enabled filtering in the table and you can now filter the results by **Product**, **Severity**, and **Date**.



We've also added 2 new fields, **Severity** and **Closed Date** in the **View Service Request** table to give you more insights about your tickets.

Export service requests Refresh Search

Filter set: Clear all

Status: Open Severity: All Date: Past 3 months Product: All

Title	Date	Ticket #	Created by	Status	Product	Severity	Closed Date
test case	6/23/2021	26283081		Agent assigned	Other		
test case for trans...	6/17/2021	26192196		Agent assigned	Other		

To check out these updates in [Microsoft 365 admin center](#), go to **Support > View Service requests** in left navigation pane.

June 2021

Microsoft 365 admin center search

We've added a couple of new categories to Search functionality.

- You can now search for Microsoft 365 admin roles in global search and quickly view and manage role assignments from any page. For example, search for **Intune administrator**.
- You can now find simplified setup experiences through global search. This can help you and your team quickly get started with how to use new features. For example, search for **set password to never expire**.

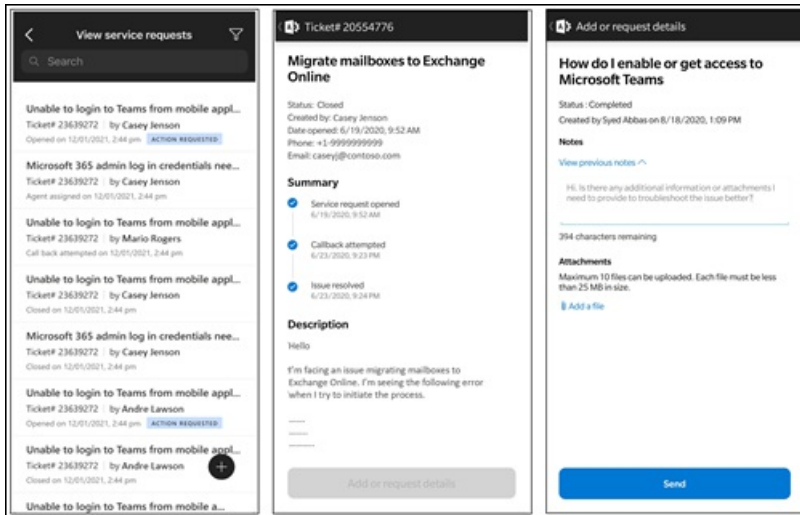
To learn more about search in the admin center, see [Search in the Microsoft 365 admin center](#).

May 2021

Admin mobile app

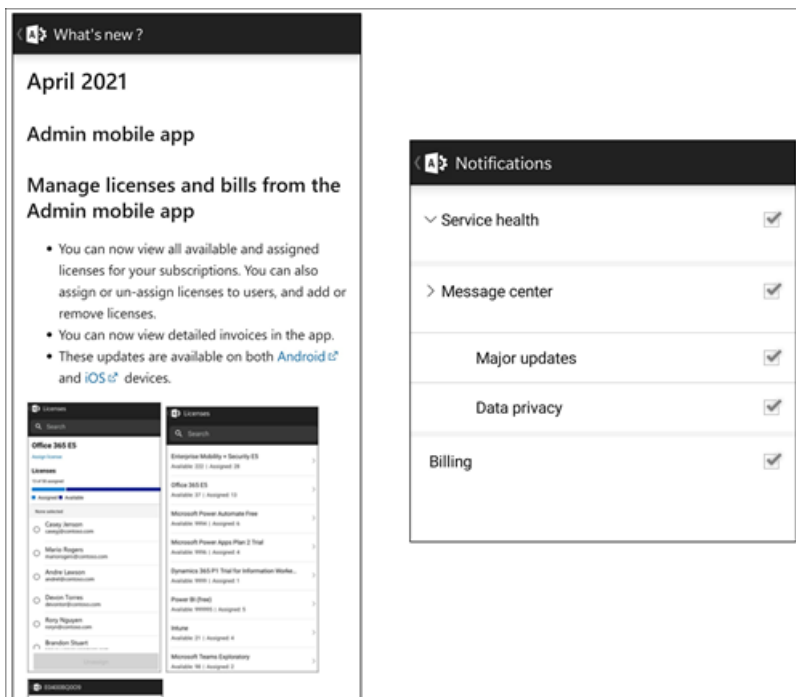
Keep track of support ticket updates using the Admin mobile app

For all the service requests created in your tenant you can now keep track of the ticket status, view ticket details and provide / request additional information by adding notes & attachments.



Stay on top of all the major updates to the app and your Microsoft 365 subscription

- Stay on top of all the major updates to your Microsoft 365 subscription through Message Center push notifications (now enabled by default).
- Keep track of the latest features available in the app using the **What's New** section. Go to **Settings > What's new?**

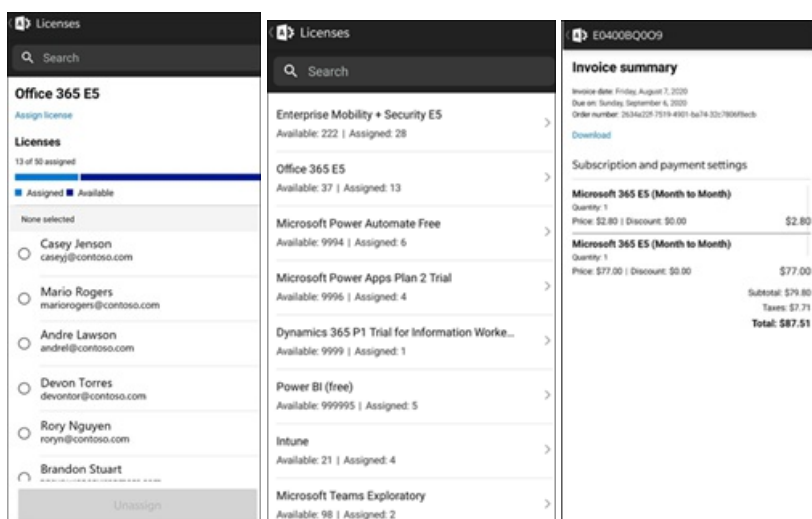


April 2021

Admin mobile app

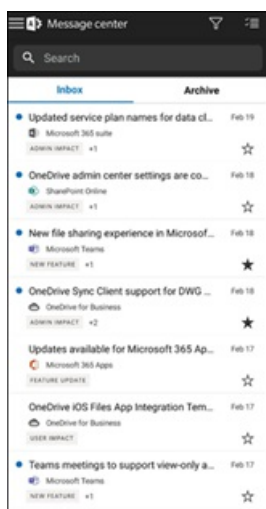
Manage licenses and bills from the Admin mobile app

- You can now view all available and assigned licenses for your subscriptions. You can also assign or un-assign licenses to users, and add or remove licenses.
- You can now view detailed invoices in the app.
- These updates are available on both [Android](#) and [iOS](#) devices.



Updated Message center feed in the Admin mobile app

- You now have a more flexible reading experience of the Message center feed. You now have the ability to filter messages based on service or tags and mark messages as favorite. Bulk actions for marking messages as read, unread or archived has also been added.
- These updates are available on both [Android](#) and [iOS](#) devices.



Ignite 2021 (March)

Welcome to Microsoft Ignite. We hope you were able to attend some of one of our sessions: [Microsoft Ignite 2021](#). Here's a few of the things we talked about at Ignite.

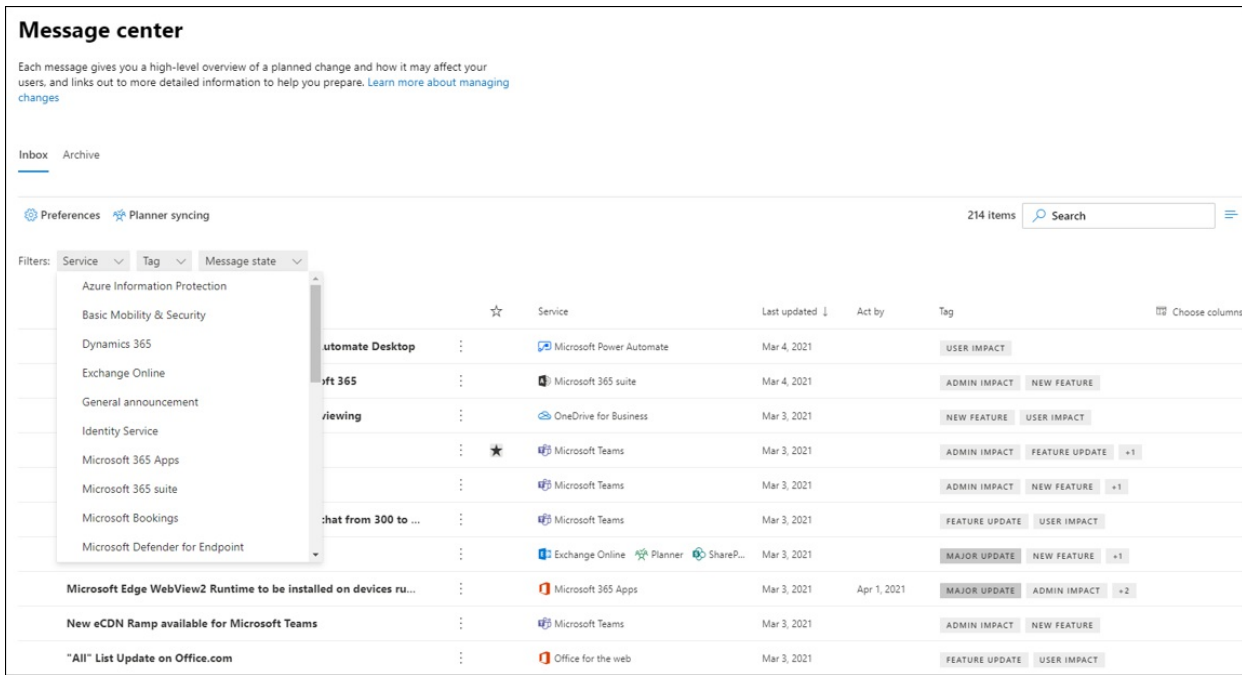
NOTE

Not all features are going to be available to everyone right away. If you aren't seeing the new features, [join Targeted Release](#).

Message center

We've revamped the Message center to help you discover relevant messages and added a more flexible reading experience. We've added a new **Service** column to help you scan which Service a message applies to and filter messages by Service and other metadata. You can favorite a message to mark it for follow up, choose which

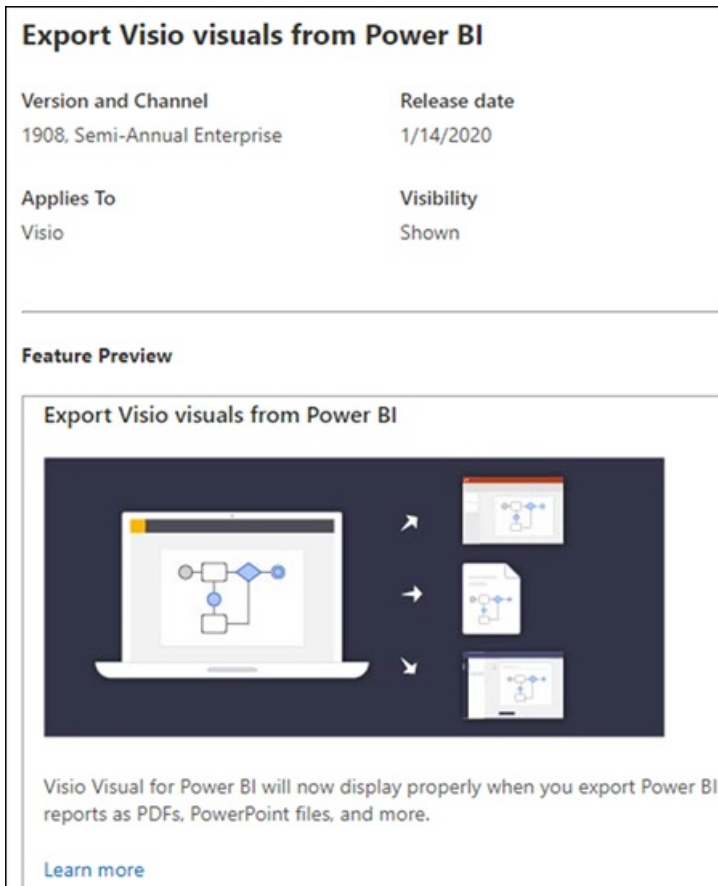
columns appear in the message list, and navigate between messages with the back and next buttons. We've also improved the process to make it easier to give feedback on Message center posts.



To learn more about the new features, check out [Message center](#).

What's new features

We've made improvements to how you view the "What's new" features for users in the Office apps. You can now see the rich content in the What's new pane that your users can see. You can also learn more about the feature before you decide to let your users know about the feature. For more info, check out [Manage which Office features appear in What's New](#).



Ignite 2020 (August & September)

Welcome to Microsoft Ignite - our first online-only Ignite. We hope to see you in one of our sessions: [Microsoft Ignite 2020 Session Catalog](#). Here's just a few of the things we'll be talking about at Ignite.

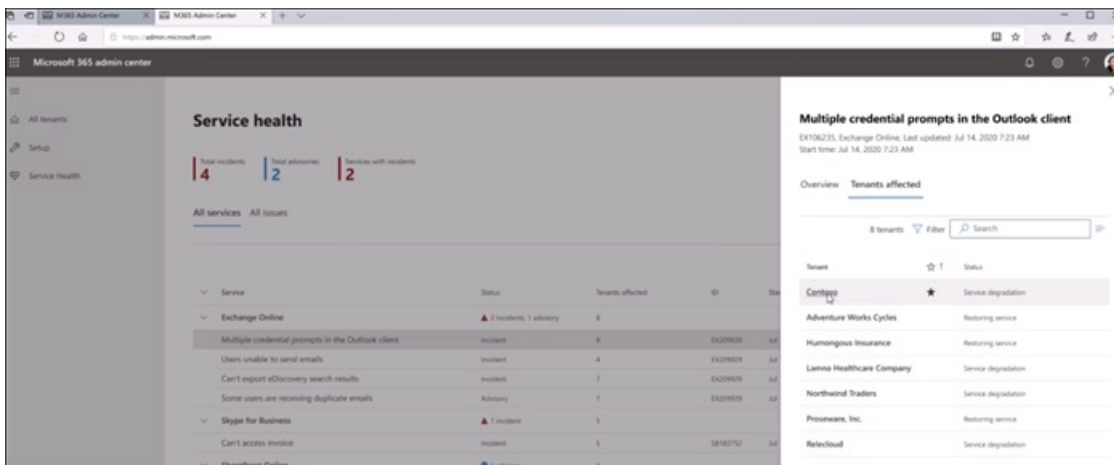
NOTE

Not all features are going to be available to everyone right away. If you aren't seeing the new features, [join Targeted Release](#).

Multi-tenant management

We've developed a set of features for multi-tenant admins like you to get your job done faster and more efficiently. For more information, see [Manage multiple tenants](#).

- **Your tenants:** Quickly switch between the tenants you manage.
- **All tenants:** A new page where you can quickly see the health of all your tenants' services, any open service requests, your products and billing, recommended setup tasks, and the number of users in that tenant.
- **Setup:** The multi-tenant Setup page gives you a list view of the Setup page, but organized for many tenants. You can see which features aren't turned on, which tasks are complete for all tenants, tasks that tenants still need to complete. This view will help you keep track of feature adoption and to make sure the recommended security setup tasks are always done.
- **Service health:** The service health view shows you if any incidents or advisories are affecting the tenants. It will even tell you how many of your managed tenants are affected. Just select an incident to get more information on the overview tab, then switch over to the Tenants affected tab to drill down and support that tenant.
- **Cross-tenant mailbox migrations** is a new service, now in public preview, that lets you move mailboxes between tenants without the need to offboard and then onboard mailboxes.
- **Cross-tenant domain sharing:** Soon, you can join a private preview for capabilities that allow you to share a domain across multiple tenants. For example, if Contoso acquires Wingtip Toys, Contoso can share the domain with Wingtip Toys so that people in both tenants can use "contoso.com" as their email addresses.



Monitor your most important accounts

You can monitor and track failed or delayed email messages sent to your users who have a high business impact, like your CEO. You track priority accounts by adding users to your priority accounts list in the [Microsoft 365 admin center](#). Add executives, leaders, managers, or other users who have access to sensitive or high priority information.

Priority accounts are only available to organizations that meet both of the following requirements:

- Office 365 E3 or Microsoft 365 E3, or Office 365 E5 or Microsoft 365 E5.
- At least 10,000 licenses and at least 50 monthly active Exchange Online users.

Monitor your most important accounts

Timely email delivery is critical for certain people, like leaders or managers. Add their accounts to the priority accounts list to actively monitor their mail flow, get alerts, and fix issues quickly.

[Manage](#) ● Completed

At a glance

Minimum role to set up: Exchange admin

Users: AD, EX, BA, +12

[View users assigned to Exchange admin role](#)

Minimum role to view reports: Global reader, Security reader

Reports available: Email issues for priority accounts

Effort to implement: Low

Helps protect against: Failed and delayed email messages

User impact

There is no impact to user experiences, but monitoring helps you resolve mail flow issues more quickly for the people using priority accounts.

About priority accounts

Add active monitoring to accounts for executives and others who have high business impact to monitor their mail flow and identify issues quickly.

You can actively monitor up to 250 critical accounts. Be thoughtful about the accounts that you add to active monitoring, because it will be harder to identify the cause if there are too many accounts. They should be your highest priority accounts.

From the Exchange admin center, you can monitor these accounts with the **Email issues for priority accounts** report and home page card. You can also set a policy to alert you when the number of failed or delayed email messages passes a threshold, and choose how often you'd like to have notifications emailed to you and others.

[Learn more](#)

[How to manage and monitor priority accounts](#)

[Learn more about the email issues report](#)

Manage this feature

[Priority accounts](#)

Related reports

[Email issues for priority accounts](#)

Related features

[Admin roles](#)

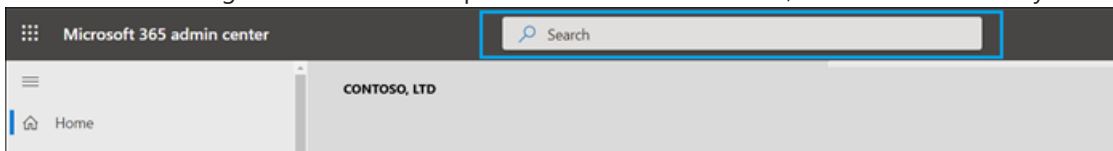
There are two ways to get started:

- Go to **Users**, and then in the three dots (more actions) menu select **Manage priority accounts** to add users to the list.
- Go to **Setup**, find the setup task **Monitor your most important accounts**, and then select **Get started**.

For more info on priority accounts, check out [Monitoring priority accounts](#).

Search faster and get better results from any page

We've started rolling out a new Search experience for the admin center, and we can't wait for you to try it out.



- The Search box moved to the header area where it says "Microsoft 365 admin center" so you now search from any page, not just the Home page. We've even got a shortcut: **Alt+S**.
- Search is smarter and will give you better results, even faster. Try typing "2fa" to get started.
- Search results are organized by the type of item or action you can take.
 - **Users:** Select the user's name and you can edit that user right there. If you select the three dots (more actions) menu next to their name, you can reset their password. You can search by display name, last name, first name, username or primary email address, and email aliases. But to get an exact match, search by primary email address or username.
 - **Groups:** Edit the group from any page, add members, assign owners.
 - **Actions:** Similar to how you can search for a user and then reset their password, you can also search "reset password" from any page and then reset one or more passwords for users.
 - **Navigation:** Results under Navigation can quickly help you get to a page in the admin center quickly. For example, searching "roles" will take you to the Roles page for Azure AD roles.
 - **Settings:** Search for any setting related to your organization, the services you subscribe to, and security and privacy settings.
 - **Domains:** You can find quick links to your domains, and then the link will take you to that domain's Overview and health page.
 - **Documentation:** If we can't find a result for you, we'll try to find some documentation to help. It takes a little longer for the curated list of articles to find a match, so wait a second to let Search find the

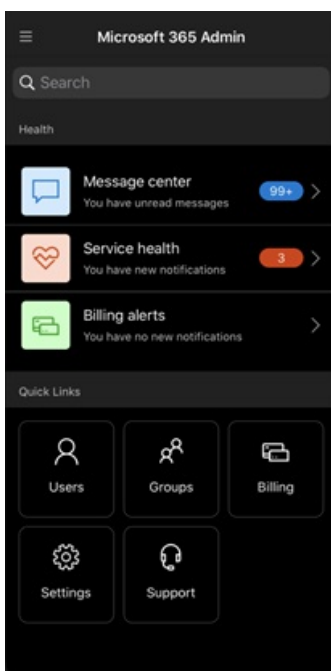
results.

- **Feedback:** Didn't find what you were looking for? Send us feedback from Search. We will add searching functionality for more pages and more features across the admin center.

Microsoft 365 admin mobile app

The [Microsoft 365 admin mobile app](#), which is included with your subscription, lets you manage Microsoft 365 from your mobile device so you can get away from your desk to do every day tasks. In fact, there are over 90 features in the app--and we just added a few more:

- **Support for Microsoft Intune's Mobile Application Management and Conditional Access policies:** You can now use your personal device to manage Microsoft 365 even if your org has turned on Intune's Mobile Application Management and conditional access policies.
- **Message center notifications:** Turn on message center notifications at **Settings > Notifications** if you wish to be alerted about new message center posts. Through notifications, we want to ensure you stay informed about important information and events across your tenant.
- **Billing alerts:** You can also turn on billing notifications at **Settings > Notifications** if you want to get billing notifications on your device if a subscription is about to expire.
- **Dark mode:** Welcome to the dark side of the mobile app. This was one of our most requested features. Go to **Settings > Themes** to turn it on.
- **Report an issue:** You can now report an issue in the app or view issues reported by other admins. Visit **Service health** to check it out.



Usage recommendations for small and medium businesses

Small and medium businesses might get a recommendation on the **Home** page if some of the people in the org aren't actively using Teams, OneDrive, or Office apps. When you view the recommendation, you can quickly email Microsoft training to inactive users to help them get started with the app and to make sure you are getting the full value from your subscriptions.

Remote work collection

In October, we'll be adding a remote work collection to help small business owners and their staff get online and working remotely. **Remote work essentials** setup is a curated list of all features Microsoft recommends to securely enable remote work and to collaborate effectively. In a couple of weeks, you can try it out in **Setup > Remote work essentials**.


Microsoft 365 admin center

Contoso organization

Remote work essentials

5 actions

This set of actions can help your organization stay safe, secure, and productive as you adapt to an increasingly remote workplace. Watch this video for an overview of remote work essentials, then complete the listed actions, in any order.



Name	Status	Description
Protect your org with security defaults	Not started	Prevent identity-related attacks like phishing, password spray, and replay with security defaults from ...
Bring people together with Teams	Not started	Set up Teams for private and group chats, audio and video calls, and file collaboration from anywhere.
Let users reset their own passwords	Not started	Reduce support costs and help your users be more self-sufficient by allowing them to register for self-...
Increase protections from advanced threats	Not started	Help protect your organization from sophisticated attacks by setting up Advanced Threat Protection (ATP)
Protect data in mobile apps	Not started	Create a mobile app protection policy to manage how users access your data from work apps on their ...
Get started with Microsoft 365 Business Voice	Not started	When you set up Microsoft 365 Business Voice, you'll have a business phone system for your company ...
Help people get started with OneDrive	Not started	Some people in your organization haven't used OneDrive in at least 30 days. Help them get started by ...

For more information about how to securely allow remote work and a handy web address that's easy to remember and share, go to aka.ms/remote-business.

Need help? moving to more admin centers

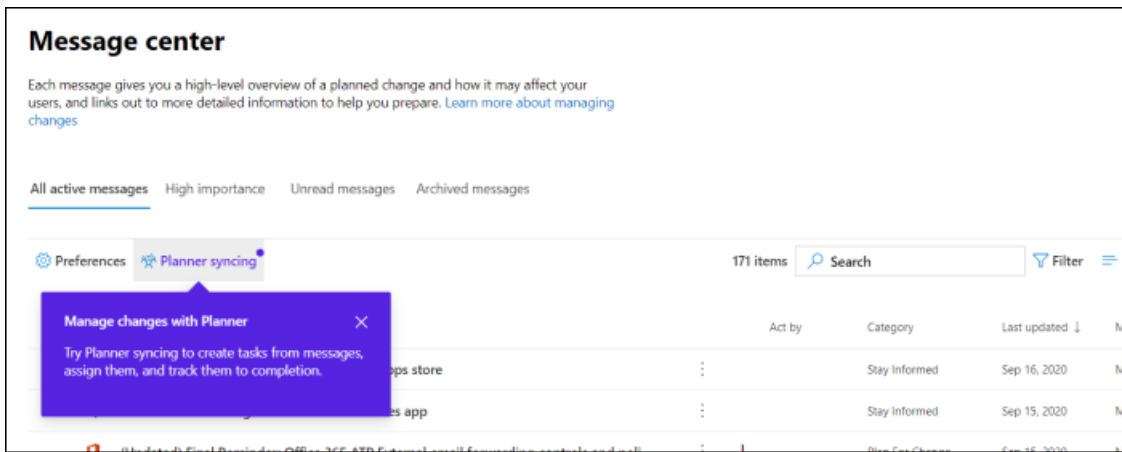
We're continuously looking at and updating the content and tools to keep up with changes in the product. We now have many more Teams self-serve diagnostic tools to help you resolve issues quickly and efficiently. Here are a few that were recently added:

- Change your Exchange Web Service throttling policy
- Checking status of Teams provisioning and validation to specific users
- Fix DKIM setup issues
- Diagnose Intune user enrollment errors

And we are rolling out the new and improved support experience you already see in the [Microsoft 365 admin center](#) to some of the other admin centers. Teams admin center and Security and Compliance admin centers already have this new experience. And soon, **Exchange admin center**, **SharePoint admin center**, and **Office.com** will be updated along with this new help experience for admins.

Manage changes with Microsoft Planner

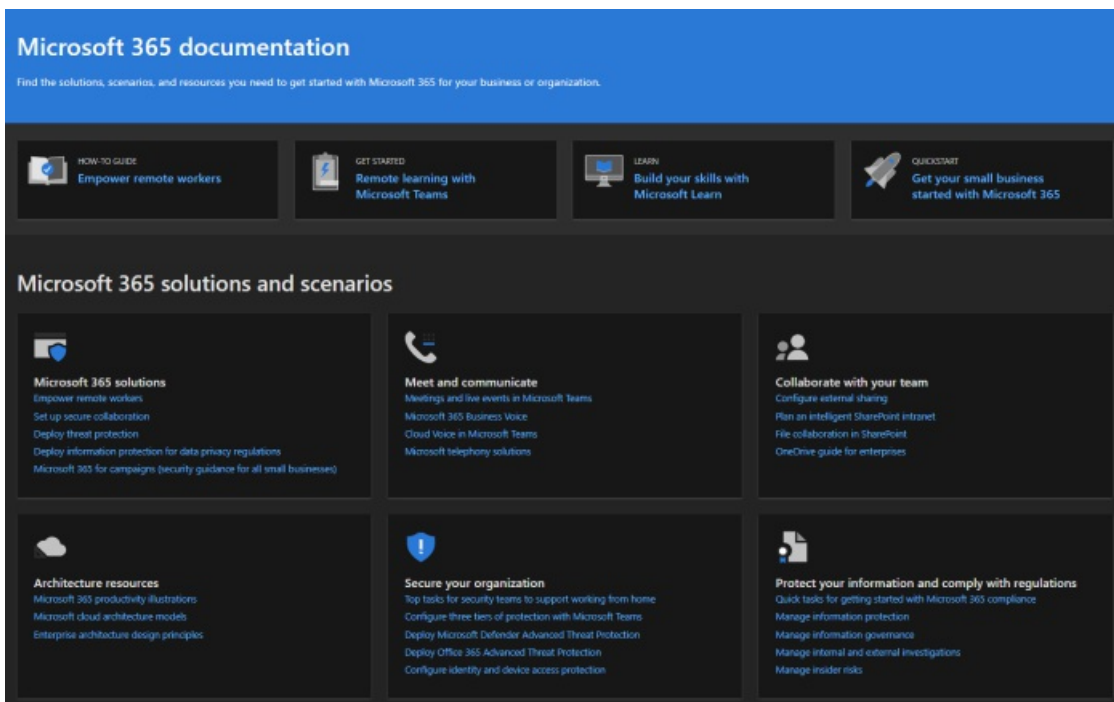
In May, we announced that you'll soon be able to sync Message center posts to Microsoft Planner and now it's available for everyone to use. You can now create tasks from messages, assign them, and track them to completion. The first time, you select **Planner syncing** you'll need to connect to the appropriate plan.



To learn more about it, check out this article and video to see how it works: [Track your message center posts in Planner](#)

Documentation, Training, and Videos

- Brand new and just in time for Microsoft Ignite--[The Virtual Hub](#). Deep dive into technical training for IT pros and developers. Quickly find around 20 new videos as part of #SIDETRACKED, the name of the Ignite admin track this year.
- [What's new with Microsoft 365](#) video series: This month, we cover new features available in Whiteboard for Teams and on the web, how to automate user provisioning to Azure AD, new Power Automate triggers and actions in Teams, and more. And stay tuned for next month, where we'll have a recap of all the great things happening at Ignite!
- We did a redesign of the [Microsoft 365 documentation](#) page that focuses on solutions first. We'll highlight new solutions as they become available on this page, so keep an eye out.



July 2020

Getting ready for Ignite 2020

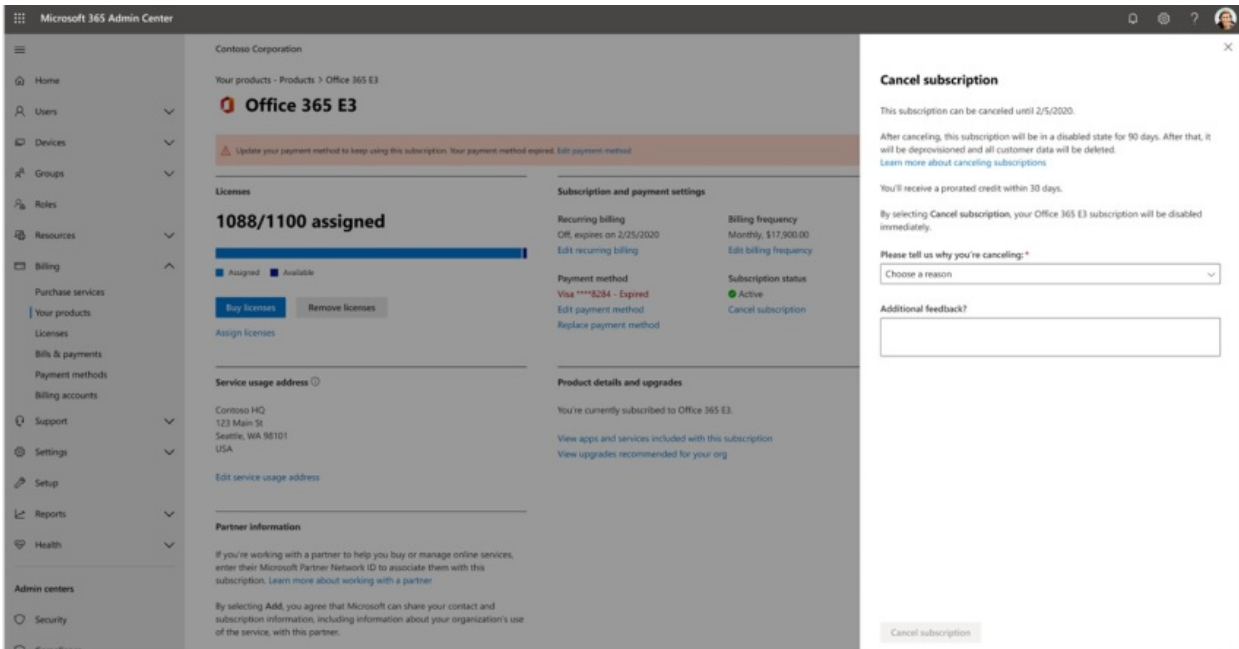
As we're moving into Ignite season at Microsoft, we're not releasing as many features so that we have a lot to talk about during our sessions.

The next update to this article will be on opening day of our first online-only Ignite. And this year, it is free to attend! Check it out, get signed up: [Microsoft Ignite 2020](#).

Your products

There has been a lot of work done in the subscriptions management to make the page faster to load, faster to find what you're looking for, and to meet the web accessibility standards ([WCAG 2.1 guidelines](#)).

- **Table redesign:** The table was redesigned so that you can group similar subscriptions. Go to **Billing > Your products**.
- **Product details:** Get more details than ever about your subscriptions by selecting the product in the list.
- **Do it all from here:** And you don't have to go to jump around several pages to manage one product. For example, if you need to cancel a subscription, the panel will open to do the action right there.



Domains

Domain management can be complicated, and we've released a new feature to make that easier. Go to **Settings > Domains** and then select a domain to get more information about your domain and the domain's health.



Domains > contoso.com

Managed at GoDaddy - Default domain

Remove domain Refresh

Overview DNS records

Domain status

Possible service issues

Some of your DNS records aren't set up correctly, which may be impacting your organization's use of Microsoft services. Go to **DNS records** to review the errors and fix the records.

Docs, training, and videos (July 2020)

[What's new with Microsoft 365](#) video series: This month, we cover the new Yammer experience for web and mobile, how to integrate the Yammer Communities app for Microsoft Teams, new policy packages to support Firstline Workers and managers, and more.

June 2020

Keeping up with Office What's New management

A few months ago, we added a setting that lets you manage the What's New messages that show up in a user's Office apps. This month, we released a new Home page card that will help you act quickly and keep track of the **What's New** messages that you want shown to the users in your organization.

Docs, training, and videos (June)

- [Getting started with Teams](#)

May 2020

New update channel for Office

On May 12, we announced the availability of a new update channel for Office: Monthly Enterprise Channel. This update channel provides your users with new Office features once a month, on the second Tuesday of the month.

If you allow your users to self-install Office from the portal, you can select Monthly Enterprise Channel for them. To do this, sign in to the Microsoft 365 admin center and go to **Show all >Settings > Org settings > Services > Office software download settings**. If you select **Once a month (Monthly Enterprise Channel)**, then any new self-installs of Office are configured to use Monthly Enterprise Channel.

In conjunction with the release of Monthly Enterprise Channel, we're also revising the names of the existing update channels. For example, Monthly Channel is being renamed to Current Channel. The new names take effect on June 9, 2020.

For more information, see [Changes to update channels for Microsoft 365 Apps](#).

New admin roles

We've added some new Azure Active Directory admin roles to the [Microsoft 365 admin center](#).

- Hybrid identity admin role gives users permission to manage cloud provisioning and authentication services.
- Network admin role lets users manage network locations and review network insights for Microsoft 365 Software as a Service apps.
- Printer admin role grants permission to manage all aspects of printers and printer connections.
- Printer technician is a subset of the Printer admin role where those users can register and unregister printers, and update printer status. To find out more about these roles, see [About admin roles](#).

Export groups list

We've heard from a lot of admins that they need to share information about groups and their usage to people who don't have access to the admin centers. You can now export the Groups list to a CSV file for auditing purposes, which means you can throw out that old PowerShell script. To try it out, go to **Groups > Groups**, and then select **Export groups** from the command bar.

Microsoft 365 solution and architecture center

Just this month, we released a new site on docs.microsoft.com called the [Microsoft 365 solution and architecture center](#), which brings together the technical guidance you need to understand, plan, and implement integrated Microsoft 365 solutions for secure and compliant collaboration. In this center, you'll find:

- Foundational solution guidance
- Workload solutions and scenario guidance
- Solution and architecture illustrations (The posters!!!)
- Industry specific guidance
- Enterprise architecture design principals

Docs, training, and videos (May)

- **What's new in Microsoft 365 video series:** This month, we cover the new support experience in the Teams admin and Security and Compliance Centers, Planner integration with the Message Center, and the new 3x3 video layout in Microsoft Teams.
- The [Microsoft 365 admin center help](#) hub page was updated to help you find what you need more quickly. And if you go look at that page right now, we've added a card to inform you of important updates and changes.

April 2020

Intune roles management

April 2020

Well, we did it! We've taken the second step towards a unified roles experience and you can now manage Intune roles in the [Microsoft 365 admin center](#). You can also leverage features such as the ability to search for roles and view role permissions. This means you don't need two separate tools to manage roles for Microsoft 365 and Intune. When you sign into the [Microsoft 365 admin center](#), you'll see that there are two pivots on the Roles page, one for Azure AD and one for Intune.

Contoso

Roles

Admin roles give users permission to view data and complete tasks in the admin centers. Give users only the access they need by assigning the least-permissive role. [Learn more](#)

Azure AD **Intune**

Name ↑	☆	Description
Application Manager	⋮	Manages the application lifecycle for mobile apps, configures Intune information and device configuration profiles
Help Desk Operator	⋮	Performs remote tasks, assigns apps and policies to users and devices
Intune Role Administrator	⋮	Assigns permissions to other admins, manages custom and built-in Intune roles
Policy and Profile manager	⋮	Manages application configuration profiles, AppLocker, and...

Sync Message Center posts to Planner

Starting in May, admins who are in Targeted release will start seeing the "Planner syncing" button in the message center. You can now track messages that need action, select the type of messages you'd like to track, assign messages to track as tasks, and tag messages for later attention.

[Join Targeted Release](#) to get started!

"Need help?" launched in Teams admin center & Security and Compliance centers

The Teams admin center, Security center, and Compliance center are now using the same "Need help?" feature that the [Microsoft 365 admin center](#) uses for finding help and contacting support. We've received a lot of feedback from admins that you wanted the same level of help and support and we're happy to bring that to you. Try it out and give us your feedback!

Need chat?

Our support agents have been working from home while still taking customer cases and limitations on internet bandwidth while working from home can impact customer call quality. In order to continue supporting you, we have launched live chat support option for commercial customers in the [Microsoft 365 admin center](#).

While creating a service request, you'll now see chat as an option, in addition to phone and email. Select chat as a preferred channel of communication and create the request. Once you've created the request, you can start the chat when you are ready to chat with Microsoft agents.

Teams updates

With the increased usage of Teams, we've added a few features to help you manage them.

- A new recommendation card on the admin center Home page shows which users have not actively used Teams for 30 days. You can send those users a training email to get them started using Teams.
- **Bring people together with teams:** Go to **Setup** to see a new page to help you turn on Teams for licensed users and allow guest access, so you can work with external customers in Teams.
- A Microsoft Teams card is now pinned by default to your Home page. It shows whether Teams is turned on, and if guest access is allowed. It also allows you to check the setup status for newly licensed Teams users, and check if network issues might be impacting Teams users.
- Finally, Teams is now a step in the initial set up flow if you purchased a license that includes Teams.

Productivity score

Productivity Score gives insights about how people use Microsoft cloud services and the technology experiences that support them. The score reflects your organization's performance against employee and technology experience measures and compares your score with organizations like yours. This month, we are introducing the following new concepts to the preview experience:

- Trend view of primary insights on home page and category detail pages -Endpoint Analytics and Network Connectivity categories added to Technology Experience
- Relevant Technology Experience insight shown in Employee Experience categories
- New Communications category as part of Employee Experience
- User details with organizational metadata in Employee Experience categories

If you'd like to learn more, check out the blog: [Measure and improve the Microsoft 365 experience with Microsoft Productivity Score](#). Productivity score is currently in private preview. [Join the Productivity score private preview](#) to get started.

Groups updates

We've got two updates for Groups this month:

- You can now edit email addresses for Office 365 groups (Also known as Groups in Outlook, and soon to be known as Microsoft 365 groups).
- We've heard your feedback and we've added clearer error messaging for why you can't convert a group to a Microsoft Team.

Docs, videos, and training (April)

What's new in Microsoft 365 video series: This month, we cover tips and resources to help small businesses transition to remote work including how to roll out Microsoft Teams, remote work training resources to stay connected with clients and partners, and the new Microsoft 365 Business Voice plan. [What's New in Microsoft 365](#)

For your users

- [Schedule a meeting](#)
- [Join a Teams meeting](#)
- [Create an org-wide team](#)

- [Create a Team with guests](#)
- [Join a Team as a guest](#)
- [Create a group email address](#)

For admins and business owners

- [Empower your small business with remote work](#)
- [Running a remote small business](#)
- [Sign up for Microsoft Business Basic](#)
- [Setting up two-factor sign-in](#)

March 2020

Featured Feedback Fix: Improve "add user" reliability for licensing

We received a lot of feedback from admins about the how hard it is to assign licenses when adding users. We've made the first update to this fix and we've migrated to a more reliable behind-the-scenes service to process those requests. And if something goes wrong, you'll now get an error message that lets you to try again.

John Doe added to active users

We sent an email to you with sign-in credentials for <John>.

User details

Display name: John Doe

Username: johndoe@contoso.com


Password: Ah53Sdf

Sending to: DefaultTennantEmail@contoso.com

Licenses bought

Microsoft 365 Business (\$20/month)

Licenses assigned

 Something went wrong, and we couldn't assign Microsoft 365 Business to John Doe. You can always assign licenses later from the User Details panel.

[Try again](#)

Microsoft Teams home page card

With the uptick in Teams usage, some orgs will get a pinned dashboard card that makes turning Teams on more discoverable. The card also has links to training and docs to help your org transition to remote work. Just go to the **Home** page to see the new card.

Bring remote workers together with Teams

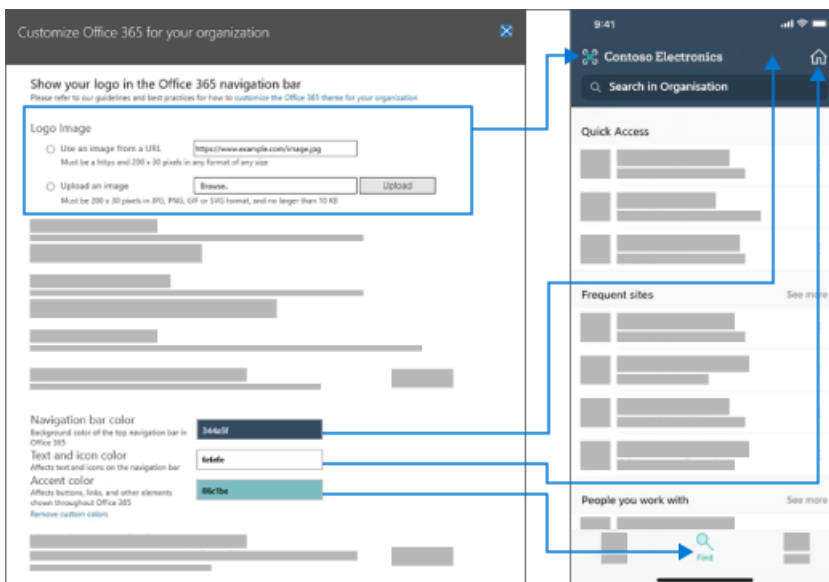
Learn how to manage Teams for remote work, with setup guidance, short videos, and tips. For assistance with Teams setup, register for Microsoft FastTrack.

- ✔ Teams is on for your organization
- ℹ Check setup status of new Teams users
- ℹ Make sure guests have access
- ℹ Get more support from Microsoft FastTrack

[Manage Teams](#)[Learn more](#)

Customize your organization's SharePoint mobile app theme

Using the [Microsoft 365 admin center](#), you can now customize your organization's theme in SharePoint mobile app for iOS and SharePoint mobile app for Android. This feature conveniently provides a mobile intranet app experience that can match your SharePoint Online for employees on the go. Theme customization includes your logo image, navigation bar color, text and icon colors, and accent colors, making for easy recognition.



Improvements to the "Add a group" wizard

When admins created a new group - and made it a Team at the same time, they could assign owners who don't have a license that includes Teams. And that created some headaches. We've updated the wizard flow to verify that owners have a Teams license and if they don't the option to turn the group into a Team is disabled.

Microsoft 365 offerings for small and medium businesses

We know that this is an announcement for next month, but we want to make sure you're prepared.

Starting on April 21, we're making changes related to our Office 365 subscriptions for small and medium businesses – and to Office 365 ProPlus. These products will now use the Microsoft 365 brand.

The new product names go into effect on April 21, 2020. This is a change to the product name only, and there are no pricing or feature changes at this time.

CURRENT NAME	NEW NAME
Office 365 Business Essentials	Microsoft 365 Business Basic
Office 365 Business Premium	Microsoft 365 Business Standard
Microsoft 365 Business	Microsoft 365 Business Premium
Office 365 Business	Microsoft 365 Apps for business
Office 365 ProPlus	Microsoft 365 apps for enterprise

Videos, training, and docs

[What's New in Microsoft 365 web series](#): In this month's episode, we highlight the 3-year anniversary of Microsoft Teams and cover new features including improved audio quality in online meetings, Targeted Communications for firstline managers with the Shifts app, Teams and Skype consumer interoperability, and more.

February 2020

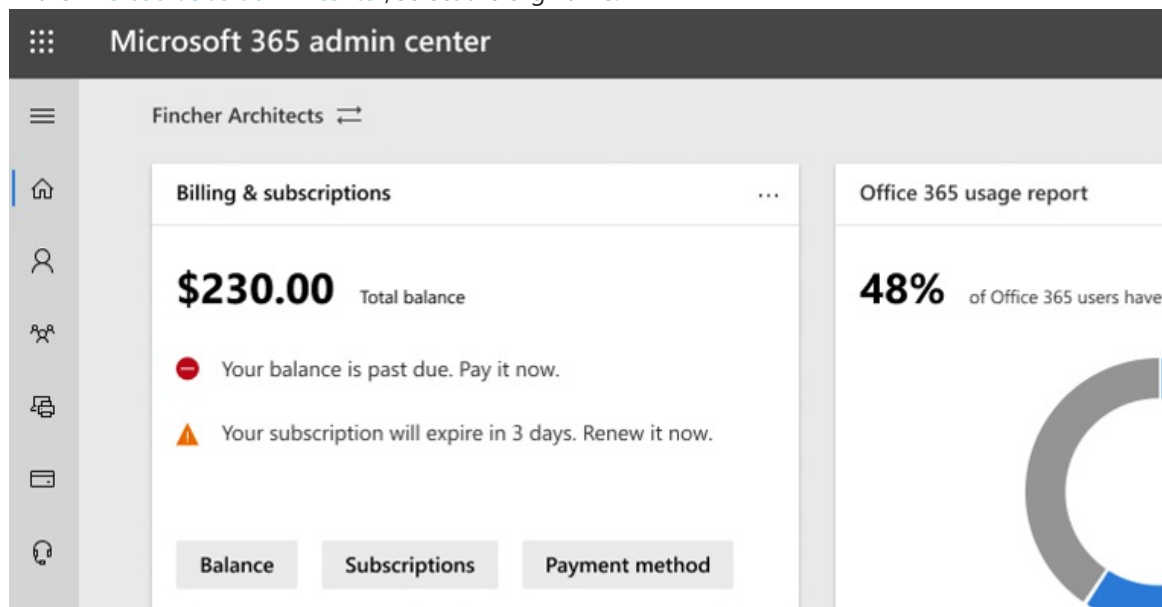
Featured Feedback Fix: Multi-organization switcher

We received a lot of feedback from partners and admins about the challenges of managing multiple Microsoft cloud orgs. One of our first multi-org management features is the **Organization switcher**, which lets you change between the orgs that you manage in just 2 clicks.

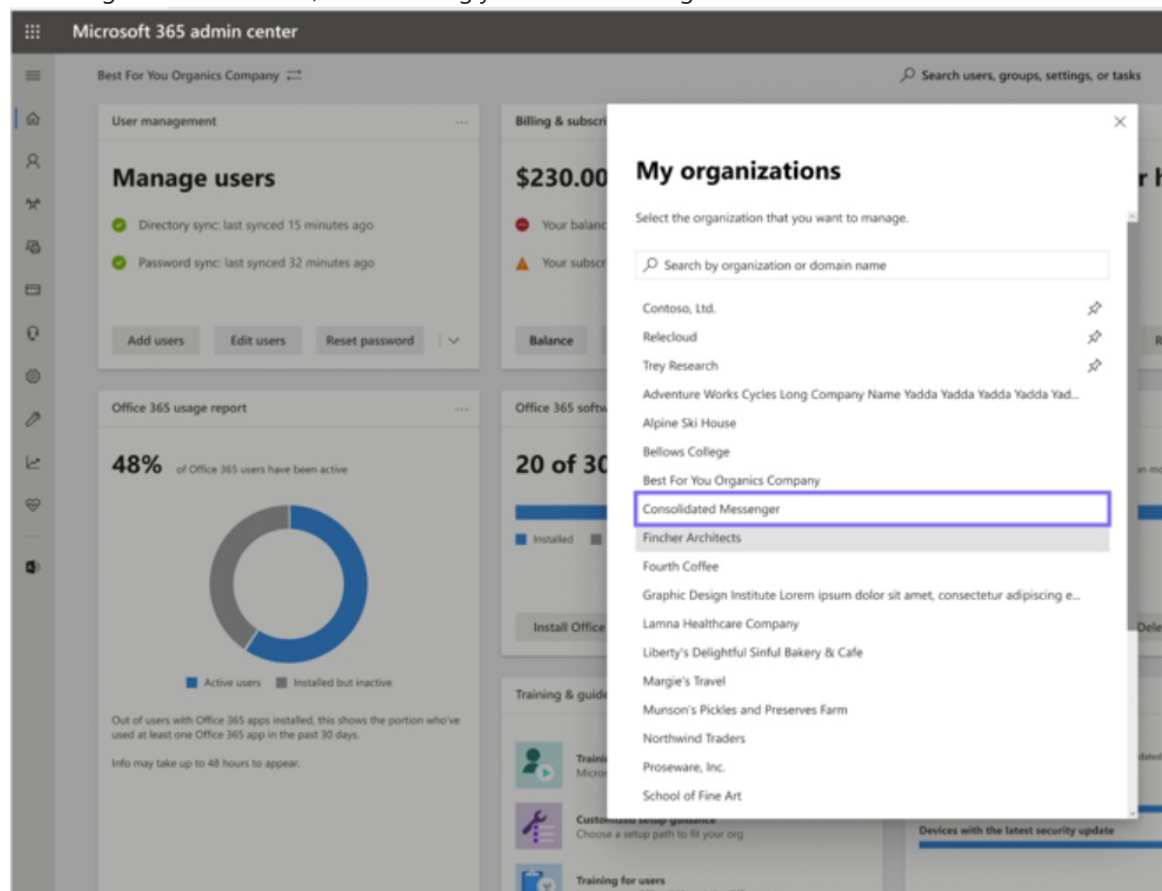
TIP

You don't have to do anything to make the organization switcher appear as long as you are the Partner of record for at least one organization.

1. In the [Microsoft 365 admin center](#), select the org name.



2. In the organization switcher, select the org you want to manage.



That's literally it!!!

Groups

A couple of changes in the groups area this month:

- **Sort by group name:** You can sort the groups list alphabetically, by selecting the **Group name** column.

- **Restore deleted Microsoft 365 groups:** You don't have to go to the Exchange admin center anymore to restore deleted Microsoft 365 groups. Go to **Microsoft 365 admin center** > **Groups** > **Deleted groups** > (select a group from the list) > **Restore group**. It'll restore the group back to the **Groups** list and restore the group's email, conversations, notebook, files, and calendar.

Videos, training, and docs (February)

- **What's new in Microsoft 365 video series:** This month, we're focused on custom search capabilities for SharePoint Online, the Office "What's New" management feature that lets you show or hide specific features from end-users via the in-app help pane, the latest security and compliance updates in Yammer, and more. Here's the latest episode: [What's New in Microsoft 365](#)
- **Docs move:** We combined the Office 365 admin web articles with the Microsoft 365 content and you might've noticed the new URL. For example, this article used to be hosted at: docs.microsoft.com/Office365/Admin/whats-new-in-preview, but the URL is now: docs.microsoft.com/microsoft-365/admin/whats-new-in-preview. If you've bookmarked pages, you should update your links; however, content links will be redirected to the new content repo.

Search in the Microsoft 365 admin center

5/14/2021 • 2 minutes to read • [Edit Online](#)

As the administrator of a Microsoft 365 organization, you can use search to find users, perform actions, navigate to different settings, and read documentation. With new search functionality, search speed has improved, and you can now search from every page in the admin center. The search box has moved to the banner area at the top of the admin center. You can use the **Alt+S shortcut** to use search from any page.



Search results are organized into different categories. Most of the categories are items in the admin center. For example, users, groups, shared mailboxes or domains. Other categories show you places you can navigate to, actions you can take or app level settings that you can change. And there's also a category related to documentation.

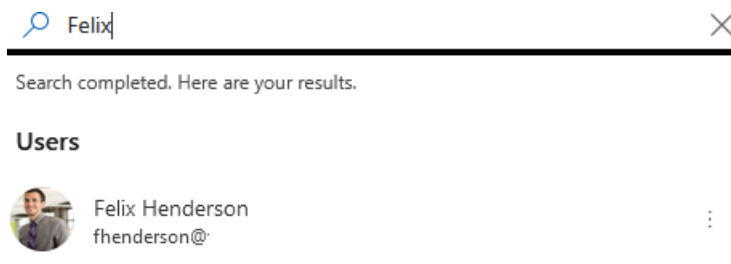
The following sections describe the different areas and categories in the admin center that are searchable.

Before you begin

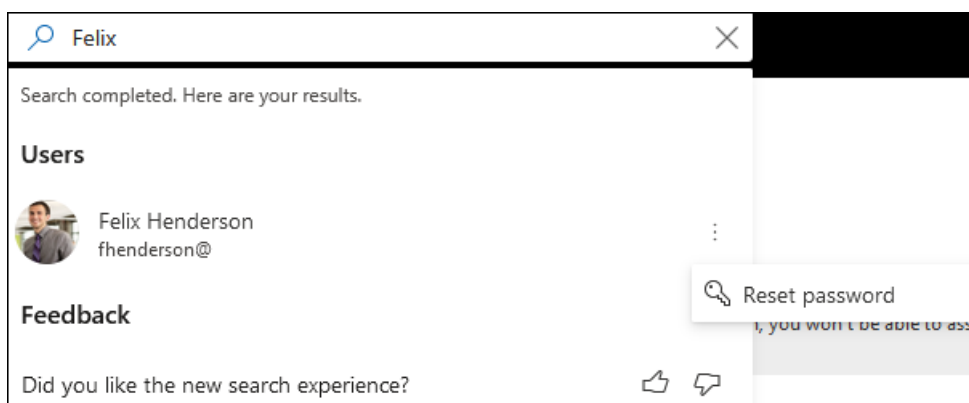
You need to be an administrator to search in the admin center. Search results are scoped to administrator permissions the logged in user has. For example, if SharePoint admin doesn't see an area or category in the admin center, they won't see it in search.

Users

Users can be found by display name, last name, first name, username, primary email address, or email aliases. Select the user's name edit to edit the user's details.



If you select the three dots (more actions) menu next to their name, you can reset their password.



Tips to improve user search results

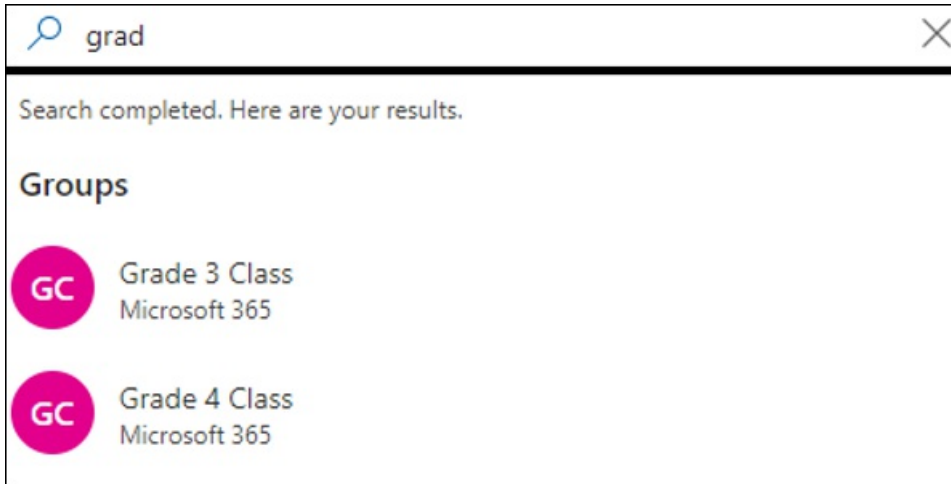
- Make sure you spell the users' names correctly as user searches are matched exactly against the earlier

mentioned properties. For example, in the above example, Jus or Malz will work but a misspelling, like, Jostin instead of Justin will not find this user.

- To get an exact match, search by primary email address or username.

Groups

You can search for Groups by group name or group email address. You can select the Group and edit the group from any page.

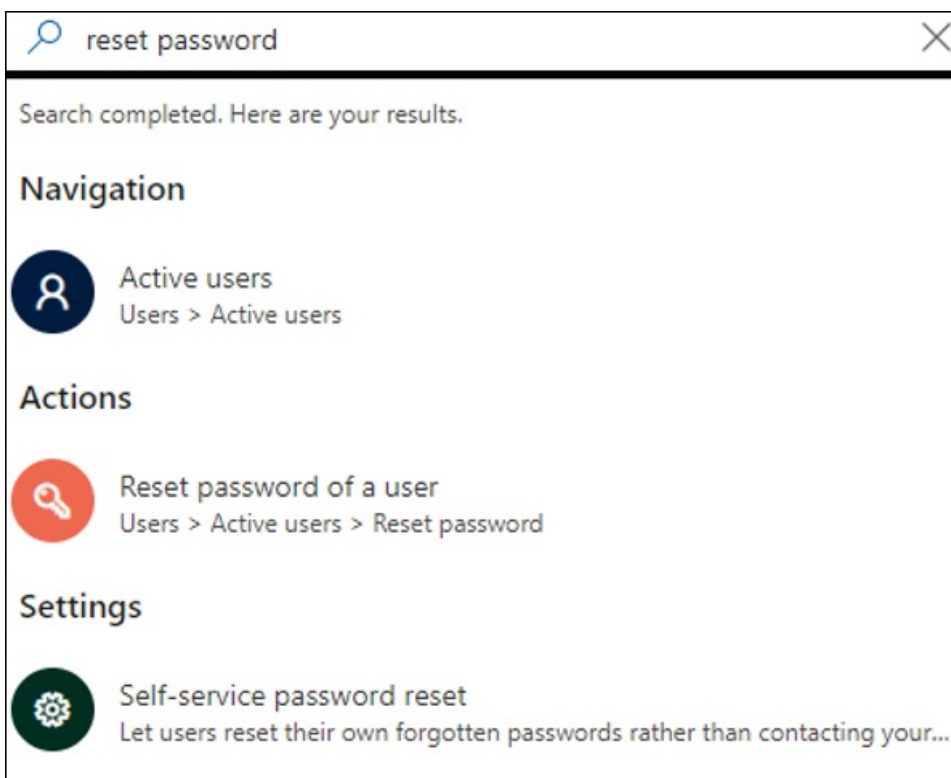


Tips to improve Group search results

Make sure you spell the group name correctly.

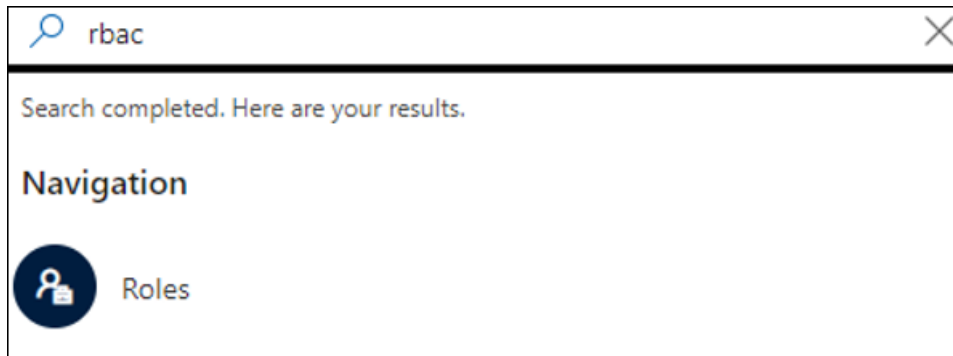
Actions

You can search for Actions category contains frequently used actions in M365 Admin Center. Think of actions as verb in the system. For example, you can also search "reset password" from any page and then reset one or more passwords for users. You can search for "delete a user" and delete the user from the Delete user page.



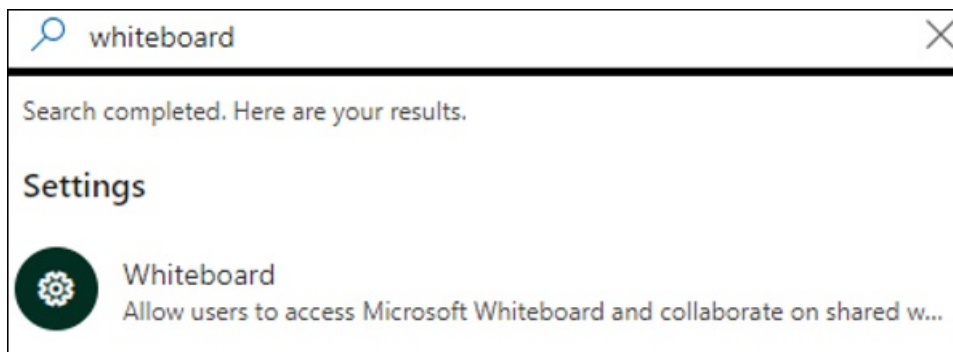
Navigation

Results provides a way to quickly navigate to a specific page in the admin center. For example, searching for RBAC will take you to the Roles page for Azure AD roles.



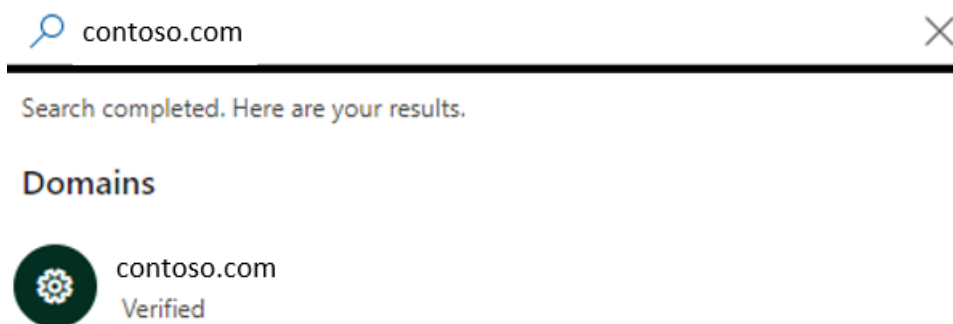
Settings

Search for supported app level settings related to your organization, the services you subscribe to, and security and privacy settings.



Domain







You can find quick links to your domains, and then the link will take you to that domain's overview page.



Documentation

A documentation search provides relevant help documentation based on your search phrase. Click on the topic to learn more.



Documentation

-  Reset user passwords - Office Support
Recommended article 
-  I forgot the username or password for the account I use ...
Recommended article 
-  Reset passwords - Microsoft 365 admin | Microsoft Docs
Recommended article 

Send us feedback

Use this section to submit feedback on the search experience. We can't respond to all feedback, but we read all of it, and use your feedback to improve the search experience. Make sure to provide as much detail as you can in your feedback.

Feedback

Did you like the new search experience?  

Stay on top of changes

6/14/2021 • 2 minutes to read • [Edit Online](#)

With Microsoft 365, you receive new product updates and features as they become available instead of scheduled updates that are months or years apart. As a result, you and your users will routinely experience new and improved ways to do your job rather than a costly and time-consuming company-wide upgrade. The challenge with such a model is keeping up with the changes and updates. Here are a few ways that you can stay on top of the Microsoft 365 updates in your organization.

Stay on top of Microsoft 365 changes

FEATURE	DESCRIPTION	HOW TO USE
Message center	Learn about official service announcements and feature changes. You can read these messages in the Microsoft 365 admin center, the admin mobile app, or receive a weekly digest in email. Share these messages with others in your organization when you see a message someone else should act on. You can also use the Service Communications API to retrieve messages.	Sign in to the admin center or admin mobile app . Select Health > Message center . Select a message to read or share. Change the services you see messages about or opt-in to the weekly digest by choosing Edit preferences in the admin center. This is also where you can opt-out of the weekly digest. Overview of the Microsoft 365 Message center
Targeted release	Sign up for Targeted release for yourself and a select group of individuals at your organization. Get the latest Microsoft 365 updates before everyone else and then inform or train your users on the new experience.	Sign in to the admin center or admin mobile app . Select Settings > Organization profile > Release preferences . Learn more about Targeted release .
Roadmap	Visit the Microsoft 365 Roadmap to learn about features that have been launched, are rolling out, are in development, have been cancelled, or previously released. The roadmap is the official site for Microsoft 365 updates and changes.	Visit the Microsoft 365 Roadmap frequently and learn about planned updates and releases.
Blogs and Community	Visit Office Blogs, Microsoft Community, and Microsoft Tech Community to learn more details about changes in Microsoft 365 and share experiences with other users.	Visit Office Blogs . Visit Microsoft Community . Visit Microsoft Tech Community .

NOTE

You need to be a global administrator to make changes to release preferences.

Multi-tenant management

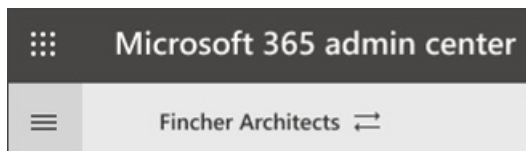
8/13/2021 • 2 minutes to read • [Edit Online](#)

Multi-tenant management offers a unified form of management that allows Microsoft 365 partner admins the ability to administer all the tenants they manage from a single location. If you're a partner who manages multiple tenants, you can:

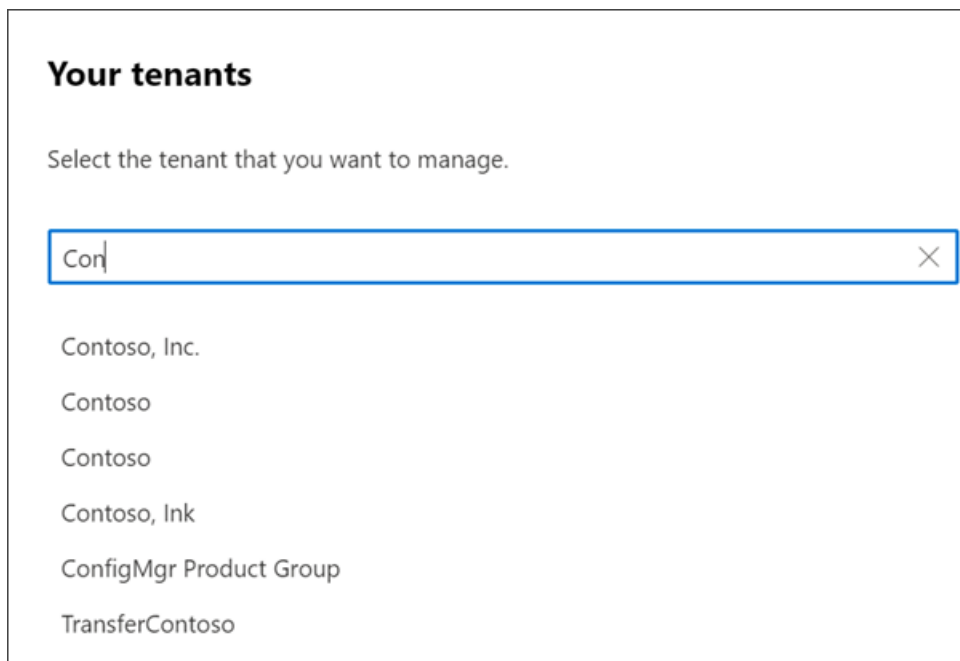
- Move quickly between tenants you manage.
- Assess service health, products, and billing across multiple tenants.
- On the **All tenants** page, you can quickly see the health of all your tenants' services, any open service requests, your products and billing, and the number of users in that tenant.

Move between tenants

1. In the [Microsoft 365 admin center](#), select the org name.



- From the **Tenant switcher**, you can move quickly between tenants you manage.



View All tenants page

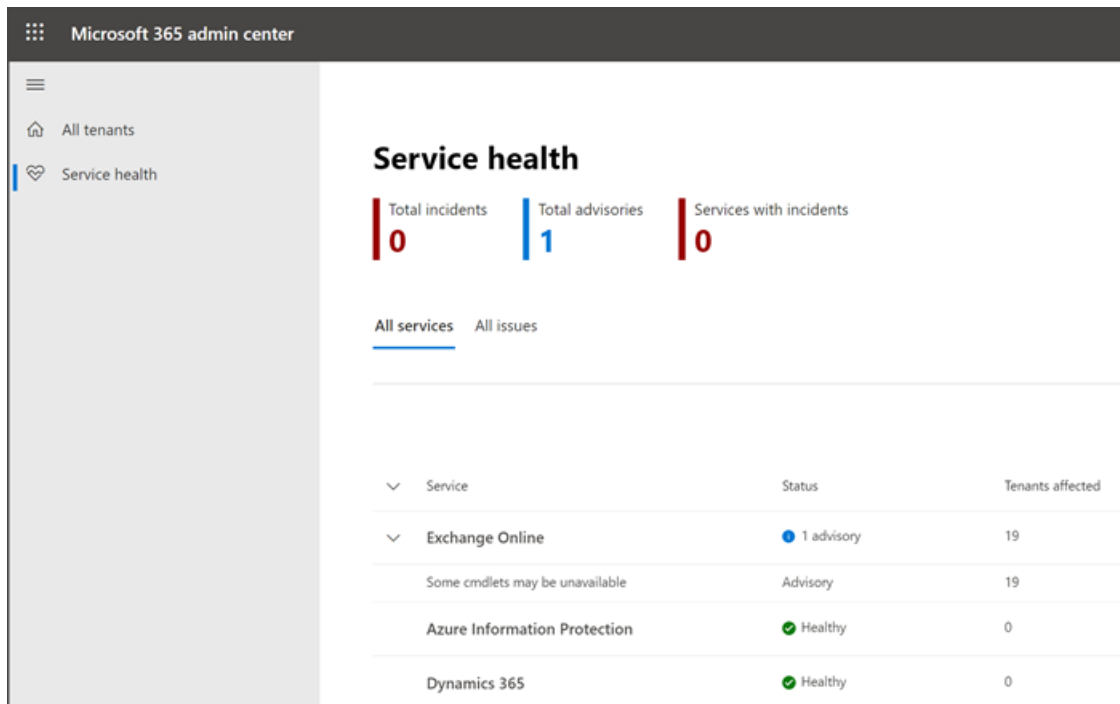
1. In the [Microsoft 365 admin center](#), in the left nav, select **All tenants**.
- On the **All tenants** page, you can
 - Assess service health
 - Review license usage
 - Search for, or select the tenant you want to manage
 - You can also pin your most often visited tenant to the top of the list.

If you've marked a tenant as a favorite, it's automatically expanded so you can immediately view the status details.

View service health for all accounts

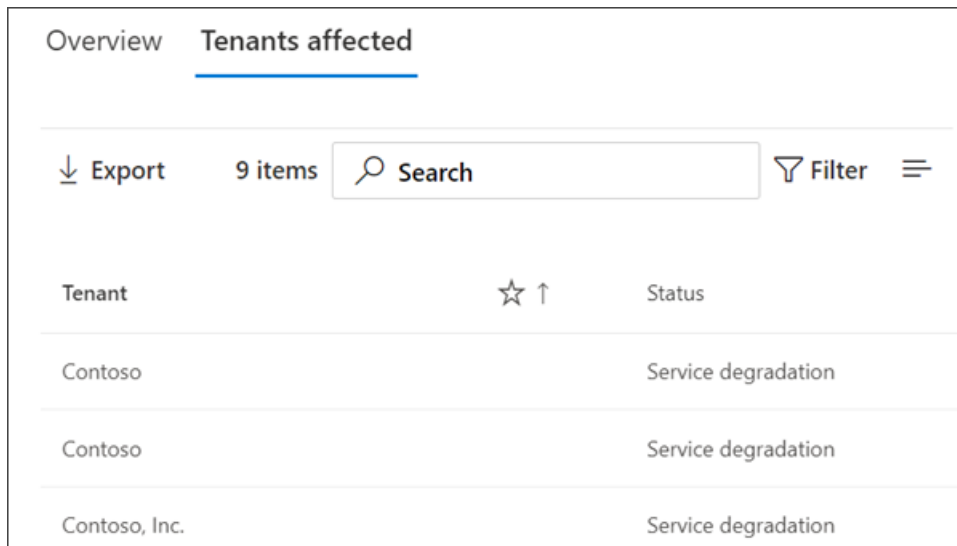
The service health view shows you if any incidents or advisories are affecting the tenants. It will even tell you how many of your managed tenants are affected.

1. In the [Microsoft 365 admin center](#), in the multi-tenant view, select **Service Health**.
2. On the **Service health** page aggregated view, you can also see the total number of incidents, the total number of advisories affecting any of the managed tenants, and the number of services with active incidents. You can also see how many of your tenants are affected by incidents and advisories.
 - You can use the filter option to view issues by issue type or by service
 - You can review issues under **All services** or **All issues** tabs.



Service	Status	Tenants affected
Exchange Online	1 advisory	19
Some cmdlets may be unavailable	Advisory	19
Azure Information Protection	Healthy	0
Dynamics 365	Healthy	0

3. Select an incident on the **All services** or **All issues** tab to get more information about any incident on the **Overview** tab. Select the **Tenants affected** tab to get a list of the affected tenants.



Tenant	Status
Contoso	Service degradation
Contoso	Service degradation
Contoso, Inc.	Service degradation

The list of affected tenants can be exported to CSV format so that admins can share it with support teams.

View a single tenant in the Microsoft 365 admin center

You can return to the Microsoft 365 admin center for any of the tenants from the **All tenants** page.

1. On the **All tenants** page, select the tenant name for which you want to view the admin center.
2. You are directed to the admin center for that tenant.

Office 365 operated by 21Vianet

7/12/2021 • 13 minutes to read • [Edit Online](#)

Office 365 operated by 21Vianet is designed to meet the needs for secure, reliable and scalable cloud services in China. This service is powered by technology that Microsoft has licensed to 21Vianet.

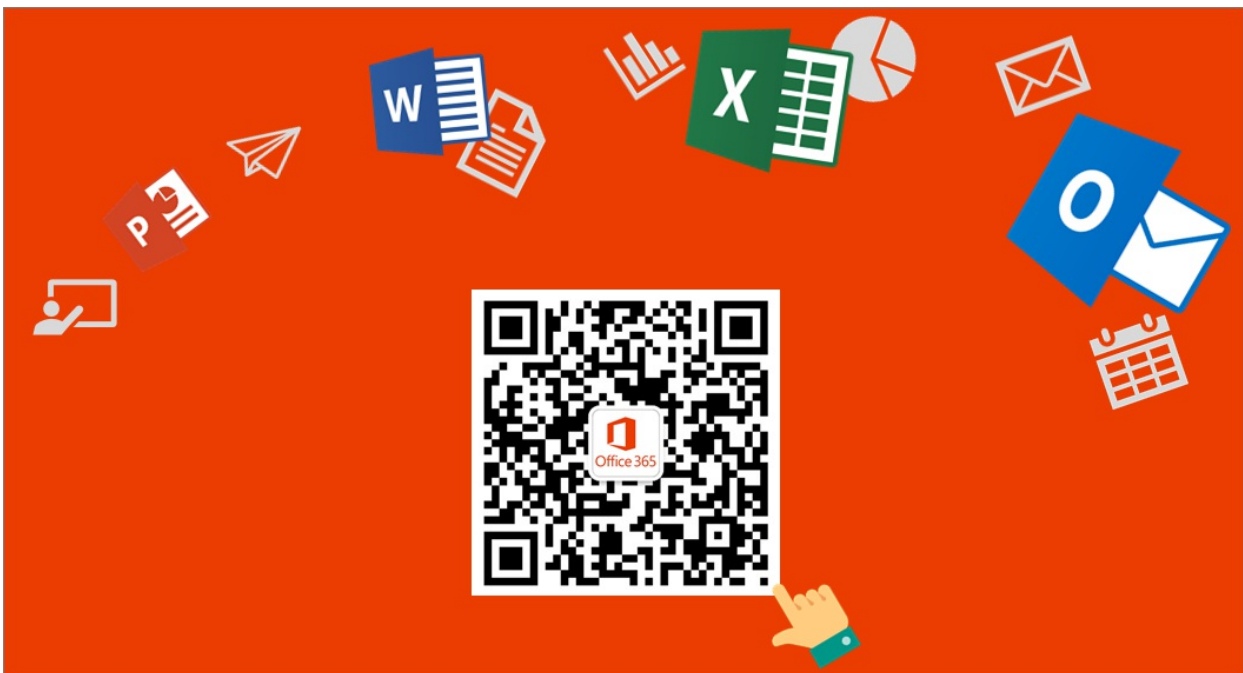
Microsoft does not operate the service itself. 21Vianet operates, provides and manages delivery of the service. 21Vianet is the largest carrier-neutral Internet data center services provider in China, providing hosting, managed network services, and cloud computing infrastructure services. By licensing Microsoft technologies, 21Vianet operates local Office 365 datacenters to provide you the ability to use Office 365 services while keeping your data within China. 21Vianet also provides your subscription and billing services, as well as support.

NOTE

These services are subject to Chinese laws.

Follow us on WeChat

Scan this QR code to follow us on WeChat and get the latest updates for Office 365 operated by 21Vianet.



About services in Office 365 operated by 21Vianet

The sections below highlight some of the differences you will find in each service. Ultimately our goal is to achieve parity with global services. However, due to the unique nature of the China services - operated by a partner from datacenters inside China - there are some features that have not yet been enabled. Customers will see the services come closer to full feature parity over time. For a more detailed look at services available for each Office 365 plan operated by 21Vianet, see the [Office 365 Service Description](#).

If you would like to learn how to get started with general Office 365 services, see [Get started](#).

Office 365 Suite

FUNCTION	AVAILABILITY
Custom domains	Administrators can create and/or use custom domains registered through Chinese-specific domain providers. If you don't have a custom domain, you can How to buy a domain name from a domain name registrar. If you already have one, Find your domain registrar or DNS hosting provider . Additionally, if you create a public website using the Office 365 SharePoint Online service, China Internet compliance policy requires that you get an Internet Content Provider (ICP) number. Note: Automatic validation for disallowed words in custom domain names is not available.
Subscriptions, billing, and technical support	Provided by 21Vianet. For information on how to contact support, see Contact Office 365 for business support .
Self-service password reset	Available for admins only. For more information, see Change or reset your password in Office 365 operated by 21Vianet .
Security, privacy, compliance, and details on levels of support	Provided by 21Vianet.
Office Desktop Setup	Office desktop setup is not available for Office 2010 and Office 2007. However, administrators can Configure current Office desktop applications to work with Office 365 .
Mobile and device support*	Coming soon are the following mobile features: Mobile Device Management (MDM) Blackberry Business Cloud Services (BBCS) is not available, but you can use Exchange ActiveSync devices or an offering from Research in Motion (RIM, the BlackBerry wireless email solution) to run Blackberry Enterprise Server (BES). For more information on mobile support, see Set up and manage mobile access for your users .
Office Lens	Not available.
Microsoft Planner	Coming soon.
Microsoft Teams	Not available.
Sway	Coming soon.
Help in multiple languages	Help is available in Simplified Chinese and English only.
Community-provided help	Community-provided help is not available yet, but you can select the Help button (?) in the upper right corner of your portal to see help articles.

*Optional services provided directly by Microsoft, and subject to Microsoft's Terms of Service and privacy statements.

SharePoint Online

FUNCTION	AVAILABILITY
Sharing a document, library, or site by email with someone outside of your organization	This feature is available, but off by default as using it could make files shared accessible outside of your country. Administrators do have the ability to turn it on, but will get a warning message indicating that it could make files shared accessible outside of your country. Users who attempt to share with someone outside of the organization will also receive a warning. For more information, see Share SharePoint files or folders in Office 365 .
Access Services	Access 2013 is supported, but adding new Access apps may not be available as this feature will be retired from Office 365 and SharePoint Online. Creation of new Access-based web apps and Access web databases in Office 365 and SharePoint Online will stop starting in June 2017 and any remaining web apps and web databases by April 2018. Additionally, Access 2010 functionality is not supported, and attempting to use an Access 2010 database will result in errors and possible data loss.
Microsoft PowerApps	Coming soon.
Information Rights Management (IRM)	The ability to set IRM capabilities to SharePoint for your organization is coming soon.
Ability to translate text or pages	Available, but off by default. Tenant admins can turn this ability on, but the translation cloud service may be located outside your country. If you do not want users to send content to a translation cloud service, you may keep these features disabled.
Public website ICP registration	China Internet compliance policy requires that you get an Internet Content Provider (ICP) number for your public website.
Public website features	Public websites are available only if you purchased Office 365 before March 9, 2015. However, Bing maps, external sharing, and comments are not available in a public web site as these features may send data outside of your country.
Newsfeed and Yammer (enterprise social networks)	Newsfeed (the social hub where you'll see updates from the people, documents, sites, and tags you're following) is available. Yammer is unavailable.
Autohosted apps	You can deploy a provider-hosted app that uses SharePoint and SQL Azure. For more information, see Create a basic provider hosted app for SharePoint . Coming soon is the ability for developers to deploy an app that uses an autohosted web site.
InfoPath	Not available.

FUNCTION	AVAILABILITY
SharePoint Store	The Office and SharePoint App Stores are optional services operated by Microsoft Corporation or its affiliate from any of Microsoft's worldwide facilities. The apps available in the Store are provided by various app publishers, and are subject to the app publisher's terms and conditions and privacy statement. Your use of any of these apps may result in your data being transferred to, stored, or processed in any country where the app publisher, its affiliates or service providers maintain facilities. Please carefully review the app publisher's terms and conditions and privacy statements before downloading and using such apps.
Office 365 Developer Site: Publish to SharePoint Store using the Seller Dashboard*	Learn about the requirements for submitting apps for SharePoint for distribution to users of Office 365 operated by 21Vianet.

*Optional services provided directly by Microsoft, and subject to Microsoft's Terms of Service and privacy statements.

Outlook Web App

FUNCTION	AVAILABILITY
Blackberry Business Cloud Services (BBCS)	Not available, but you can use Exchange ActiveSync devices or an offering from Research in Motion (RIM, the BlackBerry wireless email solution) to run Blackberry Enterprise Server (BES).
Information Rights Management	Coming soon.
Free/Busy information	Free/Busy information between on-premises and Exchange Online mailboxes is available.
Sharing your calendar	Calendar sharing between on-premises and Exchange Online mailboxes is available.
Sharing contacts	Coming soon.
Message tracking	Coming soon.
Apps	Coming soon.
Places feature	This feature shows maps of addresses in email; because it may allow data outside of your country, it is not available.
Connected Accounts	Connecting to other accounts such as Hotmail (Outlook.com) is coming soon.

Exchange

New with Exchange 2013 Cumulative Update 5 (CU5), full-featured hybrid deployments between on-premises Exchange 2013 organizations and Office 365 services are now supported. Leveraging new improvements in the Hybrid Configuration wizard, Exchange 2013 CU5 supports the following hybrid features between your on-premises and Exchange Online organizations:

- Secure mail routing between on-premises and Exchange Online organizations.
- Mail routing with a shared domain namespace. For example, both on-premises and Exchange Online organizations use the @contoso.com SMTP domain.
- A unified global address list (GAL), also called a "shared address book."
- Free/busy and calendar sharing between on-premises and Exchange Online organizations.
- Centralized control of inbound and outbound mail flow. You can configure all inbound and outbound Exchange Online messages to be routed through the on-premises Exchange organization.
- A single Office Outlook Web App URL for both the on-premises and Exchange Online organizations.
- The ability to move existing on-premises mailboxes to the Exchange Online organization. Exchange Online mailboxes can also be moved back to the on-premises organization if needed.
- Centralized mailbox management using the on-premises Exchange admin center (EAC).
- MailTips, HD photo support for Outlook contacts, and multi-mailbox search between on-premises and Exchange Online organizations.
- Cloud-based message archiving for on-premises Exchange mailboxes.

For organizations running older or mixed versions of Exchange Server, some hybrid features aren't fully supported for Office 365 tenants hosted by 21Vianet. Use the following table to learn more about hybrid feature support in different Exchange deployment scenarios:

ON-PREMISES EXCHANGE VERSION	EXCHANGE HYBRID SERVER VERSION	HYBRID CONFIGURATION WIZARD SUPPORTED?	SUPPORTED HYBRID FEATURES
2016	N/A	Yes	All
2013 CU5	N/A	Yes	All
2013 SP1	2013 CU5	Yes	All
2013 SP1	2013 SP1	Yes	All
Mixed 2013 SP1/2010 SP3	2013 CU5	Yes	All, except In-place eDiscovery/Archiving, OWA access (see table below)
Mixed 2013 SP1/2010 SP3	2013 SP1	Yes	Only manually configured free/busy
2010 SP3	2010 SP3	No	None
2007	2013 CU5	Yes	Only free/busy
2007	2013 SP1 or 2010 SP3No	N/A	Not supported
2003	2013 SP1/CU5	N/A	Not supported
2003	2010 SP3	No	None

IMPORTANT

Delegate calendar access, when a user or set of users is provided access to another user's calendar, isn't supported in hybrid deployments with Office 365 tenants hosted by 21Vianet.

Additionally, some Exchange messaging policy and compliance features aren't fully supported in hybrid deployments with Office 365 tenants hosted by 21Vianet. These features include:

- [Messaging Records Management \(MRM\)](#)
- [In-Place eDiscovery](#)
- [In-Place Hold](#)
- [In-Place Archiving](#)
- [Mailbox auditing](#)
- Accessing online archives with [Outlook Web App \(OWA\)](#)

Use the following table to learn more about feature support in different Exchange deployment scenarios:

ON-PREMISES EXCHANGE VERSION	MRM (SPLIT ARCHIVE)	OWA ACCESS (SPLIT ARCHIVE)	IN-PLACE EDISCOVERY	MAILBOX AUDITING	IN-PLACE HOLD/ARCHIVING
All 2013 CU5	Supported	Not supported	Supported	Supported	Supported
All 2010 SP3	Not supported	Not supported	Supported ¹	Supported	Supported
At least one pre-2013 CU5 server	Supported ²	Not supported	Not supported	Supported	Supported

¹ Separate searches are required for on-premises and Exchange Online mailboxes.

² MRM move-to-archive policies can be used for mailboxes located on an Exchange 2013 CU5 or greater server.

To learn more about configuring a hybrid deployment with Office 365 tenants hosted by 21Vianet, see the following topics:

- [Hybrid Deployment Prerequisites](#)
- [Certificate Requirements for Hybrid Deployments](#)
- [Create a Hybrid Deployment with the Hybrid Configuration Wizard](#)

IMPORTANT

The [Exchange Server Deployment Assistant](#) is a free web-based tool that helps you configure a hybrid deployment between your on-premises organization and Office 365, or to migrate completely to Office 365. The tool asks you a small set of simple questions and then, based on your answers, creates a customized checklist with instructions to configure your hybrid deployment. We strongly recommend using the Deployment Assistant to configure a hybrid deployment. > For organizations not wishing to upgrade to or add Exchange 2013 CU5 servers, Exchange 2013 SP1 organizations can configure shared calendar free/busy sharing between their on-premises and Exchange Online organizations. To configure this hybrid deployment feature, see [Configuring Exchange hybrid deployment features with Office 365 operated by 21Vianet](#).

FUNCTION	AVAILABILITY
Coexistence and Free/Busy Sharing	Sharing calendar free/busy information between two or more on-premises Exchange organizations or sharing between two 21Vianet Office 365 tenants isn't supported. This feature is coming soon!

FUNCTION	AVAILABILITY
Calendar sharing	Exchange 2013 SP1 and greater supports manually configuring Internet calendar sharing with other on-premises Exchange or Exchange Online organizations. For more details about configuring this feature manually, see Enable Internet Calendar Publishing .
Sharing Exchange contact data on Apple mobile devices to the Apple iCloud.	This setting/feature is enabled by default. Administrators should turn this feature off to help prevent users from sharing Exchange data outside of your organization.
Exchange Hosted Email Encryption	Not available.
Office 365 Message Encryption	Coming soon.

Office

FUNCTION	AVAILABILITY
Open an Office application from the File > Open in... button	Available. The ability to do so while roaming is coming soon.
Save to OneDrive for Business while signed in with a Microsoft account	To keep your data within your country, you cannot save a document to your organization site (OneDrive for Business) when you are signed in to Office with a Microsoft account.
Ability to translate text or pages	This feature is available, but off by default. Administrators do have the ability to turn it on, but will get a warning message indicating that it could make data accessible outside of your country.

Office client

FUNCTION	AVAILABILITY
Manage account (from within the Office client)	This feature, and others like it that are intended to go to your Office 365 portal, currently point to the worldwide Office 365 portal, and you cannot sign in with your Office 365 operated by 21Vianet account. This is a known issue that is being fixed. In the meantime, you can use the URL https://portal.partner.microsoftonline.cn/ to sign into your account and manage settings from there. For more information, see Manage your Microsoft 365 Apps for enterprise account for Office 365 operated by 21Vianet .

OneNote

FUNCTION	AVAILABILITY
Insert and playback online video	Not available.
Research pane integration to Bing services	Not available.

FUNCTION	AVAILABILITY
Accessibility checker	Not available.
Class notebook	Not available.
Forms	Not available.
Immersive reader	Not available.
Insert online picture	Not available.
Meeting details	Not available.
Researcher	Not available.
Stickers	Not available.
Live Search (ability to search in online notebooks that are not opened in the client)	Not available.
Integration with Mac and iOS platform smart look up service	Not available.
Share notebook experience and sharing notification	Not available.

Skype for Business

FUNCTION	AVAILABILITY
Domain providers to support Skype for Business	You will need to register your domain with a Chinese-specific domain provider that supports SRV records. For more information on how to register domains, see Find your domain registrar or DNS hosting provider .
Dial-in conferencing (the ability to add telephone access to meetings for users who can't get to a computer)	You may see options in Skype for Business and in the Skype for Business Admin Center for Dial-in conferencing and providers, but these features are not yet available. They are coming soon.
Skype for Business desktop help	You can find help for Skype for Business desktop here . However, desktop help is not available from the product unless you are using Office Click-To-Run.
Lync 2010	Not available.
Ability to join a meeting from your calendar when you're using a Samsung-based device with Google Chrome	Coming soon. In the meantime, you can open Skype for Business, go to the Meetings view, and join the meeting from there.
Desk Phone Devices like Polycom, Ares, and Tanjay	Not available.
Syndication partners	Not available.

FUNCTION	AVAILABILITY
Voice features, such as voice mail, ability to make and receive calls from PSTN numbers, call transferring, call forwarding	Not available. These features require syndication partners.
Archiving, or ability to tag a user and archive that user's emails and IMs in Exchange	Not available.
Skype for Business Web client (LWA) browser support for Firefox 29	Not available, but you can use an older version of Firefox.
Unified Contact Store (UCS)	The ability for users to keep all of their Skype for Business contact information in Microsoft Exchange Server 2013 is disabled.
Conferencing devices: Polycom CX5100 Unified Conference Station Logitech ConferenceCam CC3000e Polycom CX7000 Polycom CX3000 Logitech BCC950 ConferenceCam Polycom CX5000 HD	Not available.

Data Subject Requests for GDPR

GDPR grants individuals (or, data subjects) certain rights in connection with the processing of their personal data, including the right to correct inaccurate data, erase data or restrict its processing, receive their data and fulfill a request to transmit their data to another controller. The Tenant Administrator role for Office 365 operated by 21Vianet can request data on behalf of a data subject in the following ways:

- Using the Azure Active Directory Admin Center, a Tenant Administrator can permanently delete a data subject from Azure Active Directory and related services.
- System generated logs for Microsoft services operated by 21Vianet can be exported by Tenant Administrators using the Data Log Export.

For details and instructions, see [Data Subject Requests \(DSR\) for GDPR](#).

Related content

[Try or buy a Microsoft 365 for business subscription](#) (article)

[Azure Information Protection support for Office 365 operated by 21Vianet](#) (article)

[View your bill or get a Fapiao](#) (article)

Office app for Android for Office 365 operated by 21Vianet

6/8/2021 • 2 minutes to read • [Edit Online](#)

The Microsoft Office app for Android combines Word, Excel, and PowerPoint mobile apps into a single app available for download for Android phones. With the Office app for Android, you can connect to Office 365 just as you would with the Word, Excel, and PowerPoint mobile apps. The Office app for Android download won't affect any existing installations of Word, Excel, and PowerPoint.

A few Office app for Android features aren't available for Office 365 operated by 21Vianet customers:

- Image to text and Image to table
- Converting photos to Word documents from Lens
- Transfer files action
- Notes remain local and don't sync to server
- Link preview within Scan QR
- Live persona cards in the Me section
- Classification, labeling, and protection (CLP)

Download the Office app for Android

Download the Office app for Android phones from any of these China stores:

- [Baidu](#)
- [Xiaomi](#)
- [Lenovo](#)
- [360](#)
- [tencent](#)
- [wandoujia](#)

NOTE

The Office app for Android is currently available for phones only. Support for tablets will be added at a later time.

Security considerations

If your organization pushes apps to employee mobile devices, we suggest replacing the Word, Excel, and PowerPoint apps with the Office app for Android.

Office app for iOS for Office 365 operated by 21Vianet

11/2/2020 • 2 minutes to read • [Edit Online](#)

The Microsoft Office app for iOS combines Word, Excel, and PowerPoint mobile apps into a single app available for download for iOS phones. With the Office app for iOS, you can connect to Office 365 just as you would with the Word, Excel, and PowerPoint mobile apps. The Office app for iOS download won't affect any existing installations of Word, Excel, and PowerPoint.

A few Office app for iOS features isn't available for Office 365 operated by 21Vianet customers:

- Image to text and Image to table
- Converting photos to Word documents from Lens
- Transfer files action
- Notes remain local and don't sync to server
- Link preview within Scan QR
- Live persona cards in the Me section
- Classification, labeling, and protection (CLP)

Download the Office app for iOS

- Download the Office app for iPhones from the [App Store](#).

NOTE

The Office app for iOS is currently available for iPhone only. Support for iPad will be added at a later time.

Security considerations

If your organization pushes apps to employee mobile devices, we suggest replacing the Word, Excel, and PowerPoint apps with the Office app for iOS.

Apply for a Fapiao for Office 365 operated by 21Vianet

5/11/2021 • 3 minutes to read • [Edit Online](#)

You can submit your Fapiao request to the 21Vianet Fapiao management system about three days after you have paid. After you submit your Fapiao request, it will be processed in two days.



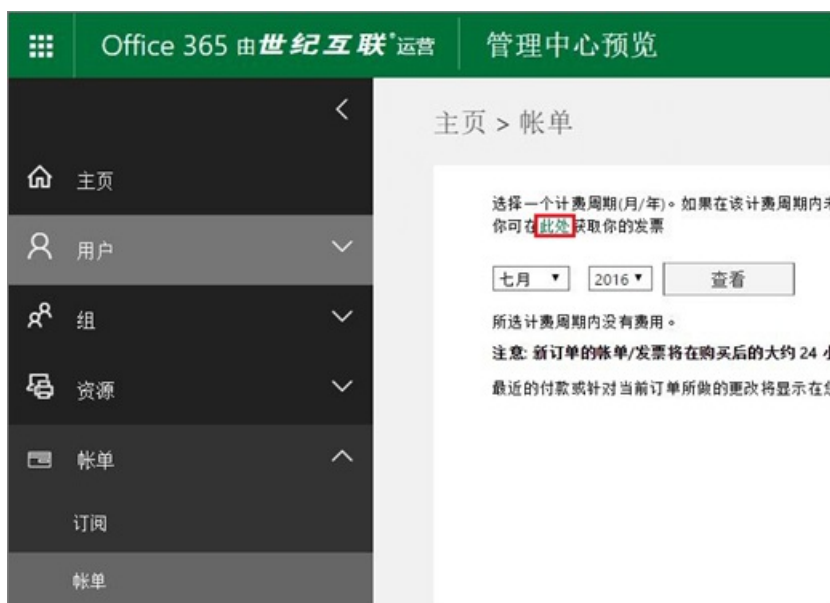
Step 1: Apply for a Fapiao

There are two ways to apply for a Fapiao:

1. After making a payment in the Office 365 operated by 21Vianet website, you'll receive an order confirmation email that contains your order number and a link to the Fapiao management system. You can use the link in the email to create an account in the [21Vianet Fapiao information management system](#).

Or

2. You can apply for a Fapiao from the [admin center](#).



Step 2: Register with the 21Vianet Fapiao management system

NOTE

You can use the same email name and password as your Office 365 account, or you can use something different.

1. Go to the [21Vianet Fapiao information management system](#).
2. In the registration form, enter your order number, email address, and password, then select **Registration**.



如何取得您的订单号

订单号 请从“订单确认”邮件中获取

Email 请输入接收账户信息的Email

密码 6—16个字符，区分大小写

确认密码 请再次输入密码

注册 返回登录 重发激活邮件

3. After your registration is complete, the system will send an activation email message to your email address. Open the email message and select the link to activate your account.

Step 3: Submit your bill for a Fapiao

1. Log in to the [Fapiao management system](#).
2. Select the billing record, then select **Apply bill**.

NOTE

The payment system is on a third-party platform and takes three days to synchronize the order and payment record.



账单	付款	申请批次	发票状态	开票方式	操作
<input type="checkbox"/>	2016-11-07日付款 ¥1.00	未申请	未申请	未选择 (未申请)	<input checked="" type="checkbox"/> 申请账单

3. Select the Fapiao type, enter the required information, then select **Next**.

NOTE

- For a normal VAT Fapiao, you only need to enter the buyer's name.
- If necessary, you can apply for a Fapiao with different a title. However, you can only apply one Fapiao title for one bill in the system. If you want to split the Fapiao into different amounts or titles, please [submit your request in the admin center](#).
- The next time you apply for a Fapiao, the system automatically presents the previous Fapiao information.
- If you need a purchase certificate or a refund, the payer name and the Fapiao title must match.

4. Select a shipping method and enter the mailing information. You can choose Yunda or SF (freight collect). You can also go to the 21Vianet Shanghai branch to get the Fapiao. select **Next**.

21Vianet Shanghai branch company address:

Shanghai, Pudong New Area Keyuan Road No. 88, German Center, building 3, 657

Contact information:

Zhu qin qin 021-28986102

5. Verify that the information is correct, then select **Confirm**.

Step 4: Check application progress

Your application is automatically transmitted to the 21Vianet Service Center, and will be completed in two working days.

After you submit the application, you can check the progress at any time. We will update the status of your application with remarks like **Issued** or **Mailed out**.

账单	付款	申请批次	发票状态	派送方式	操作
	2016-11-07付款 ¥1.00	2016-12-16日申请 G20161216_1430000117	未打印	上门自取 (未打印)	其他申请 查看发票

When Fapiao is out of use, the system will display a notice, and will indicate the expected time to issue the Fapiao.

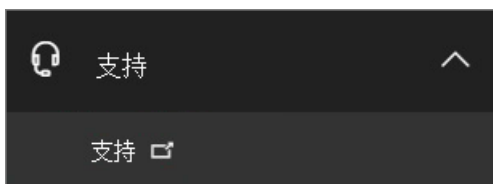
因我公司近日票源紧张,很遗憾无法及时为您提供发票,我司预计将于2016-12-20日前寄出发票,敬请谅解!

FAQs

What services can I get from online support?

You can check the progress of your Fapiao request, and find out why you haven't received the Fapiao.

If you want to change the Fapiao title, please send the Fapiao back to us and we will reissue the Fapiao. You can submit the request through the [admin center](#).



How do I change my login email address and password?

1. Log in to the [Fapiao management system](#), then select **Change email address**.



- If you forgot your login password, you can use your login email address to reset the password. The Fapiao management system will send a new password to your email address. You can use the new password to login.



- If you forgot your login email address, please contact 21Vianet customer service at (86) 400-089-0365.

How do I find my order ID?

- In the [admin center](#), go to the **Billing > Bills & payments** page.
- Find the invoice you want, select to view, or choose to download the PDF.

What if I enter the wrong email address when I register?

If you enter the wrong email address when you register, you won't receive the activation email. The registration link in the email will automatically expire after 24 hours. You can return to the [registration page](#) and register again with the correct email address.

What if I don't receive an activation email?

If you don't receive an account activation email within 24 hours after you register, go to the [21Vianet Fapiao information management system](#), enter your email address, then select **Resend the activation email**. The system will resend the account activation email to your registered email address.

如何取得您的订单号

订单号

Email

密码

确认密码

If you still don't receive an activation email, please contact 21Vianet customer service at (86) 400-089-0365.

Azure Information Protection support for Office 365 operated by 21Vianet

5/18/2021 • 9 minutes to read • [Edit Online](#)

This article covers the differences between Azure Information Protection (AIP) support for Office 365 operated by 21Vianet and commercial offerings, as well as specific instructions for configuring AIP for customers in China—including how to install the AIP on-premises scanner and manage content scan jobs.

Differences between AIP for Office 365 operated by 21Vianet and commercial offerings

While our goal is to deliver all commercial features and functionality to customers in China with our AIP for Office 365 operated by 21Vianet offer, there's some missing functionality that we'd like to highlight.

The following list includes the existing gaps between AIP for Office 365 operated by 21Vianet and our commercial offerings as of January 2021:

- Information Rights Management (IRM) is supported only for Microsoft 365 Apps for enterprise (build 11731.10000 or higher). Office 2010, Office 2013, and other Office 2016 versions are not supported.
- Migration from Active Directory Rights Management Services (AD RMS) to AIP is currently not available.
- Sharing of protected emails with users in the commercial cloud is supported.
- Sharing of documents and email attachments with users in the commercial cloud is currently not available. This includes Office 365 operated by 21Vianet users in the commercial cloud, non-Office 365 operated by 21Vianet users in the commercial cloud, and users with an RMS for Individuals license.
- IRM with SharePoint (IRM-protected sites and libraries) is currently not available.
- The Mobile Device Extension for AD RMS is currently not available.
- The [Mobile Viewer](#) is not supported by Azure China 21Vianet.
- The AIP area of the Azure portal is unavailable to customers in China. Use [PowerShell commands](#) instead of performing actions in the portal, such as managing and running your content scan jobs.

Configure AIP for customers in China

To configure AIP for customers in China:

1. [Enable Rights Management for the tenant](#).
2. [Add the Microsoft Information Protection Sync Service service principal](#).
3. [Configure DNS encryption](#).
4. [Install and configure the AIP unified labeling client](#).
5. [Configure AIP apps on Windows](#).
6. [Install the AIP on-premises scanner and manage content scan jobs](#).

Step 1: Enable Rights Management for the tenant

For the encryption to work correctly, RMS must be enabled for the tenant.

1. Check if RMS is enabled:
 - a. Launch PowerShell as an administrator.
 - b. If the AIPService module isn't installed, run `Install-Module AipService`.
 - c. Import the module using `Import-Module AipService`.
 - d. Connect to the service using `Connect-AipService -environmentname azurechinacloud`.
 - e. Run `(Get-AipServiceConfiguration).FunctionalState` and check if the state is `Enabled`.
2. If the functional state is `Disabled`, run `Enable-AipService`.

Step 2: Add the Microsoft Information Protection Sync Service service principal

The Microsoft Information Protection Sync Service service principal is not available in Azure China tenants by default, and is required for Azure Information Protection.

1. Create this service principal manually using the [New-AzADServicePrincipal](#) cmdlet and the `870c4f2e-85b6-4d43-bdda-6ed9a579b725` application ID for the Microsoft Information Protection Sync Service.

```
New-AzADServicePrincipal -ApplicationId 870c4f2e-85b6-4d43-bdda-6ed9a579b725
```

2. After adding the service principal, add the relevant permissions required to the service.

Step 3: Configure DNS encryption

For encryption to work correctly, Office client applications must connect to the China instance of the service and bootstrap from there. To redirect client applications to the right service instance, the tenant admin must configure a DNS SRV record with information about the Azure RMS URL. Without the DNS SRV record, the client application will attempt to connect to the public cloud instance by default and will fail.

Also, the assumption is that users will log in with a username based off the tenant-owned domain (for example, `joe@contoso.cn`), and not the `onmschina` username (for example, `joe@contoso.onmschina.cn`). The domain name from the username is used for DNS redirection to the correct service instance.

Configure DNS encryption - Windows

1. Get the RMS ID:
 - a. Launch PowerShell as an administrator.
 - b. If the AIPService module isn't installed, run `Install-Module AipService`.
 - c. Connect to the service using `Connect-AipService -environmentname azurechinacloud`.
 - d. Run `(Get-AipServiceConfiguration).RightsManagementServiceId` to get the RMS ID.
2. Log in to your DNS provider, navigate to the DNS settings for the domain, and then add a new SRV record.
 - Service = `_rmsredir`
 - Protocol = `_http`
 - Name = `_tcp`
 - Target = `[GUID].rms.aadrm.cn` (where GUID is the RMS ID)
 - Priority, Weight, Seconds, TTL = default values
3. Associate the custom domain with the tenant in the [Azure portal](#). This will add an entry in DNS, which might take several minutes to get verified after you add the value to the DNS settings.
4. Log in to the Microsoft 365 admin center with the corresponding global admin credentials and add the domain (for example, `contoso.cn`) for user creation. In the verification process, additional DNS changes might be required. Once verification is done, users can be created.

Configure DNS encryption - Mac, iOS, Android

Log in to your DNS provider, navigate to the DNS settings for the domain, and then add a new SRV record.

- Service = `_rmsdisco`
- Protocol = `_http`
- Name = `_tcp`
- Target = `api.aadrm.cn`
- Port = `80`
- Priority, Weight, Seconds, TTL = default values

Step 4: Install and configure the AIP unified labeling client

Download and install the AIP unified labeling client from the [Microsoft Download Center](#).

For more information, see:

- [AIP documentation](#)
- [AIP version history and support policy](#)
- [AIP system requirements](#)
- [AIP quickstart: Deploy the AIP client](#)
- [AIP administrator guide](#)
- [AIP user guide](#)
- [Learn about Microsoft 365 sensitivity labels](#)

Step 5: Configure AIP apps on Windows

AIP apps on Windows need the following registry key to point them to the correct sovereign cloud for Azure China:

- Registry node = `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSIP`
- Name = `C1oudEnvType`
- Value = `6` (default = 0)
- Type = `REG_DWORD`

IMPORTANT

Make sure you don't delete the registry key after an uninstall. If the key is empty, incorrect, or non-existent, the functionality will behave as the default value (default value = 0 for the commercial cloud). If the key is empty or incorrect, a print error is also added to the log.

Step 6: Install the AIP on-premises scanner and manage content scan jobs

Install the AIP on-premises scanner to scan your network and content shares for sensitive data, and apply classification and protection labels as configured in your organization's policy.

When configuring and managing your content scan jobs, use the following procedure instead of the [Azure portal interface](#) that's used by the commercial offerings.

For more information, see [What is the Azure Information Protection unified labeling scanner?](#) and [Manage your content scan jobs using PowerShell only](#).

To install and configure your scanner:

1. Sign in to the Windows Server computer that will run the scanner. Use an account that has local administrator rights and that has permissions to write to the SQL Server master database.
2. Start with PowerShell closed. If you've previously installed the AIP client and scanner, make sure that the

AIPScanner service is stopped.

3. Open a Windows PowerShell session with the **Run as an administrator** option.
4. Run the [Install-AIPScanner](#) cmdlet, specifying your SQL Server instance on which to create a database for the Azure Information Protection scanner, and a meaningful name for your scanner cluster.

```
Install-AIPScanner -SqlServerInstance <name> -Cluster <cluster name>
```

TIP

You can use the same cluster name in the [Install-AIPScanner](#) command to associate multiple scanner nodes to the same cluster. Using the same cluster for multiple scanner nodes enables multiple scanners to work together to perform your scans.

5. Verify that the service is now installed by using **Administrative Tools > Services**.

The installed service is named **Azure Information Protection Scanner** and is configured to run by using the scanner service account that you created.

6. Get an Azure token to use with your scanner. An Azure AD token allows the scanner to authenticate to the Azure Information Protection service, enabling the scanner to run non-interactively.

- a. Open the Azure portal and create an Azure AD application to specify an access token for authentication. For more information, see [How to label files non-interactively for Azure Information Protection](#).

TIP

When creating and configuring Azure AD applications for the [Set-AIPAuthentication](#) command, the **Request API permissions** pane shows the **APIs my organization uses** tab instead of the **Microsoft APIs** tab. Select the **APIs my organization uses** to then select **Azure Rights Management Services**.

- b. From the Windows Server computer, if your scanner service account has been granted the **Log on locally** right for the installation, sign in with this account and start a PowerShell session.

If your scanner service account cannot be granted the **Log on locally** right for the installation, use the *OnBehalfOf* parameter with [Set-AIPAuthentication](#), as described in [How to label files non-interactively for Azure Information Protection](#).

- c. Run [Set-AIPAuthentication](#), specifying values copied from your Azure AD application:

```
Set-AIPAuthentication -AppId <ID of the registered app> -AppSecret <client secret sting> -TenantId <your tenant ID> -DelegatedUser <Azure AD account>
```

For example:

```
$pscreds = Get-Credential CONTOSO\scanner
Set-AIPAuthentication -AppId "77c3c1c3-abf9-404e-8b2b-4652836c8c66" -AppSecret
"0Akk+rnuYc/u+]ah2kNxVbtrDGbS47L4" -DelegatedUser scanner@contoso.com -TenantId "9c11c87a-ac8b-46a3-
8d5c-f4d0b72ee29a" -OnBehalfOf $pscreds
Acquired application access token on behalf of CONTOSO\scanner.
```

The scanner now has a token to authenticate to Azure AD. This token is valid for one year, two years, or

never, according to your configuration of the **Web app /API** client secret in Azure AD. When the token expires, you must repeat this procedure.

7. Run the [Set-AIPScannerConfiguration](#) cmdlet to set the scanner to function in offline mode. Run:

```
Set-AIPScannerConfiguration -OnlineConfiguration Off
```

8. Run the [Set-AIPScannerContentScanJob](#) cmdlet to create a default content scan job.

The only required parameter in the **Set-AIPScannerContentScanJob** cmdlet is **Enforce**. However, you may want to define other settings for your content scan job at this time. For example:

```
Set-AIPScannerContentScanJob -Schedule Manual -DiscoverInformationTypes PolicyOnly -Enforce Off -DefaultLabelType PolicyDefault -RelabelFiles Off -PreserveFileDetails On -IncludeFileTypes '' -ExcludeFileTypes '.msg,.tmp' -DefaultOwner <account running the scanner>
```

The syntax above configures the following settings while you continue the configuration:

- Keeps the scanner run scheduling to *manual*
 - Sets the information types to be discovered based on the sensitivity labeling policy
 - Does *not* enforce a sensitivity labeling policy
 - Automatically labels files based on content, using the default label defined for the sensitivity labeling policy
 - Does *not* allow for relabeling files
 - Preserves file details while scanning and auto-labeling, including *date modified*, *last modified*, and *modified by* values
 - Sets the scanner to exclude .msg and .tmp files when running
 - Sets the default owner to the account you want to use when running the scanner
9. Use the [Add-AIPScannerRepository](#) cmdlet to define the repositories you want to scan in your content scan job. For example, run:

```
Add-AIPScannerRepository -OverrideContentScanJob Off -Path 'c:\repoToScan'
```

Use one of the following syntaxes, depending on the type of repository you're adding:

- For a network share, use `\\Server\Folder`.
- For a SharePoint library, use `http://sharepoint.contoso.com/Shared%20Documents/Folder`.
- For a local path: `C:\Folder`
- For a UNC path: `\\Server\Folder`

NOTE

Wildcards are not supported and WebDav locations are not supported.

To modify the repository later on, use the [Set-AIPScannerRepository](#) cmdlet instead.

Continue with the following steps as needed:

- [Run a discovery cycle and view reports for the scanner](#)
- [Use PowerShell to configure the scanner to apply classification and protection](#)
- [Use PowerShell to configure a DLP policy with the scanner](#)

The following table lists PowerShell cmdlets that are relevant for installing the scanner and managing your

content scan jobs:

CMDLET	DESCRIPTION
Add-AIPScannerRepository	Adds a new repository to your content scan job.
Get-AIPScannerConfiguration	Returns details about your cluster.
Get-AIPScannerContentScanJob	Gets details about your content scan job.
Get-AIPScannerRepository	Gets details about repositories defined for your content scan job.
Remove-AIPScannerContentScanJob	Deletes your content scan job.
Remove-AIPScannerRepository	Removes a repository from your content scan job.
Set-AIPScannerContentScanJob	Defines settings for your content scan job.
Set-AIPScannerRepository	Defines settings for an existing repository in your content scan job.

For more information, see:

- [What is the Azure Information Protection unified labeling scanner?](#)
- [Configuring and installing the Azure Information Protection \(AIP\) unified labeling scanner](#)
- [Manage your content scan jobs using PowerShell only.](#)

Add users and assign licenses at the same time

8/13/2021 • 4 minutes to read • [Edit Online](#)

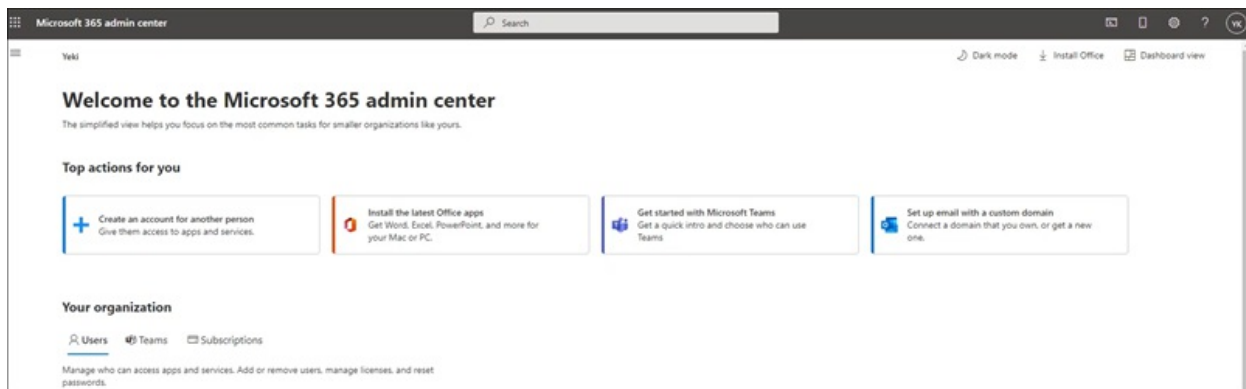
The people on your team each need a user account before they can sign in and access [Microsoft 365 for business](#). The easiest way to add user accounts is to add them one at a time in the [Microsoft 365 admin center](#). After you do this step, your users have Microsoft 365 licenses, sign in credentials, and Microsoft 365 mailboxes.

Before you begin

You must be a global, license, or a user admin to add users and assign licenses. For more information, see [About admin roles](#).

Add a user in the admin simplified view

If you're seeing this page in the admin center, you're on the **admin simplified view**. Follow the steps below to add a user.



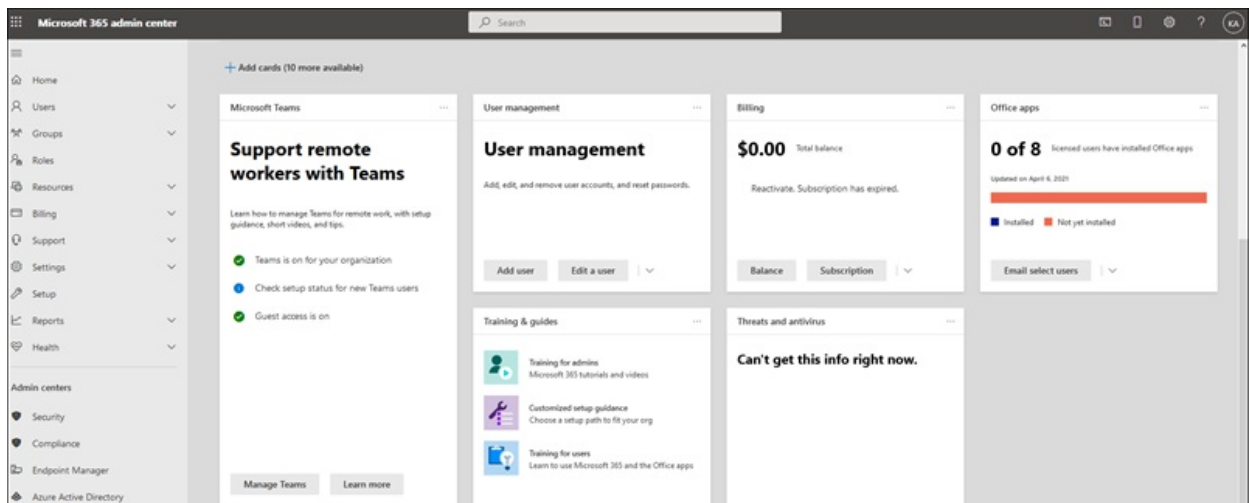
1. Go to the admin center at <https://admin.microsoft.com>.
1. Go to the admin center at <https://portal.office.de>.
1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Select **Create an account for another person**.
3. On the **Add a user account** page, fill in the first and last name, display name, and username they'll use to sign in.
4. Add the email address of the user in the **Up to 5 email addresses...** text box. This will make sure the new user gets the information they need to sign into Microsoft 365 services.
5. Select **Add user** and **Download sign-in info** if you want to save this info.

Watch: Add users in the dashboard view

NOTE

The steps used in the video show a different starting point for adding users, but the remaining steps are the same as the following procedure.

Add users one at a time in the dashboard view



1. Go to the admin center at <https://admin.microsoft.com>.
1. Go to the admin center at <https://portal.office.de>.
1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Go to **Users > Active users**, and select **Add a user**.
3. In the **Set up the basics** pane, fill in the basic user information, and then select **Next**.
 - **Name** Fill in the first and last name, display name, and username.
 - **Domain** Choose the domain for the user's account. For example, if the user's username is Jakob, and the domain is contoso.com, they'll sign in by using jakob@contoso.com.
 - **Password settings** Choose to use the autogenerated password or to create your own strong password for the user.
 - The user must change their password after 90 days. Or you can choose to **Require this user to change their password when they first sign in**.
 - Choose whether you want to send the password in email when the user is added.
4. In the **Assign product licenses** pane, select the location and the appropriate license for the user. If you don't have any licenses available, you can still add a user and buy additional licenses. Expand **Apps** and select or deselect apps to limit the apps the user has a license for. Select **Next**.
5. In the **Optional settings** pane, expand **Roles** to make this user an admin. Expand **Profile info** to add additional information about the user.
6. Select **Next**, review your new user's settings, make any changes you like, then select **Finish adding**, then **Close**.

Add multiple users at the same time

You can use any of the following methods to add multiple users at the same time:

- **Use a spreadsheet to add people in bulk.** See [Add several users at the same time](#).
- **Automate adding accounts and assigning licenses.** See [Create user accounts with Microsoft 365 PowerShell](#). Choose this method if you're already familiar with using Windows PowerShell cmdlets.
- **Using ActiveDirectory?** [Set up directory synchronization for Microsoft 365](#). Use the Azure AD Connect tool to replicate Active Directory user accounts (and other Active Directory objects) in Microsoft 365. The sync only adds the user accounts. You must assign licenses to the synced users before they can use email and other Office apps.
- **Migrating from Exchange?** See [Ways to migrate multiple email accounts to Office 365](#). When you migrate multiple mailboxes to Microsoft 365 by using either cutover, staged, or a hybrid Exchange method, you

automatically add users as part of the migration. The migration only adds the user accounts. You must assign licenses to the users before they can use email and other Office apps. If you don't assign a license to a user, their mailbox is disabled after a grace period of 30 days. Learn how to [assign licenses to users](#) in the Microsoft 365 admin center.

Next steps

After you add a user, you get an email notification from Microsoft. The email contains the person's user ID and password so they can sign in to Microsoft 365. Use your normal process for communicating new passwords. Share the [Employee quickstart guide](#) with your new users to set up things, like how to [download and install Office apps on a PC or Mac](#) and how to [set up Office apps and email on a mobile device](#).

Related content

[Add a new employee to Microsoft 365](#) (article)

[Add several users at the same time to Microsoft 365](#) (article)

[Restore a user in Microsoft 365](#) (article)

[Assign licenses to users](#) (article)

[Delete a user from your organization](#) (article)

Add a new employee to Microsoft 365

7/12/2021 • 4 minutes to read • [Edit Online](#)

This article helps you onboard a new employee to Microsoft 365 for business. We assume you're an Admin and you've already [completed Microsoft 365 set up](#), and now you have someone new joining your company.

You're in the right place if your new employee needs Microsoft 365, and you're using a [Microsoft 365 plan](#) that lets you install Office apps like Word and Excel on a computer.

Not an admin? [Learn your way around Microsoft 365](#) helps business and home users with set up.

No Office apps in your plan? Follow the steps below, but skip the sections for installing apps. Use the [Online versions of Office](#) instead.

Here's a quick overview:

STEP	WHY DO THIS?
Step 1: Create a Microsoft 365 account for the employee	Each time a new employee joins your business, create an account for them so they can start using Microsoft 365.
Step 2: Give the employee their user ID and password	When you create an account, you'll get an ID and password that you can pass to your employee so they can sign in.
Step 3: Explain where to sign in	The sign in location is https://www.office.com
Step 4: Help your employee get started	Let your employee know how to use OneDrive or any team sites in your organization.

Step 1: Create a Microsoft 365 account for the employee

For instructions, see [Add users and assign licenses at the same time](#). When you set up your new employee, you can choose to send log-in details to the employee's personal account. This way, they'll receive an email from Microsoft Online Service Team that tells them how to log in to Microsoft 365.

Step 2: Give the employee their user ID and password

Unless you sent it to their personal email address, print out the employee's sign in name and password, and hand it to them. Or tell them the information over the phone.

Because they won't yet have access to their email, don't send the information to that email address.

Step 3: Explain where to sign in

Just like Facebook, Amazon, or Gmail, your employee signs in to use Microsoft 365. Give them the following sign in information:

- Sign in at <https://www.office.com>.
- Select **Sign in**, then type the user ID and password.

Step 4: Help your employee get started

Share with them the [Employee quick setup for Microsoft 365](#) to sign in, install software, set up email, and more.

And here's a quick reference to help get them started:

TASK	FIND THE DETAILS
Sign in to Office	Go to https://www.office.com , select Sign in , and then enter your user ID and password.
Install Office apps onto your computer.	When you sign in, the home page has a link to download and install apps like Word and Outlook. Select Install Office . For instructions, see How to install Office .
Set up your email in Outlook 2016 .	Once Office apps are installed on your computer, set up your email. For instructions, see How to set up Outlook .
Set up Skype for Business so you can connect with co-workers or business partners in your company or around the world. You can start conversations with IM, voice, or video calls.	Install Skype for Business on your computer . To learn how to use Skype for Business, watch a video . Have you set up Skype for Business so your employees can contact people external to your business who are using the free Skype app? If not, tell your new employee so they know what to expect when using Skype for Business.
Install apps on your mobile device if you want to get email or use Skype for Business on your phone.	If you want to set up the Outlook mobile app so you can get email via your phone. For instructions, see iOS , Android , Windows Phone If you want to use Skype for Business on your mobile device, download and install the mobile app. For instructions, see iOS , Android , Windows Phone
Complete the OneDrive for Business training to help you learn how to store and organize your documents, presentations, and spreadsheets in the cloud.	Keep your business-related documents in the cloud by using OneDrive for Business. You can always get to your content, even if you're signed in to Microsoft 365 on a different computer. Watch a video to learn how to use your OneDrive for Business Training: OneDrive for Business training (Select OneDrive for Business).
Complete the SharePoint Online training to help you collaborate with coworkers and share content.	The best place to keep documents that your coworkers will also access is in SharePoint Online. Training: Video: Collaborate with team content using SharePoint Online Find out: How is your organization using SharePoint Online, and what type of documents get stored there. Also, which documents are stored in OneDrive for Business.

Related content

[Remove a former employee from Microsoft 365](#) (article)

[Add users and assign licenses at the same time](#)65 (article)

Assign licenses to users

7/12/2021 • 4 minutes to read • [Edit Online](#)

You can assign licenses to users on either the **Active users** page, or on the **Licenses** page. The method you use depends on whether you want to assign product licenses to specific users or assign users licenses to a specific product.

NOTE

As an admin, you can't assign or unassign licenses for a self-service purchase subscription bought by a user in your organization. You can [take over a self-service purchase subscription](#), and then assign or unassign licenses.

[Learn how to add a user and assign a license at the same time.](#)

Before you begin

- You must be a Global, License, or User admin to assign licenses. For more information, see [About Microsoft 365 admin roles](#).
- You can [assign Microsoft 365 licenses to user accounts with PowerShell](#).
- To use group-based licensing, see [Assign licenses to users by group membership in Azure Active Directory](#)
- Some services, like Sway, are automatically assigned to users, and don't need to be assigned individually.

Use the Licenses page to assign licenses to users

When you use the **Licenses** page to assign licenses, you assign licenses for a specific product to up to 20 users. On the **Licenses** page, you see a list of all the products that you have subscriptions for. You also see the total number of licenses for each product, how many licenses are assigned, and how many are available.

1. In the admin center, go to the **Billing** > [Licenses](#) page.
1. In the admin center, go to the **Billing** > [Licenses](#) page.
1. In the admin center, go to the **Billing** > [Licenses](#) page.
2. Select a product.
3. On the product details page, select **Assign licenses**.
4. In the **Assign licenses to users** pane, begin typing a name, and then choose it from the results to add it to the list. You can add up to 20 users at a time.
5. Select **Turn apps and services on or off** to assign or remove access to specific items.
6. When you're finished, select **Assign**, then select **Close**.

If there's a conflict, a message displays, tells you what the problem is, and tells you how to fix it. For example, if you selected licenses that contain conflicting services, the error message says to review the services included with each license and try again.

Change the apps and services a user has access to

1. In the admin center, go to the **Billing** > [Licenses](#) page.
1. In the admin center, go to the **Billing** > [Licenses](#) page.

1. In the admin center, go to the **Billing** > [Licenses](#) page.
2. On the **Licenses** page, select the row for a specific user.
3. In the right pane, select or deselect the apps and services that you want to give access to or remove access from.
4. When you're finished, select **Save**, then select **Close**.

Use the Active users page to assign licenses

When you use the **Active users** page to assign licenses, you assign users licenses to products.

Assign licenses to multiple users

1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the circles next to the names of the users that you want to assign licenses to.
3. At the top, select **Manage product licenses**.
4. In the **Manage product licenses** pane, select **Assign more: Keep the existing licenses and assign more** > **Next**.
5. Under **Licenses**, select the box for the license(s) that you want the selected users to have.
By default, all services associated with those licenses are automatically assigned to the users. You can limit which services are available to the users. Deselect the boxes for the services that you don't want the users to have.
6. At the bottom of the pane, select **Save changes**.
You might have to buy additional licenses if you don't have enough licenses for everyone.

NOTE

If you want to assign licenses for a large number of users, use [Assign licenses to users by group membership in Azure Active Directory](#)

Assign licenses to one user

1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the row of the user that you want to assign a license to.
3. In the right pane, select **Licenses and Apps**.
4. Expand the **Licenses** section, select the boxes for the licenses that you want to assign, then select **Save changes**.

Assign a license to a guest user

You can invite guest users to collaborate with your organization in the Azure Active Directory admin center. To learn about guest users, see [What is guest user access in Azure Active Directory B2B?](#). If you don't have any guest users, see [Quickstart: Add guest users to your directory in the Azure portal](#).

IMPORTANT

You must be a Global admin to do these steps.

1. Go to the [Azure Active Directory admin center](#)
2. In the navigation pane, select **Users**.
3. On the **Users | All Users (Preview)** page, select **Add filters**.
4. In the **Pick a field** menu, choose **User type**, then select **Apply**.
5. In the next menu, select **Guest**.
6. In the list of results, select the user who needs a license.
7. Under **Manage**, select **Licenses**.
8. Select **Assignments**.
9. On the **Update license assignments** page, select the product you want to assign a license for.
10. On the right, clear the check boxes for any services you don't want the guest user to have access to.
11. Select **Save**.

Next steps

If your users don't yet have the Office apps installed, you can share the [Employee quick start guide](#) with your users to set up things, like [how to download and install Microsoft 365 or Office 2019 on a PC or Mac](#) and [how to set up Office apps and email on a mobile device](#).

Related content

[Understand subscriptions and licenses](#) (article)

[Unassign licenses from users](#) (article)

[Buy or remove licenses for your subscription](#) (article)

Assign admin roles

8/13/2021 • 2 minutes to read • [Edit Online](#)

If you're the person who purchased your Microsoft business subscription, you are the global admin. This means you have unlimited control over the products in your subscriptions and you can access most data.

For more information, see [About admin roles](#).

When you add new users, if you don't assign them an admin role then they are in the *user role* and don't have admin privileges to any of the Microsoft admin centers. But if you need help getting things done, you can assign an admin role to a user. For example, if you need someone to help reset passwords, you shouldn't assign them the global admin role, you should assign them the password admin role. Having too many global admins, with unlimited access to your data and online business, is a security risk.

Watch: Add an admin

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

Assign admin roles

You can assign users to a role in 2 different ways:

- You can go to the user's details and **Manage roles** to assign a role to the user.
- Or you can go to **Roles** and select the role, and then add multiple users to it.

Assign admin roles to users using Roles

1. In the admin center, go to [Role assignments](#). Choose the **Azure AD** or **Intune** tabs to view the admin roles available for your organization.
2. Select the admin role that you want to assign the user to.
3. Select **Assigned admins** > **Add**.
4. Type the user's **display name** or **username**, and then select the user from the list of suggestions.
5. Add multiple users until you're done.
6. Select **Save**, and then the user will be added to the list of assigned admins.

Assign a user to an admin role from Active users

1. In the admin center, go to **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
2. On the **Active users** page, select the user whose admin role you want to change. In the flyout pane, under **Roles**, select **Manage roles**.
3. Select the admin role that you want to assign to the user. If you don't see the role you're looking for, select **Show all** at the bottom of the list.

Assign admin roles to multiple users

If you know PowerShell, see [Assign roles to user accounts with PowerShell](#). It's ideal for assigning roles to hundreds of users.

Use the following instructions to assign roles to tens of users.

Check admin roles in your organization

You might not have the correct permissions to assign admin roles to other users. Check to make sure you have the correct permissions or ask another admin to assign roles for you.

You can check admin role permissions in 2 different ways:

- You can go to the user's details and look under **Roles** on the **Account** page.
- Or you can go to **Roles** and select the admin role, and select assigned admins to see which users are assigned.

Related content

[About Microsoft 365 admin roles](#) (article)

[Administrator role permissions in Azure Active Directory](#) (article)

[Assign roles to user accounts with PowerShell](#) (article)

[Authorize or remove partner relationships](#) (article)

Unassign licenses from users

7/12/2021 • 3 minutes to read • [Edit Online](#)

You can unassign licenses from users on either the **Active users** page, or on the **Licenses** page. The method you use depends on whether you want to unassign product licenses from specific users or unassign users licenses from a specific product.

NOTE

As an admin, you can't assign or unassign licenses for a self-service purchase subscription bought by a user in your organization. You can [take over a self-service purchase subscription](#), and then assign or unassign licenses.

Before you begin

- You must be a Global, License, User admin to unassign licenses. For more information, see [About Microsoft 365 admin roles](#).
- You can [remove licenses from user accounts with Office 365 PowerShell](#).
- You can also [delete user accounts](#) that were assigned a license to make their license available to other users. When you delete a user account, their license is immediately available to assign to someone else.

Use the Licenses page to unassign licenses

When you use the **Licenses** page to unassign licenses, you unassign licenses for a specific product for up to 20 users.

1. In the admin center, go to the **Billing** > **Licenses** page.
1. In the admin center, go to the **Billing** > **Licenses** page.
1. In the admin center, go to the **Billing** > **Licenses** page.
2. Select the product for which you want to unassign licenses.
3. Select the users for which you want to unassign licenses.
4. Select **Unassign licenses**.
5. In the **Unassign licenses** box, select **Unassign**.

Use the Active users page to unassign licenses

When you use the **Active users** page to unassign licenses, you unassign product licenses from users.

Unassign licenses from one user

1. In the admin center, go to the **Users** > **Active users** page.
1. In the admin center, go to the **Users** > **Active users** page.
1. In the admin center, go to the **Users** > **Active users** page.
2. Select the row of the user that you want to unassign a license for.
3. In the right pane, select **Licenses and Apps**.
4. Expand the **Licenses** section, clear the boxes for the licenses that you want to unassign, then select **Save changes**.

Unassign licenses from multiple users

1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the circles next to the names of the users who you want to unassign licenses for.
3. At the top, select **Manage product licenses**.
4. In the **Manage product licenses** pane, select **Unassign all** > **Save changes**.
5. At the bottom of the pane, select **Done**.

What happens to a user's data when you remove their license?

- When a license is removed from a user, Exchange online data that is associated with that account is held for 30 days. After the 30-day grace period, the data is deleted and can't be recovered.
- Files saved in OneDrive for Business aren't deleted unless the user is deleted from the Microsoft 365 admin center or is removed through Active Directory synchronization. For more information, see [OneDrive retention and deletion](#).
- When the license is removed, the user's mailbox is no longer searchable by using an eDiscovery tool such as Content Search or Advanced eDiscovery. For more information, see "Searching disconnected or de-licensed mailboxes" in [Content Search in Microsoft 365](#).
- If you have an Enterprise subscription, like Office 365 Enterprise E3, Exchange Online lets you preserve the mailbox data of a deleted user account by using [inactive mailboxes](#). For more information, see [Create and manage inactive mailboxes in Exchange Online](#).
- To learn how to block a user's access to Microsoft 365 data after their license is removed, and how to get access to the data afterwards, see [Remove a former employee](#).
- If you remove a user's license and they still have Office apps installed, they see [Unlicensed Product and activation errors in Office](#) when they use Office apps.

Next steps

If you're not going to [reassign the unused licenses to other users](#), consider [removing the licenses from your subscription](#) so that you're not paying for more licenses than you need.

Related content

[Remove licenses from your subscription](#) (article)

[Assign licenses to users](#) (article)

[Understand subscriptions and licenses in Microsoft 365 for business](#) (article)

Guest users in Microsoft 365 admin center

8/13/2021 • 2 minutes to read • [Edit Online](#)

Any guests you add to your Microsoft Teams, SharePoint, or Azure Active Directory are also added to the **Guest users** list in the [Microsoft 365 admin center](#). Guests can attend meetings, view documents and chat in Teams they're invited to. Once a user shows up in the **Guest users** list, you can remove their access there.

To view guest users, in the [Microsoft 365 admin center](#), in the left nav, expand **Users**, and then choose **Guest users**.

Before you begin

You must be a global administrator to perform this task.

Watch: Add guests to Teams

Watch: Join a team as a guest

Steps: Add guests in Azure Active Directory

To add guests in the Azure Active Directory, see [add guest users](#).

After you add a user you can also assign them to a group, or give them access to an app in your organization. Once you have added a user in the Azure AD portal, that user will also be listed on the **Guest users** page in the [Microsoft 365 admin center](#). After a user is added to the **Guest users** list, they can be [added to Groups](#) in the [Microsoft 365 admin center](#).

See [add guests in bulk](#) to invite multiple guests to collaborate with your organization.

Next steps: Remove a guest

Once you're done collaborating with a guest user, you can remove them and they'll no longer have access to your organization.

1. In the Microsoft 365 admin center, expand **Users** and then choose **Guest users**.
2. On the **Guest users** page, choose the user you want to remove and then choose **Delete a user**.

To remove users in the Azure AD portal, see [remove a guest user and resources](#).

Related content

[guest users in microsoft 365 admin center](#)

[prevent guests from being added to a specific microsoft 365 group or microsoft teams team](#)

Manage guest access in Microsoft 365 groups

8/13/2021 • 2 minutes to read • [Edit Online](#)

By default, guest access for Microsoft 365 groups is turned on for your organization. Admins can control whether to allow guest access to groups for their whole organization or for individual groups.

When it's turned on, group members can invite guest users to a Microsoft 365 group through Outlook on Web. Invitations are sent to the group owner for approval.

Once approved, the guest user is added to the directory and the group.

NOTE

Yammer Enterprise networks that are in Native Mode or the [EU Geo](#) do not support network guests. Microsoft 365 Connected Yammer groups do not currently support guest access, but you can create non-connected, external groups in your Yammer network. See [Create and manage external groups in Yammer](#) for instructions.

Guest access in groups is often used as part of a broader scenario that includes SharePoint or Teams. These services have their own guest sharing settings. For complete instructions for setting up guest sharing across groups, SharePoint, and Teams, see:

- [Collaborate with guests in a site](#)
- [Collaborate with guests in a team](#)

Manage groups guest access

If you want to enable or disable guest access in groups, you can do so in the [Groups](#).

1. In the admin center, go to **Show all** > **Settings** > **Org settings** and on the **Services** tab, select [Microsoft 365 Groups](#).
2. On the **Microsoft 365 Groups** page, choose whether you want to let people outside your organization access group resources or let group owners add people outside your organization to groups.

Add guests to a Microsoft 365 group from the admin center

If the guest already exists in your directory, you can add them to your groups from the [Microsoft 365 admin center](#). (Groups with dynamic membership must be [managed in Azure Active Directory](#).)

1. In the admin center, go to the **Groups** > [Groups](#).
2. Click the group you want to add the guest to, and select **View all and manage members** on the **Members** tab.
3. Select **Add members**, and choose the name of the guest you want to add.
4. Select **Save**.

If you want to add a guest to the directory directly, you can [Add Azure Active Directory B2B collaboration users in the Azure portal](#).

If you want to edit any of a guest's information, you can [Add or update a user's profile information using Azure Active Directory](#).

Related content

[Block guest users from a specific group](#) (article)

[Manage group membership in the Microsoft 365 admin center](#) (article)

[Azure Active Directory access reviews](#) (article)

[Set-AzureADUser](#) (article)

Change a user name and email address

7/12/2021 • 5 minutes to read • [Edit Online](#)

You may need to change someone's email address and display name if, for example, they get married and their last name changes.

Watch: Change a user's name or email address

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

You must be a [global admin](#) to complete these steps.

Change a user's email address

1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. Select the user's name, and then on the **Account** tab select **Manage username**.
2. In the first box, type the first part of the new email address. If you added your own domain to Microsoft 365, choose the domain for the new email alias by using the drop-down list. [Learn how to add a domain](#).
3. Select **Save changes**.

IMPORTANT

If you get an error message, see [Resolve error messages](#).

Set the primary email address

1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the user's name, and then on the **Account** tab select **Manage email aliases**.
3. Select **Set as Primary** for the email address that you want to set as the primary email address for that person.

IMPORTANT

You won't see this option to Set as Primary if you purchased Microsoft 365 from GoDaddy or another Partner service that provides a management console. Instead, sign in to the GoDaddy / partner's management console to set the primary alias.

Also, you'll only see this option if you're a global admin. If you don't see the option, you don't have permissions to change a user's name and primary email address.

4. You'll see a big yellow warning that you're about to change the person's sign-in information. Select **Save**, then **Close**.
5. Give the person the following information:
 - This change could take a while.
 - Their new username. They'll need it to sign in to Microsoft 365.
 - If they are using Skype for Business Online, they must reschedule any Skype for Business Online meetings that they organized, and tell their external contacts to update their contact information.
 - If they are using OneDrive, the URL to this location has changed. If they have OneNote notebooks in their OneDrive, they might need to close and reopen them in OneNote. If they have shared files from their OneDrive, the links to the files might not work and the user can reshare.
 - If their password changed too, they are prompted to enter the new password on their mobile device, or it won't sync.

Change a user's display name

1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the user's name, and then on the **Account** tab select **Manage contact information**.
3. In the **Display name** box, type a new name for the person, and then select **Save**.

If you get the error message "**We're sorry, the user couldn't be edited. Review the user information and try again**", see [Resolve error messages](#).

It might take up to 24 hours for this change to take effect across all services. After the change has taken effect, the person will have to sign in to Outlook, Skype for Business and SharePoint with their updated username.

Resolve error messages

"A parameter cannot be found that matches parameter name 'EmailAddresses'"

If you get the error message " **A parameter cannot be found that matches parameter name 'EmailAddresses'**" it means that it's taking a bit longer to finish setting up your tenant, or your custom domain if you recently added one. The setup process can take up to 4 hours to complete. Wait a while so the setup process has time to finish, and then try again. If the problem persists, call [support](#) and ask them to do a full sync for you.

"We're sorry, the user couldn't be edited. Review the user information and try again"

If you get the error message " **We're sorry, the user couldn't be edited. Review the user information**

and try again." it means you aren't a global admin and you don't have permissions to change the user name. Find the global admin in your business and ask them to make the change.

What to do with old email addresses

A person's previous primary email address is retained as an additional email address. **We strongly recommend that you don't remove the old email address.**

Some people might continue to send email to the person's old email address and deleting it may result in NDR failures. Microsoft automatically routes it to the new one. Also, do not reuse old SMTP email addresses and apply them to new accounts. This can also cause NDR failures or delivery to an unintended mailbox.

What if the person's offline address book won't sync with the Global Address List?

If they are using Exchange Online or if their account is linked with your organization's on-premises Exchange environment, you might see this error when you try to change a username and email address: "This user is synchronized with your local Active Directory. Some details can be edited only through your local Active Directory."

This is due to the Microsoft Online Email Routing Address (MOERA). The MOERA is constructed from the person's *userPrincipalName* attribute in Active Directory and is automatically assigned to the cloud account during the initial sync and once created, it cannot be modified or removed in Microsoft 365. You can subsequently change the username in the Active Directory, but it doesn't change the MOERA and you may run into issues displaying the newly changed name in the Global Address List.

To fix this, log in to the [Azure Active Directory Module for PowerShell](#) with your Microsoft 365 administrator credentials. and use the following syntax:

```
Set-MsolUserPrincipalName -UserPrincipalName anne.wallace@contoso.onmicrosoft.com -NewUserPrincipalName anne.jones@contoso.com
```

TIP

This changes the person's **userPrincipalName** attribute and has no bearing on their Microsoft Online Email Routing Address (MOERA) email address. It is best practice, however, to have the person's logon UPN match their primary SMTP address.

To learn how to change someone's username in Active Directory, in Windows Server 2003 and earlier, see [Rename a user account](#).

Related content

[Add a domain Admins: Reset a password for one or more users](#) [Add another email address to a user](#) [Create a shared mailbox](#)

Restore a user

7/12/2021 • 2 minutes to read • [Edit Online](#)

When you restore a user account within 30 days after deleting it, the account and all associated data are restored. The user can sign in with the same work or school account. Their mailbox will be fully restored. To find out how much time remains before a specific user account can no longer be restored, [contact us](#).

Here are a couple of tips:

- Make sure licenses are available to assign to the account.
- If your business uses Active Directory, for instructions on restoring a user account, see [How to troubleshoot deleted user accounts in Office 365](#).

Restore one or more user accounts

You must be a Microsoft 365 global admin or user management admin to do these steps.

1. In the admin center, go to the **Users** > [Deleted users](#) page.
2. On the **Deleted users** page, select the names of the users who you want to restore, and then select **Restore**.
3. Follow the prompts to set their password, and then select **Restore**.
4. If the user is successfully restored, select **Send email and close**. If you encounter a name conflict or proxy address conflict, see the instructions below for how to restore those accounts.

After you've restored a user, make sure you notify them that their password changed and you follow up with them.

Restore a user that has a user name conflict

A user name conflict occurs when you delete a user account, create a new user account with the same user name (either for the same user or another user with a similar name), and later try to restore the deleted account.

To fix this, replace the active user account with the one that you are restoring. Or, assign a different user name to the account that you are restoring so that there aren't two accounts with the same user name. Here are the steps.

1. In the admin center, go to the **Users** > [Deleted users](#) page.
2. On the **Deleted users** page, select the names of the users that you want to restore, and then select **Restore**.

NOTE

If two or more users fail to be restored, an error message advises you that the restore operation failed for some users. View the log to see which users were not restored, and then restore the failed accounts one at a time.

3. Follow the prompts to set the password and select **Restore**.
4. A message pops up that says there was a problem restoring the account. Do one of the following:

- Cancel the restore and rename the current active user. Then attempt the restore again.
 - OR, type a new primary email address for the user and select **Restore**.
5. Review the results, and then select **Close**.

Restore a user that has a proxy address conflict

A proxy address conflict occurs when you delete a user account that contains a proxy address, assign the same proxy address to another account, and then try to restore the deleted account. Follow the steps below to fix this issue.

You must have [admin permissions](#) in Microsoft 365 to do this.

1. In the admin center, go to the **Users** > [Deleted users](#) page.
2. On the **Deleted users** page, select the user that you want to restore, and then select **Restore**.
3. On the **Restore** page, follow the instructions to set the password and select **Restore**. Any conflicting proxy addresses are automatically removed from the user you are restoring.
4. Review the results, and then select **Close**.

Related content

[Delete a user](#) (article)

[Assign admin roles](#) (video)

[Assign licenses to users](#) (article)

Create and use a template to add users

4/3/2021 • 2 minutes to read • [Edit Online](#)

You can create and use a template to save time and standardize settings when you are adding multiple users. Templates are particularly useful if you have users who share many common properties, like those who have the same role and work at the same location and those who require the same software. For example, you might have a team of support engineers who work in the same office.

Create a template

Templates are easy to create—you can select **Users > Active users > User templates**, and then select **Add a template** from the drop-down list, or you can add a new user and when you are finished, you will have the option of saving the entry as a template.

When you create a template after adding a user, the values you choose for the following settings are saved in the template:

- Domain name
- Password settings choice: you can choose to create passwords or have them auto-generated
- One-time password choice: you can require the user to create a new password after first sign in
- License location
- License choices
- Application choices
- Role
- Most profile information, such as **Job profile**, **Department**, **Office**, **Office phone**, and **Street address**

The following information is user-specific and isn't saved in the template:

- First and last name
- Display name
- User name
- Choice to send the password in email and who the password email is sent to
- Mobile phone number

If you choose not to enter information for a setting within a section, that value will be blank and that setting will not display in the template. For example, if you leave **Job title** blank, when you review your template and when you use your template, **Job title** will not appear at all. If you leave all the **Profile** section settings blank, the **Profile** section will display **None provided** in your final template.

When you create a template by selecting the **Add a template** option, you can choose which values to complete. Anything that is left blank will appear as **None provided** in the template.

Use a template to add a user

To use an existing template to add a user:

1. In the admin center, select **Users > Active users**.
2. Select **User templates**, and then select a template from the drop-down list. (The list will contain only the templates that you created, not those created by other admins.)

NOTE

You can also use a template to add a user by selecting **User templates > Manage templates**, selecting a template, and then selecting **Use template**.

3. Follow the steps to create a user from the template you selected.

NOTE

If you have insufficient licenses available for a user that you add, and your payment information is available, we will attempt to purchase another license using your existing payment information. If your payment information is unavailable, the user will be created as an unlicensed user.

Manage templates

You can only delete templates you no longer need and add new ones. To delete a template:

1. In the admin center, select **Users > Active users**.
2. Select **Templates**, and then select **Manage templates** from the drop-down list.
3. A list of templates will appear. You can delete a template by doing any of the following:
 - Select one or more templates, and then select **Delete**.
 - Select the three dots to the right of the template name, and then select **Delete**.
 - Select the template name. When the template details appear on the right side of your screen, select **Delete template**.

Related articles

[Add users and assign licenses at the same time](#)

[Remove a former employee from Microsoft 365](#)

Upgrade your Microsoft 365 for business users to the latest Office client

6/14/2021 • 4 minutes to read • [Edit Online](#)

Office 2010 reaches end-of-support

Office 2010 reached its end of support on October 13, 2020. Microsoft will no longer provide the following:

- Technical support for issues
- Bug fixes for issues that are discovered
- Security fixes for vulnerabilities that are discovered

See [Office 2010 end of support roadmap](#) for more information.

Is this the right topic for you?

If you're the admin responsible for the Microsoft 365 for business subscription in your organization, you're in the right place. Admins are typically responsible for tasks like managing users, resetting passwords, managing Office installs and adding or removing licenses.

If you're not an admin and you have a [Microsoft 365 Family](#) product, see [How do I upgrade Office](#) for information about upgrading your older, home use version of Office.

Get ready to upgrade to Microsoft 365

As an admin, you control what version of Office people in your organization can install. We highly recommend that you help users in your organization running older versions of Office such as Office 2010, Office 2013, or Office 2016 upgrade to the latest version to take advantage of its security and productivity improvements.

Upgrade steps

The steps below will guide you through the process of upgrading your users to the latest Office desktop client. We recommend you read through these steps before beginning the upgrade process.

Step 1 - Check system requirements

[Check the system requirements](#) for Office to make sure your devices are compatible with the latest version of Office. For example, newer versions of Office can't be installed on computers running Windows XP or Windows Vista.

TIP

If you have users in your organization running older versions of Windows on their PCs or laptops, we recommend upgrading to Windows 10. Windows 7 has reached end of support. Read [Support for Windows 7 ends in January 2020](#) for more info.

Check out the [Windows 10 system requirements](#) to see if you can upgrade their operating systems.

Check application compatibility

To ensure a successful upgrade, we recommend identifying your Office applications--including VBA scripts,

macros, third-party add-ins, and complex documents and spreadsheets--and assessing their compatibility with the latest version of Office.

For example, if you're using third-party add-ins with your current Office install, contact the manufacture to make sure they're compatible with the latest version of Office.

Step 2 - Check your existing subscription plan

Some Microsoft 365 plans don't include the full desktop versions of Office and the steps to upgrade are different if your plan doesn't include Office.

Not sure which subscription plan you have? See [What Microsoft 365 for business subscription do I have?](#)

If your existing plan includes Office, move on to [Step 3 - Uninstall Office](#).

If your existing plan doesn't include Office, then select from the options below:

Upgrade options for plans that don't include Office

Option 1: Switch Office subscriptions

Switch to a subscription that includes Office. See [Switch to a different Microsoft 365 for business plan](#).

Option 2: Buy individual, one-time purchases of Office, or buy Office through a volume license

- Buy an individual, one-time purchase of Office. See [Office Home & Business](#) or [Office Professional](#)
- OR
- Buy multiple copies of Office through a volume license. See, [Compare suites available through volume licensing](#).

Step 3 - Uninstall Office

Before installing the latest version of Office, we recommend you uninstall all older versions of Office. However, if you change your mind about upgrading Office, note the following instances where you won't be able to reinstall Office after uninstalling it.

We recommend if you have third-party add-ins, contact the manufacturer to see if there's an update that will work with the latest version of Office.

TIP

If you run into issues while uninstalling Office, you can use the Microsoft Support and Recovery Assistant tool to help you remove Office: [Download and run the Microsoft Support and Recovery Assistant](#).

Select the version of Office you want to uninstall

- [From a PC](#)
- [From a Mac](#)

Known issues trying to reinstall older versions of Office after an uninstall

Office through a volume license If you no longer have access to the source files of these volume license versions of Office, you won't be able to reinstall it.

Office pre-installed on your computer If you no longer have a disc or product key (if Office came with one) you won't be able to reinstall it.

Non-supported subscriptions If your copy of Office was obtained through discontinued subscriptions, such

as Office 365 Small Business Premium or Office 365 Mid-size Business, you won't be able to install an older version of Office unless you have the product key that came with your subscription.

If you'd prefer to install your older version of Office side-by-side with the latest version, you can see a list of versions where this is supported in, [Install and use different versions of Office on the same PC](#). A side-by-side installation might be the right choice for you, if for example, you've installed third-party add-ins you're using with your older version of Office and you're not yet sure they're compatible with the latest version.

Step 4 - Assign Office licenses to users

If you haven't already done so, assign licenses to any users in your organization who need to install Office, see [Assign licenses to users in Microsoft 365 for business](#).

Step 5 - Install Office

After you've verified the users you want to upgrade all have licenses, the final step is to have them install Office, see [Download and install or reinstall Office on your PC or Mac](#).

TIP

If you don't want your users installing Office themselves, see [Manage software download settings in Office 365](#). You can use the [Office Deployment Tool](#) to download the Office software to your local network and then deploy Office by using the software deployment method you typically use.

Overview: Remove a former employee and secure data

7/28/2021 • 2 minutes to read • [Edit Online](#)

A question we often get is, "What should I do to secure data and protect access when an employee leaves my organization?" This article series explains how to block access to Microsoft 365 so these user's can't sign in to Microsoft 365, the steps you should take to secure organization data, and how to allow other employees to access email and OneDrive data.

Before you begin

You need to be a global administrator to complete the steps in this solution.

To complete the steps in this series, you use these Microsoft 365 capabilities and features.

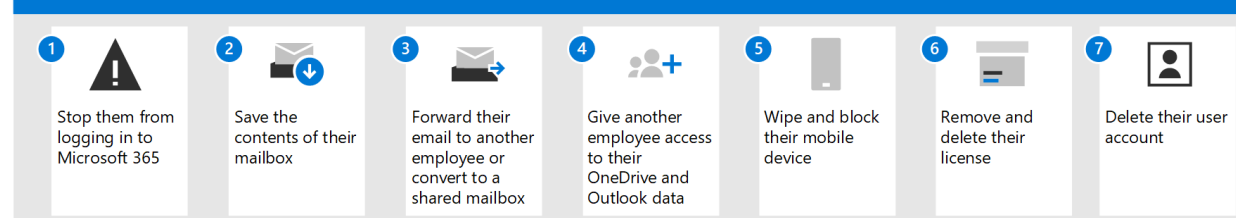
PRODUCT OR COMPONENT	CAPABILITY OR FEATURE
Microsoft 365 admin center	Convert mailbox, forward email, revoke access, remove user
Exchange admin center	Block user, block access to email, wipe device
OneDrive and SharePoint	Give access to other users
Outlook	Import pst files, add mailbox
Active Directory	Remove users in hybrid environments

Solution: Remove a former employee

IMPORTANT

Although we've numbered the steps in this solution and you don't have to complete the solution using the exact order, we do recommend doing the steps this way.

Steps to remove a former employee from Microsoft 365



STEP	WHY DO THIS
------	-------------

STEP	WHY DO THIS
Step 1 - Prevent a former employee from logging in and block access to Microsoft 365 services	<p>This blocks your former employee from logging in to Microsoft 365 and prevents the person from accessing Microsoft 365 services.</p>
Step 2 - Save the contents of a former employee's mailbox	<p>This is useful for the person who is going to take over the employee's work, or if there is litigation.</p>
Step 3 - Forward a former employee's email to another employee or convert to a shared mailbox	<p>This lets you keep the former employee's email address active. If you have customers or partners still sending email to the former employee's address, this gets them to the person taking over the work.</p>
Step 4 - Give another employee access to OneDrive and Outlook data	<p>If you only remove a user's license but don't delete the account, the content in the user's OneDrive will remain accessible to you even after 30 days.</p> <p>Before you delete the account, you should give access of their OneDrive and Outlook to another user. After you delete an employee's account, the content in their OneDrive and Outlook is retained for 30 days. During that 30 days, however, you can restore the user's account, and gain access to their content. If you restore the user's account, the OneDrive and Outlook content will remain accessible to you even after 30 days.</p>
Step 5 - Wipe and block a former employee's mobile device	<p>Removes your business data from the phone or tablet.</p>
Step 6 - Remove and delete the Microsoft 365 license from a former employee	<p>When you remove a license, you can assign it to someone else. Or, you can delete the license so you don't pay for it until you hire another person.</p> <p>When you remove or delete a license, the user's old email, contacts, and calendar are retained for 30 days, then permanently deleted. If you remove or delete a license but don't delete the account, the content in the user's OneDrive will remain accessible to you even after 30 days.</p>
Step 7 - Delete a former employee's user account	<p>This removes the account from your admin center. Keeps things clean.</p>

Related content

[Restore a user \(article\)](#)

[Add a new employee to Microsoft 365 \(article\)](#)

[Assign licenses to users \(article\)](#)

[Unassign licenses from users \(article\)](#)

Step 1 - Prevent a former employee from logging in and block access to Microsoft 365 services

7/28/2021 • 2 minutes to read • [Edit Online](#)

If you need to immediately prevent a user's sign-in access, you should reset their password. In this step, force a sign out of the user from Microsoft 365.

NOTE

You need to be a global administrator to initiate sign-out for other administrators. For non administrator users, you can use a User Administrator or a Helpdesk Administrator user to perform this action. [Learn more about the Admin Roles](#)

1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the box next to the user's name, and then select **Reset password**.
3. Enter a new password, and then select **Reset**. (Don't send it to them.)
4. Select the user's name to go to their properties pane, and on the **Account** tab, select **Sign out of all sessions**.

Within an hour - or after they leave the current Microsoft 365 page they are on - they're prompted to sign in again. An access token is good for an hour, so the timeline depends on how much time is left on that token, and whether they navigate out of their current webpage.

IMPORTANT

If the user is in Outlook on the web, just clicking around in their mailbox, they may not be kicked out immediately. As soon as they select a different tile, such as OneDrive, or refresh their browser, the sign-out is initiated.

To use PowerShell to sign out a user immediately, see the [Revoke-AzureADUserAllRefreshToken](#) cmdlet.

For more information about how long it takes to get someone out of email, see [What you need to know about terminating an employee's email session](#).

Block a former employee's access to Microsoft 365 services

IMPORTANT

Blocking an account can take up to 24 hours to take effect. If you need to immediately prevent a user's sign-in access, follow the steps above and reset their password.

1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the name of the employee that you want to block, and under the user's name, select the symbol for **Block this user**.
3. Select **Block the user from signing in**, and then select **Save**.

Block a former employee's access to email (Exchange Online)

If you have email as part of your Microsoft 365 subscription, sign in to the Exchange admin center and follow these steps to block your former employee from accessing their email.

1. Go to the [Exchange admin center](#).
2. In the Exchange admin center, navigate to **Recipients > Mailboxes**.
3. Select the user mailbox from the list and then, in the *Details Pane* (on the right-hand side), select **Manage email apps settings** under **Email apps**. Turn **Off** the slider for all the options; **Mobile (Exchange ActiveSync)**, **Outlook on the web**, **Outlook desktop (MAPI)**, **Exchange web services**, **POP3**, and **IMAP**.
4. Select **Save**.

Related content

[Exchange admin center in Exchange Online](#)

[Restore a user](#)

Step 2 - Save the contents of a former employee's mailbox

7/28/2021 • 2 minutes to read • [Edit Online](#)

In this step, place a Litigation Hold or In-place Hold on the user or export their Outlook data to a .pst file.

Place hold or export user's data to a .pst file

Once you've blocked a user from being able to log into your organization you can save the contents of their mailbox. There are two ways you can save the contents of the former employee's mailbox.

1. Place a Litigation Hold or In-Place Hold on the mailbox before the deleting the user account. This is much more complicated than the second option but worth doing if: your Enterprise plan includes archiving and legal hold, litigation is a possibility, and you have a technically strong IT department.

After you convert the mailbox to an "inactive mailbox," administrators, compliance officers, or records managers can use In-Place eDiscovery tools in Exchange Online to access and search the contents.

Inactive mailboxes can't receive email and aren't displayed in your organization's shared address book or other lists.

To learn how to place a hold on a mailbox, see [Manage inactive mailboxes in Exchange Online](#).

OR

2. Add the former employee's email address to your version of Outlook on Desktop, and then export the data to a .pst file. You can import the data to another email account as needed. Check out [Step 6 - Give another employee access to OneDrive and Outlook data](#).

Related content

[Exchange admin center in Exchange Online](#)

[Restore a user](#)

Step 3 - Forward a former employee's email to another employee or convert to a shared mailbox

7/28/2021 • 2 minutes to read • [Edit Online](#)

In this step, you assign the former employee's email address to another employee, or convert the user's mailbox to a shared mailbox.

Convert former employee's mailbox to a shared mailbox

When you convert a user's mailbox to a shared mailbox, all of the existing email and calendar is retained. Only now it's in a shared mailbox where several people will be able to access it instead of one person. You can convert a shared mailbox back to a user (private) mailbox at a later date if you want.

- Creating a shared mailbox is the less expensive way to go because you won't have to pay for a license as long as the mailbox is smaller than 50GB. Over 50GB and you'll need to assign a license to it.
- If you convert the mailbox to a shared mailbox, all the old email will be available, too. This can take up a lot of space.
- If you set up email forwarding, only *new* emails sent to the former employee will now be sent to the current employee.

Follow these steps on how to [convert the user's mailbox to a shared mailbox](#).

Forward a former employee's email to another employee

IMPORTANT

If you're setting up email forwarding or a shared mailbox, at the end, don't delete the former employee's account. The account needs to be there to anchor the email forwarding or shared mailbox.

1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the name of the employee that you want to block, and then select the **Mail** tab.
3. Under **Email Forwarding**, select **Manage email forwarding**.
4. Turn on **Forward all email sent to this mailbox**. In the **Forwarding address** box, type the email address of the current employee who's going to get the email.
5. Select **Save**.
6. Remember, don't delete the former employee's account.

Related content

[Open and use a shared mailbox in Outlook](#)

[Access another person's mailbox](#)

[Exchange admin center in Exchange Online](#)

[Manager another person's mail and calendar items](#)

Step 4 - Give another employee access to OneDrive and Outlook data

7/28/2021 • 5 minutes to read • [Edit Online](#)

When an employee leaves your organization, you'll want to access their OneDrive and Outlook data, back it up, and choose whether to give it to another employee.

Access a former user's OneDrive documents

If you remove a user's license but don't delete the account, you can give yourself access to the content in the user's OneDrive. If you delete the user's account, you have 30 days by default to access the former user's OneDrive data. [Learn how to set the OneDrive retention for deleted users](#). If you don't [restore a user account](#) within this time, their OneDrive content is deleted.

To preserve a former user's OneDrive files, first give yourself access to their OneDrive, and then move the files you want to keep.

1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select a user.
3. In the right pane, select **OneDrive**. Under **Get access to files**, select **Create link to files**.
4. Select the link to open the file location. Download the files to your computer, or select **Move to** or **Copy to** to move or copy them to your own OneDrive or to a shared library.

NOTE

You can move or copy up to 500 MB of files and folders at a time.

When you move or copy documents that have version history, only the latest version is moved.

You can also grant access to another user to access a former employee's OneDrive.

1. Sign in to the [admin center](#) as a global admin or SharePoint admin.

If you get a message that you don't have permission to access the admin center, then you don't have administrator permissions in your organization.
2. In the left pane, select **Admin centers** > **SharePoint**. (You might need to select **Show all** to see the list of admin centers.)
3. If the classic SharePoint admin center appears, select **Open it now** at the top of the page to open the SharePoint admin center.
4. In the left pane, select **More features**.
5. Under **User profiles**, select **Open**.
6. Under **People**, select **Manage User Profiles**.
7. Enter the former employee's name and select **Find**.
8. Right-click the user, and then choose **Manage site collection owners**.

9. Add the user to **Site collection administrators** and select **Ok**.
10. The user will now be able to access the former employee's OneDrive using the OneDrive URL.

Revoke admin access to a user's OneDrive

You can give yourself access to the content in a user's OneDrive, but you may want to remove your access when you no longer need it.

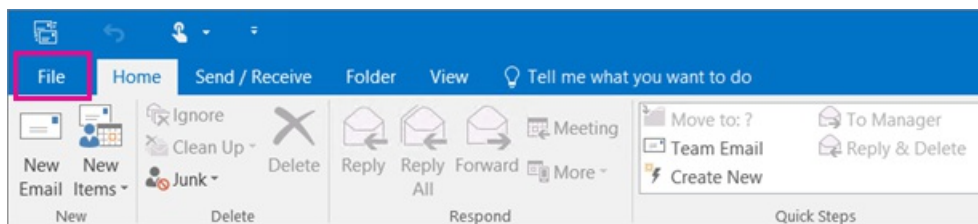
1. Sign in to the [admin center](#) as a global admin or SharePoint admin.

If you get a message that you don't have permission to access the admin center, then you don't have administrator permissions in your organization.
2. In the left pane, select **Admin centers** > **SharePoint**. (You might need to select **Show all** to see the list of admin centers.)
3. If the classic SharePoint admin center appears, select **Open it now** at the top of the page to open the SharePoint admin center.
4. In the left pane, select **More features**.
5. Under **User profiles**, select **Open**.
6. Under **People**, select **Manage User Profiles**.
7. Enter the user's name and select **Find**.
8. Right-click the user, and then choose **Manage site collection owners**.
9. Remove the person who no longer needs access to the user's data, and then select **OK**.

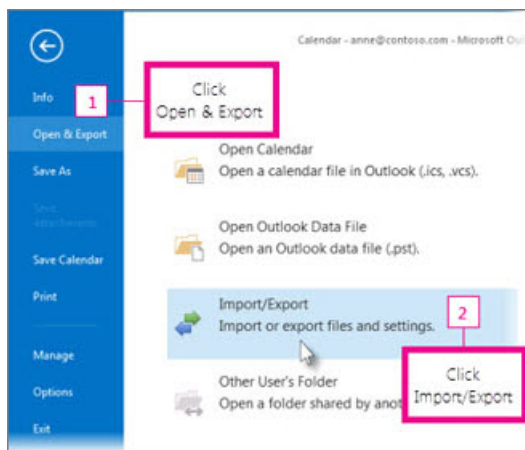
Access the Outlook data of a former user

To save the email messages, calendar, tasks, and contacts of the former employee, export the information to an Outlook Data File (.pst).

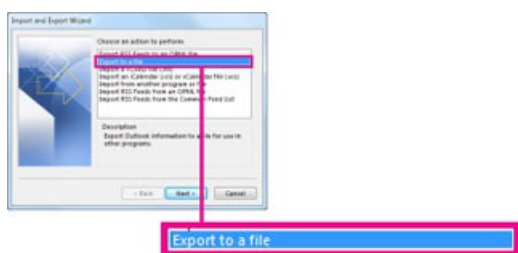
1. [Add the former employee's email](#) to your Outlook (If you [reset the user's password](#), you can set it to something only you know.)
2. In Outlook, select **File**.



3. Select **Open & Export** > **Import/Export**.



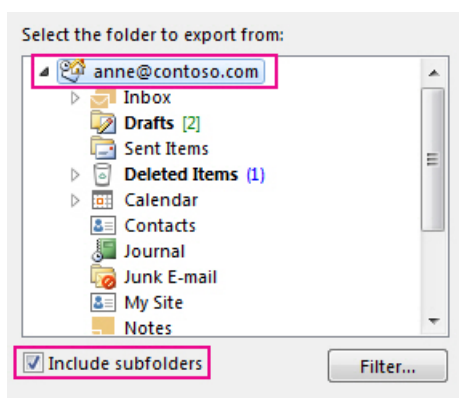
4. Select **Export to a file**, and then select **Next**.



5. Select **Outlook Data File (.pst)**, and then select **Next**.

6. Select the account you want to export by selecting the name or email address, such as Mailbox - Anne Weiler or anne@contoso.com. If you want to export everything in your account, including mail, calendar, contacts, tasks, and notes, make sure the **Include subfolders** check box is selected.

NOTE
You can export one account at a time. If you want to export multiple accounts, after one account is exported, repeat these steps.



7. Select **Next**.

8. Select **Browse** to select where to save the Outlook Data File (.pst). Type a *file name*, and then select **OK** to continue.

NOTE
If you've used export before, the previous folder location and file name appear. Type a *different file name* before selecting **OK**.

9. If you are exporting to an existing Outlook Data File (.pst), under **Options**, specify what to do when

exporting items that already exist in the file.

10. Select **Finish**.

Outlook begins the export immediately unless a new Outlook Data File (.pst) is created or a password-protected file is used.

- If you're creating an Outlook Data File (.pst), an optional password can help protect the file. When the **Create Outlook Data File** dialog box appears, type the *password* in the **Password** and **Verify Password** boxes, and then select **OK**. In the **Outlook Data File Password** dialog box, type the *password*, and then select **OK**.
- If you're exporting to an existing Outlook Data File (.pst) that is password protected, in the **Outlook Data File Password** dialog box, type the *password*, and then select **OK**.

See how to [Export or backup email, contacts, and calendar to an Outlook .pst file](#) in Outlook 2010.

NOTE

By default, your email is available offline for a period of 12 months. If required, see how to [increase the data available offline](#).

Give another user access to a former user's email

To give access to the email messages, calendar, tasks, and contacts of the former employee to another employee, import the information to another employee's Outlook inbox.

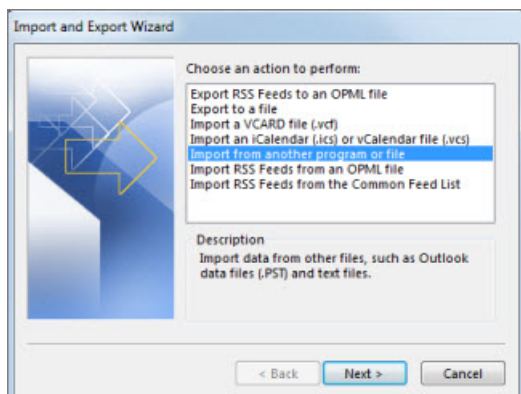
NOTE

You can also [convert the former user's mailbox to a shared mailbox](#) or [forward a former employee's email to another employee](#).

1. In Outlook, go to **File > Open & Export > Import/Export**.

This starts the Import and Export Wizard.

2. Select **Import from another program or file**, and then select **Next**.



3. Select **Outlook Data File (.pst)**, and select **Next**.

4. Browse to the .pst file you want to import.

5. Under **Options**, choose how you want to deal with duplicates

6. Select **Next**.

7. If a password was assigned to the Outlook Data File (.pst), enter the password, and then select **OK**.

8. Set the options for importing items. The default settings usually don't need to be changed.

9. Select **Finish**.

NOTE

The steps remain the same for accessing an existing user's OneDrive and email data.

TIP

If you want to import or restore only a few items from an Outlook Data File (.pst), you can open the Outlook Data File. Then, in the navigation pane, drag the items from Outlook Data File folders to your existing Outlook folders.

Related content

[Add and remove admins on a OneDrive account](#) (article)

[Restore a deleted OneDrive](#) (article)

[OneDrive retention and deletion](#) (article)


[Share OneDrive files and folders](#)

Step 5 - Wipe and block a former employee's mobile device

7/20/2021 • 2 minutes to read • [Edit Online](#)

If your former employee had an organization phone, you can use the Exchange admin center to wipe and block that device so that all organization data is removed from the device and it can no longer connect to Office 365. If your organization uses Basic Mobility and Security to manage mobile devices, you can wipe and block those devices using Basic Mobility and Security.

Wipe mobile device using the Exchange admin center

1. Go to the [Exchange admin center](#).
2. In the Exchange admin center, navigate to **Recipients** > **Mailboxes**.
3. Select the user, and under **Mobile Devices**, select **View details**.
4. On the **Mobile Device Details** page, under **Mobile devices**, select the mobile device, select **Wipe Data** , and then select **Block**.
5. Select **Save**.

TIP

Be sure you remove or disable the user from your on-premises Blackberry Enterprise Service. You should also disable any Blackberry devices for the user. Refer to the Blackberry Business Cloud Services Administration Guide if you need specific steps on how to disable the user.

Related content

[Exchange admin center in Exchange Online](#)

Step 6 - Remove the Microsoft 365 license from a former employee

7/20/2021 • 2 minutes to read • [Edit Online](#)

If you don't want to pay for a license after someone leaves your organization, you need to remove their Microsoft 365 license and then delete it from your subscription. You can assign a license to another user if you don't delete it.

When you remove the license, all that user's data is held for 30 days. You can [access](#) the data, or [restore](#) the account if the user comes back. After 30 days, all the user's data (except for documents stored on SharePoint Online) is permanently deleted from Microsoft 365 and can't be recovered.

1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the name of the employee that you want to block, and then select the **Licenses and Apps** tab.
3. Clear the check boxes for the license(s) you want to remove, and then select **Save changes**.

To reduce the number of licenses you're paying for until you hire another person, do the following steps:

1. In the admin center, go to the **Billing** > [Your products](#) page, and select the **Products** tab.
2. Select the subscription from which you want to remove licenses.
3. On the details page, select **Remove licenses**.
4. In the **Remove licenses** pane, under **New quantity**, in the **Total licenses** box, enter the total number of licenses that you want for this subscription. For example, if you have 25 licenses and you want to remove one of them, enter 24.
5. Select **Save**.

When you [add another person](#) to your business, you'll be prompted to buy a license at the same time, with just one step!

For more information about managing user licenses for Microsoft 365 for business, see [Assign licenses to users in Microsoft 365 for business](#), and [Unassign licenses from users in Microsoft 365 for business](#).

How the deleted employee account affects Skype for Business

When you remove a user's license from Office 365, the PSTN calling number associated with the user will be released. You can assign it to another user.

If the user belongs to a queue group, they will no longer be a viable target of the call queue agents. So, we recommend also removing the user from the groups associated with the call queue.

Set up call forwarding to people in your organization

If you need to set up call forwarding for the terminated employee's phone number, the call forwarding setting under calling policies can set up forwarding where incoming calls can be forwarded to other users or can ring another person at the same time. For more information, see [Calling policies in Microsoft Teams](#).

Step 7 - Delete a former employee's user account

7/28/2021 • 2 minutes to read • [Edit Online](#)

After you've saved and accessed all the former employee's user data, you can delete the former employee's account.

IMPORTANT

Don't delete the account if you've set up email forwarding or converted it to a shared mailbox. Both need the account to anchor the forwarding or shared mailbox.

1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the name of the employee that you want to delete.
3. Under the user's name, select **Delete user**. Choose the options you want for this user, and then select **Delete user**. If you've already given another user access to this user's email and OneDrive, you don't have to do it again here.

When you delete a user, the account becomes inactive for approximately 30 days. You have until then to restore the account before it is permanently deleted.

Watch: Delete a former employee's user account

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

Does your organization use Active Directory?

If your organization synchronizes user accounts to Microsoft 365 from a local Active Directory environment, you must delete and restore those user accounts in your local Active Directory service. You can't delete or restore them in Office 365.

To learn how to delete and restore user account in Active Directory, see [Delete a User Account](#).

If you're using Azure Active Directory, see the [Remove-MsolUser](#) PowerShell cmdlet.

What you need to know about terminating an employee's email session

Here's information about how to get an employee out of email (Exchange).

WHAT YOU CAN DO	HOW YOU DO IT
Terminate a session (such as Outlook on the web, Outlook, Exchange active sync, etc.) and force to open a new session	Reset password

WHAT YOU CAN DO	HOW YOU DO IT
Terminate a session and block access to future sessions (for all protocols)	Disable the account. For example, (in the Exchange admin center or using PowerShell): <pre>Set-Mailbox user@contoso.com - AccountDisabled:\$true</pre>
Terminate the session for a particular protocol (such as ActiveSync)	Disable the protocol. For example, (in the Exchange admin center or using PowerShell): <pre>Set-CASMailbox user@contoso.com - ActiveSyncEnabled:\$false</pre>

The above operations can be done in three places:

IF YOU TERMINATE THE SESSION HERE	HOW LONG IT TAKES
In the Exchange admin center or using PowerShell	Expected delay is within 30 min
In the Azure Active Directory admin center	Expected delay is 60 min
In an on-premises environment	Expected delay is 3 hours or more

How to get fastest response for account termination

Fastest: Use the Exchange admin center (use PowerShell) or Azure Active Directory admin center. In an on-premises environment, it can take several hours to sync the change through DirSync.

Fastest for a user with presence on-premises and in the Exchange Datacenter: Terminate the session using Azure Active Directory admin center/Exchange admin center AND make the change in the on-premises environment as well. Otherwise, the change in Azure Active Directory admin center/Exchange admin center will be overwritten by DirSync.

Related content

[Restore a user](#) (article)

[Reset passwords](#) (article)

Overview of Microsoft 365 Groups for administrators

8/13/2021 • 5 minutes to read • [Edit Online](#)

Microsoft 365 Groups is the foundational membership service that drives all teamwork across Microsoft 365. With Microsoft 365 Groups, you can give a group of people access to a collection of shared resources. These resources include:

- A shared Outlook inbox
- A shared calendar
- A SharePoint document library
- A Planner
- A OneNote notebook
- Power BI
- Yammer (if the group was created from Yammer)
- A Team (if the group was created from Teams)
- Roadmap (if you have Project for the web)
- Stream

With a Microsoft 365 group, you don't have to manually assign permissions to each of these resources. Adding people to the group automatically gives them the permissions they need.

Any user can create a group unless you [limit group creation to a specific set of people](#). If you limit group creation, users who cannot create groups will not be able to create SharePoint sites, Planners, teams, Outlook group calendars, Stream groups, Yammer groups, Shared libraries in OneDrive, or shared Power BI workspaces. These services require the people creating them to be able to create a group. Users can still participate in group activities, such as creating tasks in Planner or using Teams chat, provided they are a member of the group.

Groups have the following roles:

- **Owners** - Group owners can add or remove members and have unique permissions like the ability to delete conversations from the shared inbox or change different settings about the group. Group owners can rename the group, update the description or picture and more.
- **Members** - Members can access everything in the group, but can't change group settings. By default group members can invite guests to join your group, though you can [control that setting](#).
- **Guests** - Group guests are members who are from outside your organization.

Only global admins, user admins, and groups admins can create and manage groups in the [Microsoft 365 admin center](#). You can't be a delegated admin (for example, a consultant who is an admin on behalf of).

As an administrator, you can:

- [Specify who can create groups](#)
- [Create a naming policy for groups in your organization](#)
- [Choose which domain to use when creating a group](#)
- [Manage guest access to groups](#)
- [Recover a deleted group](#) (within 30 days of deletion)

If you prefer a more automated way to manage the lifecycle of your Microsoft 365 groups, you can use expiration policies to expire groups at a specific time interval. The group's owners will get an email 30, 15, and 1

day before the group expiration that allows them to renew the group if it's still needed. See: [Microsoft 365 group Expiration Policy](#).

You can administer your groups from the Microsoft 365 admin center or [by using PowerShell](#).

If you have many users, such as in a large corporation or enterprise, you may have many users who create groups for various purposes. We highly recommend that you review [Plan for governance in Microsoft 365 groups](#) for best practices.

Group limits

The following limits apply to Microsoft 365 Groups:

MAXIMUM...	VALUE
Owners per group	100
Groups a user can create	250
Groups an admin can create	Up to default tenant limit of 500 K
Number of members	More than 1,000, though only 1,000 can access the Group conversations concurrently. Users might notice delays when accessing the calendar and conversations in large groups in Outlook.
Number of Groups a user can be a member of	7,000
File storage	1 Terabyte + 10 GB per subscribed user + any other storage purchased. You can purchase an unlimited amount of extra storage.
Group Mailbox size	50 GB

The default maximum number of Microsoft 365 groups that an organization can have is 500,000. To go beyond the default limit, you must contact Microsoft Support. For more information on Microsoft 365 Groups limits, see [Microsoft 365 Groups - Admin help](#).

Managing your Microsoft 365 groups is more effective when you have actionable information about groups usage. The Microsoft 365 admin center has a reporting tool that lets you see storage use, how many active groups you have, and how users are using the groups. See: [Microsoft 365 Reports in the admin center](#) for more information.

Sensitivity labels

You can create sensitivity labels that the users in your organization can set when they create a Microsoft 365 group. With sensitivity labels, you can configure:

- Privacy (public or private)
- External users access
- Unmanaged device access

For example, you can create a label called *Highly Confidential* and specify that any group created with this label will be private and not allow external users. When users in your organization select this label during group creation, the group will be set to private and group members will not be allowed to add external users to the group.

IMPORTANT

If you are currently using classification labels, they will no longer be available to users who create groups once sensitivity labels are enabled.

For information about creating, managing, and using sensitivity labels, see [Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites](#).

Which Microsoft 365 plans include groups?

Any Microsoft 365 subscription that has Exchange Online and SharePoint Online will support groups. That includes the Business Essentials and Business Premium plans, and the Enterprise E1, E3, and E5 plans. The group takes on the licensing of the person who creates the group (also known as the "organizer" of the group). As long as the organizer has the proper license for whatever features you want the group to have, that license will convey to the group.

NOTE

For more details about Microsoft 365 service families and plans, see [Microsoft 365 plan options](#).

If you have an Exchange-only plan you can still get the shared inbox and shared calendar features of groups in Outlook but you won't get the document library, Planner or any of the other capabilities.

Microsoft 365 groups work with Azure Active Directory. The groups features you get depends on which Azure Active Directory subscription you have, and what licenses are assigned to the organizer of the group.

IMPORTANT

For all the groups features, if you have an Azure AD Premium subscription, users can join the group whether or not they have an AAD P1 license assigned to them. Licensing isn't enforced. Periodically we will generate usage reports that tell you which users are missing a license, and need one assigned to them to be compliant with the licensing requirements. For example, let's say a user doesn't have a license and they are added to a group where the naming policy is enforced. The report will flag for you that they need a license.

Related content

[Learn about Microsoft 365 Groups](#) (article)

[Upgrade distribution lists to Microsoft 365 Groups](#) (article)

[Manage Microsoft 365 Groups with PowerShell](#) (article)

[SharePoint Online Limits](#) (article)

[Organize groups and channels in Microsoft Stream](#) (article)

Compare groups

8/13/2021 • 3 minutes to read • [Edit Online](#)

In the **Groups** section of the Microsoft 365 admin center, you can create and manage these types of groups:

- **Microsoft 365 groups** are used for collaboration between users, both inside and outside your company. They include collaboration services such as SharePoint and Planner.
- **Distribution groups** are used for sending email notifications to a group of people.
- **Security groups** are used for granting access to resources such as SharePoint sites.
- **Mail-enabled security groups** are used for granting access to resources such as SharePoint, and emailing notifications to those users.
- **Shared mailboxes** are used when multiple people need access to the same mailbox, such as a company information or support email address.

Some groups allow dynamic membership or email.

	MICROSOFT 365 GROUPS	DISTRIBUTION GROUPS	SECURITY GROUPS	MAIL-ENABLED SECURITY GROUPS	SHARED MAILBOXES
Mail-enabled	Yes	Yes	No	Yes	Yes
Dynamic membership in Azure AD	Yes	No	Yes	No	No

All of these group types can be used with Power Automate.

Microsoft 365 groups

Microsoft 365 groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 group, members get a group email and shared workspace for conversations, files, and calendar events, Stream and a Planner.

You can add people from outside your organization to a group as long as this has been [enabled by the administrator](#). You can also allow external senders to send email to the group email address.

Microsoft 365 groups can be [configured for dynamic membership in Azure Active Directory](#), allowing group members to be added or removed automatically based on user attributes such as department, location, title, etc.

Microsoft 365 groups can be accessed through mobile apps such as Outlook for iOS and Outlook for Android.

Group members can send as or send on behalf of the group email address if this has been [enabled by the administrator](#).

Microsoft 365 groups don't support nesting with other Microsoft 365 groups or with distribution or security groups.

Distribution groups

Distribution groups are used for sending notifications to a group of people. They can receive external email if enabled by the administrator.

Distribution groups are best for situations where you need to broadcast information to a set group of people, such as "People in Building A" or "Everyone at Contoso."

Distribution groups can be [upgraded to Microsoft 365 groups](#).

Distribution groups can be added to a team in Microsoft Teams.

Microsoft 365 groups can't be members of distribution groups.

Security groups

[Security groups](#) are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.

Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.

Security groups can be [configured for dynamic membership in Azure Active Directory](#), allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.

Security groups can be added to a team.

Microsoft 365 groups can't be members of security groups.

Mail-enabled security groups

Mail-enabled security groups function the same as regular security groups, except that they cannot be dynamically managed through Azure Active Directory and cannot contain devices.

They include the ability to send mail to all the members of the group.

Mail-enabled security groups can be added to a team.

Shared mailboxes

[Shared mailboxes](#) are used when multiple people need access to the same mailbox, such as a company information or support email address, reception desk, or other function that might be shared by multiple people.

Shared mailboxes can receive external emails if the administrator has enabled this.

Shared mailboxes include a calendar that can be used for collaboration.

Users with permissions to the group mailbox can send as or send on behalf of the mailbox email address if the administrator has given that user permissions to do that. This is particularly useful for help and support mailboxes because users can send emails from "Contoso Support" or "Building A Reception Desk."

It's not possible to migrate a shared mailbox to a Microsoft 365 group.

Related content

[Learn about Microsoft 365 groups](#)

[Upgrade distribution lists to Microsoft 365 Groups in Outlook](#)

[Why you should upgrade your distribution lists to groups in Outlook](#)

Create a group in the Microsoft 365 admin center

8/13/2021 • 2 minutes to read • [Edit Online](#)

While users can create a Microsoft 365 group from Outlook or other apps, as an admin, you may need to create or delete groups, add or remove members, and customize how they work. The [Microsoft 365 admin center](#) is the place to do this.

TIP

Microsoft 365 connected Yammer groups must be created in Yammer, but can be managed in the Microsoft 365 admin center like other Microsoft 365 groups. To learn more, see [Yammer and Microsoft 365 groups](#).

Create a Microsoft 365 group

1. In the admin center, expand **Groups**, and then click **Groups**.
2. Select **Add a group**.
3. On the **Choose a group type** page, select **Office 365**, and select **Next**.
4. On the **Basics** page, type a name for the group, and, optionally, a description. Select **Next**.
5. On the **Edit settings** page, type a unique email address for the group, choose a privacy option and whether you want to add Microsoft Teams, and then select **Next**.
6. On the **Owners** choose the name of one or more people who will be designated to manage the group. Anyone who is a group owner will be able to delete email from the Group inbox. Other members won't be able to delete email from the Group inbox. Select **Next**.
7. After reviewing your settings and making any changes, select **Create group**.
8. Select **Close**.

Add members to the group

Once the group has been created, you can add members and configure additional settings.

Users can [add themselves or request approval](#), or you can add them now.

1. In the admin center, refresh the page so your new group appears, and then select the name of the group that you want to add members to.
2. On the **Members** tab, select **View all and manage members**.
3. Select **Add members**.
4. Select the users you want to add, and then select **Save**.
5. Select **Close** three times.

The group will appear in Outlook with members assigned to it.

Who can delete email from the Group inbox?

The Group owner can delete any emails from the Group Inbox, regardless of whether they were the initial

author.

A member can delete an email conversation from the Group inbox if they initiated it, and only using Outlook on the web (right-click the email, then choose **Delete**). They can't do it from the Outlook app (Outlook 2016).

When an email is deleted from the group mailbox, it is not deleted from any of the group members' personal mailboxes.

Next steps

After creating a new group and adding members, you can further configure your group, such as editing the group name or description, changing owners or members, and specifying whether external senders can email the group and whether to send copies of group conversations to members. See [Manage a Microsoft 365 group](#) for information.

Related content

[Manage guest access to Microsoft 365 groups](#) (article)

[Choose the domain to use when creating Microsoft 365 groups](#) (article)

[Upgrade distribution lists to Microsoft 365 groups](#) (article)

Explaining Microsoft 365 Groups to your users

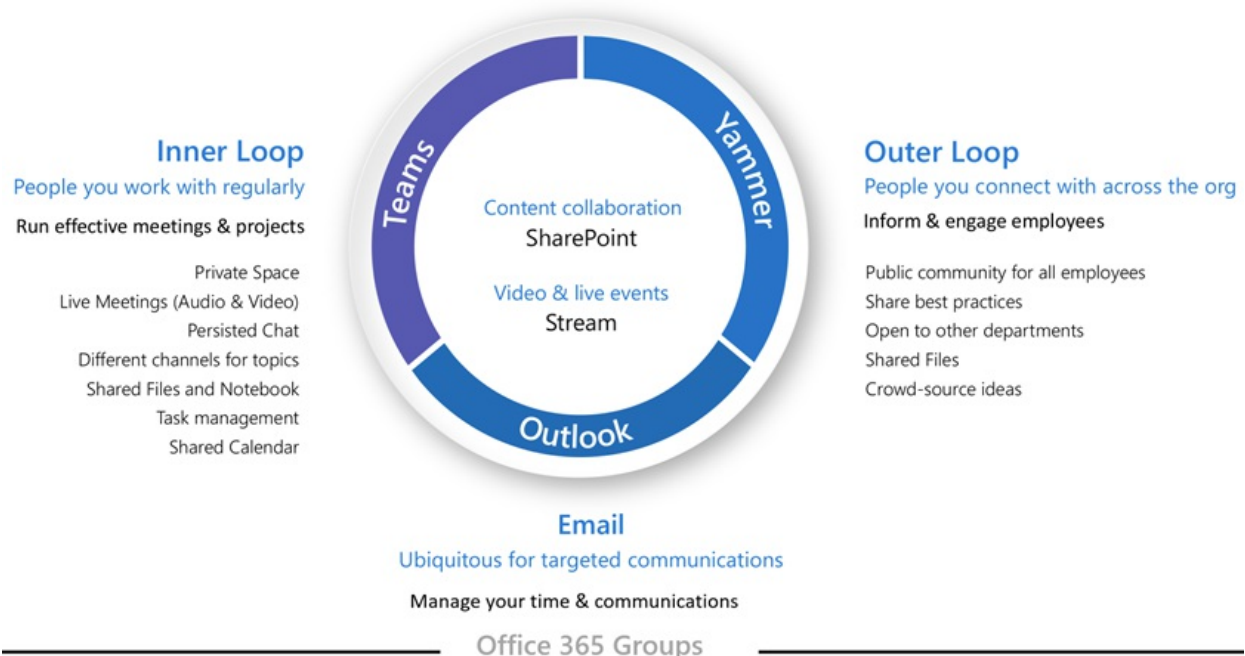
3/5/2021 • 2 minutes to read • [Edit Online](#)

Microsoft 365 Groups allow you to set up a collection of resources to share, including a shared mailbox and calendar, a SharePoint site with a OneNote notebook, and a Microsoft Planner among others. Microsoft Teams can also be included when you create a group, or it can be added later. Permissions groups resources are managed via the group.

Groups can be created by creating any of the shared resources. Creating a group in Outlook yields the same result as creating a group-connected SharePoint team site or a plan in Planner. If your users are new to Microsoft 365 Groups, they may not realize this. This can lead to confusion for your users and the possibility of creating duplicate resources. (For examples, someone might create a SharePoint site for document collaboration and later create a separate instance of Planner, not realizing Planner was already available as part of the group.)

Because groups can be created in several ways, we recommend training your users to use the method that fits your organization the best:

- If your organization does most of its communication using email, instruct your users to create groups in Outlook.
- If your organization heavily uses SharePoint or is migrating from SharePoint on-premises, instruct your users to create SharePoint team sites for collaboration.
- If your organization has deployed Teams, instruct your users to create a team when they need a collaboration space.



If you train your users to always use the group creation method that most aligns with their way of working when they need a space to collaborate with others, you can help avoid confusion and duplication of resources. As users become more experienced, they will understand better the collection of services that come with a group and that different creation methods lead to the same result.

You can use the [Microsoft 365 Groups for Business User - PowerPoint template](#) as a starting point for training presentations for your users.

Related topics

[Learn about Microsoft 365 Groups](#)

Manage a group in the Microsoft 365 admin center

8/13/2021 • 3 minutes to read • [Edit Online](#)

After you have [created a Microsoft 365 group](#) and added group members, you can configure your group. You can edit the group name or description, manage owners or members, and specify whether external senders can email the group and whether to send copies of group conversations to members.

Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.

Edit the group name or description

1. In the admin center, expand **Groups**, and then click **Groups**.
2. Select the group that you want to edit, and then click **Edit name and description**.
3. Update the name and description, and then select **Save**.

Manage group owners and members

1. In the admin center, expand **Groups**, and then click **Groups**.
2. Click the name of the group you want to manage to open the settings pane.
3. On the **Members** tab, choose if you want to manage owners or members.
4. Choose **Add** to add someone or click **X** to remove someone.
5. Click **Close**.

Send copies of conversations to group members' inboxes

When you use the admin center to create a group, by default users do not get copies of group emails sent to their inboxes though users get copies of group meeting invitations sent to their inboxes. They'll need to go to the group to see conversations. You can change this setting in the admin center.

When you turn this setting on, group members will get a copy of group emails and meeting invitations sent to their Outlook Inbox. They can read and delete this copy of the email and not affect anyone else. In the Group inbox, a copy of the email still exists.

Group members can opt out of receiving these emails by choosing to stop following the group in Outlook.

1. In the admin center, expand **Groups**, and then click **Groups**.
2. Click the name of the group you want to manage to open the settings pane.
3. On the **Settings** tab, select **Send copies of group conversations and events to group members** if you want members to receive copies of group messages and calendar items in their own inbox.
4. Select **Save**.

Let people outside the organization email the group

This option is great if you want to have a company email address such as info@contoso.com.

1. In the admin center, expand **Groups**, and then click **Groups**.

2. Click the name of the group you want to manage to open the settings pane.
3. In the admin center groups list, select the name of the group you want to change, and then on the **Settings** tab, select **Allow external senders to email this group**.
4. Select **Save**.

Permanently delete a Microsoft 365 group

Sometimes you may want to permanently purge a group without waiting for the 30 day soft-deletion period to expire. To do that, start PowerShell and run this command to get the object ID of the group:

```
`Get-AzureADMSDeletedGroup`
```

Take note of the object ID of the group, or groups, that you want to permanently delete.

Caution

Purging the group removes the group and its data forever.

To purge the group run this command in PowerShell:

```
`Remove-AzureADMSDeletedDirectoryObject -Id <objectId>`
```

To confirm that the group has been successfully purged, run the *Get-AzureADMSDeletedGroup* cmdlet again to confirm that the group no longer appears on the list of soft-deleted groups. In some cases it may take as long as 24 hours for the group and all of its data to be permanently deleted.

Related articles

[Create a Microsoft 365 group](#)

[Manage guest access to Microsoft 365 groups](#)

[Choose the domain to use when creating Microsoft 365 groups](#)

[Allow members to send as or send on behalf of a Microsoft 365 group](#)

[Upgrade distribution lists to Microsoft 365 groups](#)

[Manage Microsoft 365 groups with PowerShell](#)

Add or remove members from Microsoft 365 groups using the admin center

7/12/2021 • 2 minutes to read • [Edit Online](#)

In Microsoft 365, group members typically create their own groups, add themselves to groups they want to join, or are invited by group owners. If group ownership changes, or if you determine that a member should be added or removed, as the admin you can also make that change. Only a global administrator, Exchange administrator, Groups administrator, or user administrator can make these changes. [What is a Microsoft 365 group?](#)

TIP

If you're not an admin, you can [add or remove members using Outlook](#).

Add a member to a group in the admin center

1. In the admin center, go to the [Active groups](#) page.
2. Click a group name.
3. In the details pane, on the **Members** tab, select **View all and manage members**, and then select **Add members**.
4. Search for or select the name of the member you want to add.
5. Select **Save**.

Add a group to a member in the admin center

1. In the admin center, go to the [Active users](#) page.
2. Click a user.
3. In the details pane, on the **Account** tab, select **Manage groups**.
4. Search for or select the name of the group you want to add.
5. Select **Save**.

Remove a member from a group in the admin center

NOTE

When you remove a member from a private group, it takes 5 minutes for the person to be blocked from the group.

1. In the admin center, go to the [Active groups](#) page.
2. Click a group name.
3. In the details pane, on the **Members** tab, select **View all and manage members**.
4. Next to the member you want to remove, select the X.

5. Select **Save** to remove the member.

Manage group owner status

By default, the person who created the group is the group owner. Often a group will have multiple owners for backup support or other reasons. Members can be promoted to owner status and owners can be demoted to member status.

Promote a member to owner status in the admin center

1. In the admin center, go to the [Active groups](#) page.
2. Click a group name.
3. In the details pane, on the **Members** tab, select **View all and manage owners**.
4. Select **Add owners**.
5. Select the check box next to the name of the member you want to add.
6. Select **Save**, and then **Close**.

Remove owner status in the admin center

1. In the admin center, go to the [Active groups](#) page.
2. Click a group name.
3. In the details pane, on the **Members** tab, select **View all and manage owners**.
4. Select the X next to the owner's name.
5. Select **Save**.

Next steps

- [Manage groups dynamically in Azure Active Directory](#): see the section "How can I manage the membership of a group dynamically?"
- To add hundreds or thousands of users to groups, use the [Add-UnifiedGroupLinks](#).
- [Assign a new owner to an orphaned group](#)

Related content

[Upgrade distribution lists to Microsoft 365 groups in Outlook](#) (article)

[Why you should upgrade your distribution lists to groups in Outlook](#) (article)

[Manage guest access in Microsoft 365 groups](#) (article)

[Manage Microsoft 365 groups with PowerShell](#): this article introduces you to key cmdlets and provides examples (article)

[Microsoft 365 groups naming policy](#) (article)

Restore a deleted Microsoft 365 group

7/12/2021 • 2 minutes to read • [Edit Online](#)

If you've deleted a group, it will be retained for 30 days by default. This 30-day period is considered a "soft-delete" because you can still restore the group. After 30 days, the group and its associated contents are permanently deleted and cannot be restored.

When a group is restored, the following content is restored:

- Azure Active Directory (AD) Microsoft 365 Groups object, properties, and members.
- Group's e-mail addresses.
- Exchange Online shared Inbox and calendar.
- SharePoint Online team site and files.
- OneNote notebook
- Planner
- Teams
- Yammer group and group content (If the Microsoft 365 group was created from Yammer)

NOTE

This article describes restoring only Microsoft 365 groups. All other groups cannot be restored once deleted.

Restore a group

- [Outlook](#)
- [Admin center](#)

If you are the owner of a Microsoft 365 group, you can restore the group yourself in Outlook on the web by following these steps:

1. On the [deleted groups page](#), select the **Manage groups** option under the **Groups** node, and then choose **Deleted**.
2. Click on the **Restore** tab next to the group you want to restore.

If the deleted group doesn't appear here, contact an administrator.

Got questions about Microsoft 365 Groups?

Visit the [Microsoft Tech Community](#) to post questions and participate in conversations about Microsoft 365 groups.

Related content

[Manage Microsoft 365 Groups with PowerShell](#) (article)

[Delete groups using the Remove-UnifiedGroup cmdlet](#) (article)

[Manage your group-connected team site settings](#) (article)

[Delete a group in Outlook \(article\)](#)

Manage guest access in Microsoft 365 groups

8/13/2021 • 2 minutes to read • [Edit Online](#)

By default, guest access for Microsoft 365 groups is turned on for your organization. Admins can control whether to allow guest access to groups for their whole organization or for individual groups.

When it's turned on, group members can invite guest users to a Microsoft 365 group through Outlook on Web. Invitations are sent to the group owner for approval.

Once approved, the guest user is added to the directory and the group.

NOTE

Yammer Enterprise networks that are in Native Mode or the [EU Geo](#) do not support network guests. Microsoft 365 Connected Yammer groups do not currently support guest access, but you can create non-connected, external groups in your Yammer network. See [Create and manage external groups in Yammer](#) for instructions.

Guest access in groups is often used as part of a broader scenario that includes SharePoint or Teams. These services have their own guest sharing settings. For complete instructions for setting up guest sharing across groups, SharePoint, and Teams, see:

- [Collaborate with guests in a site](#)
- [Collaborate with guests in a team](#)

Manage groups guest access

If you want to enable or disable guest access in groups, you can do so in the [Groups](#).

1. In the admin center, go to **Show all** > **Settings** > **Org settings** and on the **Services** tab, select [Microsoft 365 Groups](#).
2. On the **Microsoft 365 Groups** page, choose whether you want to let people outside your organization access group resources or let group owners add people outside your organization to groups.

Add guests to a Microsoft 365 group from the admin center

If the guest already exists in your directory, you can add them to your groups from the [Microsoft 365 admin center](#). (Groups with dynamic membership must be [managed in Azure Active Directory](#).)

1. In the admin center, go to the **Groups** > [Groups](#).
2. Click the group you want to add the guest to, and select **View all and manage members** on the **Members** tab.
3. Select **Add members**, and choose the name of the guest you want to add.
4. Select **Save**.

If you want to add a guest to the directory directly, you can [Add Azure Active Directory B2B collaboration users in the Azure portal](#).

If you want to edit any of a guest's information, you can [Add or update a user's profile information using Azure Active Directory](#).

Related content

[Block guest users from a specific group](#) (article)

[Manage group membership in the Microsoft 365 admin center](#) (article)

[Azure Active Directory access reviews](#) (article)

[Set-AzureADUser](#) (article)

Reset passwords

7/12/2021 • 3 minutes to read • [Edit Online](#)

This article explains how to reset passwords for yourself and for your users when you have an Microsoft 365 for business subscription.

Before you begin

This article is for people who set password expiration policy for a business, school, or nonprofit. To complete these steps, you need to sign in with your Microsoft 365 admin account. [What's an admin account?](#)

You must be an [global admin or password administrator](#) to perform these steps.

Watch: Reset a business password for a user

Watch a short video about resetting user passwords.

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

Steps: Reset a business password for a user

1. In the admin center, go to the **Users** > [Active users](#) page.
2. On the **Active users** page, select the user and then select **Reset password**.
3. Follow the instructions on the **Reset password** page to auto-generate a new password for the user or create one for them, and then select **Reset**.
4. Enter an email address the user can get to so they receive the new password, and follow up with them to make sure they got it.

Let users reset their own passwords

We strongly recommend that you set up self-service password reset. This way you don't have to manually reset passwords for your users. To learn how, see [Let users reset their own passwords in Office 365](#).

Reset my admin password

Use these steps if you forgot your password but you're able to sign in to Microsoft 365 because, for example, your password is saved in your browser:

1. Select your name (icon) in upper right corner > **My Account** > **Personal Info**.
2. Under **Contact details**, double-check that your **Alternate email** is accurate and that you've provided a mobile phone number. If not, change them now.
3. Sign out: select your name in the upper right corner > **Sign out**.
4. Now sign in again: type your user name > **Next** > and then select **Forgot password**.
5. Follow the steps in the wizard to reset your password. It uses your alternate contact info to verify you're

the right person to reset your password.

If you forgot your password and can't sign in:

- Ask another global admin in your business to reset your password for you.
- Make sure you've provided alternate contact information, including a mobile phone number.
- Or, [call Microsoft Support](#).

Reset all business passwords for everyone in your organization at the same time

These steps work for a business with tens of users. If you have hundreds or thousands of users, see the next section on resetting passwords in bulk (maximum 40 users at a time).

1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the option next to **Display name** to select everyone in your business. Then unselect yourself. You can't reset your own password at the same time you reset everyone else's password.
3. Select **Reset password**.
4. Follow the instructions on the **Reset password** page, and select **Reset**. If you opted for auto-generating the passwords, the new temporary passwords will be displayed.
5. Enter an email address where you can receive the temporary passwords. You'll need to notify your users what their temporary passwords are.

Reset business passwords in bulk

Use PowerShell! Check out this post by Eyal Doron: [Managing passwords with PowerShell](#).

For overview information, see [Manage Microsoft 365 with PowerShell](#).

Force a password change for all users in your business

Check out this great blog post by Vasil Michev, Microsoft MVP: [Force password change for all users in Office 365](#).

I don't have a Microsoft 365 for business subscription

Try this article: [I forgot the username or password for the account I use with Office](#).

Related content

[Let users reset their own passwords](#) (article)

[Reset passwords](#) (article)

[Set an individual user's password to never expire](#) (article)

[Set the password expiration policy for your organization](#) (article)

[Microsoft 365 for business training videos](#) (link page)

Let users reset their own passwords

7/27/2021 • 2 minutes to read • [Edit Online](#)

As the Microsoft 365 admin, you can let people use the [self-service password reset tool](#) so you don't have to reset passwords for them. Less work for you!

Before you begin

- You get self-service password reset for cloud users **free** with any Microsoft 365 business, education, or nonprofit paid plan. It doesn't work with Microsoft 365 trial.
- It uses Azure. You'll automatically get this feature in Azure for **free** when you do these steps. It won't cost you anything to turn on self-service password reset if you don't use other Azure features.
- **If you're using an on-premises Active Directory**, the above two points don't apply. Rather, you can set this up but it **requires a paid subscription to Azure AD Premium**.

This article is for people who set password expiration policy for a business, school, or nonprofit. To complete these steps, you need to sign in with your Microsoft 365 admin account. [What's an admin account?](#)

You must be an [global admin or password administrator](#) to perform these steps.

Watch: Let users reset their own passwords

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

Steps: Let people reset their own passwords

These steps turn on self-service password reset for everyone in your business.

1. In the [admin center](#), go to the **Settings > Org settings** page.
2. At the top of the **Org settings** page, select the **Security & Privacy** tab.
3. Select **Self-service Password Reset**.
4. Under **Self-service password reset**, select **Go to the Azure portal to turn on self-service password reset**.
5. On the **Properties** page, select **All** to enable it for everyone in your business, and then select **Save**.
6. When your users sign in, they will be prompted to enter additional contact information that will help them reset their password in the future.

Related content

[Set the password expiration policy for your organization](#) (article)

[Set an individual user's password to never expire](#) (article)

[Microsoft 365 Business training videos](#) (link page)

Set an individual user's password to never expire

7/12/2021 • 2 minutes to read • [Edit Online](#)

This article explains how to set a password for an individual user to not expire. You have to complete these steps using PowerShell.

Before you begin

This article is for people who set password expiration policy for a business, school, or nonprofit. To complete these steps, you need to sign in with your Microsoft 365 admin account. [What's an admin account?](#)

You must be an [global admin or password administrator](#) to perform these steps.

A global admin for a Microsoft cloud service can use the [Azure Active Directory PowerShell for Graph](#) to set passwords not to expire for specific users. You can also use [AzureAD](#) cmdlets to remove the never-expires configuration or to see which user passwords are set to never expire.

This guide applies to other providers, such as Intune and Microsoft 365, which also rely on Azure AD for identity and directory services. Password expiration is the only part of the policy that can be changed.

How to check the expiration policy for a password

For more information about the `Get-AzureADUser` command in the `AzureAD` module, see the reference article [Get-AzureADUser](#).

Run one of the following commands:

- To see if a single user's password is set to never expire, run the following cmdlet by using the UPN (for example, `user@contoso.onmicrosoft.com`) or the user ID of the user you want to check:

```
Get-AzureADUser -ObjectId <user id or UPN> | Select-Object UserprincipalName,@{
    N="PasswordNeverExpires";E={$_.PasswordPolicies -contains "DisablePasswordExpiration"}
}
```

Example:

```
Get-AzureADUser -ObjectId userUPN@contoso.com | Select-Object UserprincipalName,@{
    N="PasswordNeverExpires";E={$_.PasswordPolicies -contains "DisablePasswordExpiration"}
}
```

- To see the **Password never expires** setting for all users, run the following cmdlet:

```
Get-AzureADUser -All $true | Select-Object UserprincipalName,@{
    N="PasswordNeverExpires";E={$_.PasswordPolicies -contains "DisablePasswordExpiration"}
}
```

- To get a report of all the users with `PasswordNeverExpires` in HTML on the desktop of the current user with name `ReportPasswordNeverExpires.html`

```
Get-AzureADUser -All $true | Select-Object UserprincipalName,@{
    N="PasswordNeverExpires";E={$_.PasswordPolicies -contains "DisablePasswordExpiration"}
} | ConvertTo-Html | Out-File $env:userprofile\Desktop\ReportPasswordNeverExpires.html
```

- To get a report of all the users with PasswordNeverExpires in CSV on the desktop of the current user with name **ReportPasswordNeverExpires.csv**

```
Get-AzureADUser -All $true | Select-Object UserprincipalName,@{
    N="PasswordNeverExpires";E={$_.PasswordPolicies -contains "DisablePasswordExpiration"}
} | ConvertTo-Csv -NoTypeInfo | Out-File
$env:userprofile\Desktop\ReportPasswordNeverExpires.csv
```

Set a password to never expire

Run one of the following commands:

- To set the password of one user to never expire, run the following cmdlet by using the UPN or the user ID of the user:

```
Set-AzureADUser -ObjectId <user ID> -PasswordPolicies DisablePasswordExpiration
```

- To set the passwords of all the users in an organization to never expire, run the following cmdlet:

```
Get-AzureADUser -All $true | Set-AzureADUser -PasswordPolicies DisablePasswordExpiration
```

WARNING

User accounts configured with the `-PasswordPolicies DisablePasswordExpiration` parameter still age based on the `pwdLastSet` attribute. Based on the `pwdLastSet` attribute, if you change the expiration to `-PasswordPolicies None`, all passwords that have a `pwdLastSet` older than 90 days require the user to change them the next time they sign in. This change can affect a large number of users.

Set a password to expire

Run one of the following commands:

- To set the password of one user so that the password expires, run the following cmdlet by using the UPN or the user ID of the user:

```
Set-AzureADUser -ObjectId <user ID> -PasswordPolicies None
```

- To set the passwords of all users in the organization so that they expire, use the following cmdlet:

```
Get-AzureADUser -All $true | Set-AzureADUser -PasswordPolicies None
```

Related content

[Let users reset their own passwords](#) (article)

[Reset passwords](#) (article)

[Set the password expiration policy for your organization](#) (article)

Resend a user's password - Admin Help

6/8/2021 • 2 minutes to read • [Edit Online](#)

This article explains how to resend the notification email to a new user in Office 365. This can happen when you create a new user and they don't get an email with their new password. You do this by resetting the user's password.

Before you begin

This article is for people who set password expiration policy for a business, school, or nonprofit. To complete these steps, you need to sign in with your Microsoft 365 admin account. [What's an admin account?](#)

You must be an [global admin](#) or [password administrator](#) to perform these steps.

Resend user password

1. In the admin center, go to the **Users** > [Active users](#) page.
2. On the **Active users** page, select the user and then select **Reset password**.
3. Follow the instructions on the **Reset password** page to auto-generate a new password for the user or create one for them, and then select **Reset**.
4. Enter an email address the user can get to so they receive the new password, and follow up with them to make sure they got it.

Related content

[Let users reset their own passwords](#)

[Reset passwords](#)

Turn off strong password requirements for users

7/19/2021 • 2 minutes to read • [Edit Online](#)

This article explains how to turn off strong password requirements for your users. Strong password requirements are turned on by default in your Microsoft 365 for business organization. Your organization might have requirements to disable strong passwords. Follow the steps below to turn off strong password requirements. You have to complete these steps using PowerShell.

Before you begin

This article is for people who manage password policy for a business, school, or nonprofit. To complete these steps, you need to sign in with your Microsoft 365 admin account. [What's an admin account?](#) You must be an [global admin or password administrator](#) to perform these steps.

You must also connect to Microsoft 365 with PowerShell.

Set strong passwords

1. [Connect to Microsoft 365 with PowerShell.](#)
2. Using PowerShell, you can turn off strong password requirements for all users with the following command:

```
Get-MsolUser | Set-MsolUser -StrongPasswordRequired $false
```

3. You can turn OFF strong password requirements for specific users with this command:

```
Set-MsolUser -UserPrincipalName -StrongPasswordRequired $false
```

NOTE

The userPrincipalName must be in the Internet-style sign-in format where the user name is followed by the at sign (@) and a domain name. For example: user@contoso.com.

Related content

[How to connect to Microsoft 365 with PowerShell](#)

[More information on PowerShell MsolUser commands](#)

[More information on password policy](#)

Set the password expiration policy for your organization

8/13/2021 • 3 minutes to read • [Edit Online](#)

Before you begin

This article is for people who set password expiration policy for a business, school, or nonprofit. To complete these steps, you need to sign in with your Microsoft 365 admin account. [What's an admin account?](#)

As an admin, you can make user passwords expire after a certain number of days, or set passwords to never expire. By default, passwords are set to never expire for your organization.

Current research strongly indicates that mandated password changes do more harm than good. They drive users to choose weaker passwords, re-use passwords, or update old passwords in ways that are easily guessed by hackers. We recommend enabling [multi-factor authentication](#). To learn more about password policy, check out [Password policy recommendations](#).

You must be a [global admin](#) to perform these steps.

If you're a user, you don't have the permissions to set your password to never expire. Ask your work or school technical support to do the steps in this article for you.

Set password expiration policy

Follow the steps below if you want to set user passwords to expire after a specific amount of time.

1. In the Microsoft 365 admin center, go to the [Security & privacy tab](#).
If you aren't a global admin, you won't see the Security and privacy option.
2. Select **Password expiration policy**.
3. If you don't want users to have to change passwords, uncheck the box next to **Set user passwords to expire after a number of days**.
4. Type how often passwords should expire. Choose a number of days from 14 to 730.
5. In the second box type when users are notified that their password will expire, and then select **Save**.
Choose a number of days from 1 to 30.

NOTE

Password expiration notifications are no longer supported in the Office 365 portal or any Office apps except Outlook.

Important things you need to know about the password expiration feature

People who only use the Outlook app won't be forced to reset their Microsoft 365 password until it expires in the cache. This can be several days after the actual expiration date. There's no workaround for this at the admin level.

Prevent last password from being used again

If you want to prevent your users from recycling old passwords, you can do so by enforcing password history in on-premises Active Directory (AD). See [Create a custom password policy](#).

In Azure AD, The last password can't be used again when the user changes a password. The password policy is applied to all user accounts that are created and managed directly in Azure AD. This password policy can't be modified. See [Azure AD password policies](#).

Synchronize user passwords hashes from an on-premises Active Directory to Azure AD (Microsoft 365)

This article is for setting the expiration policy for cloud-only users (Azure AD). It doesn't apply to hybrid identity users who use password hash sync, pass-through authentication, or on-premises federation like ADFS.

To learn how to synchronize user password hashes from on premises AD to Azure AD, see [Implement password hash synchronization with Azure AD Connect sync](#).

Password policies and account restrictions in Azure Active Directory

You can set more password policies and restrictions in Azure active directory. Check out [Password policies and account restrictions in Azure Active Directory](#) for more info.

Update password Policy

The Set-MsolPasswordPolicy cmdlet updates the password policy of a specified domain or tenant. Two settings are required; the first is to indicate the length of time that a password remains valid before it must be changed and the second is to indicate the number of days before the password expiration date that will trigger when users will receive their first notification that their password will soon expire.

To learn how to update password policy for a specific domain or tenant, see [Set-MsolPasswordPolicy](#).

Related content

[Let users reset their own passwords](#) (article)\

[Reset passwords](#) (article)

User email settings

3/17/2021 • 2 minutes to read • [Edit Online](#)

As the admin of an organization, there are email settings you can manage on your users. This article gives you information on managing these settings.

Summary of email settings

This table explains the various email settings you can change for a user in Microsoft 365.

MAIL SETTING	DESCRIPTION
Mailbox permissions	Read and manage allows you to set whether people can read and manage other people's mailboxes. You can also set Send as and Send on behalf permissions for a person. Check out Give mailbox permissions to another user in Microsoft 365 - Admin Help for more details.
Email apps	Email apps allows you to choose the apps a user can use to access their Microsoft email.
Show in global address list	Show in global address list allows you to enable or disable the visibility of the user's mailbox in the organization's address list.
Email forwarding	Email forwarding allows you to add a forwarding email address to a user. You might want to do this if the person has multiple email addresses and they want to receive emails at all their email addresses. Check out Configure email forwarding in Microsoft 365 for more details.
Automatic replies	Automatic replies allows you to set an automatic reply when someone sends an email to the person's email address. You might want to do this if an employee leaves your company and you want to let the email sender know.
More actions	Convert to shared mailbox allows you to convert the user's mailbox to a shared mailbox. You might do this if the person leaves your organization and you want to keep their mailbox data around for a while. Check out Convert a user mailbox to a shared mailbox and Open and use a shared mailbox . Edit Exchange properties allows you to manage additional Exchange Online tasks using the Exchange admin center. Read about managing user mailboxes in Exchange Online .

NOTE

¹ You can only manage email apps for mailboxes that are hosted fully in Microsoft 365. You cannot use this feature to manage email apps for mailboxes that are hosted on-premises.

Add another email alias for a user

7/12/2021 • 3 minutes to read • [Edit Online](#)

This article is for Microsoft 365 administrators who have business subscriptions. It's not for home users.

A primary email address in Microsoft 365 is usually the email address a user was assigned when their account was created. When the user sends email to someone else, their primary email address is what typically appears in the *From* field in email apps. They can also have more than one email address associated with their Microsoft 365 for business account. These additional addresses are called aliases.

For example, let's say Jenna has the email address jenna@contosoco.com, but she also wants to receive email at jen@contosoco.com because some people refer to her by that name. You can create aliases for her so that both email addresses go to Jenna's inbox.

You can create up to 400 aliases for a user. No additional fees or licenses are required.

TIP

If you want multiple people to manage email sent to a single email address like info@NodPublishers.com or sales@NodPublishers.com, create a shared mailbox. To learn more, see [Create a shared mailbox](#).

Add email aliases to a user

You must have [admin permissions](#) to do this.

1. In the admin center, go to the **Users** > [Active users](#) page.
2. On the **Active Users** page, select the user > **Manage username and email**. You won't see this option if the person doesn't have a license assigned to them.
3. Select **+ Add an alias** and enter a new alias for the user.

IMPORTANT

If you get the error message "**A parameter cannot be found that matches parameter name 'EmailAddresses,**" it means that it's taking a bit longer to finish setting up your tenant, or your custom domain if you recently added one. The setup process can take up to 4 hours to complete. Wait a while so the set up process has time to finish, and then try again. If the problem persists, call Support and they will do a full sync for you.

IMPORTANT

If you purchased your subscription from GoDaddy or another Partner, to set the new alias as the primary, you must go to the GoDaddy/partner management console.

TIP

The email alias must end with a domain from the drop-down list. To add another domain name to the list, see [Add a domain to Microsoft 365](#).

4. When you're done, choose **Save changes**.

5. Wait 24 hours for the new aliases to populate throughout Microsoft 365.

The user will now have a primary address and an alias. For example, all mail sent to Eliza Hoffman's primary address, Eliza@NodPublishers.com, and her alias, Sales@NodPublishers.com, will go to Eliza's Inbox.

6. **When the user replies, the *From* address will depend on her Outlook client. Outlook on the web will use the alias at which the email was received (we'll call this the ping-pong principle). Outlook desktop will use her primary email alias.** For example, let's say a message is sent to Sales@NodPublishers.com, and it arrives in Eliza's inbox. When Eliza replies to the message using Outlook desktop, her primary email address will appear as Eliza@NodPublishers.com, not Sales@NodPublishers.com.

Did you get "A parameter cannot be found that matches parameter name EmailAddresses"?

If you get the error message "A parameter cannot be found that matches parameter name EmailAddresses" it means that it's taking a bit longer to finish setting up your tenant, or your custom domain if you recently added one. The setup process can take up to 4 hours to complete. Wait a while so the set up process has time to finish, and then try again. If the problem persists, call Support and they will do a full sync for you.

Did you purchase your subscription from GoDaddy or another Partner?

If you purchased your subscription from GoDaddy or another Partner, to set the new alias as the primary, you must go to the GoDaddy/partner management console.

Sending email from the proxy address easily

A new feature is rolling out in July 2021 that allows users to send from their aliases easily when using Outlook on the web. When the feature rolls out to a tenancy where the tenant admin uses the

`Set-OrganizationConfig -SendFromAliasEnabled $true` cmdlet, users within the tenancy will get access to a list of checkboxes where each entry corresponds to an alias in their Outlook settings. Selecting an alias will make it appear in the From dropdown in the Compose form.

Related content

[Send email from a different address](#) (article)

[Change a user name and email address](#) (article)

[Configure email forwarding in Microsoft 365](#) (article)

Change your email address to use your custom domain

7/12/2021 • 2 minutes to read • [Edit Online](#)

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

Your initial email address in Microsoft 365 includes .onmicrosoft.com, like tom@fourthcoffee.onmicrosoft.com. You can change it to a friendlier address like tom@fourthcoffee.com. You'll need your own domain name, like fourthcoffee.com first. If you already have one, great! If not, you can learn how to [buy one from a domain registrar](#).

Your initial email address in Office 365 Germany includes .onmicrosoft.de, like tom@fourthcoffee.onmicrosoft.de. You can change it to a friendlier address like tom@fourthcoffee.de. You'll need your own domain name, like fourthcoffee.de first. If you already have one, great! If not, you can learn how to [buy one from a domain registrar](#).

Your initial email address in Office 365 operated by 21Vianet includes partner.onmschina.cn, like tom@fourthcoffee.partner.onmschina.cn. You can change it to a friendlier address like tom@fourthcoffee.cn. You'll need your own domain name, like fourthcoffee.cn first. If you already have one, great! If not, you can learn how to [buy one from a domain registrar](#).

When you change your domain's email to come to Microsoft 365, by updating your domain's MX record during setup, ALL email sent to that domain will start coming to Microsoft 365. Make sure you've added users and created mailboxes in Microsoft 365 for everyone who has email on your domain BEFORE you change the MX record. Don't want to move email for everyone on your domain to Microsoft 365? You can take steps to [pilot Microsoft 365 with just a few email addresses instead](#).

Change your email address to use your custom domain using the Microsoft 365 admin center

You must be a global admin to perform these steps.

1. Go to the admin center at <https://admin.microsoft.com>.
1. Go to the admin center at <https://portal.office.de/adminportal>.
1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Go to the **Setup > Domains** page.
3. On the **Domains** page, select **Add domain**.
4. Follow the steps to confirm that you own your domain. You'll be guided to get everything set up correctly with your domain in Microsoft 365.
5. Go to **Users > Active users**.
6. Select a user to edit their username and change it to the domain you just added.

NOTE

If you are not using an Exchange license, you cannot use the domain to send or receive emails from the Microsoft 365 tenant.

Related content

[Buy a custom domain using Microsoft 365](#) (article)

[Manage domains](#) (link page)

[Domains FAQ](#) (article)

Migrate email and contacts to Microsoft 365

7/12/2021 • 2 minutes to read • [Edit Online](#)

Import or migrate email from Gmail or another email provider to Microsoft 365.

Want help with this? [Contact Microsoft 365 for business support](#) .

You need to use a version of Outlook that is installed on your desktop for this task. Outlook is included in most Microsoft 365 [plans](#).

Migrate Gmail to Microsoft 365

Follow these steps to import or migrate email, contacts, and calendar from Gmail into Outlook with Microsoft 365:

- [Import Gmail to Outlook](#)
- [Import contacts to Outlook](#)
- [Import Google Calendar](#)

Watch: Import calendars

Import Outlook pst files to Microsoft 365 (desktop)

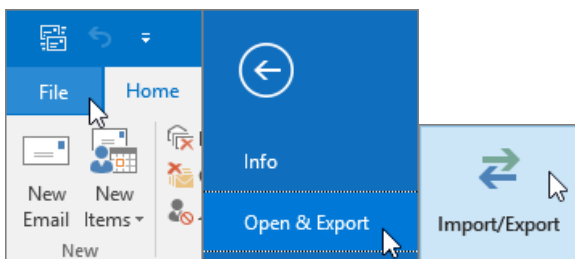
Follow these steps to export email, contacts and calendars from Outlook to a .pst file, and then import that file to Outlook with Microsoft 365:

1. [Export email, contacts, and calendar](#)
2. [Import mail, contacts, and calendar](#)

If you just want contacts, follow these steps:

1. [Export contacts from Outlook](#)
2. [Import contacts to Outlook](#)

To start the process, open Outlook and choose **File > Open & Export > Import/Export**.



See other email accounts in Outlook

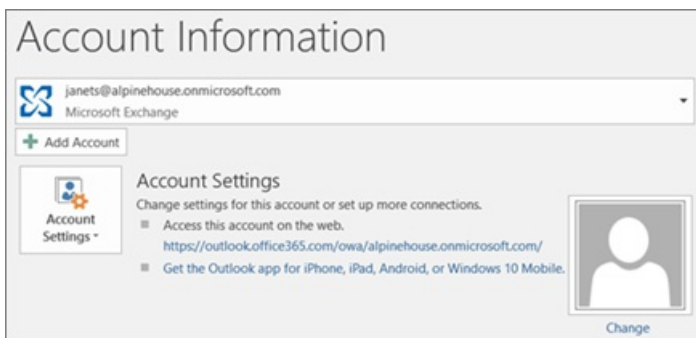
Just want to see your email from another provider (like Gmail, Yahoo, or Live.com) in Outlook? No need to import or migrate. You can set up Outlook or Outlook Web App so you can access your other accounts from the same place as your Microsoft 365 mailbox and send, receive, and read email sent to those accounts.

Outlook (desktop)

Add an account, such as your private Gmail account, to Outlook.

- Open Outlook, then go to **File > Add account**.

Need more detailed steps? See [Add an account](#).



Multiple mailboxes: Admins can bulk import email, contacts, and calendars to Microsoft 365

Depending on your source email system, you can choose from several bulk migration methods. Read [Ways to migrate multiple email accounts to Microsoft 365](#) to decide which method works for you.

Related content

[Plan your setup of Microsoft 365 for business](#) (article)

[Install Office applications](#) (link page)

[Overview of the Microsoft 365 admin center](#) (video)

Create organization-wide signatures and disclaimers

7/12/2021 • 2 minutes to read • [Edit Online](#)

You can manage email signatures by adding an email signature, legal disclaimer, or disclosure statement to the email messages that enter or leave your organization. You can set it up to apply to all incoming and outgoing messages as shown below. Or you can apply it to certain messages like those containing specific words or text patterns.

Watch: Create a company-wide email signature

If you found this video helpful, check out the [complete training series for small businesses and those new to Microsoft 365](#).

Create a signature that applies to all messages

TIP

Organization-wide signatures are called "disclaimers," regardless of what they include. For example, they can just be a signature, or also include your address, legal disclaimer, or other information you want.

Go to the admin center at <https://admin.microsoft.com>.

Go to the admin center at <https://portal.office.de/adminportal>.

Go to the admin center at <https://portal.partner.microsoftonline.cn/adminportal>.

1. Select the app launcher , and then select **Admin**.

Can't find the app you're looking for? From the app launcher, select **All apps** to see an alphabetical list of the apps available to you. From there, you can search for a specific app.

2. Select **Admin centers**, and then choose **Exchange**.
3. Under Mail flow, select **Rules**.
4. Select the + (Add) icon and choose **Apply disclaimers**.
5. Give the rule a name.
6. Under **Apply this rule**, select **[Apply to all messages]**.

TIP

[Learn more](#) about applying conditions if you don't want the disclaimer applied to all messages. (This scoping article is for Exchange Server, but it also applies to Microsoft 365.)

7. Under Do the following, leave **Append the disclaimer** selected.
8. Select **Enter text** and type your disclaimer.

TIP

[Learn more](#) about formatting disclaimers. (This formatting article is for Exchange Server, but it also applies to Microsoft 365.)

9. Select **Select one** and choose **Wrap** as a fallback option. Then **OK**. This means that if the disclaimer can't be added because of encryption or another mail setting, it will be wrapped in a message envelope.
10. Leave **Audit this rule with severity level** selected. Then choose **Low**, **Medium**, or **High** to be used in the message log.
11. Choose **Enforce** to turn on the disclaimer immediately, unless you want to test it first.
12. Choose **More options** to include additional conditions or exceptions.
13. Choose **Save** when finished.

Limitations of organization wide signatures

You can't do the following when managing email signatures in Microsoft 365:

- Insert the signature directly under the latest email reply or forward
- Display server-side email signatures in users' Sent Items folders
- Embed images in email signatures
- Skip lines which contain variables that couldn't be updated (e.g. because the value wasn't provided for a user)

To gain these and other capabilities to manage email signatures, use a third-party tool. Please do an internet search for **email signature software**. A number of these providers are Microsoft Gold Partners and their software provides these capabilities.

More resources

For information about using PowerShell, see [Organization-wide message disclaimers, signatures, footers, or headers in Exchange Online](#).

Related content

[Migrate email and contacts to Microsoft 365](#) (video)

[User email settings](#) (article)

[Overview of the Microsoft 365 admin center](#) (video)

Create, edit, or delete a security group in the Microsoft 365 admin center

7/12/2021 • 3 minutes to read • [Edit Online](#)

On the Microsoft 365 **Groups** page, you can create groups of user accounts that you can use to assign the same permissions to in SharePoint Online and CRM Online. For example, an administrator can create a security group to grant a certain group of people access to a SharePoint site. Only global and user management administrators have permissions to create, edit, or delete security groups; for more information about administrator roles, see [Assigning admin roles](#).

There are also [Groups in Exchange Online and SharePoint Online](#) that you can use to send email or assign permissions to a group of users, and [Groups in Exchange Online and SharePoint Online](#) that grant users rights and access to sites and site collections.

IMPORTANT

Planning on using site mailboxes? All the users that are added to a SharePoint site via a security group rather than being added individually can use only the site mailbox from SharePoint. These users won't be able to access the site mailbox from Outlook. For more information, see [Use Microsoft 365 Groups instead of Site Mailboxes](#).

Manage security groups in the admin center

Add a security group

1. In the Microsoft 365 admin center, go to the **Groups** > [Groups](#) page.
2. On the **Groups** page, select **Add a group**.
3. On the **Choose a group type** page, choose **Security**.
4. Follow the steps to complete creation of the group.

Add members to a security group

1. Select the security group name on the **Groups** page, and on the **Members** tab, select **View all and manage members**.
2. In the group pane, select **Add members** and choose the person from the list or type the name of the person you want to add in the **Search** box, and then select **Save**.

To remove members, select the X next to their name.

Edit a security group

1. In the admin center, go to the **Groups** > [Groups](#) page.
2. On the **Groups** page, select the group's name.
3. In the settings pane, select the **General** tab or the **Members** tab to edit either group details or members.

Delete a security group

1. In the admin center, go to the **Groups** > [Groups](#) page.
2. On the **Groups** page, select the group's name.

3. Select **Delete group** (wastebin icon), and then confirm by selecting **Delete**.

Select **Close** once the group is deleted.

Groups in Exchange Online and SharePoint Online

If you want to create groups of users so you can send email to them all at the same time, you can do that in the Exchange admin center by going to **Admin > Exchange > Recipients > Groups**. Next, select **New+**, and select the kind of group you want to create:

- **Distribution group**: Used to distribute messages to a group of users. It's also called a *mail-enabled distribution group*, or, a *distribution list*. For more information, see [Manage distribution groups](#).
- **Security group**: Can be used to distribute messages to a group of users, or to grant access permissions to resources. This group is also called a *mail-enabled security group*. For more information, see [Manage mail-enabled security groups](#).
- **Dynamic distribution group**: A type of distribution group whose list of recipients is recalculated every time you send a message based on filters and conditions that you define. For more information, see [Manage dynamic distribution groups](#).

After you create distribution groups and mail-enabled security groups in the Exchange admin center, their names and user lists appear on the **Security groups** page. You can delete these groups in both locations, but you can edit them only in the Exchange admin center. Dynamic distribution groups don't show up on the **Security groups** page.

SharePoint groups are created automatically when you make a site collection. The default groups use the default permission levels in SharePoint—sometimes called SharePoint roles—to grant users rights and access. For more information, see [Default SharePoint groups in SharePoint Online](#).

How is a security group different from security groups I create in SharePoint?

Security groups can be used with SharePoint, Exchange, MDM, Windows, and more. A security group you create in SharePoint is only recognized by that SharePoint site collection.

Do I have to use security groups for my organization to be secure?

No. This is just one more way you can manage security for your organization. You can always grant user permissions and access to sites individually. But with security groups, you can easily manage larger groups of users.

Can I send email to a security group?

Yes. But if you want to use groups for email and collaboration, we recommend that you [create a Microsoft 365 group](#) instead.

Related content

[Create a group in the Microsoft 365 admin center](#) (article)

[Explaining Microsoft 365 Groups to your users](#) (article)

[Manage a group in the Microsoft 365 admin center](#) (article)

Configure email forwarding in Microsoft 365

7/12/2021 • 4 minutes to read • [Edit Online](#)

As the admin of an organization, you might have company requirements to set up email forwarding for a user's mailbox. Email forwarding lets you forward email messages sent to a user's mailbox to another user's mailbox inside or outside of your organization.

IMPORTANT

You can use outbound spam filter policies to control automatic forwarding to external recipients. For more information, see [Control automatic external email forwarding in Microsoft 365](#).

Configure email forwarding

Before you set up email forwarding, note the following:

- Allow automatically forwarded messages to be sent to people on the remote domain. See [Manage remote domains](#) for details.
- Once you set up email forwarding, only **new** emails sent to the *from* mailbox will be forwarded.
- Email forwarding requires that the *from* account has a license. If you're setting up email forwarding because the user has left your organization, another option is to [convert their mailbox to a shared mailbox](#). This way several people can access it. However, a shared mailbox cannot exceed 50GB.

You must be an Exchange administrator or Global administrator in Microsoft 365 to do these steps. For more information, see the topic [About admin roles](#).

1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the name of the user whose email you want to forward, then open the properties page.
3. On the **Mail** tab, select **Manage email forwarding**.
4. On the email forwarding page, select **Forward all emails sent to this mailbox**, enter the forwarding address, and choose whether you want to keep a copy of forwarded emails. If you don't see this option, make sure a license is assigned to the user account. Select **Save changes**.

To forward to multiple email addresses, you can ask the user to set up a rule in Outlook to forward to the addresses.

- a. Open **outlook** > **Home** > **Rules** > Select **Manage Rules & Alerts**
- b. Select **New Rule** > **Select Apply rule on message I receive** located near bottom of list, then click **Next**.
- c. Click **Yes** when asked This rule will be applied to every message you receive.
- d. On the next list select the actions **redirect it to people or public group** and **stop processing more rules**
- e. Click the underlined phrase **people or public group** in the bottom part of window.
- f. Type the **email address** to forward mail to in the To field, then click **OK**.
- g. Select **Finish**

Or, in the admin center, [create a distribution group](#), [add the addresses to it](#), and then set up forwarding to point to the DL using the instructions in this article.

5. Don't delete the account of the user whose email you're forwarding or remove their license! If you do, email forwarding will stop.
1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the name of the user whose email you want to forward to open the properties page.
3. Expand **Mail settings**, and then in the **Email forwarding** section, select **Edit**.
4. On the email forwarding page, set the toggle to **On**, enter the forwarding address, and choose whether you want to keep a copy of forwarded emails. If you don't see this option, make sure a license is assigned to the user account. Select **Save**.

To forward to multiple email addresses, you can ask the user to set up a rule in Outlook to forward to the addresses. To learn more, see [Use rules to automatically forward messages](#).

Or, in the admin center, [create a distribution group](#), [add the addresses to it](#), and then set up forwarding to point to the DL using the instructions in this article.

5. Don't delete the account of the user whose email you're forwarding or remove their license! If you do, email forwarding will stop.
1. In the admin center, go to the **Users** > [Active users](#) page.
2. Select the name of the user whose email you want to forward to open the properties page.
3. Expand **Mail settings**, and then in the **Email forwarding** section, select **Edit**.
4. On the email forwarding page, set the toggle to **On**, enter the forwarding address, and choose whether you want to keep a copy of forwarded emails. If you don't see this option, make sure a license is assigned to the user account. Select **Save**.

To forward to multiple email addresses, you can ask the user to set up a rule in Outlook to forward to the addresses. To learn more, see [Use rules to automatically forward messages](#).

Or, in the admin center, [create a distribution group](#), [add the addresses to it](#), and then set up forwarding to point to the DL using the instructions in this article.

5. Don't delete the account of the user whose email you're forwarding or remove their license! If you do, email forwarding will stop.

Related content

[Create a shared mailbox](#) (article)

[Send email from a different address](#) (article)

[Change a user name and email address](#) (article)

About shared mailboxes

7/21/2021 • 4 minutes to read • [Edit Online](#)

Shared mailboxes are used when multiple people need access to the same mailbox, such as a company information or support email address, reception desk, or other function that might be shared by multiple people.

Users with permissions to the group mailbox can send as or send on behalf of the mailbox email address if the administrator has given that user permissions to do that. This is particularly useful for help and support mailboxes because users can send emails from "Contoso Support" or "Building A Reception Desk."

Before you begin

Before you [create a shared mailbox](#), here are some things you should know:

- **Licenses:** Your shared mailbox can store up to 50GB of data without you assigning a license to it. After that, you need to assign a license to the mailbox to store more data. For more details on shared mailbox licensing, please see [Exchange Online Limits](#). When a shared mailbox reaches the storage limit, you'll be able to receive email for a while, but you won't be able to send new email. Then, after that, it will stop receiving email. Senders to the mailbox will get a non-delivery receipt.
- **User permissions:** You need to give users permissions (membership) to use the shared mailbox. Only people inside your organization can use a shared mailbox.
- **External users:** You can't give people outside your business (such as people with a Gmail account) access to your shared mailbox. If you want to do this, consider creating a group for Outlook instead. To learn more, see [Create a Microsoft 365 group in the admin center](#).
- **Use with Outlook:** In addition to using Outlook on the web from your browser to access shared mailboxes, you can also use the Outlook for iOS app or the Outlook for Android app. To learn more, see [Add a shared mailbox to Outlook mobile](#). Another option is to create a group for your shared mailbox. To learn more, see [Compare Groups](#).
- **Encryption:** You can't encrypt email sent from a shared mailbox. This is because a shared mailbox does not have its own security context (username/password) so it cannot be assigned a key. If more than one person is a member, and they send/receive emails they encrypted with their own keys, other members might be able to read the email and others might not, depending which public key the email was encrypted with.
- **Mailbox conversion:** You can convert user mailboxes to shared mailboxes. See [Convert a user mailbox to a shared mailbox](#).
- **Admin roles:** Users with global admin or Exchange admin roles can create shared mailboxes.
- **Subscription requirements:** To create a shared mailbox, you need to subscribe to a Microsoft 365 for business plan that includes email (the Exchange Online service). The Microsoft 365 Apps for business subscription doesn't include email. Microsoft 365 Business Standard does include email.
- **Signing in:** A shared mailbox is not intended for direct sign-in by its associated user account. You should always block sign-in for the shared mailbox account and keep it blocked.
- **Too many users:** When there are too many designated users concurrently accessing a shared mailbox (no more than 25 is recommended), they may intermittently fail to connect to this mailbox or have

inconsistencies like messages being duplicated in the outbox. In this case, you can consider reducing the number of users or using a different workload, such as a Microsoft 365 group or a Public folder.

- **Message deletion:** Unfortunately, you can't prevent people from deleting messages in a shared mailbox. The only way around this is to create a Microsoft 365 group instead of a shared mailbox. A group in Outlook is like a shared mailbox. For a comparison of the two, see [Compare groups](#). To learn more about groups, see [Learn more about groups](#).

NOTE

To access a shared mailbox, a user must have an Exchange Online license, but the shared mailbox doesn't require a separate license. Every shared mailbox has a corresponding user account. Notice how you weren't asked to provide a password when you created the shared mailbox? The account has a password, but it's system-generated (unknown). You shouldn't use the account to log in to the shared mailbox. Without a license, shared mailboxes are limited to 50 GB. To increase the size limit to 100 GB, the shared mailbox must be assigned an Exchange Online Plan 2 license or an Exchange Online Plan 1 license with an Exchange Online Archiving add-on license. This will also let you enable auto-expanding archiving for an unlimited amount of archive storage capacity. Similarly, if you want to place a shared mailbox on litigation hold, the shared mailbox must have an Exchange Online Plan 2 license or an Exchange Online Plan 1 license with an Exchange Online Archiving add-on license. If you want to apply advanced features such as Microsoft Defender for Office 365, Advanced eDiscovery, or automatic retention policies, the shared mailbox must be licensed for those features.

Related content

[Create a shared mailbox](#) (article)

[Configure a shared mailbox](#) (article)

[Convert a user mailbox to a shared mailbox](#) (article)

[Remove a license from a shared mailbox](#) (article)

[Resolve issues with shared mailboxes](#) (article)

Create a shared mailbox

7/12/2021 • 6 minutes to read • [Edit Online](#)

NOTE

If your organization uses a hybrid Exchange environment, you should use the on-premises Exchange admin center (EAC) to create and manage shared mailboxes. See [Create shared mailboxes in the Exchange admin center](#)

If you're not sure if you should create a shared mailbox or a Microsoft 365 group for Outlook, see [Compare groups](#) for some guidance. Note that currently, it's not possible to migrate a shared mailbox to a Microsoft 365 group. If this is something you want, let us know by [voting here](#).

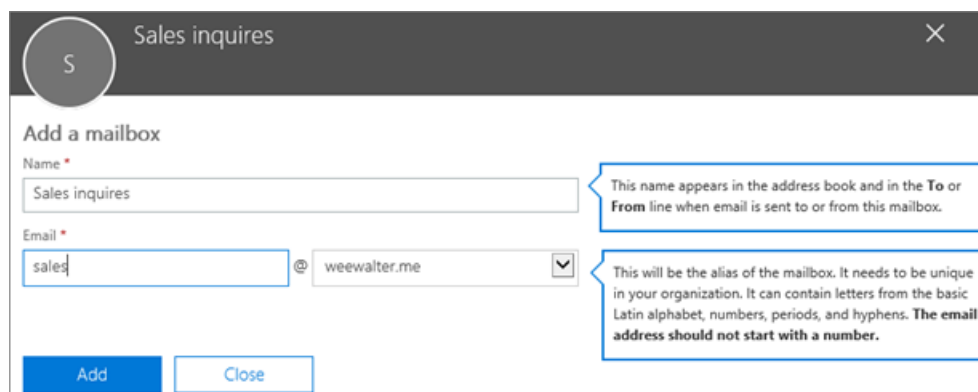
It's easy to create shared mailboxes so a group of people can monitor and send email from a common email addresses, like info@contoso.com. When a person in the group replies to a message sent to the shared mailbox, the email appears to be from the shared mailbox, not from the individual user.

Shared mailboxes include a shared calendar. A lot of small businesses like to use the shared calendar as a place for everyone to enter their appointments. For example, if you have 3 people who do customer visits, all can use the shared calendar to enter the appointments. This is an easy way to keep everyone informed where people are.

Before creating a shared mailbox, be sure to read [About shared mailboxes](#) for more information.

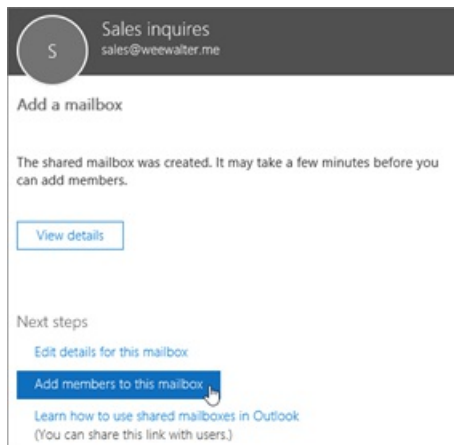
Create a shared mailbox and add members

1. Sign in with a global admin account or Exchange admin account. If you get the message "**You don't have permission to access this page or perform this action,**" then you aren't an admin.
2. In the admin center, go to the **Groups** > [Shared mailboxes](#) page.
2. In the [admin center](#), go to the **Groups** > **Shared mailboxes** page.
2. In the [admin center](#), go to the **Groups** > **Shared mailboxes** page.
3. On the **Shared mailboxes** page, select **+ Add a mailbox**. Enter a name for the shared mailbox. Then the wizard chooses the email address, but you can edit it.

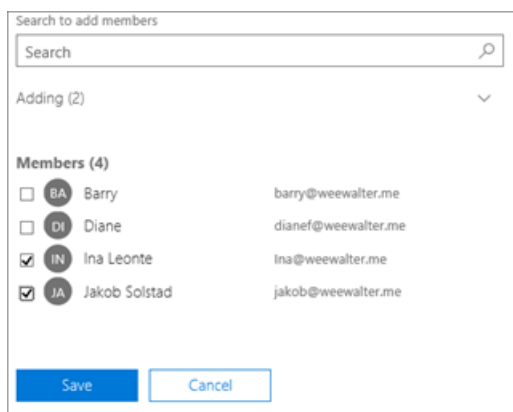


The screenshot shows a dialog box titled "Sales inquires" with a close button (X) in the top right corner. Below the title is the heading "Add a mailbox". There are two input fields: "Name" and "Email". The "Name" field contains "Sales inquires". The "Email" field contains "sales" followed by a dropdown menu showing "weewalter.me". There are two callout boxes with blue borders and white backgrounds. The first callout box points to the "Name" field and contains the text: "This name appears in the address book and in the **To** or **From** line when email is sent to or from this mailbox." The second callout box points to the "Email" field and contains the text: "This will be the alias of the mailbox. It needs to be unique in your organization. It can contain letters from the basic Latin alphabet, numbers, periods, and hyphens. **The email address should not start with a number.**" At the bottom of the dialog, there are two buttons: "Add" (highlighted in blue) and "Close".

4. Select **Add**. It may take a few minutes before you can add members.
5. Under **Next steps**, select **Add members to this mailbox**. Members are the people who will be able to view the incoming mail to this shared mailbox, and the outgoing replies.



6. Select the **+Add members** button. Put a check mark next to the people who you want to use this shared mailbox, and select **Save**.



7. Select **Close**.


You have a shared mailbox and it includes a shared calendar. Now go on to the next step: block sign-in for the shared mailbox account.

Which permissions should you use?

You can use the following permissions with a shared mailbox:

- **Full Access:** The Full Access permission lets a user open the shared mailbox and act as the owner of that mailbox. After accessing the shared mailbox, a user can create calendar items, read, view, delete, and change email messages, and create tasks and calendar contacts. However, a user with Full Access permission can't send email from the shared mailbox unless they also have Send As or Send on Behalf permission.
- **Send As:** The Send As permission lets a user impersonate the shared mailbox when sending mail. For example, if Katerina logs into the shared mailbox Marketing Department and sends an email, it will look like the Marketing Department sent the email.
- **Send on Behalf:** The Send on Behalf permission lets a user send email on behalf of the shared mailbox. For example, if John logs into the shared mailbox Reception Building 32 and sends an email, it will look like the mail was sent by "John on behalf of Reception Building 32". You can't use the EAC to grant Send on Behalf permissions, you must use the **Set-Mailbox** cmdlet with the *GrantSendonBehalf* parameter.

Use the EAC to edit shared mailbox delegation

1. In the EAC, go to **Recipients > Shared**. Select the shared mailbox, and then select **Edit** .
2. Select **Mailbox delegation**.
3. To grant or remove Full Access and Send As permissions, select **Add +** or **Remove -** and then select the

users you want to grant permissions to.

NOTE

The Full Access permission allows a user to open the mailbox as well as create and modify items in it. The Send As permission allows anyone other than the mailbox owner to send email from this shared mailbox. Both permissions are required for successful shared mailbox operation.

4. Select **Save** to save your changes.

Block sign-in for the shared mailbox account

Every shared mailbox has a corresponding user account. Notice how you weren't asked to provide a password when you created the shared mailbox? The account has a password, but it's system-generated (unknown). You aren't supposed to use the account to log in to the shared mailbox.


But what if an admin simply resets the password of the shared mailbox user account? Or what if an attacker gains access to the shared mailbox account credentials? This would allow the user account to log in to the shared mailbox and send email. To prevent this, you need to block sign-in for the account that's associated with the shared mailbox.

1. In the admin center, go to the **Users** > [Active users](#) page.

1. In the admin center, go to the **Users** > [Active users](#) page.

1. In the admin center, go to the **Users** > [Active users](#) page.

1. In the list of user accounts, find the account for the shared mailbox (for example, change the filter to **Unlicensed users**).

2. Select the user to open their properties pane, and then select the **Block this user** icon .

Note: If the account is already blocked, **Sign in blocked** will appear at the top and the icon will read **Unblock this user**.

3. In the **Block this user?** pane, select **Block the user from signing in**, and then select **Save changes**.

For instructions on how to block sign-in for accounts using Azure AD PowerShell (including many accounts at the same time), see [Block user accounts with Office 365 PowerShell](#).

Add the shared mailbox to Outlook

If you have automapping enabled in your business (by default, most people do), the shared mailbox will appear in your user's Outlook app automatically after they close and restart Outlook.

Automapping is set on the user's mailbox, not the shared mailbox. This means if you try to use a security group to manage who has access to the shared mailbox, automapping won't work. So, if you want automapping, you have to assign permissions explicitly. Automapping is on by default. To learn how to turn it off, see [Remove automapping for a shared mailbox](#).

To learn more about shared mailboxes in Outlook, see:

- [Open and use a shared mailbox in Outlook](#)
- [Add a shared mailbox to Outlook on the web](#)
- [Add a shared mailbox to Outlook mobile](#)

- [Open a shared folder or mailbox in Outlook for Mac](#)
- [Add rules to a shared mailbox](#)

Use a shared mailbox on a mobile device (phone or tablet)

You can access a shared mailbox on a mobile device in two ways:

- Add the shared mailbox in the [Outlook for iOS app](#) or the [Outlook for Android mobile app](#).

For instructions, see [Add a shared mailbox to Outlook mobile](#).

- Open your browser, sign in, and then go to Outlook on the web. From Outlook on the web you'll be able to access the shared mailbox.

For instructions, see [Add a shared mailbox to Outlook on the web](#).

NOTE

Shared mailbox can only be added to Outlook for iOS app or the Outlook for Android mobile app

Use the shared calendar

When you created the shared mailbox, you automatically created a shared calendar. We like the shared mailbox calendar rather than a SharePoint calendar for keeping track of appointments and where people are. A shared calendar is integrated with Outlook and it's much easier to use than a SharePoint calendar.

1. In the Outlook app, go to calendar view, and select the shared mailbox.
2. When you enter appointments, everyone who is a member of the shared mailbox will be able to see them.
3. Any member of the shared mailbox can create, view, and manage appointments on the calendar, just like they would their personal appointments. Everyone who is a member of shared mailbox can see their changes to the shared calendar.

Related content

[About shared mailboxes](#) (article)

[Configure a shared mailbox](#) (article)

[Convert a user mailbox to a shared mailbox](#) (article)

[Remove a license from a shared mailbox](#) (article)

[Resolve issues with shared mailboxes](#) (article)

Configure shared mailbox settings

7/12/2021 • 4 minutes to read • [Edit Online](#)

After you have [created a shared mailbox](#), you'll want to configure some settings for the mailbox users, such as email forwarding and automatic replies. Later, you might want to change other settings, such as the mailbox name, members, or member permissions.

Change the name or email alias of a shared mailbox, or change the primary email address

1. In the admin center, go to the **Groups** > [Shared mailboxes](#) page.
2. Select the shared mailbox you want to edit, and then select **Edit** next to **Name, Email, Email aliases**.
3. Enter a new name, or add another alias. If you want to change the primary email address, your mailbox must have more than one email alias.
4. Select **Save**.

Forward emails that are sent to a shared mailbox

You do not need to assign a license to the shared mailbox in order to forward email that's sent to it. You can forward the messages to any valid email address or distribution list.

1. In the admin center, go to the **Groups** > [Shared mailboxes](#) page.
2. Select the shared mailbox you want to edit, then select **Email forwarding** > **Edit**.
3. Set the toggle to **On**, and enter one email address to forward the messages to. It can be any valid email address. To forward to multiple addresses, you need to [create a distribution group](#) for the addresses, and then enter the name of the group in this box.
4. Select **Save**.

Send automatic replies from a shared mailbox

1. In the admin center, go to the **Groups** > [Shared mailboxes](#) page.
2. Select the shared mailbox you want to edit, then select **Automatic replies** > **Edit**.
3. Set the toggle to **On**, and choose whether to send the reply to people inside your organization or outside your organization.
4. Enter the reply you want to send to people inside your organization. You can't add images, only text.
5. If you want to *also* send a reply to people outside your organization, select the check box, who you want to get the reply, and type the text. There's no way to only send to people outside your organization but not to people inside your organization.
6. Select **Save**.

Allow everyone to see the Sent email (the replies)

By default, messages sent from the shared mailbox aren't saved to the Sent Items folder of the shared mailbox.

Instead, they are saved to the Sent Items folder of the person who sent the message.

If you want to allow everyone to see the Sent email, in the admin center, edit the shared mailbox settings, and select **Sent items > Edit**.

Choose the apps that a shared mailbox can use to access Microsoft email

1. In the admin center, go to the **Groups > Shared mailboxes** page.
2. Select the shared mailbox you want to edit, then select **Email apps > Edit**.
3. Set the toggle to **On** for all of the apps you want members to be able to use to access the shared mailbox. Set the toggle to **Off** for any apps you don't want them to use.
4. Select **Save**.

Put a shared mailbox on litigation hold

To learn more about litigation hold, see [Create a Litigation Hold](#).

1. In the admin center, go to the **Groups > Shared mailboxes** page.
2. Select the shared mailbox you want to edit, then select **Litigation hold > Edit**.
3. Set the toggle to **On**.
4. Optionally, enter a duration, a note about the hold, and a URL with more information.
5. Select **Save**.

Add or remove members

1. In the admin center, go to the **Groups > Shared mailboxes** page.
2. Select the shared mailbox you want to edit, then select **Members > Edit**.
3. Do one of the following:
 - To add members, select **Add members**, search for or select a member to add, and then select **Save**.
 - To remove members, use the Search box to search for the member if necessary, select the **X** next to the member's name, and then select **Save**.
4. Select **Save** again.

Add or remove permissions of members

1. In the admin center, go to the **Groups > Shared mailboxes** page.
2. Select the shared mailbox you want to edit, then select **Members > Customize permissions**.
3. Select **Edit** next to the permission you want to change for a member.
4. Do one of the following:
 - To give that permission to an additional member, select **Add permissions**, search for or select a member to add, and then select **Save**.
 - To remove the permission from a member, use the Search box to search for the member if necessary, select the **X** next to the member's name, and then select **Save**.
5. Select **Save** again.

Show or hide a shared mailbox in the global address list

If you choose not to show the shared mailbox in the global address list, the mailbox won't appear in your organization's address list, but it will still receive email sent to it.

1. In the admin center, go to the **Groups** > [Shared mailboxes](#) page.
2. Select the shared mailbox you want to edit, then select **Show in global address list** > **Edit**.
3. Set the toggle to **On** or **Off**.
4. Select **Save**.

NOTE

Hiding a shared mailbox from address list will make it impossible for new shared mailbox members to add the hidden mailbox to their Outlook profile until the shared mailbox is again shown in the address list.

Related content

[About shared mailboxes](#) (article)

[Create a shared mailbox](#) (article)

[Convert a user mailbox to a shared mailbox](#) (article)

[Remove a license from a shared mailbox](#) (article)

[Resolve issues with shared mailboxes](#) (article)

Convert a user mailbox to a shared mailbox

7/12/2021 • 3 minutes to read • [Edit Online](#)

When you convert a user's mailbox to a shared mailbox, all of the existing email and calendar is retained. Only now it's in a shared mailbox where several people will be able to access it instead of one person. At a later date, you can convert a shared mailbox back to a user (private) mailbox.

Before you begin

Here are some really important things that you need to know:

- The user mailbox you're converting needs a license assigned to it before you convert it to a shared mailbox. Otherwise, you won't see the option to convert the mailbox. If you've removed the license, add it back so you can convert the mailbox. After converting the mailbox to a shared one, you can remove the license from the user's account.
- Shared mailboxes can have up to 50 GB of data without a license assigned to them. To hold more data than that, you need a license assigned to it. You may need to delete a bunch of large emails (say, ones with attachments) from the shared mailbox to shrink it down so you can remove the license.
- Don't delete the old user's account. That's required to anchor the shared mailbox. If you've already deleted the user account, see [Convert the mailbox of a deleted user](#).
- The rules are intact after the mailbox is converted to a shared mailbox.

Use the Exchange admin center to convert a mailbox

1. Go to the [Exchange admin center](#).
2. Select **Recipients > Mailboxes**.
3. Select the user mailbox. Under **Convert to Shared Mailbox**, select **Convert**.
4. If the mailbox is smaller than 50 GB, you can remove the [license from the user](#), and stop paying for it. Don't delete the user's account. The shared mailbox needs it there as an anchor. If you are converting the mailbox of an employee that is leaving your organization, you should take additional steps to make sure that they cannot log in anymore. Please see [Remove a former employee from Microsoft 365](#).

NOTE

It's not required to reset the user's password during mailbox conversion. However, if the password is not reset, **the original username and password continue to work** after the mailbox conversion is finished.

For everything else you need to know about shared mailboxes, see [About shared mailboxes](#) and [Create a shared mailbox](#).

NOTE

Shared mailboxes don't require a separate license. However, if you want to enable In-Place Archive or put an In-Place Hold or a Litigation Hold on a shared mailbox, you must assign an Exchange Online Plan 1 with Exchange Online Archiving or Exchange Online Plan 2 license to the mailbox.

Convert the mailbox of a deleted user

Let's say you've deleted a user account and now you want to convert their old mailbox to a share mailbox. Here's what you need to do:

1. [Restore the user's account](#).
2. Make sure a Microsoft 365 license is assigned to it.
3. Reset the user's password.
4. Wait 20-30 minutes for their mailbox to be recreated.
5. Now follow the instructions on this page to convert their mailbox to a shared mailbox.
6. After that's done, you can remove the license from the user's mailbox. Don't delete the user's old mailbox. The shared mailbox needs it there as an anchor.
7. Add members to the shared mailbox.

Convert a shared mailbox back to a user's (private) mailbox

1. Go to the [Exchange admin center](#).
2. Select **Recipients > Shared**.
3. Select the shared mailbox. Under **Convert to Regular Mailbox**, select **Convert**.
4. Go back to the admin center. Under **Users**, choose the user account associated with the old shared mailbox. Assign a license to the account, and reset the password.

It will take a few minutes for the mailbox to get set up, but after that, the person who is going to use that account is ready to go. When they sign in, they'll see the email and calendar items that used to be in the shared mailbox.

Convert a user's mailbox in a hybrid environment

For more info about converting a user mailbox to a shared mailbox in an Exchange Hybrid environment, see:

- [Cmdlets to create or modify a remote shared mailbox in an on-premises Exchange environment](#)
- [Shared mailboxes are unexpectedly converted to user mailboxes after directory synchronization runs in an Exchange hybrid deployment](#)

NOTE

If you are a member of the Organization Management or Recipient Management role group, you can use the Exchange Management Shell to change a user mailbox to a shared mailbox on-premises. For example,

```
Set-Mailbox -Identity mailbox1@contoso.com -Type Shared .
```

Related content

- [About shared mailboxes](#) (article)
- [Create a shared mailbox](#) (article)
- [Configure a shared mailbox](#) (article)
- [Remove a license from a shared mailbox](#) (article)
- [Resolve issues with shared mailboxes](#) (article)

Remove a license from a shared mailbox

6/8/2021 • 2 minutes to read • [Edit Online](#)

Shared mailboxes usually don't require a license. Follow these instructions to remove a license from a shared mailbox so that you can either assign it to a user or return the license so that you aren't paying for a license you don't need.

NOTE

A license is required in the following scenarios:

1. The shared mailbox has more than 50 GB of storage in use.
2. The shared mailbox uses in-place archiving.
3. The shared mailbox is placed in litigation hold.
4. The shared mailbox has a Microsoft Defender license assigned.

Remove the license

1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.
1. In the admin center, go to the **Users** > [Active users](#) page.

NOTE

You need to remove the license from the Active users page. You can't remove the license from the Shared mailbox page because licenses are user settings.

2. Select the shared mailbox.
3. On the **Licenses and Apps** tab, expand **Licenses** and uncheck the box for the license you want to remove.
4. Select **Save changes**.
5. When you return to the **Active users** page, the status of the shared mailbox will be **Unlicensed**.
6. You're still paying for the license. To stop paying for it, [remove the license from your subscription](#).

Related content

- [About shared mailboxes](#) (article)
- [Create a shared mailbox](#) (article)
- [Configure a shared mailbox](#) (article)
- [Convert a user mailbox to a shared mailbox](#) (article)
- [Resolve issues with shared mailboxes](#) (article)

Resolve issues with shared mailboxes

7/12/2021 • 2 minutes to read • [Edit Online](#)

If you see error messages when creating or using a shared mailbox, try these possible solutions.

Error when creating shared mailboxes

If you see the error message, **The proxy address "smtp:<shared mailbox name>" is already being used by the proxy addresses or LegacyExchangeDN of "<name>". Please choose another proxy address,** it means you're trying to give the shared mailbox a name that's already in use. For example, let's say you want shared mailboxes named info@domain1 and info@domain2. There are two ways to do this:

- Use Windows PowerShell. See this blog post for instructions: [Create Shared Mailboxes with Same Alias at Different Domains](#)
- Name the second shared mailbox something different from the start to get around the error. Then in the admin center, rename the shared mailbox to what you want it to be.

Error about not having send permissions when using a shared mailbox

If you created a shared mailbox and then try to send a message from it, you might get this:

This message could not be sent. You do not have the permission to send the message on behalf of the specified user.

This message appears when Microsoft 365 is experiencing a replication latency issue. It should go away in an hour or so, when the information about your new shared mailbox (or added user) is replicated across all of our data centers. Wait an hour and then try again to send a message.

Related content

[About shared mailboxes](#) (article)

[Create a shared mailbox](#) (article)

[Configure a shared mailbox](#) (article)

[Convert a user mailbox to a shared mailbox](#) (article)

[Remove a license from a shared mailbox](#) (article)

Configure Focused Inbox for everyone in your organization

7/12/2021 • 7 minutes to read • [Edit Online](#)

If you're responsible for configuring how email works for EVERYONE in a business this article is for you! It explains how to customize it or turn it off for your business, and answers [frequently asked questions](#).

If you would like to turn off Focused Inbox for just yourself, please see [Turn off Focused Inbox](#).

If you want to be sure that your users receive business-specific email messages, for example, from HR or payroll, you can configure Focused Inbox so these messages reach the Focused view. You can also control whether users in your organization see the Focused Inbox in their mailbox.

Turn Focused Inbox On or Off in your organization

You use PowerShell to turn Focused Inbox on or off for everyone in your organization. Do you want to do this in the Microsoft 365 admin center? Let our Engineering team know. [Vote here!](#)

To turn off Focused Inbox:

The following PowerShell example turns Focused Inbox **Off** in your organization. However, it doesn't block the availability of the feature for your users. If they want, they can still re-enable Focused Inbox again on each of their clients.

1. [Connect to Exchange Online using remote PowerShell](#).
2. You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Transport rules" entry in [Messaging policy and compliance permissions](#).
3. Run the **Get-OrganizationConfig** cmdlet.

```
Get-OrganizationConfig
```

4. Look for **FocusedInboxOn** to view its current setting:

```
GuestsUsageGuidelinesLink      :  
FocusedInboxOn                  : True  
FocusedInboxOnLastUpdateTime    : 11/27/2017
```

5. Run the following cmdlet to turn Focused Inbox off.

```
Set-OrganizationConfig -FocusedInboxOn $false
```

6. Run the **Get-OrganizationConfig** cmdlet again and you'll see that FocusedInboxOn is set to \$false, which means it's been turned off.

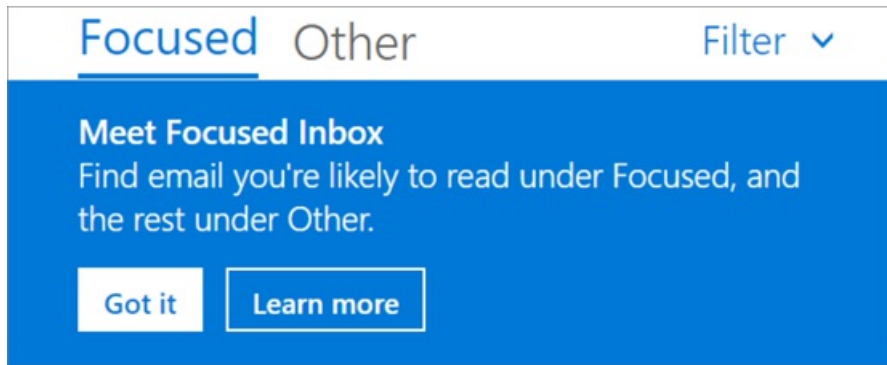
To turn on Focused Inbox:

- In Step 5 above, run the following cmdlet to turn Focused Inbox on.

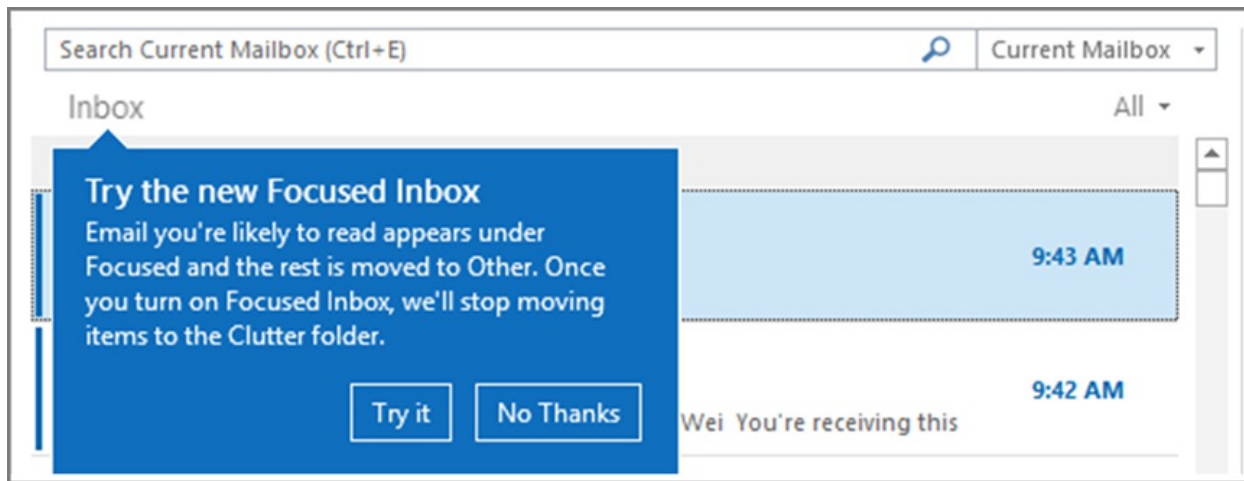
```
Set-OrganizationConfig -FocusedInboxOn $true
```

What do users see after I turn on Focused Inbox?

Your users will see the Focused view only after they close and restart Outlook. When they restart Outlook, they'll see a Tip in the Outlook user interface giving them to the option to use the new Focused Inbox.



If you're switching from Clutter to Focused Inbox, they can decide to enable it ("Try it") or dismiss the feature. If the user has multiple (supported) clients, they can enable/disable Focused Inbox individually on each one. The tip looks like this:



When a user decides to start using Focused Inbox, Clutter gets disabled automatically. The Clutter folder gets converted into a standard folder, that allows the user to rename or delete it.

Turn Focused Inbox On or Off for specific users

This example turns Focused Inbox Off for Tim Matthews in the Contoso organization. However, it doesn't block the availability of the feature to him. If he wants, he can still re-enable Focused Inbox again on each of his clients.

1. [Connect to Exchange Online using remote PowerShell.](#)
2. You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Transport rules" entry in the Messaging policy and compliance permissions topic.
3. Run the `Get-FocusedInbox` cmdlet, for example:

```
Get-FocusedInbox -Identity <tim@contoso.com>
```

4. Look for `FocusedInboxOn` to view its current setting:

```
GuestsUsageGuidelinesLink :  
FocusedInboxOn : True  
FocusedInboxOnLastUpdateTime : 11/27/2017
```

5. Run the following cmdlet to turn off Focused Inbox:

```
Set-FocusedInbox -Identity <tim@contoso.com> -FocusedInboxOn $false
```

OR, run the following cmdlet to turn it on:

```
Set-FocusedInbox -Identity <tim@contoso.com> -FocusedInboxOn $true
```

Use the UI to create a transport rule to direct email messages to the Focused view for all your users

1. Go to the [Exchange admin center](#).
2. Navigate to **mail flow** > **Rules**. Select **+** and then select **Create a new rule....**
3. After you're done creating the new rule, select **Save** to start the rule.

The following image shows an example where all messages From "Payroll Department" are to be delivered to the Focused Inbox.

Name: Payroll Department Focused Inbox

*Apply this rule if...
The sender is... 'Payroll Department'
add condition

*Do the following...
Set the message header to this value... Set the message header 'X-MS-Exchange-Organization-BypassFocusedInbox' to the value true
add action

Except if...

NOTE

The message header value text in this example is, X-MS-Exchange-Organization-BypassFocusedInbox.

Use PowerShell to create a transport rule to direct email messages to the Focused view for all your users

1. [Connect to Exchange Online using remote PowerShell](#).
2. You need to be assigned permissions before you can perform this procedure or procedures. To see what permissions you need, see the "Transport rules" entry in [Messaging policy and compliance permissions](#).
3. Run the following command to allow all messages from "Payroll Department," for example, to be delivered to the Focused Inbox.

```
New-TransportRule -Name <name_of_the_rule> -From "Payroll Department" -SetHeaderName "X-MS-Exchange-Organization-BypassFocusedInbox" -SetHeaderValue "true"
```

IMPORTANT

In this example, both "X-MS-Exchange-Organization-BypassFocusedInbox" and "true" are case sensitive. Also, Focused Inbox will honor the X-header that bypasses Clutter, so if you use this setting in Clutter, it will be used in Focused Inbox. For detailed syntax and parameter information, see [New-TransportRule](#).

How do you know this worked?

You can check email message headers to see if the email messages are landing in the Inbox due to the Focused Inbox transport rule bypass. Pick an email message from a mailbox in your organization that has the Focused Inbox transport rule applied. Look at the headers stamped on the message, and you should see the **X-MS-Exchange-Organization-BypassFocusedInbox: true** header. This means the bypass is working. Check out the [View the Internet header information for an email message](#) article for info on how to find the header information.

What will the user see?

If a transport rule is in place, a notification will be shown for the override. Outlook on the web will disable the "Always move to Other" and show a tooltip. Outlook clients on desktop will allow selection for "Always move to Other" and will pop up a dialog.

Turn on/off Clutter

We've received reports that Clutter suddenly stopped working for some users. If this happens, you can enable it again for specific users. See [Configure Clutter for your organization](#).

FAQ for Focused Inbox

Here are answers to Frequently Asked Questions about Focused Inbox.

Can I control how I roll out Focused Inbox in my organization?

Yes. You can turn Focused Inbox on or off for your entire organization, or you can turn it on or off for specified users. See above.

Is the Focused Inbox feature ONLY available for Office 2016 clients?

Yes, only users with Office 2016 are affected. The feature is not going to be backported to Outlook 2013 or earlier.

How long does it take for Focused Inbox changes to take place in Outlook?

Once you turn on or turn off Focused Inbox, the settings will take effect once your users close and restart Outlook.

What happens to Clutter once I turn on Focused Inbox?

After switching, you'll no longer receive less actionable email in the Clutter folder. Instead, email will be split between the Focused and Other tabs in your inbox. The same algorithm that moved items to the Clutter folder now powers Focused Inbox, meaning that any emails that were set to move to Clutter will now be moved to Other. Any messages already in your Clutter folder will remain there until you decide to delete or move them.

Check out this post by [Tony Redmond](#), Microsoft MVP: [How the Focused Inbox Replaces Clutter Inside Office 365](#).

Can I keep users on Clutter? What is Microsoft's recommendation when it comes to using Clutter vs Focused Inbox?

Yes, you can keep users on Clutter and disable Focused Inbox, however, eventually Clutter will be fully replaced with Focused Inbox so Microsoft's recommends moving to Focused Inbox now. To learn more about when you use Clutter with Exchange Online, see this blog post: [Update on Focused Inbox and our plans for Clutter](#).

Should I disable Clutter for my end users if we are going to move everyone to Focused Inbox?

No. It's possible to disable Clutter for a mailbox explicitly by running the Set-Clutter cmdlet. However, if you do this, the mailbox owner will see messages that were previously redirected to the Clutter folder remain in the Inbox and they'll have to process those messages until their client is upgraded to a version that supports the Focused Inbox. It's therefore best not to disable Clutter until the upgraded clients are available.

Why are there two different cmdlets for managing Focused Inbox?

There are two states associated with Focused Inbox.

- **Organization Level:** Focused Inbox state, and an associated last update time-stamp.
- **Mailbox Level:** Focused Inbox state, and an associated last update time-stamp

How does Outlook decide to show the Focused Inbox experience with these two states?

Outlook decides to show the experience by choosing which cmdlet has the latest time stamp. By default, both time stamps are "null" and in this case, the feature is enabled.

Why does the Get-FocusedInbox cmdlet return "true", when I've turned Focused Inbox off in my organization?

There are two cmdlets for controlling Focused Inbox. When you run Get-FocusedInbox for a mailbox, it returns the mailbox level state of the feature. The experience in Outlook is chosen based on which cmdlet state was last modified.

Can I run a script to see who has turned on Focused Inbox?

No, and this is by design. Focused Inbox enablement is a client-side setting, so all the cmdlet can do is tell you if the user's mailbox is eligible for the client experience. It is possible for it to be simultaneously enabled in some clients and disabled in others, for example, enabled in Outlook app and Outlook Mobile but disabled in Outlook on the web.

Related content

[Configure Clutter for your organization](#) (article)

[Configure shared mailbox settings](#) (article)

[Create signatures and disclaimers](#) (video)

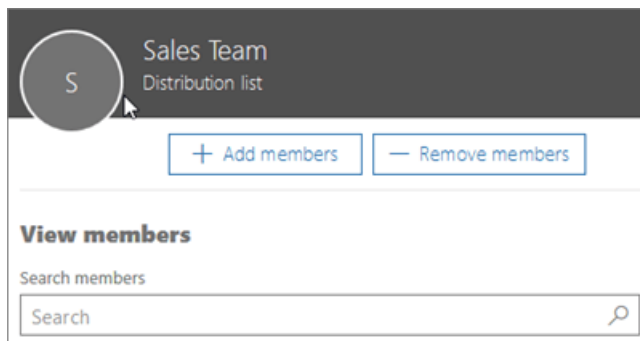
Add a user or contact to a distribution group

7/12/2021 • 2 minutes to read • [Edit Online](#)

As the admin of an organization, you may need to add one of your users or contacts to a distribution group (see [Create distribution groups in Microsoft 365](#)). For example, you can add employees or external partners or vendors to an email distribution group.

Add a user or contact to a distribution group

1. In the admin center, go to the **Groups** > **Groups** page.
2. On the **Groups** page, select the name of the group you want to add a contact to.
3. On the **Members** tab, select **View all and manage members**.
4. On the **View Members** page, select **Add members**, and select the user or contact you want to add to the distribution group.



5. Select **Save** and then **Close**.

Watch: Add a user to a distribution list

Next steps

Learn to [send email as a distribution group in Microsoft 365](#).

Related content

[Manage clutter for your organization](#) (article)

[Create a shared mailbox](#) (article)

Configure Clutter for your organization

7/12/2021 • 2 minutes to read • [Edit Online](#)

TIP

Focused Inbox is going to replace Clutter. Learn more: [Update on Focused Inbox and our plans for Clutter](#)

As an admin, you may have to manage the Clutter feature in Microsoft 365. To turn the Clutter feature on/off for users in your organization, you must use Exchange PowerShell. (Individuals can turn it on/off using these instructions: [Turn off/on Clutter in Outlook](#).)

Check out [Using PowerShell with Exchange Online](#) and [Connect to Exchange Online PowerShell](#) for details on using Exchange PowerShell. You need to have an account that has at least the Exchange Service administrator role and the ability to connect to Exchange Online with PowerShell.

Turn Clutter on using Exchange PowerShell

You can enable Clutter manually for a mailbox by running the [Set-Clutter](#) cmdlet. You can also view Clutter settings for mailboxes in your organization by running the [Get-Clutter](#) cmdlet.

Turn on Clutter for a single user named Allie Bellew

```
Set-Clutter -Identity "Allie Bellew" -Enable $true
```

Turn Clutter off using Exchange PowerShell

You can disable Clutter manually for a mailbox by running the [Set-Clutter](#) cmdlet. You can also view Clutter settings for mailboxes in your organization by running the [Get-Clutter](#) cmdlet.

Turn off Clutter for a single user named Allie Bellew:

```
Set-Clutter -Identity "Allie Bellew" -Enable $false
```

If you use PowerShell to bulk create your users, then you'll need to run [Set-Clutter](#) against each user's mailbox to manage Clutter.

When does the Clutter on/off switch appear to users in Outlook on the web?

As an admin, you can re-enable Clutter using Exchange PowerShell. Once this is done, Focused Inbox will be turned off and Clutter will be active again.

If you're using Outlook on the web with a Microsoft 365 Business Premium subscription:

- If user currently has Clutter enabled:
 - Clutter settings appear
- If user currently has Focused Inbox enabled:
 - Clutter settings will not appear
- If neither Clutter or Focused Inbox is enabled:

- Both Clutter and Focused Inbox appear as options in the user's Mail Settings

If you're using Outlook.com:

- If user currently has Clutter enabled:
 - Clutter settings appear
- If user currently has Focused Inbox enabled:
 - Clutter settings will not appear
- If neither Clutter or Focused Inbox is enabled:
 - Both Clutter and Focused Inbox appear as options in the user's Mail Settings
- If user enabled Focused Inbox at some point in the past:
 - Clutter settings will never appear

Otherwise,

- Clutter settings will appear

Related content

[Use Clutter to sort low priority messages in Outlook](#) (article)

[Use Clutter to sort low priority messages in OWA](#) (article)

[Turn off Clutter in Outlook](#) (article)

Add a domain to Microsoft 365

7/12/2021 • 3 minutes to read • [Edit Online](#)

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

*To Add, modify or remove domains you **must** be a **Global Administrator** of a [business or enterprise plan](#). These changes affect the whole tenant, Customized administrators or regular users won't be able to make these changes.*

Add a domain

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

1. Go to the admin center at <https://admin.microsoft.com>.
1. Go to the admin center at <https://portal.office.de/adminportal>.
1. Go to the admin center at <https://portal.partner.microsoftonline.cn>.
2. Go to the **Settings > Domains** page.
3. Select **Add domain**.
4. Enter the name of the domain you want to add, then select **Next**.
5. Choose how you want to verify that you own the domain.
 - a. If your domain registrar uses [Domain Connect](#), Microsoft [will set up your records automatically](#) by having you sign in to your registrar and confirm the connection to Microsoft 365. You'll be returned to the admin center and Microsoft will then automatically verify your domain.
 - b. You can use a TXT record to verify your domain. Select this and select **Next** to see instructions for how to add this DNS record to your registrar's website. This can take up to 30 minutes to verify after you've added the record.
 - c. You can add a text file to your domain's website. Select and download the .txt file from the setup wizard, then upload the file to your website's top level folder. The path to the file should look similar to: `http://mydomain.com/ms39978200.txt`. We'll confirm you own the domain by finding the file on your website.
6. Choose how you want to make the DNS changes required for Microsoft to use your domain.
 - a. Choose **Add the DNS records for me** if your registrar supports [Domain Connect](#), and Microsoft [will set up your records automatically](#) by having you sign in to your registrar and confirm the connection to Microsoft 365.
 - b. Choose **I'll add the DNS records myself** if you want to attach only specific Microsoft 365 services to your domain or if you want to skip this for now and do this later. **Choose this option if you know exactly what you're doing.**
7. If you chose to *add DNS records yourself*, select **Next** and you'll see a page with all the records that you need to add to your registrars website to set up your domain.

If the portal doesn't recognize your registrar, you can [follow these general instructions](#).

If you don't know the DNS hosting provider or domain registrar for your domain, see [Find your domain registrar or DNS hosting provider](#).

If you want to wait for later, either unselect all the services and click **Continue**, or in the previous domain connection step choose **More Options** and select **Skip this for now**.

8. Select **Finish** - you're done!

Add or edit custom DNS records

Follow the steps below to add a custom record for a website or 3rd party service.

1. Sign in to the Microsoft admin center at <https://admin.microsoft.com>.
2. Go to the **Settings > Domains** page.
3. On the **Domains** page, select a domain.
4. Under **DNS settings**, select **Custom Records**; then select **New custom record**.
5. Select the type of DNS record you want to add and type the information for the new record.
6. Select **Save**.

Registrars with Domain Connect

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

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

NOTE

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

Domain Connect registrars integrating with Microsoft 365

- [1&1 IONOS](#)
- [EuroDNS](#)
- [Cloudflare](#)
- [GoDaddy](#)
- [WordPress.com](#)
- [Plesk](#)
- [MediaTemple](#)
- SecureServer or WildWestDomains (GoDaddy resellers using SecureServer DNS hosting)
 - Examples:
 - [DomainsPricedRight](#)
 - [DomainRightNow](#)

What happens to my email and website?

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

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

Related content

[Domains FAQ \(article\)](#)

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

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

Buy a domain name

7/12/2021 • 2 minutes to read • [Edit Online](#)

NOTE

If your organization uses Office 365 operated by 21Vianet in China, see [How to buy a domain for Office 365 operated by 21Vianet in China](#).

*To Add, modify or remove domains you **must** be a **Global Administrator** of a [business or enterprise plan](#). These changes affect the whole tenant, Customized administrators or regular users won't be able to make these changes.*

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

Sign in and go to Settings > Domains > Buy a domain

1. In the admin center, go to the **Settings** > **Domains** page.
2. On the **Domains** page, select **Buy domain**.

You can choose from the following top level domains for your domain.

- .biz
- .com
- .info
- .me
- .mobi
- .net
- .org
- .tv
- .co.uk
- org.uk

NOTE

When you select **Buy domain**, you may be redirected to your Microsoft partner's website if the tenant is purchased/managed through a Microsoft partner.

Domain Privacy

We offer a free Domain Privacy Subscription with the purchase of a domain. This keeps your contact information attached to the registration of your domain with ICANN private. [Learn more](#).

Buy a domain from another domain registrar

If you want to buy a domain from a domain registrar other than [GoDaddy](#), we recommend you use one below that supports automatic setup (Domain Connect).

- [1&1 IONOS](#)
- [WordPress](#)

Transfer your domain to a different domain registrar

If your domain is managed by a provider that doesn't support all the necessary DNS records, you can transfer it to a different registrar. When you transfer the domain, you change who you send payments to in order to renew and keep your domain name.

Request the transfer at the registrar that you want to move your domain to. Look on their website for an option such as **Transfer DNS**. Be aware that after they make the changes, it can take a few days update across the Internet.

How to buy a domain for Office 365 operated by 21Vianet

If you don't already have your own domain, you can easily buy one online at a domain name registrar, domain reseller, or even at your current Internet provider. You get a domain name when you sign up for Office 365 operated by 21Vianet, for example, contoso.partner.onmschina.cn. But you may want to use a custom domain name, like fourthcoffee.com.

To set up a domain in Microsoft 365, you must own a domain and change some of the DNS records for your domain.

Caution

Some domain registrars or DNS hosting providers do not allow creating all the DNS records required by Microsoft 365. The following list of hosting providers supports all the needed records. If you're thinking of using a different hosting provider, [Service limitations when your hosting provider does not support SRV, CNAME, TXT, or redirection](#).

After you register your domain (at a domain registrar), you sign in to Microsoft 365 as an admin and set up your domain so you can use it with your email address and other services..

NOTE

The SharePoint Online Public Website information in this article only applies if your organization purchased Microsoft 365 prior to March 9, 2015.

Domain registrars that support all DNS records required for Microsoft 365

- [Oray](#)
- [HiChina](#)
- [east.net](#)
- [BIZCN](#)

Related content

[Add a domain to Microsoft 365](#) (article)

[Domains FAQ](#) (article)

[Update DNS records to keep your website with your current hosting provider](#) (article)

Remove a domain

7/12/2021 • 3 minutes to read • [Edit Online](#)

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

Are you removing your domain because you want to add it to a different Microsoft 365 subscription plan? Or do you just want to cancel your subscription? You can [change your plan or subscription](#) or [cancel your subscription](#).

Step 1: Move users to another domain

Move users

1. Go to the [admin center](#).
1. Go to the [admin center](#).
1. Go to the [admin center](#).
2. Select **Users > Active users**.
3. Select the boxes next to the names of all the users you want to move.
4. At the top of the page, and then choose **Change domains**.
5. In the **Change domains** pane, select a different domain.

You'll need to do this for yourself, too, if you're on the domain that you want to remove. When you edit the domain for your account, you'll have to log out and log back in using the new domain you chose to continue.

Move yourself

1. Go to the [admin center](#).
1. Go to the [admin center](#).
1. Go to the [admin center](#).
2. Go to **Users > Active Users**, and select your account from the list.
3. On the **Account** tab, select **Manage username**, and then choose a different domain.
4. At the top, select your account name, then select **Sign Out**.
5. Sign in with the new domain and your same password.

You can also use PowerShell to move users to another domain. See [Set-MsolUserPrincipalName](#) for more information. To set the default domain, use [Set-MsolDomain](#).

Step 2: Move groups to another domain

1. In the admin center, go to the **Groups > Groups** page.
1. In the [admin center](#), go to the **Groups > Groups** page.
1. In the [admin center](#), go to the **Groups > Groups** page.
2. Select the group name, and then on the **General** tab under **Email address, Primary**, select **Edit**.
3. Use the drop-down list to choose another domain.
4. Select **Save**, then **Close**. Repeat this process for any groups or distribution lists associated with the

domain that you want to remove.

Step 3: Remove the old domain

1. In the admin center, go to the **Settings** > [Domains](#) page.
1. In the admin center, go to the **Setup** > [Domains](#) page.
1. In the admin center, go to the **Setup** > [Domains](#) page.
2. On the **Domains** page, select the domain that you want to remove.
3. In the right pane, select **Remove**.
4. Follow any additional prompts, and then select **Close**.

How long does it take for a domain to be removed?

It can take as little as 5 minutes for Microsoft 365 to remove a domain if it's not referenced in a lot of places such as security groups, distribution lists, users, and Microsoft 365 groups. If there are many references that use the domain it can take several hours (a day) for the domain to be removed.

If you have hundreds or thousands of users, use PowerShell to query for all users and then move them to another domain. Otherwise, it's possible for a handful of users to be missed in the UI, and then when you go to remove the domain, you won't be able to and you won't know why. See [Set-MsolUserPrincipalName](#) for more information. To set the default domain, use [Set-MsolDomain](#).

Still need help?

NOTE

You can't remove the ".onmicrosoft.com" domain from your account. When you remove a domain, user accounts will revert back to the ".onmicrosoft.com" address as the Primary SMTP/UserprincipalName.

Still not working? Your domain might need to be manually removed. [Give us a call](#) and we'll help you take care of it!

NOTE

You can't remove the ".onmicrosoft.de" domain from your account. When you remove a domain, user accounts will revert back to the ".onmicrosoft.de" address as the Primary SMTP/UserprincipalName.

Still not working? Your domain might need to be manually removed. [Give us a call](#) and we'll help you take care of it!

NOTE

You can't remove the ".partner.onmschina.cn" domain from your account. When you remove a domain, user accounts will revert back to the ".partner.onmschina.cn" address as the Primary SMTP/UserprincipalName.

Still not working? Your domain might need to be manually removed. [Give us a call](#) and we'll help you take care of it!

Related content

[Domains FAQ](#) (article)

[Switch to a different Microsoft 365 for business plan \(article\)](#)

[Cancel your subscription \(article\)](#)

Transfer a domain from Microsoft to another host

3/5/2021 • 2 minutes to read • [Edit Online](#)

You can't transfer a Microsoft 365 domain to another registrar for 60 days after you purchase the domain from Microsoft.

NOTE

A *Whoisquery* shows a Microsoft purchased domain registrar as Wild West Domains LLC. However, only Microsoft should be contacted regarding your Microsoft 365 purchased domain.

Follow these steps to get a code at Microsoft 365, and then go to the other domain registrar website to set up transferring your domain name to the new registrar.

Transfer a domain

1. In the admin center, go to **Settings > Domains**.
2. On the **Domains** page, select the Microsoft 365 domain that you want to transfer to another domain registrar, and then select **Check health**.
3. At the top of the page, select **Transfer domain**.
4. On the **Choose where to transfer your domain** page, select **A different registrar**, and then click **Next**.
5. On the **Unlock domain transfer** page, select **Unlock transfer for <your domain>**, and then select **Next**.
6. Check your domain transfer contact information, and then select **Next**.
7. Copy the authorization code and wait about 30 minutes for your domain transfer status to change to **Unlocked for transfer** on the **Registration** tab before you proceed with next steps.
8. Go to the website of the domain registrar you want to manage your domain name going forward. Follow directions for transferring a domain (search for help on their website). This usually means paying transfer fees and giving the Authcode to the new registrar so they can initiate the transfer. Microsoft will email you to confirm we've received the transfer request, and the domain will transfer within 5 days.

You can find the authorization code **Registration** tab on the **Domains** page in Microsoft 365.

TIP

.uk domains require a different procedure. Contact Microsoft Support and request an **IPS Tag change** to match the registrar you want to manage your domain going forward. Once the tag changes, the domain immediately transfers to the new registrar. You will then need to work with the new registrar to complete the transfer, likely paying transfer fees and adding the transferred domain to your account with your new registrar.

9. After the transfer is complete, you'll renew your domain at the new domain registrar.
10. To finish the process, go back to the **Domains** page in the admin center, and then select **Complete domain transfer**. This will mark the domain as no longer purchased from Microsoft 365, and will disable the domain subscription. It will not remove the domain from the tenant, and will not affect

existing users and mailboxes on the domain.

NOTE

Microsoft 365 purchased domains are not eligible for nameserver changes or transferring the domain between Microsoft 365 organizations. If either of these are required, the domain registration must be transferred to another registrar.

Pilot Microsoft 365 from my custom domain

8/13/2021 • 7 minutes to read • [Edit Online](#)

You can pilot Microsoft 365 with these requirements and limitations:

- Your current email provider must provide email forwarding.
- You must manage your Microsoft 365 DNS records at your DNS hosting provider, rather than have Microsoft 365 manage these records for you.

To learn more, see [Add DNS records to connect your domain](#).

- Free/busy information for users on the other email server is not available.
- Admins can't administer all user accounts from a single location.
- Users might not be able to use Microsoft 365 spam filtering.
- This is recommended for a very small number of users and only applies to the use of email for a pilot.

Set up a Microsoft 365 pilot

Follow these steps to set up a Microsoft 365 pilot:

Step 1: Sign in to the Microsoft 365 admin center

1. Sign in to the [Microsoft 365 admin center](#) with your work or school account.
2. Select **Settings** > **Domains** in the left navigation pane.

Step 2: Verify that you own the domain you want to use

1. On the **Domains** page, select **Add domain**.
2. Type the domain name in the box, select **Use this domain**, and then select **Continue**.
3. Select the services you want to test with your domain, like email and instant messaging.
4. On the **Verify** domain page, follow the step-by-step instructions, and then select **Verify**.

It takes between a few minutes and 72 hours for DNS changes to take effect.

When verification is successful, you are asked to modify your DNS records.

Step 3: Mark the domain as shared in Exchange Online

1. In the Exchange admin center, in the **Mail flow** section, select **Accepted domains**, and then select the domain you want to modify.
2. Double-click to open the window, and then select **Internal Relay**.
3. Select **Save**.

This setting might require a few minutes to take effect.

Step 4: Unblock the existing email server (optional)

Microsoft 365 uses Exchange Online Protection (EOP) for spam protection. EOP might block your existing mail server if it detects a high volume of spam being forwarded by your current mail server. If you trust the spam protection for your other email provider, you can unblock the server in Microsoft 365.

NOTE

Unblocking your existing email server allows any spam that arrives through your original server to come to the Microsoft 365 mailboxes, and you can't evaluate how well Microsoft 365 prevents spam.

1. In the Exchange admin center navigation pane, select **Protection**, and then select **Connection filter**.
2. In the **IP Allow list**, select +, and add the mail server IP address for your current email provider.

Step 5: Create user accounts and set the primary reply-to address

1. In the Microsoft 365 admin center left navigation, select **Users** > **Active users**.
2. Create two test accounts by adding two existing users.

For each account, select + **Add a user**, and fill out the required information, including the password method you want to test.

To ensure a user's email stays the same, the **User name** field must match the user's current email address.

3. Choose the appropriate license, click **Next**, and then click **Finish adding**.
4. Next to **User name**, select your custom domain name from the drop-down list.
5. Select **Create** > **Close**.

Step 6: **Configure mail to flow from Microsoft 365 or Office 365 to Email server

There are two steps for this:

1. Configure your Microsoft 365 or Office 365 environment.
2. Set up a connector from Microsoft 365 or Office 365 to your email server.

1. Configure your Microsoft 365 or Office 365 environment

Make sure you have completed the following in Microsoft 365 or Office 365:

1. To set up connectors, you need permissions assigned before you can begin. To check what permissions you need, see the Microsoft 365 and Office 365 connectors entry in the [Feature permissions in Exchange Online](#) topic.
2. If you want EOP or Exchange Online to relay email from your email servers to the Internet, either:
 - Use a certificate configured with a subject name that matches an accepted domain in Microsoft 365 or Office 365. We recommend that your certificate's common name or subject alternative name matches the primary SMTP domain for your organization. For details, see [Prerequisites for your on-premises email environment](#).

-OR-

- Make sure that all your organization sender domains and subdomains are configured as accepted domains in Microsoft 365 or Office 365.

For more information about defining accepted domains, see [Manage accepted domains in Exchange Online](#) and [Enable mail flow for subdomains in Exchange Online](#).

3. Decide whether you want to use mail flow rules (also known as transport rules) or domain names to deliver mail from Microsoft 365 or Office 365 to your email servers. Most businesses choose to deliver mail for all accepted domains. For more information, see [Scenario: Conditional mail routing in Exchange Online](#).

NOTE

You can set up mail flow rules as described in [Mail flow rule actions in Exchange Online](#). For example, you might want to use mail flow rules with connectors if your mail is currently directed via distribution lists to multiple sites.

2. Set up a connector from Microsoft 365 or Office 365 to your email server

To create a connector in Microsoft 365 or Office 365, click **Admin**, and then click **Exchange** to go to the Exchange admin center. Next, click **mail flow**, and click **connectors**.

Set up connectors using the wizard.

To start the wizard, click the plus symbol +. On the first screen, choose **From** Office 365 and **To** Your Organization Mail server.

Click **Next**, and follow the instructions in the wizard. Click the **Help** or **Learn More** links if you need more information. The wizard will guide you through setup. At the end, make sure your connector validates. If the connector does not validate, double-click the message displayed to get more information, and see [Validate connectors](#) for help resolving issues.

Step 7: Update DNS records at your DNS hosting provider

Sign in to your DNS hosting provider's website, and follow the instructions at [Add DNS records to connect your domain](#).

Make the following two exceptions:

- Do not create a new MX record or change your existing MX record.
- If you already have a Sender Policy Framework (SPF) record for your previous email provider, instead of creating a new SPF (TXT) record for Exchange Online, add "include:spf.protection.outlook.com" to the current TXT record.

For example, "v=spf1 mx include:adatum.com include:spf.protection.outlook.com ~all".

If you don't have an SPF record, modify the one recommended by Microsoft 365 to include the domain for your current email provider, and add spf.protection.outlook.com. This authorizes outgoing messages from both email systems.

Step 8: Set up email forwarding at your current provider

At your current email provider, set up forwarding for your users email accounts to your onmicrosoft.com domain:

- Forward User A mailbox to `usera@yourcompany.onmicrosoft.com`
- Forward User B mailbox to `userb@yourcompany.onmicrosoft.com`

When you complete this step, all email sent to `usera@yourcompany.com` and `userb@yourcompany.com` is available in Microsoft 365.

NOTE

Contact your current email provider for the exact steps to set up email forwarding.

You don't need to keep a copy of messages at the current email provider.

Most providers forward email by leaving the Reply-to address of the sender intact so that replies go to the original sender.

Step 9: Test mail flow

1. Sign in to Outlook Web App using the credentials for User A.
2. Perform these tests:
 - Test local Microsoft email by sending an email, for example, to User B. The email is delivered immediately. In this scenario, the message is not routed to the mailbox for User B on your original server because the Microsoft 365 mailbox is local.
 - Test email to a user on the existing email system by sending an email, for example, to User C. The email is delivered to the mailbox for User C on your original mail server.
 - Verify that forwarding is set up properly from an outside account, or from an employee email account on the existing email system. For example, from the original server account for User C or a Hotmail account, send User A an email and verify that it arrives in the Microsoft 365 mailbox for User A.

Step 10: Move mailbox contents

Because you are moving only two test users, and User A and User B are both using Outlook, you can move the email by opening the old .PST file in the new Outlook profile and copying the messages, calendar items, contacts, and so on. For more information, see [Import email, contacts, and calendar from an Outlook .pst file](#).

After they're imported to the appropriate locations in the Microsoft 365 mailbox, the items can be accessed from any device, anywhere.

Change nameservers to set up Microsoft 365 with any domain registrar

8/5/2021 • 7 minutes to read • [Edit Online](#)

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

Follow these instructions to add and set up your domain in Microsoft 365 so your services like email and Teams will use your own domain name. To do this, you'll verify your domain, and then change your domain's nameservers to Microsoft 365 so the correct DNS records can be set up for you. Follow these steps if the following statements describe your situation:

- You have your own domain and want to set it up to work with Microsoft 365.
- You want Microsoft 365 to manage your DNS records for you. (If you prefer, you can [manage your own DNS records](#).)

Add a TXT or MX record for verification

NOTE

You will create only one or the other of these records. TXT is the preferred record type, but some DNS hosting providers don't support it, in which case you can create an MX record instead.

Before you use your domain with Microsoft 365, we have to make sure that you own it. Your ability to log in to your account at your domain registrar and create the DNS record proves to Microsoft 365 that you own the domain.

NOTE

This record is used only to verify that you own your domain; it doesn't affect anything else. You can delete it later, if you like.

Find the area on your DNS hosting provider's website where you can create a new record

1. Sign in to your DNS hosting provider's website.
2. Choose your domain.
3. Find the page where you can edit DNS records for your domain.

Create the record

Depending on whether you are creating a TXT record or an MX record, do one of the following:

If you create a TXT record, use these values:

RECORD TYPE	ALIAS OR HOST NAME	VALUE	TTL
-------------	--------------------	-------	-----

RECORD TYPE	ALIAS OR HOST NAME	VALUE	TTL
TXT	Do one of the following: Type @ or leave the field empty or type your domain name. Note: Different DNS hosts have different requirements for this field.	MS=ms XXXXXXXX Note: This is an example. Use your specific Destination or Points to Address value here, from the table in Microsoft 365. How do I find this?	Set this value to 1 hour or to the equivalent in minutes (60), seconds (3600), etc.

If you create an MX record, use these values:

RECORD TYPE	ALIAS OR HOST NAME	VALUE	PRIORITY	TTL
MX	Type either @ or your domain name.	MS=ms XXXXXXXX Note: This is an example. Use your specific Destination or Points to Address value here, from the table in Microsoft 365. How do I find this?	For Priority , to avoid conflicts with the MX record used for mail flow, use a lower priority than the priority for any existing MX records. For more information about priority, see What is MX priority?	Set this value to 1 hour or to the equivalent in minutes (60), seconds (3600), etc.

Save the record

Now that you've added the record at your domain registrar's site, you'll go back to Microsoft 365 and request Microsoft 365 to look for the record.

When Microsoft 365 finds the correct TXT record, your domain is verified.

1. In the admin center, go to the **Settings** > **Domains** page.
2. On the **Domains** page, select the domain that you are verifying.
3. On the **Setup** page, select **Start setup**.
4. On the **Verify domain** page, select **Verify**.

NOTE

Typically it takes about 15 minutes for DNS changes to take effect. However, it can occasionally take longer for a change you've made to update across the Internet's DNS system. If you're having trouble with mail flow or other issues after adding DNS records, see [Troubleshoot issues after changing your domain name or DNS records](#).

Change your domain's nameserver (NS) records

When you get to the last step of the domains setup wizard in Microsoft 365, you have one task remaining. To set up your domain with Microsoft 365 services, like email, you change your domain's nameserver (or NS) records at your domain registrar to point to the Microsoft 365 primary and secondary nameservers. Then, because

Microsoft 365 hosts your DNS, the required DNS records for your services are set up automatically for you. You can update the nameserver records yourself by following the steps your domain registrar may provide in the help content at their website. If you're not familiar with DNS, contact support at the domain registrar.

To change your domain's nameservers at your domain registrar's website yourself, follow these steps:

1. Find the area on the domain registrar's website where you can change the nameservers for your domain or an area where you can use custom nameservers.
2. Create nameserver records, or edit the existing nameserver records to match the following values:
 - First nameserver: ns1.bdm.microsoftonline.com
 - Second nameserver: ns2.bdm.microsoftonline.com
 - Third nameserver: ns3.bdm.microsoftonline.com
 - Fourth nameserver: ns4.bdm.microsoftonline.com

TIP

It's best to add all four records, but if your registrar only supports two, add **ns1.bdm.microsoftonline.com** and **ns2.bdm.microsoftonline.com**.

3. Save your changes.

Caution

When you change your domain's NS records to point to the Microsoft 365 nameservers, all the services that are currently associated with your domain are affected. If you skipped any steps of the wizard, such as adding email addresses, or if you're using your domain for blogs, shopping carts, or other services, there are additional steps that are required. Otherwise this change could result in service downtime, such as lack of email access or your current website being inaccessible.

1. Find the area on the domain registrar's website where you can edit the nameservers for your domain.
2. Create two nameserver records, or edit the existing nameserver records to match the following values:
 - First nameserver: ns1.dns.partner.microsoftonline.cn
 - Second nameserver: ns2.dns.partner.microsoftonline.cn

TIP

You should use at least two nameserver records. If there are any other nameservers listed, you can either delete them, or change them to **ns3.dns.partner.microsoftonline.cn** and **ns4.dns.partner.microsoftonline.cn**.

3. Save your changes.

Caution

When you change your domain's NS records to point to the Office 365 operated by 21Vianet nameservers, all the services that are currently associated with your domain are affected. If you skipped any steps of the wizard, such as adding email addresses, or if you're using your domain for blogs, shopping carts, or other services, there are additional steps that are required. Otherwise this change could result in service downtime, such as lack of email access or your current website being inaccessible.

For example, here are some additional steps that might be required for email and website hosting:

- Move all email addresses that use your domain to Microsoft 365 before you change your NS records.
- Want to add a domain that's currently used with a website address, like `https://www.fourthcoffee.com`? You can take below steps while you add the domain to keep its website hosted where the site is hosted now so people can still get to the website after you change the domain's NS records to point to Microsoft

365.

1. In the admin center, go to the **Settings** > **Domains** page.
2. On the **Domains** page, select a domain.
3. On the domain details page, select the **DNS records** tab.
4. Select **Add record**.
5. In the **Add a custom DNS record** pane, from the **Type** dropdown list, select **A (Address)**.
6. In the **Host name or Alias** box, type @.
7. In the **IP Address** box, type the static IP address for the website where it's currently hosted. For example, 172.16.140.1.

IMPORTANT

This must be a *static* IP address for the website, not a *dynamic* IP address. To make sure you can get a static IP address for your public website, check with the site that hosts your website.

8. If you want to change the TTL setting for the record, select a new length of time from the **TTL** dropdown list. Otherwise, continue to step 9.
9. Select **Save**.

In addition, you can create a CNAME record to help customers find your website.

1. Select **Add record**.
2. In the **Add a custom DNS record** pane, from the **Type** dropdown list, select **CNAME (Alias)**.
3. In the **Host name or Alias** box, type **www**.
4. In the **Points to address** box, type the fully qualified domain name (FQDN) for your website. For example, **contoso.5om**.
5. If you want to change the TTL setting for the record, select a new length of time from the **TTL** dropdown list. Otherwise, continue to step 6.
6. Select **Save**.

After the nameserver records are updated to point to Microsoft, your domain setup is complete. Email is routed to Microsoft, and traffic to your website address continues to go to your current website host.`

NOTE

Your nameserver record updates may take up to several hours to update across the Internet's DNS system. Then your Microsoft email and other services will be all set to work with your domain.

Related content

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

[Find and fix issues after adding your domain or DNS records](#) (article)

[Manage domains](#) (link page)

Add DNS records to connect your domain

8/13/2021 • 6 minutes to read • [Edit Online](#)

If you purchased a domain from a third-party hosting provider, you can connect it to Microsoft 365 by updating the DNS records in your registrar's account.

At the end of these steps, your domain will stay registered with the host that you purchased the domain from, but Microsoft 365 can use it for your email addresses (like user@yourdomain.com) and other services.

If you don't add a domain, people in your organization will use the onmicrosoft.com domain for their email addresses until you do. It's important to add your domain before you add users, so you don't have to set them up twice.

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

Step 1: Add a TXT or MX record to verify you own the domain

Recommended: Verify with a TXT record

First, you need to prove you own the domain you want to add to Microsoft 365.

1. Sign in to the Microsoft 365 admin center and select **Show all** > **Settings** > **Domains**.
2. In a new browser tab or window, sign in to your DNS hosting provider, and then find where you manage your DNS settings (e.g., Zone File Settings, Manage Domains, Domain Manager, DNS Manager).
3. Go to your provider's DNS Manager page, and add the TXT record indicated in the admin center to your domain.

Adding this record won't affect your existing email or other services and you can safely remove it once your domain is connected to Microsoft 365.

Example:

- TXT Name: @
 - TXT Value: MS=ms##### (unique ID from the admin center)
 - TTL: 3600 (or your provider default)
4. Save the record, go back to the admin center, and then select **Verify**. It typically takes around 15 minutes for record changes to register, but sometimes it can take longer. Give it some time and a few tries to pick up the change.

When Microsoft finds the correct TXT record, your domain is verified.

Verify with an MX record

If your registrar doesn't support adding TXT records, you can verify by adding an MX record.

1. Sign in to the Microsoft 365 admin center and select **Show all** > **Settings** > **Domains**.
2. In a new browser tab or window, sign in to your DNS hosting provider, and then find where you manage your DNS settings (e.g., Zone File Settings, Manage Domains, Domain Manager, DNS Manager).
3. Go to your provider's DNS Manager page, and add the MX record indicated in the admin center to your domain.

This MX record's **Priority** must be the highest of all existing MX records for the domain. Otherwise, it can interfere with sending and receiving email. You should delete this records as soon as domain verification is

complete.

Make sure that the fields are set to the following values:

- Record Type:
- Priority: Set to the highest value available, typically .
- Host Name:
- Points to address: Copy the value from the admin center and paste it here.
- TTL: (or your provider default)

When Microsoft finds the correct MX record, your domain is verified.

Step 2: Add DNS records to connect Microsoft services

In a new browser tab or window, sign in to your DNS hosting provider, and find where you manage your DNS settings (e.g., Zone File Settings, Manage Domains, Domain Manager, DNS Manager).

You'll be adding several different types of DNS records depending on the services you want to enable.

Add an MX record for email (Outlook, Exchange Online)

Before you begin: If users already have email with your domain (such as user@yourdomain.com), create their accounts in the admin center before you set up your MX records. That way, they'll continue to receive email. When you update your domain's MX record, all new email for anyone who uses your domain will now come to Microsoft 365. Any email you already have will stay at your current email host, unless you decide to [migrate email and contacts to Microsoft 365](#).

You'll get the information for the MX record from the admin center domain setup wizard.

On your hosting provider's website, add a new MX record. Make sure that the fields are set to the following values:

- Record Type:
- Priority: Set to the highest value available, typically .
- Host Name:
- Points to address: Copy the value from the admin center and paste it here.
- TTL: (or your provider default)

Save the record, and then remove any other MX records.

Add CNAME records to connect other services (Teams, Exchange Online, AAD, MDM)

You'll get the information for the CNAME records from the admin center domain setup wizard.

On your hosting provider's website, add CNAME records for each service that you want to connect. Make sure that the fields are set to the following values for each:

- Record Type:
- Host: Paste the values you copy from the admin center here.
- Points to address: Copy the value from the admin center and paste it here.
- TTL: (or your provider default)

Add or edit an SPF TXT record to help prevent email spam (Outlook, Exchange Online)

Before you begin: If you already have an SPF record for your domain, don't create a new one for Microsoft 365. Instead, add the required Microsoft 365 values to the current record on your hosting providers website so that you have a *single* SPF record that includes both sets of values.

On your hosting provider's website, edit the existing SPF record or create an SPF record. Make sure that the

fields are set to the following values:

- Record Type:
- Host:
- TXT Value:
- TTL: (or your provider default)

Save the record.

Validate your SPF record by using one of these [SPF validation tools](#)

SPF is designed to help prevent spoofing, but there are spoofing techniques that SPF cannot protect against. To protect against these, once you've set up SPF, you should also set up DKIM and DMARC for Microsoft 365.

To get started, see [Use DKIM to validate outbound email sent from your domain in Microsoft 365](#) and [Use DMARC to validate email in Microsoft 365](#).

Add SRV records for communications services (Teams, Skype for Business)

On your hosting provider's website, add SRV records for each service you want to connect. Make sure that the fields are set to the following values for each:

- Record Type:
- Name:
- Target: Copy the value from the admin center and paste it here.
- Protocol: Copy the value from the admin center and paste it here.
- Service: Copy the value from the admin center and paste it here.
- Priority:
- Weight:
- Port: Copy the value from the admin center and paste it here.
- TTL: (or your provider default)

Save the record.

SRV record field restrictions and workarounds

Some hosting providers impose restrictions on field values within SRV records. Here are some common workarounds for these restrictions.

Name

If your hosting provider doesn't allow setting this field to @, leave it blank. Use this approach *only* when your hosting provider has separate fields for the Service and Protocol values. Otherwise, see the Service and Protocol notes below.

Service and Protocol

If your hosting provider doesn't provide these fields for SRV records, you must specify the **Service** and **Protocol** values in the record's **Name** field. (Note: Depending on your hosting provider, the **Name** field might be called something else, like: **Host**, **Hostname**, or **Subdomain**.) To add these values, you create a single string, separating the values with a dot.

Example:

Priority, Weight, and Port

If your hosting provider doesn't provide these fields for SRV records, you must specify them in the record's **Target** field. (Note: Depending on your hosting provider, the **Target** field might be called something else, like: **Content**, **IP Address**, or **Target Host**.)

To add these values, create a single string, separating the values with spaces and *sometimes ending with a dot* (check with your provider if you are unsure). The values must be included in this order: Priority, Weight, Port,

Target.

- Example 1: `100 1 443 sipdir.online.lync.com.`
- Example 2: `100 1 443 sipdir.online.lync.com`

Related content

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

[Find and fix issues after adding your domain or DNS records](#) (article)

[Manage domains](#) (link page)

Find and fix issues after adding your domain or DNS records

7/12/2021 • 3 minutes to read • [Edit Online](#)

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

Getting your domain set up to work with Microsoft 365 can be challenging. The DNS system is nitpicky to work with, and the DNS setup for your domain affects important business activities, like email!

NOTE

You can check for problems with your domain by checking its status. Go to **Setup > Domains** and view the notifications in the **Status** column. If you see an issue, select the three dots (more actions), and then choose **Check health**. The pane that opens will describe any issues occurring with your domain.

What's going on?

- [Can't verify your domain?](#)
- [Outlook isn't working?](#)
- [Everyone's email got switched to Microsoft 365 and you only wanted YOUR email to switch?](#)
- [Can't confirm non-profit or school account status?](#)
- [Services not working with your domain?](#)
- [Accessing your website isn't working?](#)

Can't verify your domain?

There are a couple of common reasons that domain verification doesn't work as it should:

1. **The verification record value isn't quite correct.** Doublecheck that you've copied and pasted the exact value into the TXT verification record at your DNS host. One common issue is not including the "MS=" part of the record. We need that too!
2. **The record hasn't been saved.** At some DNS hosts, you have to take an extra step to save the zone file (where the DNS record is stored) so that it will update across the Internet. Make sure you've saved your changes so Microsoft 365 can see and verify the record.
3. **The record hasn't updated across the Internet.** It typically only takes a few minutes for us to be able to see the new record, but occasionally it can take as long as a few hours.

Outlook isn't working?

If you've set up your MX record and other DNS records correctly for your domain, but mail doesn't work, let us help you [fix your Outlook problems](#).

Everyone's email got switched to Microsoft 365 and you only wanted

YOUR email to switch?

When you add your domain to Microsoft 365, typically your domain's MX record is updated (by you or Microsoft 365) to point to Microsoft 365, and ALL email sent to that domain will start coming to Microsoft 365. Make sure you've created mailboxes in Microsoft 365 for everyone who has email on your domain BEFORE you change the MX record.

What if you don't want to move email for everyone on your domain to Microsoft 365? You can take steps to [pilot Microsoft 365 with just a few email addresses instead](#).

Can't confirm non-profit or school account status?

There are a couple of scenarios when you just need to verify your organization's domain and not set up any services. For example, to prove to Microsoft 365 that your organization qualifies for a school subscription.

Check out the guidance in [Verify your Microsoft 365 domain to prove ownership, nonprofit or education status, or to activate Yammer](#) to make sure you've completed all the required steps. It's a little different for each situation.

Services not working with your domain?

We can help you track down issues with your domain's DNS setup. The domains troubleshooter in Microsoft 365 will show you any records that need fixing, and exactly what the records need to be set to.

TIP

Got your DNS set up correctly, but mail doesn't work in Outlook on your desktop? Check out the [different mail flow scenarios you can have with Microsoft 365](#) to make sure you've got things set up correctly for your business. Or get more troubleshooting help with email here: [Fix Outlook problems](#).

Accessing your website isn't working?

If you've fixed any DNS issues and you're still having trouble, try one of the following.

- People can't get to your website at [www.mydomain.com](#): [Track down website issues](#)
- You can't update your A record or CNAME record to point to your website: [Update custom DNS records in Microsoft 365](#)

Related content

[Troubleshoot: Audit data on verified domain change](#) (article)

[Domains FAQ](#) (article)

Microsoft 365 Reports in the admin center

7/12/2021 • 3 minutes to read • [Edit Online](#)

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need an Microsoft 365 license at all. Perpetual license model will not be included in the reports.

Reports are available for the last 7 days, 30 days, 90 days, and 180 days. Data won't exist for all reporting periods right away. The reports become available within 48 hours.

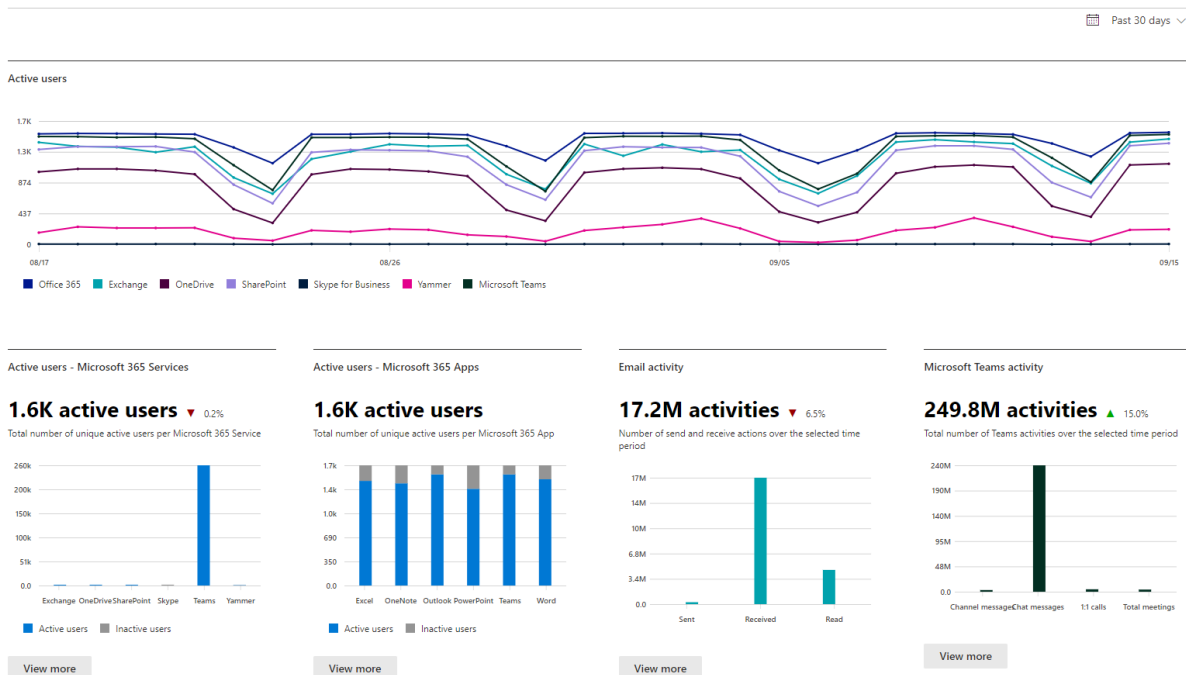
Watch: Act on a usage report in Office 365

How to get to the Reports dashboard

1. In the admin center, go to the **Reports** > **Usage** page.
1. In the **admin center**, go to the **Reports** > **Usage** page.
1. In the **admin center**, go to the **Reports** > **Usage** page.
2. Click on the **View more** button from the at-a-glance activity card for a service (such as email or OneDrive) to see the report detail page. In there different reports for the service are provided in tabs.

Usage

M365 usage reports show how people in your business are using M365 services. Reports are available for the last 7 days, 30 days, 90 days, and 180 days. Data won't exist for all reporting periods right away. The reports become available within 48 hours. [Learn more about M365 usage reports](#)



Who can see reports

People who have the following permissions:

- Global admins: We recommend that only a few people in your company have this role. It reduces the risk to your business.

- Exchange admins
- SharePoint admins
- Skype for Business admins
- Global reader
- Reports reader
- Teams Service Administrator
- Teams Communications Administrator

To learn more, see [About admin roles](#) and [Assign admin roles](#).

Which activity reports are available in the admin center

Depending on your subscription, here are the available reports.

- [Microsoft browser usage](#)
- [Email activity](#)
- [Mailbox usage](#)
- [Office activations](#)
- [Active Users](#)
- [Email apps usage](#)
- [Forms activity](#)
- [Dynamics 365 Customer Voice activity](#)
- [Microsoft 365 groups](#)
- [OneDrive for Business user activity](#)
- [OneDrive for Business usage](#)
- [Microsoft 365 Apps usage](#)
- [SharePoint site usage](#)
- [SharePoint activity](#)
- [Skype for Business Online activity](#)
- [Skype for Business Online conference organized activity](#)
- [Skype for Business Online conference participant activity](#)
- [Skype for Business Online peer-to-peer activity](#)
- [Yammer activity](#)
- [Yammer device usage](#)
- [Yammer groups activity report](#)
- [Microsoft Teams user activity](#)
- [Microsoft Teams device usage](#)

How to view licensing information

- To see how many licenses you have assigned and unassigned, in the admin center, go to the **Billing** > [Licenses](#) page.
- To see who is licensed, unlicensed, or guest, in the admin center, go to the **Users** > [Active users](#) page.

How to view usage information for a specific user

Use the service reports to research how much a specific user is using the service. For example, to find out how much mailbox storage a specific user has consumed, open the Mailbox usage report, and sort the users by name. If you have thousands of users, export the report to Excel so you filter through the list quickly.

You can't generate a report where you enter a user's account and then get a list of which services they are using and how much.

There are circumstances where new users show up as **unknown**. This is usually due to occasional delays in creating user profiles.

Hide user details in the reports

If you want to hide user level information when you're generating your reports, you can quickly make that change in the admin center.

1. In the admin center, go to the **Settings** > [Services & add-ins](#) page.
2. Select **Reports**.
3. In the **Reports** pane, select the options you want, and then save your changes.

Your user list will look like this:

User details					Manage columns	Export
User name	Last activity date (UTC)	Email sent	Email received	Email read		
AC23A081E88119A1E4407C8011EABF61	Wednesday, April 06, 2016	308	2,143	2,153		
4797E2FD78CC562671A4D5E5B3D093C3	Wednesday, April 06, 2016	64	470	491		
AA02F49A7A93023AEC7A2C97BEBASEFF	Wednesday, April 06, 2016	15	44	51		
B3DED5B41D044DBBD5F6A1E8EBC4BDC0	Wednesday, April 06, 2016	141	1,563	694		
B25CEE890D926131ACA4C006D24E97BF	Wednesday, April 06, 2016	759	6,123	2,078		
B79C253F4E3B4785CAB06C2AF851BFC7	Wednesday, April 06, 2016	1,797	1,524	2,714		
D2A359E54D15AA2BA67AD67EA39C18A1	Wednesday, April 06, 2016	321	1,307	1,750		
FA6E361CFD868C8CACAFAFAA36EDEB86	Wednesday, April 06, 2016	686	376	473		

It'll take a few minutes for these changes to take effect on the reports in the reports dashboard. This setting also applies to the reports API.

What happens to usage data when a user account is closed?

Whenever you close a user's account, Microsoft will delete that user's usage data within 30 days. That user will still be included in the Activity chart totals (see number 1) for the periods she was active in, but will not appear in the User Details table (see number 2).

However, when you select a particular day (see number 3), up to 28 days from the current date, the report show the user's usage for that day in the User Details table (see number 2).

Related content

[Reports in the Security & Compliance Center](#) (article)

[Microsoft 365 usage analytics](#) (article)

[Customize the reports in Microsoft 365 usage analytics \(article\)](#)

Microsoft Productivity Score

7/12/2021 • 5 minutes to read • [Edit Online](#)

Productivity Score supports the journey to digital transformation with insights about how your organization uses Microsoft 365 and the technology experiences that support it. Your organization's score reflects people and technology experience measurements and can be compared to benchmarks from organizations similar in size to yours.

It provides:

- **Metrics** to help you see where you are on your digital transformation journey.
- **Insights** about the data to help you identify opportunities to improve productivity and satisfaction in your organization.
- **Recommended actions** you can take to help your organization use Microsoft 365 products efficiently.

We provide metrics, insights, and recommendations in two areas:

- **People experiences:** Quantifies how the organization works using Microsoft 365 categories like content collaboration, mobility, communication, meetings, and teamwork.

For each of the mentioned categories, we look at public research to identify some best practices and associated benefits in the form of organizational effectiveness. For example, Forrester research has shown that when people collaborate and share content in the cloud (instead of emailing attachments), they can save up to 100 minutes a week. Furthermore, we quantify the use of these best practices in your organization to help you see where you are on your digital transformation journey.

- **Technology experiences:** Your organization depends on reliable and well-performing technology, as well as the efficient use of Microsoft 365. [Endpoint analytics](#) helps you understand how your organization can be impacted by performance and health issues with your hardware and software. Microsoft 365 apps health helps you understand whether the devices in your organization are running Microsoft 365 apps on recommended channels.

Before you begin

See [What is Endpoint Analytics](#) for an overview and prerequisite details. To learn more about Microsoft 365 network connectivity insights, read [the network connectivity overview](#).

For people experiences data, you need a Microsoft 365 for business or Office 365 for enterprise subscription. For endpoint analytics data for your tenant, you need to add Microsoft Intune to your subscription. Intune helps protect your organization's data by managing devices and apps. Once you have Intune, you can turn on endpoint analytics within the Intune experience. To learn more about Microsoft Intune, see the [Microsoft Intune documentation](#).

NOTE

A license to Workplace Analytics is not required to get the Productivity Score features.

Productivity Score is only available in the Microsoft 365 admin center and can only be accessed by IT professionals who have one of the following roles:

- Global admin
- Exchange admins

- SharePoint admin
- Skype for Business admin
- Teams admin
- Global Reader
- Reports Reader
- Usage Summary Reports Reader

NOTE

Only an IT professional with the Global Administrator role can sign up or opt in a tenant for Productivity Score.

The role-based access control model for Productivity Score helps organizations further digital transformation efforts with Microsoft 365 by providing the flexibility to assign roles to IT professionals within an organization.

Microsoft is committed to protecting individual privacy. This [privacy document](#) explains the controls we provide you, as your organization's IT administrator, to ensure that the information is actionable while not compromising the trust you place in Microsoft.

You can access the experience from Microsoft 365 Admin home under **Reports > Productivity Score**.

How the score is calculated

Your Productivity Score is based on the combined scores of your people and technology experiences categories. Each category is weighted equally, with a total of 100 points. The highest possible Productivity Score is 800.

Score categories

- Communication (100 points)
- Meetings (100 points)
- Content collaboration (100 points)
- Teamwork (100 points)
- Mobility (100 points)
- Endpoint analytics (100 points)
- Network connectivity (100 points)
- Microsoft 365 Apps Health (100 points)
- **Total possible = 800 points**

In each score category, we quantify the key indicators for how your organization is using Microsoft 365 in its journey towards digital transformation. We provide 28-day and 180-day views of the key activities. We also provide supporting metrics that are not part of the score calculation, but are important for helping you identify underlying usage statistics and configurations that you can address.

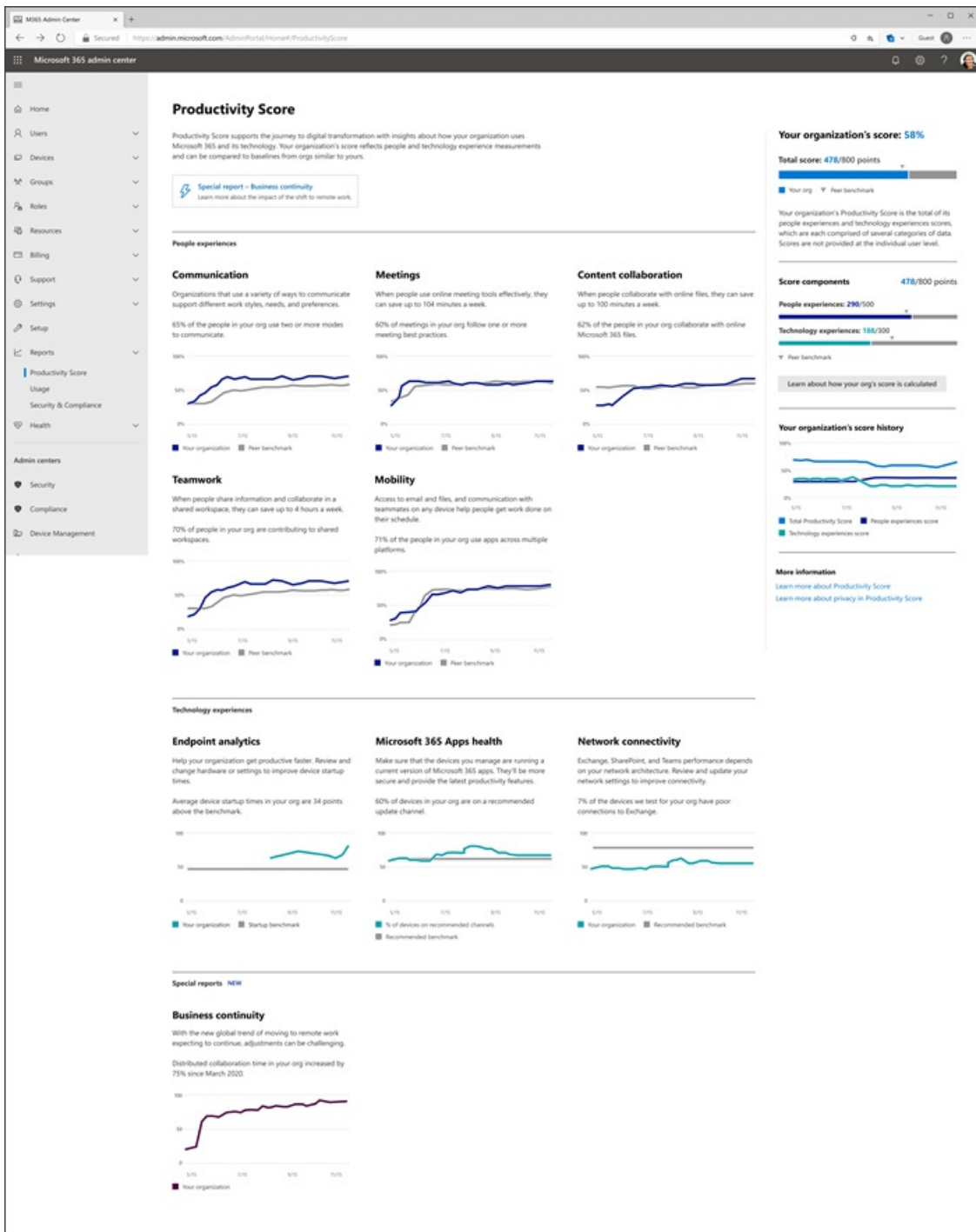
Products included in Productivity Score

Productivity Score includes data from Exchange, SharePoint, OneDrive, Teams, Word, Excel, PowerPoint, OneNote, Outlook, Yammer, and Skype.

Your organization's score is updated daily and reflects user actions completed in the last 28 (including the current day).

Interpreting your organization's Productivity Score

The Productivity Score home page shows your organization's total score and score history and the primary insight for each category.



Your organization's score is shown as a percent value and in points. You can see your points in the numerator and the maximum possible points in the denominator.

Peer benchmarks allow you to compare your organization's score with organizations like yours. The peer benchmark for the People experiences categories is calculated as the average of measures within a set of similar organizations. The set of organizations is composed of organizations in your region with a similar number of licensed users, types of licenses, industry, and tenure with Microsoft 365.

NOTE

Microsoft uses internal data to determine the industry that an organization maps to. Tenants under a parent organization get mapped to the same industry as the parent organization. Organizations cannot view or modify industry mappings.

The endpoint analytics peer benchmark includes targets for device startup performance and recommended software configuration based on aggregated median values across all tenants.

For network connectivity, the recommended benchmark is 80 points.

The **Score breakdown** section provides a breakdown of your Productivity Score with benchmarks by people and technology experience areas.

Score history displays how your score in each category has changed in the past six months.

The **People experiences** and **Technology experiences** areas contain the primary insights for the categories in those areas. You can select each category to see deeper insights.

Category details pages

Each category details page shows the primary insight and supporting metrics as well as related research and actions you can take to drive change in your organization. Research supports the importance and rationale behind the primary insights for each category. For more information, [read the Forrester report](#).

The details pages are:

- [Content collaboration – people experiences](#)
- [Communication – people experiences](#)
- [Meetings – people experiences](#)
- [Mobility – people experiences](#)
- [Teamwork – people experiences](#)
- [Microsoft 365 Apps health – technology experiences](#)
- [Endpoint Analytics](#)

Business continuity special report

The Business continuity report is a limited-time Workplace Intelligence report available to all Microsoft 365 customers to help them guide their organizations during this challenging time.

This report helps organizations understand:

- How collaboration and communication are affected by the shift to remote work.
- The impact on work-life balance as people adjust to working from home.
- Whether remote meetings support effective decision-making.

[Learn more about the Business continuity report](#)

[Learn more about Microsoft Graph](#)

NOTE

Users also have the option to get productivity insights from the [MyAnalytics dashboard](#).

We want to hear from you

Share your thoughts about Productivity Score and your ideas about how to improve it. Use the **Feedback** sections within the product and/or reach out to the Productivity Score team at prodscorefeedback@microsoft.com.

Related content

[Monitor Microsoft 365 activity by using reports](#) (article)

[Enable Microsoft 365 usage analytics](#) (article)

[Overview of the Microsoft 365 admin center \(video\)](#)

Content collaboration – People experiences

7/23/2021 • 10 minutes to read • [Edit Online](#)

Productivity Score provides insights into your organization's digital transformation journey through its use of Microsoft 365 and the technology experiences that support it. Your organization's score reflects people and technology experience measurements and can be compared to benchmarks from organizations similar to yours. The content collaboration category is part of the people experiences measurements. To learn more, check out the [Productivity Score overview](#) and read [Microsoft's Privacy Statement](#).

Prerequisites

To get started with Content collaboration insights, people in your organization need to be licensed for:

- OneDrive for Business
- SharePoint
- Exchange Online

For more information, see [assign licenses to users](#).

After people have been active in the above products at least once in the last 28 days, you will start to see the insights.

Why your organization's content collaboration score matters

A key aspect of digital transformation is how people collaborate in files. With your content on Microsoft 365, people access, create, modify, and collaborate on content with other people from any location. Research shows that when people collaborate with online files, each person saves an average of 100 minutes per week.

How we calculate the content collaboration score

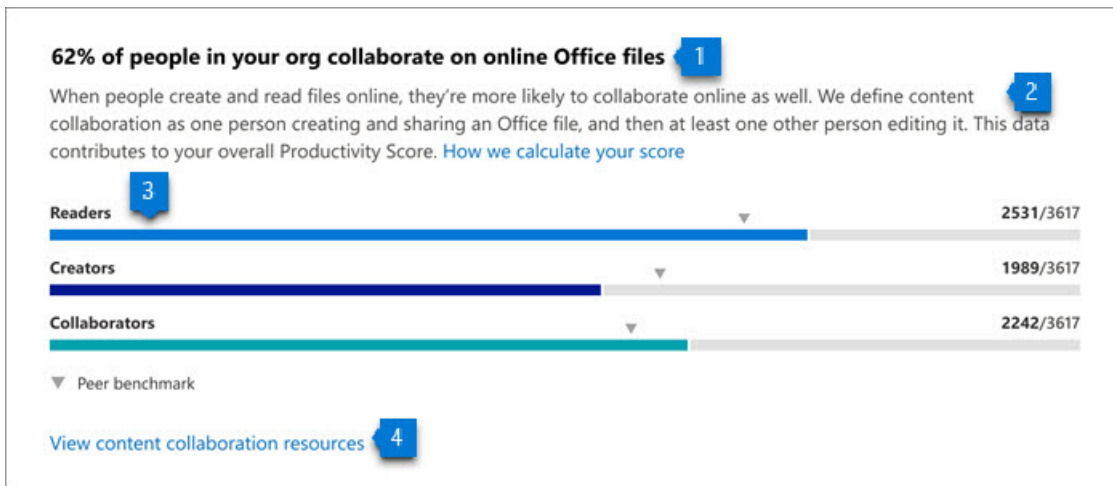
We provide a primary insight that contains the key metrics for content collaboration in your organization. Then, a scoring framework detailed below is used for these metrics to calculate your organization's score.

NOTE

On April 22, 2021, we changed how the collaborators metric is calculated. This affects the [primary insight](#), the [file collaboration insight](#), and the way the content collaboration score is measured. This change helps reduce noise in the data from non-human agents (or bots) from Microsoft and other third-party applications, resulting in a more accurate and actionable score.

Primary insight

Microsoft OneDrive for Business and SharePoint help people to easily create, read, and discover their individual and shared content in Microsoft 365 from across devices and applications. They also allow people to securely share and collaborate on content. The primary insight contains information from everyone who can use OneDrive for Business and SharePoint. Additionally it breaks down the details about how many people read, create, and collaborate on content stored in OneDrive for Business and SharePoint.



Types considered for this information include Word, Excel, PowerPoint, OneNote, and PDF files.

1. **Header:** Shows the percentage of people in your org who have access to OneDrive or SharePoint who are collaborating on content.
2. **Body:** Provides more information on how the behaviors of reading and creating files online are linked to collaborating on files.

3. **Visualization (current state):**

- Horizontal bars where the blue-colored portions represent the percentage of people enabled for file collaboration through OneDrive or SharePoint who have been **readers**, **creators**, or **collaborators** on online files in the last 28 days.

They're defined as follows:

Readers: People who access or download online files in OneDrive or SharePoint.

Creators: People who create, modify, upload, sync, check in, copy, or move online OneDrive or SharePoint files.

Collaborators: People who collaborate with online files by using OneDrive or SharePoint. Two people are collaborators if one of them reads or edits an online Office app or PDF after the other person has created or modified it, within a 28-day window.

NOTE

The files considered in the visualization are Word, Excel, PowerPoint, OneNote, or PDF files that are online and saved to OneDrive or SharePoint.

- Highlight (numerator/denominator) of the fraction is used to calculate the percentage expressed in each of the horizontal bars.
 - **Readers:**
 - Numerator: Number of people who access or download online files in OneDrive or SharePoint in the last 28 days
 - Denominator: Number of people who had access to OneDrive or SharePoint for at least 1 of the last 28 days
 - **Creators:**
 - Numerator: Number of people who create, modify, upload, sync, check in, copy, or move online files in OneDrive or SharePoint in the last 28 days
 - Denominator: Number of people who have had access to OneDrive or SharePoint for at least 1 of the last 28 days.
 - **Collaborators:**

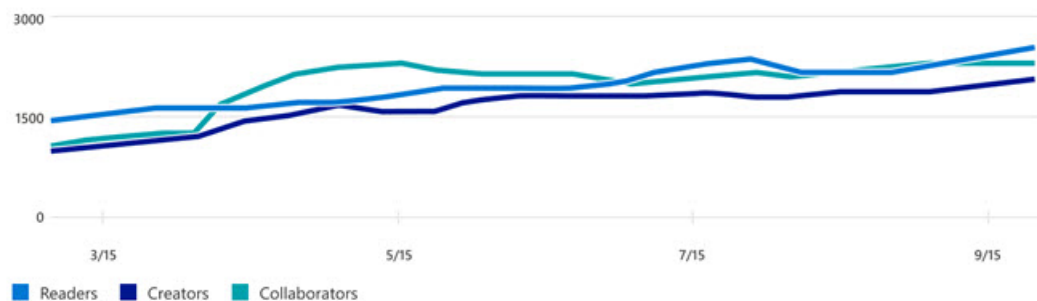
- Numerator: Number of people who have collaborated on online files in OneDrive or SharePoint in the last 28 days
- Denominator: Number of people who have had access to for OneDrive or SharePoint for at least 1 of the last 28 days
- Peer benchmark value for each of readers, creators, and collaborators is also shown as a percentage. In other words, the value of the number of creators is shown as a percentage of the number of people who have access to OneDrive or SharePoint.

4. **Link to resources:** Select this link to view collated videos, and other related help content.

Trend visualization of primary insight

The trend visualizations chart shows the trend-line of the primary insight key metrics for readers, creators, and collaborators, over the last 180 days. Each data point on the chart is an aggregate of activity for the last 28 days. Each creator data-point provides a count of all people who were tagged as creators within the last 28 days for each date on the x axis.

Number of readers, creators, and collaborators over time



Scoring framework

The content collaboration score for your organization measures at an aggregate (organization) level whether people are consistently reading, creating, or collaborating on online Office files such as Word, Excel, PowerPoint, OneNote, or PDFs, or in OneDrive or SharePoint.

Scores are not provided at the individual user level.

Explore how your organization collaborates

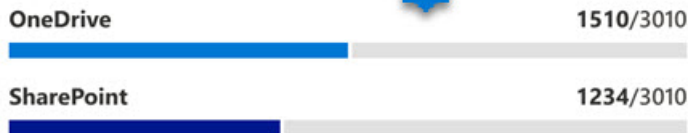
We also provide you with information that helps you gain visibility into how your organization collaborates on content. These additional metrics don't directly contribute to your Productivity Score but help you create an action plan as part of your digital transformation to help optimize the way people work.

Creating files in OneDrive or SharePoint

51% of people who use Office create files in OneDrive or SharePoint 1

Creating files in OneDrive or SharePoint means they're backed up, available from other devices, and ready for real-time collaboration. 2

People saving files online ⓘ 3



[View related content](#) 4

- 1. Header:** Highlights the percentage of people active on Microsoft 365 Office applications who create files on OneDrive or SharePoint.
- 2. Body:** Provides information about the value of content creation in OneDrive and SharePoint.
- 3. Visualization:** The breakdown in the visualization represents the extent to which people who are using Microsoft Office apps to create files in OneDrive and SharePoint, as follows:
 - **OneDrive:** The blue (colored) portion of the bar and the fraction on the bar represent the percentage of people active on Office applications creating content on OneDrive as follows:
 - Numerator: The number of people who create, modify, upload, sync, check in, copy, or move online Office files in OneDrive within the last 28 days.
 - Denominator: The number of people who have access to OneDrive or SharePoint and access office files within the last 28 days.
 - **SharePoint:** The blue (colored) portion of the bar and the fraction on the bar represent the percentage of people who are active on Office applications and create content on SharePoint as:
 - Numerator: The number of people who create, modify, upload, sync, check in, copy, or move online Office files (Microsoft Word, Excel, PowerPoint, or OneNote files) on SharePoint within the last 28 days.
 - Denominator: The number of people who have access to OneDrive or SharePoint and have accessed Office files within the last 28 days.
- 4. Link to resources:** Select this link to view help content.

Use of attachments in email

Use of attachments in email Understand how many users are attaching physical files in email rather than links to content in the cloud, and monitor the reduction of this number over time.

89% of people share files as an email attachment

Sharing a link to a file instead of attaching a copy in email makes sharing more secure and allows people to collaborate in real time.

People sharing files in email, by type ⓘ



[View related content](#)

1. **Header:** Highlights the percentage of people who use attachments in emails that were not saved to online files.
2. **Body:** Provides information about the value of sharing links to online files from a collaboration and security perspective.
3. **Visualization:** The breakdown in the visualization is meant to represent the extent to which people who are attaching content in emails are using different modes (files not saved to online files, links to online files):
 - **Attach files:** The blue (colored) portion of the bar and the fraction (numerator/denominator) on the bar represents the percentage of people using attachments in emails.
 - Numerator: The number of people who attach files to email that weren't saved to online file within the last 28 days.
 - Denominator: The number of people who have had access to Exchange and OneDrive, SharePoint, or both within the last 28 days.
 - **Links to online files:** The blue (colored) portion of the bar and the fraction (numerator/denominator) on the bar represent the percentage of people using attachments and attaching links to files in emails.
 - Numerator: The number of people attaching links to online files to emails within the last 28 days.
 - Denominator: The number of people who have access to Exchange and OneDrive, SharePoint, or both within the last 28 days.
4. **Link to resources:** Select this link to view help content.

Sharing of online files

10% of people share content externally 1

Customize SharePoint's sharing settings to help people collaborate with external partners or people in your organization who have different licenses. 2

People sharing content 3



[View related content](#) 4

1. **Header:** Highlights the percentage of people who have access to for OneDrive or SharePoint who are sharing files externally.
2. **Body:** Provides information about the admins' ability to change the file- sharing settings in the organization to enable the level of collaboration best suited to your organization.
3. **Visualization:** Represents the extent to which people who have access to OneDrive or SharePoint are sharing files internally or externally:
 - **Externally:** The blue (colored) portion of the bar and the fraction (numerator/denominator) on the bar represent the percentage of people who have access to OneDrive or SharePoint and are sharing files externally.
 - Numerator: The number of people who have shared files externally with in the last 28 days
 - Denominator: The total number of people who have had access to OneDrive or SharePoint for at least 1 of the last 28 days.
 - **Internally only:** The blue (colored) portion of the bar and the fraction (numerator/denominator) on the bar represent the percentage of people who have access to OneDrive or SharePoint and are sharing files internally only.
 - Numerator: The number of people who have shared files internally only within the last 28 days
 - Denominator: The total number of people who have had access to OneDrive or SharePoint for at least 1 of the last 28 days.
4. **Link to resources:** Select this link to view help content.

Number of files collaborated on

**92% of people collaborate on 4 or more
Microsoft 365 files**

1

Invite people to learn about saving and sharing files in the cloud, coauthoring in real time, and collaborating with @mentions.

2

People collaborating, by number of online files

3



[View related content](#)

4

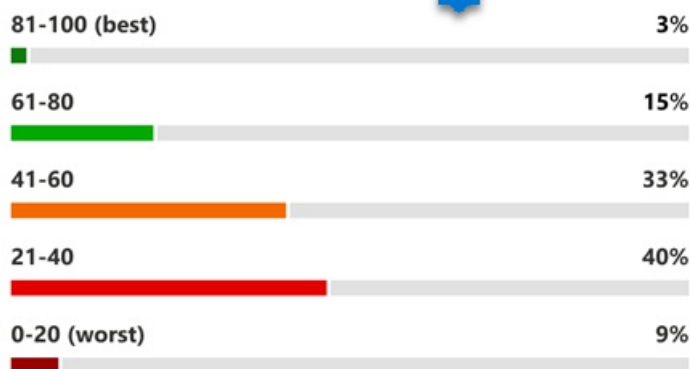
1. **Header:** Highlights the percentage of people who have access to OneDrive or SharePoint who are collaborating on 4 or more files.
2. **Body:** Provides information about how people can leverage online files for better collaboration.
3. **Visualization:** Shows a distribution of the people who have access to OneDrive or SharePoint, based on the number of files they collaborate on. This is shown through the following 4 categories (for each, the blue portion of the bar and the fraction represent the percentage of people who have access to OneDrive or SharePoint that fall into that category):
 - **No collaboration:**
 - Numerator: Number of people not collaborating on any files in the last 28 days.
 - Denominator: Total number of people who have access to OneDrive or SharePoint for at least 1 of the last 28 days.
 - **Collaboration on 1-3 files:**
 - Numerator: Number of people collaborating on 1-3 files in the last 28 days.
 - Denominator: Total number of people who have had access to OneDrive or SharePoint for at least 1 of the last 28 days.
 - **Collaboration on 4-10 files:**
 - Numerator: Number of people collaborating on 4-10 files in the last 28 days.
 - Denominator: Total number of people who have had access to OneDrive or SharePoint for at least 1 of the last 28 days.
 - **Collaboration on 11 or more files:**
 - Numerator: Number of people collaborating on 11 or more files in the last 28 days.
 - Denominator: Total number of people who have had access to OneDrive or SharePoint for at least 1 of the last 28 days.
4. **Link to resources:** Select this link to view help content.

Network performance strength for OneDrive and SharePoint

9% of devices we test for your org have poor connections to OneDrive and SharePoint 1

A good network connection is critical for using SharePoint and OneDrive to collaborate. 2

Percentage of devices, by network performance quality 3



[Review network improvement actions](#)

1. **Header:** Highlights the percentage of devices out of all tested that has poor network connection to OneDrive and SharePoint.
2. **Body:** Provides information about why network connection performance important for collaboration.
3. **Visualization:** Shows a percentage of devices with different levels of network connectivity performance related to OneDrive and SharePoint:
 - **81-100 (best):** The dark green (colored) portion of the bar represents the percentage of devices with the best performance.
 - **61-80:** The green (colored) portion of the bar represents the percentage of devices with a network performance score between 60-80.
 - **41-60:** The orange (colored) portion of the bar represents the percentage of devices with a network performance score between 40-60.
 - **21-40:** The red (colored) portion of the bar represents the percentage of devices with a network performance score between 20-40.
 - **0-20:** The dark red (colored) portion of the bar represents the percentage of devices with the worst network performance score between 0-20.

Related content

[Microsoft 365 apps health – Technology experiences](#) (article)

[Communication – People experiences](#) (article)

[Meetings – People experiences](#) (article)

[Mobility – People experiences](#) (article)

[Privacy controls for Productivity Score](#) (article)

[Teamwork – People experiences](#) (article)

Communication – People experiences

7/2/2021 • 7 minutes to read • [Edit Online](#)

Productivity Score supports the journey to digital transformation with insights about how your organization uses Microsoft 365 and the technology experiences that support it. Your organization's score reflects people and technology experience measurements and can be compared to benchmarks from organizations similar in size to yours. The communication category is part of the people experiences measures. To learn more, check out the [Productivity Score overview](#) and read [Microsoft's Privacy Statement](#).

Prerequisites

To get started with Communication insights, people in your organization need to be licensed for:

- Microsoft Teams
- Yammer
- Exchange Online

For more information, see [assign licenses to users](#).

After people have been active in the above products at least once in the last 28 days, you will start to see the insights.

Why your organization's Communication score matters

Microsoft understands that people have different communication needs. To get a quick response to a question, you might choose to send an instant message. If you want to send status updates to your leadership, you may choose an email message. To reach a broader audience, you may choose to post a community message. Microsoft 365 enables this flexibility in communication modes to fit everyone's needs. Research shows that using real-time communication tools creates a more unified organization and builds morale, regardless of location.

How we calculate the communication score

For Communication, we provide a primary insight, which contains the key metrics associated with communication in your organization, combined with a scoring framework for using these metrics to calculate your organization's score.

Primary insight

Microsoft 365 provides people the flexibility to fit everyone's communication style by offering multiple modes. The primary insight provides a measure of people in your org that are using multiple modes to communicate.

65% of people in your org use more than one mode to communicate 1

Collaboration improves when people have choices in the way they communicate, using the right mode to fit their needs. Microsoft 365 offers flexibility in communications, with email, messages, and community posts. [How we calculate your score](#)



▼ Peer benchmark

[View communication resources](#) 4

1. **Header:** Provides the key metric of people using more than one communication mode, namely:

- Sending emails through Exchange
- Sending messages through Teams
- Posting on communities in Yammer

This key metric is shown as a percentage of all people who are using two or more of Exchange, Teams, or Yammer.

2. **Body:** Provides more information on how flexibility in the modes of communication is valuable to people in your org.

3. **Visualization of current state:**

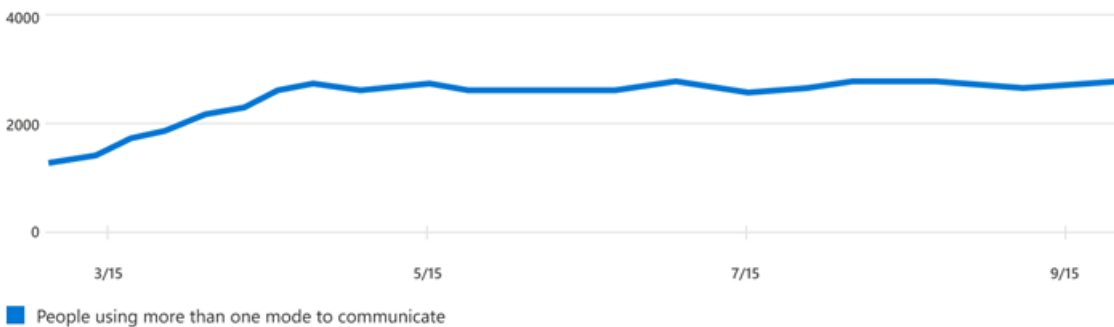
- Horizontal bar where the blue portion represents the percentage expressed in the header
- Highlights the (numerator/denominator) used for computing the percentage expressed in the header:
 - **Numerator:** # of people using more than one communication mode in the last 28 days
 - **Denominator:** # of people marked as enabled for more than one communication product in the last 28 days
- **Peer Benchmark** value of the key metric is also shown as a percentage

4. **View communication resources:** Clicking here would enlist all the support content in the form of videos/articles related to Communication. From these you can navigate to the custom playlist for Communication and subsequently, for all Productivity Score categories.

Trend visualization of primary insight

This chart provides the trend of numerator of the key metric in the primary insight – that is, the number of people in your org using more than one communication mode over the last 180 days. Here that the daily value is an aggregate of the number of people who use multiple forms of communication over the last 28 days.

Number of people using more than one mode to communicate over time



Scoring model

The communication score for your organization measures at an aggregate (organization) level whether people are consistently communicating using multiple modes among email, chat, and community posts over a 28-day window.

Scores are not provided at the individual user level.

Explore how your organization communicates

We also provide you with information that helps you gain visibility into how your organization communicates. These additional metrics don't directly influence your Productivity Score, but can help you create an action plan as a part of your digital transformation.

Breakdown of communication by modes

Breakdown of how people in your org use different modes to communicate 1

Encourage people to use email, messages, or community posts to share knowledge and access resources, when and where they need. 2

People communicating 3



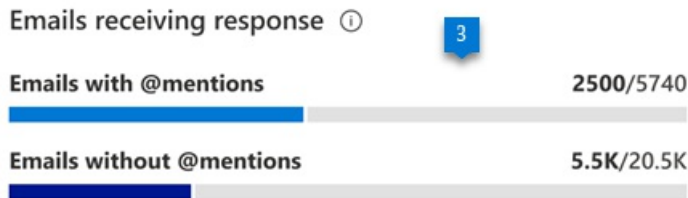
[View related content](#) 4

1. **Header:** Highlights the goal of the insight to provide a detailed breakdown across the different communication modes being considered within Communication.
2. **Body:** Provides information on the value of using different modes for sharing knowledge.
3. **Visualization:** The breakdown represents the use for each mode. The colored portion and the fraction on each bar represent the number of people sending emails, messages, or community posts as a percentage of number of people enabled for that mode:
 - **People sending emails:** The colored portion and the fraction represent the percentage of users enabled for Exchange who are sending emails. This fraction is constructed from:
 - **Numerator:** People sending emails in the last 28 days.
 - **Denominator:** People enabled for Exchange in the last 28 days.
 - **People sending messages in Microsoft Teams:** The colored portion and the fraction represent the percentage of users enabled for Microsoft Teams who are sending messages. This fraction is constructed from:
 - **Numerator:** People sending messages on Microsoft Teams in the last 28 days.
 - **Denominator:** People enabled for Microsoft Teams in the last 28 days.
 - **People posting in communities:** The colored portion and the fraction represent the percentage of users enabled for Yammer that are posting in communities. This fraction is constructed from:
 - **Numerator:** People posting in Yammer communities in the last 28 days.
 - **Denominator:** People enabled for Yammer in the last 28 days.
4. **View related content:** Select this link to view collated videos, and other related help content.

@mentions in emails

New email threads with @mentions have a 16% higher response rate in your org 1

Using @mentions in email improves email response rates and helps focus attention in a crowded inbox. 2
In your org, 20% of people use @mentions in emails.



[View related content](#) 4

1. **Header:** Highlights the increase in response rate for new email threads started in the last 28 days when they contain @mentions.
2. **Body:** Provides information on the value of using @mentions in emails. Additionally, people using @mentions is expressed as a percentage of all users who have sent an email in the last 28 days.
3. **Visualization:** Breaks down the response rate for new email threads based on whether they had @mentions or not:
 - **Responses to emails with @mentions:** The colored portion and the fraction represent the response rate for new email threads containing @mentions. This fraction is constructed from:
 - **Numerator:** New email threads containing @mentions that were started and received a response in the last 28 days.
 - **Denominator:** New email threads containing @mentions that were started in the last 28 days.
 - **Responses to emails without @mentions:** The colored portion and the fraction represent the response rate for new email threads containing @mentions. This fraction is constructed from:
 - **Numerator:** New email threads that do not contain @mentions, which were started and also received a response in the last 28 days.
 - **Denominator:** New email threads not containing @mentions that were started in the last 28 days.
4. **View related content:** Select this link to view collated videos, and other related help content.

Breakdown of messages by type in Microsoft Teams

51% of people use Microsoft Teams channels to communicate

1

Microsoft Teams channels help people organize their work by project or topic, keeping messages, files, and meeting notes all in one place.

2

People messaging in Microsoft Teams ⓘ

3

Chat messages 2409/2480

Channel messages 1264/2480

[View related content](#)

4

1. **Header:** Highlights the people who sent channel messages as a percentage of people who sent any kind of message (including chat and channel messages) in the last 28 days.
2. **Body:** Provides information on the value of using channel messages within Microsoft Teams.
3. **Visualization:** Breaks down the use of chat and channel messages:
 - **People sending chat messages:** The colored portion and the fraction represent the use of chat messages within people who sent messages on Microsoft Teams. The fraction is constructed from:
 - **Numerator:** People who sent chat messages on Microsoft Teams in the last 28 days.
 - **Denominator:** People who sent messages on Microsoft Teams in the last 28 days.
 - **People sending Channel messages:** The colored portion and the fraction represent the use of channel messages within people sending messages on Microsoft Teams. The fraction is constructed from:
 - **Numerator:** People who sent channel messages on Microsoft Teams in the last 28 days.
 - **Denominator:** People who sent messages on Microsoft Teams in the last 28 days.
4. **View related content:** Select this link to view collated videos, and other related help content.

Questions and Answers in Yammer

35% of the questions posted in Yammer have answers or best answers

1

Using the question format in Yammer helps community members tune out noise and find posts with the answers they need.

2

Questions in Yammer ⓘ

3

With answers 43/124

With best answers 35/124

[View related content](#)

4

1. **Header:** Highlights the posts marked as questions on Yammer that have received an answer marked as "Best answer" as a percentage of all posts marked as questions on Yammer in the last 28 days.
2. **Body:** Provides information on the value of using questions and answers in Yammer to share knowledge.
3. **Visualization:** Breaks down the use of the questions and answers feature in your organization:
 - **Questions:** The colored portion of the bar and associated number represents the total number of posts marked as questions in the last 28 days.
 - **Questions with answers:** The colored portion of the bar and the associated number represents the number of posts marked as questions and have received answers in the last 28 days.
 - **Questions with best answers:** The colored portion of the bar and the associated number represents the number of posts that were marked as questions and have also received a "best answer" in the last 28 days.
4. **View related content:** Select this link to view collated videos, and other related help content.

Related content

[Microsoft 365 apps health – Technology experiences](#) (article)

[Content collaboration – People experiences](#) (article)

[Meetings – People experiences](#) (article)

[Mobility – People experiences](#) (article)

[Privacy controls for Productivity Score](#) (article)

[Teamwork – People experiences](#) (article)

Mobility – People experiences

4/3/2021 • 6 minutes to read • [Edit Online](#)

Productivity Score provides insights into your organization's digital transformation journey through its use of Microsoft 365 and the technology experiences that support it. Your organization's score reflects people and technology experience measurements and can be compared to benchmarks from organizations similar to yours. The mobility category is part of the people experiences measures. To learn more, check out the [Productivity Score overview](#) and read [Microsoft's Privacy Statement](#).

Prerequisites

To get started with Mobility insights, people in your organization need to be licensed for:

- Microsoft Teams
- Exchange Online
- Word
- Excel
- PowerPoint
- OneNote

For more information, see [assign licenses to users](#).

After people have been active in the above products at least once in the last 28 days, you will start to see the insights.

Why your organization's mobility score matters

A fundamental pillar of organizational productivity is how well people are able to work flexibly from wherever they are. With Microsoft 365, people can stay connected with Outlook, Microsoft Teams, and Yammer. People can also seamlessly collaborate on content by using Word, Excel, PowerPoint, and OneNote from any location, and platforms.

How we calculate the score

We provide a primary insight in the experience that contains the key metrics for this category. Then, a scoring framework detailed below is used for these metrics to calculate your organization's score.

Primary insight

Microsoft 365 lets people work flexibly across apps, including Microsoft Outlook, Word, Excel, PowerPoint, OneNote, Microsoft Teams, Yammer, and Skype for Business. People can also work from anywhere by using a seamless experience across desktop, web, and mobile platforms. The primary insight looks at the products that are enabled for people in your organization – and how many of these people are active on at least two platforms.

71% of people in your org use Microsoft 365 products on more than one platform

When people can quickly reach coworkers and access their email and files on any device, they're more efficient and satisfied. This data contributes to your overall Productivity Score. [How we calculate your score](#)

People using more than one platform

2568/3617

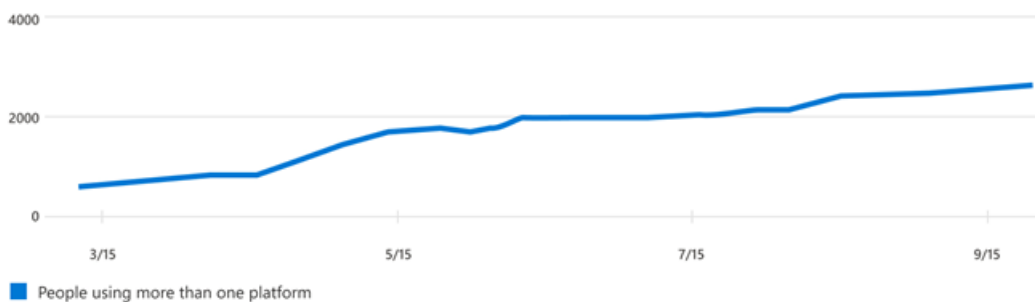
Peer benchmark

[View Mobility resources](#)

- Header:** Shows the percentage of people in your org who have access to any of Microsoft 365 Apps, and who are active on at least one of these applications on more than one platform.
- Body:** Provides more information on how the use of these applications on multiple platforms can promote efficiency and satisfaction.
- Visualization (current state):** Shows how many people use more than one platform across desktop, mobile, and web for at least one Microsoft 365 (list below) as follows:
 - **Horizontal bar** where the blue (colored) portion represents the percentage expressed in the header.
 - **The fraction** on the bar highlights the (numerator/denominator) used for calculating the percentage in the header.
 - **Numerator:** The number of people in your org using any application within Microsoft Outlook, Word, Excel, PowerPoint, OneNote and Microsoft Teams, Yammer, and Skype on more than one platform from desktop, web, and mobile in the last 28 days.
 - **Denominator:** The number of people licensed for Microsoft 365 Apps, Exchange, Yammer, Microsoft Teams, or Skype for at least 1 of the last 28 days.
 - The **peer benchmark** value for the key metric is also shown as a percentage.
- View Mobility resources:** Select this link to view help content.

Trend visualization of the primary insight

People using more than one platform over time



This chart shows the trend-line, where the numerator is the number of people who have used apps, over the last 180 days. Each data point on the line chart is an aggregate of activity for the last 28 days. Each data point provides a count of all people in your org using an application across at least two platforms in the last 28 days for each date on the x-axis.

Scoring framework

The mobility score for your organization measures at an organization (aggregate) level whether people are using Microsoft 365 Apps - Outlook, Teams, Word, Excel, PowerPoint, OneNote, Yammer, and Skype - across the different platforms - desktop, web, and mobile.

The scores are not provided at the individual user level.

Explore how your org works across platforms and locations

We also provide you with information that helps you gain visibility into how people in your organization work across platforms. These additional metrics do not directly contribute to your Productivity Score, but help you create an action plan as part of your digital transformation.

Use of Outlook across platforms

68% of people use Outlook on more than one platform

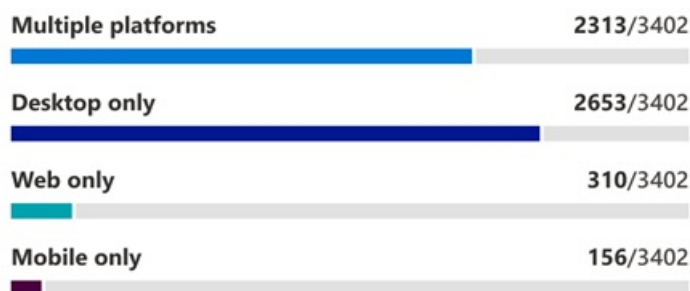
1

Using Outlook on mobile devices helps people stay connected and respond quickly when needed.

2

People using Outlook across platforms ⓘ

3



[View related content](#)

4

1. **Header:** Shows the percentage of people active on Outlook who are using Outlook on multiple platforms.
2. **Body:** Provides information about the value of using Outlook on mobile devices to help stay connected from anywhere on email.
3. **Visualization:** Shows the percentage of people who are active on Outlook and are using either one or more than one platform:
 - **Multiple platforms:**
 - Numerator: The number of people who have used Outlook on at least two platforms from desktop, mobile, or web in the last 28 days.
 - Denominator: The number of people who have used Outlook at least once in the last 28 days.
 - **Desktop only:**
 - Numerator: The number of people who have used Outlook on only a desktop platform in the last 28 days.
 - Denominator: The number of people who have used Outlook at least once in the last 28 days
 - **Web only:**
 - Numerator: The number of people who have used Outlook on only a web platform in the last 28 days.
 - Denominator: The number of people who have used Outlook at least once in the last 28 days.
 - **Mobile only:**
 - Numerator: Number of people who have used Outlook on only a mobile platform in the last 28 days.
 - *Denominator: Number of people who have used Outlook at least once in the last 28 days.

Use of Teams across platforms

20% of people use Microsoft Teams on more than one platform

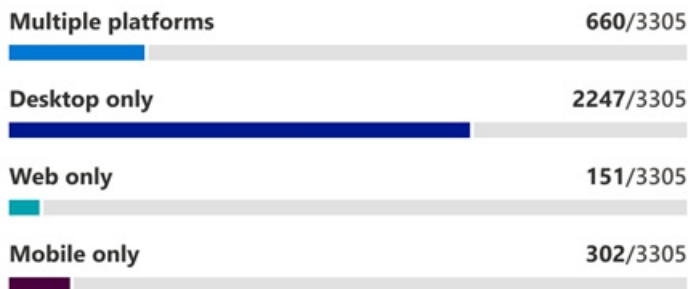
1

Using Microsoft Teams across platforms supports productivity with just-in-time access to coworkers and convenient meeting management.

2

People using Microsoft Teams across platforms

3



[View related content](#)

4

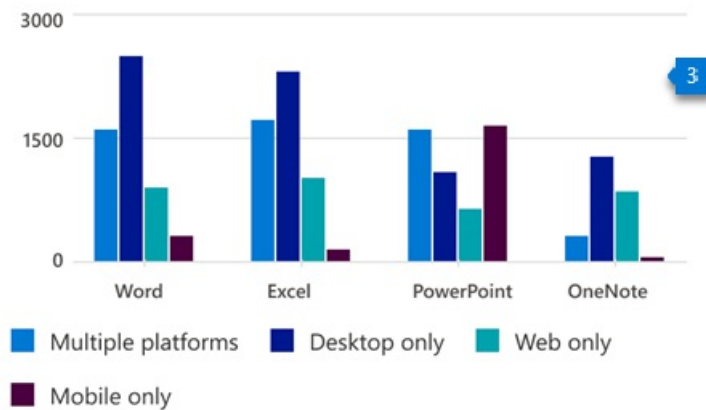
1. **Header:** Shows what percentage of people who are active on Microsoft Teams are using it on multiple platforms.
2. **Body:** Provides information about the value of using Teams on mobile devices to help people stay up to date on messages while working from any location.
3. **Visualization:** Shows the percentage of people active on Microsoft Teams who are using it on either a single platform, or multiple ones:
 - **Multiple platforms:**
 - Numerator: The number of people who have used Teams in the last 28 days on 2 or more of the following platforms: desktop, mobile, or web.
 - Denominator: The number of people who have used Microsoft Teams at least once in the last 28 days.
 - **Desktop only:**
 - Numerator: The number of people who have used Microsoft Teams only on a desktop platform in the last 28 days
 - Denominator: The number of people who have used Teams at least once in the last 28 days
 - **Web only:**
 - Numerator: The number of people who have used Microsoft Teams only on a web platform in the last 28 days
 - Denominator: The number of people who have used Microsoft Teams at least once in the last 28 days
 - **Mobile only:**
 - Numerator: The number of people who have used Microsoft Teams only on a mobile platform in the last 28 days
 - Denominator: The number of people who have used Teams at least once in the last 28 days

Use of Microsoft 365 Apps across platforms

63% of people who use Microsoft 365 apps access files on more than one platform 1

People save time and are more satisfied at work when they have access to files on any device at any time. 2

People accessing files across platforms, by app 1



[View related content](#) 4

1. **Header:** Shows the percentage of people active on Microsoft 365 Apps (Word, Excel, PowerPoint, and OneNote) on multiple platforms.
2. **Body:** Provides information about the value of providing people in your organization the flexibility to access their files from anywhere.
3. **Visualization:** The grouped vertical is meant to represent the number of people who are using each of the apps considered—Word, Excel, PowerPoint, and OneNote — across single or multiple platforms. For each of these applications, bars represent the following:
 - **Multiple platforms:** The number of users active on an app across at least two platforms in the last 28 days.
 - **Desktop only:** The number of users active on app on only the desktop platform in the last 28 days.
 - **Web only:** The number of users active on app on only the web platform in the last 28 days.
 - **Mobile only:** The number of users active on app on only mobile platform in the last 28 days.

Remote work

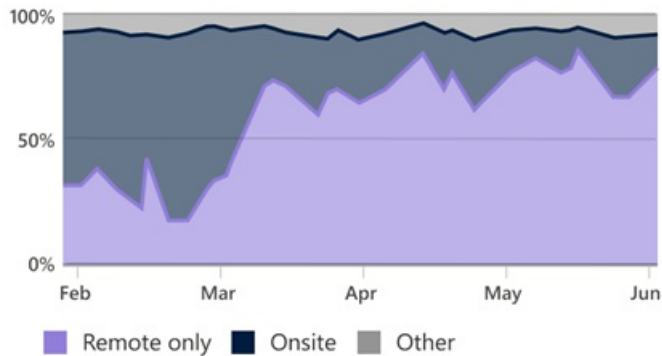
91% of people do all their work remotely

1

By facilitating remote work, you can support continued productivity for people without access to any of your organization's physical offices.

2

Percent of people working remotely and onsite [ⓘ]



3

[View related content](#)

4

1. **Header:** Shows the percentage of people working only from home or location outside of their company's network.
2. **Body:** Highlights the importance of facilitating remote work for people without access to your organization's physical offices.
3. **Visualization:** Shows trend-line for daily percentage of people who only work remotely as well as daily percentage of people who also work onsite. Users are considered onsite if they perform at least three hours of activity in Microsoft 365 Apps in a day.

Related content

[Microsoft 365 apps health – Technology experiences](#) (article)

[Communication – People experiences](#) (article)

[Content collaboration – People experiences](#) (article)

[Meetings – People experiences](#) (article)

[Privacy controls for Productivity Score](#) (article)

[Teamwork – People experiences](#) (article)

Teamwork – People experiences

4/3/2021 • 8 minutes to read • [Edit Online](#)

Productivity Score provides insights into your organization's digital transformation journey through its use of Microsoft 365 and the technology experiences that support it. Your organization's score reflects people and technology experience measurements and can be compared to benchmarks from organizations similar to yours. The teamwork category is part of the measurements that falls under people experiences. To learn more, check out the [Productivity Score overview](#) and read [Microsoft's Privacy Statement](#).

Prerequisites

To get started with teamwork insights, people in your organization need to be licensed for:

- Microsoft Teams
- SharePoint
- Exchange Online

For more information, see [assign licenses to users](#).

After people have been active in the above products at least once in the last 28 days, you will start to see the insights.

Why your org's teamwork score matters

A fundamental pillar for organizational productivity is when a group of people with a common goal work with each other and with common resources for collective success. Research indicates that when people share information and collaborate in shared workspaces, they save up to 4 hours a week. They can find related documents, find context for previous discussions, and deliver towards shared goals. See the [evidence](#)

How we calculate the teamwork score

We provide a primary insight in the experience that contains the key metrics for this category in your organization. Then, a scoring framework, detailed below, is used for these metrics to calculate your organization's score.

Primary insight

The primary insight looks at all the people who are communicating using email and messages on Microsoft Teams, and interacting with content on the cloud in shared workspaces. Within Microsoft 365, Microsoft 365 Groups are the foundation for people to come together in a shared workspace with the ability to send emails to the group mailbox, share files on the SharePoint team site, and send channel messages through Microsoft Teams.

70% of people in your org contribute to shared workspaces 1

Top-performing teams consider diverse perspectives and engage each member on a consistent basis. They also regularly encourage collaboration, such as the creation of shared files and participation in conversations in email and Microsoft Teams message threads. [How we calculate your score](#) 2

People engaged in shared workspaces 3

2483/3548

▼ Peer benchmark

[View resources about teamwork](#) 4

1. **Header:** Provides the key metric of people in your org performing any one of the following activities:

- Sending email to a group mailbox through Exchange.
- Sending channel messages through Teams
- Reading and creating content (what we collectively refer to as content interaction) in SharePoint team sites.

As a percentage of all people in your org who are performing any of the following activities (within or outside of shared workspaces):

- Sending email through Exchange.
- Sending messages (chat or channel messages) on Microsoft Teams.
- Reading and creating content on OneDrive or SharePoint.

And have access to at least one of the following services: Exchange, Microsoft Teams, or SharePoint

2. **Body:** Provides more information on how communicating and interacting with content, when done within a shared workspace, can have positive outcomes for productivity in your organization.

3. **Visualization (current state):**

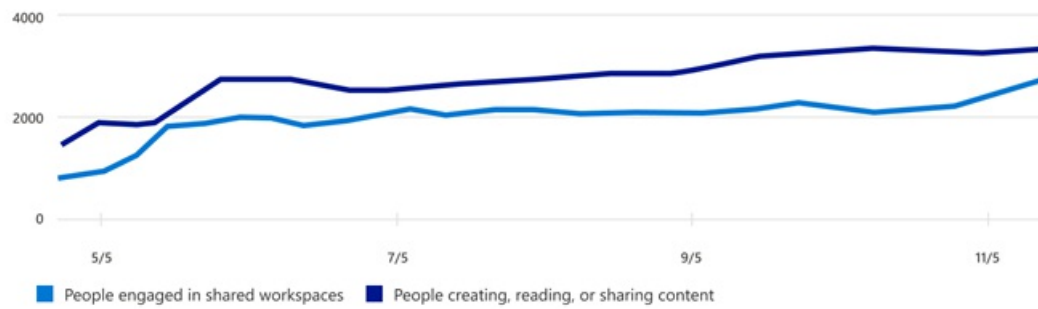
- Horizontal bar where the blue portion represents the percentage expressed in the header
- Highlights the fraction (numerator/denominator) used for computing the percentage shown in the header
 - Numerator: The number of people in your organization who send email to a group mailbox through Exchange, OR who are sending channel messages through Teams, OR reading and creating content in SharePoint team sites.
 - Denominator: The number of people in your org who send emails through Exchange, OR send messages (chat or channel messages) on Microsoft Teams, OR read and create content on OneDrive or SharePoint, AND have access to at least one of the following services: Exchange, Microsoft Teams, or SharePoint.
- The peer benchmark value of the key metric is also shown as a percentage.

4. **View resources about teamwork:** Select this link to view help content.

Trend visualization of the primary insight

The following chart provides the trend of the numerator and the denominator of the key metric in the primary insight. It shows the number of people engaged in shared workspaces, and the number of people communicating or interacting with content within the last 180 days. Each data point on the line chart is an aggregate of activity for the last 28 days.

Number of people who engage in shared workspaces over time



Scoring framework

The teamwork score for your organization measures at an aggregate (organizational) level whether users are consistently communicating or engaging in file activity in shared workspaces within the last 28 days.

Scores are not provided at the individual user level .

Explore more about teamwork in your organization

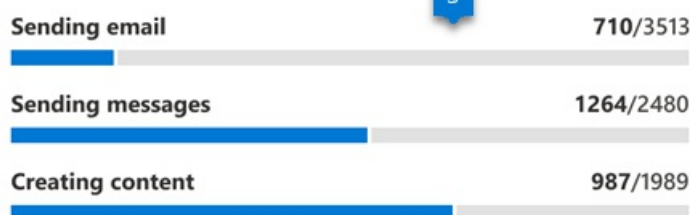
We also provide additional information about how people in your organization work together. These additional metrics don't directly contribute to your Productivity Score, but are relevant in helping you create an action plan as part of your digital transformation.

Breakdown of how people engage in shared workspaces

Breakdown of how people in your organization engage in shared workspaces

If users aren't yet contributing to a shared workspace, encourage them to start. Team dynamics improve and teams are more efficient when members create content in a collaborative way.

People in shared workspaces



[View related content](#)

1. **Header:** Shows a detailed breakdown across the different types of teamwork being measured.
2. **Body:** Provides information on the value of working in shared workspaces to help teams be more effective.
3. **Visualization:** The visualization shows the extent to which people who are communicating or interacting with content are doing so in shared workspaces, as follows:
 - **Sending email:** The colored portion and the fraction represent the percentage of people sending email to group mailboxes. The fraction is comprised of:

- Numerator: People sending emails to group mailboxes in the last 28 days.
- Denominator: People sending emails in the last 28 days. This is the same group of people who are marked as sending email in the primary insight of communication productivity score.
- **Sending messages:** The colored portion and the fraction represent the percentage of people sending messages in channels in Microsoft Teams. The fraction is comprised of:
 - Numerator: People sending channel messages within the last 28 days.
 - Denominator: People sending chat or channel messages in the last 28 days. This is the same group of people who are marked as sending messages in Microsoft Teams in the primary insight of the communication category in Productivity Score.
- **Creating content:** The colored portion and the fraction represent the percentage of people reading or creating content on Microsoft 365 SharePoint team sites.
 - Numerator: Number of people reading or creating content on Microsoft 365 group connected team sites.
 - Denominator: Number of people with access to SharePoint, who read or created content of any kind in OneDrive or SharePoint sites in the last 28 days.

4. **View related content:** Select this link to view help content.

Breakdown of workspace engagement by size and age

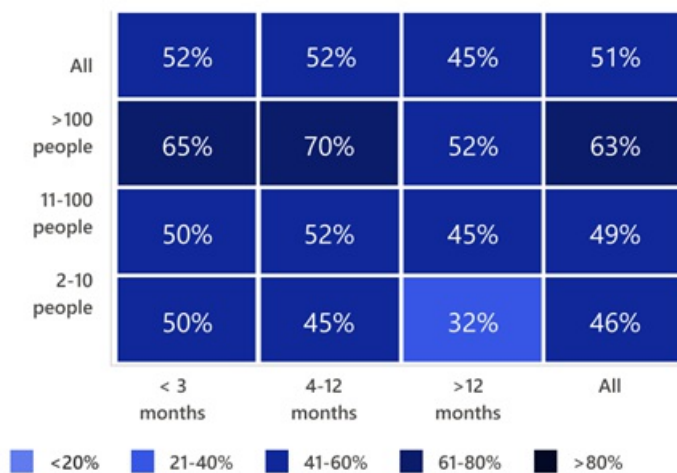
51% of shared workspaces have some degree of engagement



Help ensure that people can focus more easily by archiving or deleting Microsoft Teams channels that are no longer active.



Percentage of engaged shared workspaces, by workspace size and age



[View related content](#)



1. **Header:** Shows the categorization of engagement in workspaces, broken out by size for the number of members in the workspace, and the workspace age in months.
2. **Body:** Provides information about the value of encouraging people in your organization to keep only the workspaces that are needed to promote more effective teamwork.

3. **Visualization:** The engagement breakdown is shown in the form of a heat-map across two dimensions.

- **Size of workspace:** Workspaces are broken down into three categories based on the number of members: 2-10 people, 11-100 people, and over 100 people. The "All" category includes all size categories.
- **Age of workspace:** Workspaces are categorized by the number of months since the workspace was first created. The "All" category includes all age categories.

Each cell in the chart has a number and color based on the percentage of engaged workspaces that belong in that category. The workspace categories are based on the age and size shown in the intersection of that cell. For example, if the cell at the intersection of 11-100 people and 4-12 months has a value of 52%, it means that 52% of the workspaces with 11-100 members that are between 4-12 months old, have some form of engagement. The percentage is calculated as:

- **Numerator:** Workspaces that have engagement in the form of communication (email and channel messages) or content interaction in the last 28 days
- **Denominator:** all workspaces that are available in your org for the last 28 days

4. **View related content:** Select this link to view help content.

Breakdown of workspaces by level of engagement

10% of shared workspaces have over 3 days of engagement per week

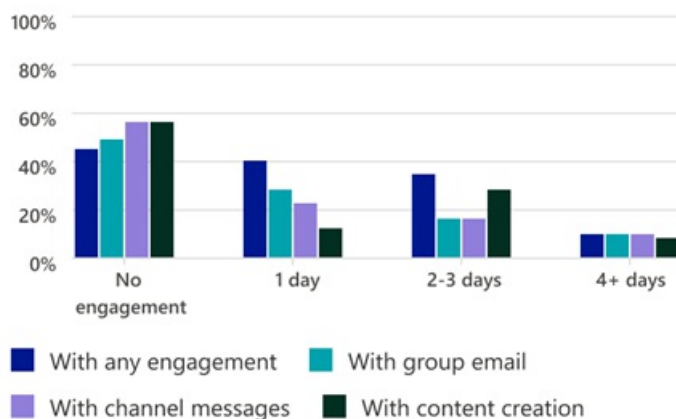
1

People are better connected when they collaborate frequently. Teams can stay informed and organized with channels and searchable conversations in Microsoft Teams, and emails to group mailboxes.

2

Percentage of engaged shared workspaces, by number of days per week ⓘ

3



[View related content](#)

4

1. **Header:** Provides a breakdown of workspaces broken out by level of engagement, using group email, channel messages, and content interaction.
2. **Body:** Provides information on the value of consistent engagement in the shared workspaces to help make them more effective at teamwork.
3. **Visualization:** Provides a view of the workspaces in your organization based on the intensity of

engagement per week. The view includes distributions for different activity types measured within teamwork, in addition to any engagement, which covers the following categories:

- **Group email:** Percent of workspaces that have no days/1 day/2-3 days/4+ days of group email activity per week over the last 28 days.
- **Channel messages:** Percent of workspaces that have no days/1 day/2-3 days/4+ days of channel messages per week over the last 28 days.
- **Content reading or creation:** Percent of workspaces that have no days/1 day/2-3 days/4+ days of reading or creating content per week over the last 28 days.

4. **View related content:** Select this link to view help content.

Use of teams within Microsoft Teams

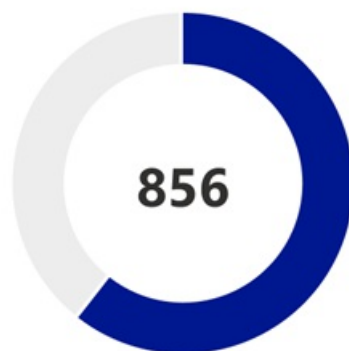
61% of shared workspaces use Microsoft Teams for better collaboration

1

Having a shared workspace in Microsoft Teams helps groups to quickly and easily collaborate on content, communicate over channels, and share and make decisions in meetings.

2

Shared workspaces using Microsoft Teams ⓘ



3

[View related content](#)

4

1. **Header:** Shows the number of shared workspaces that have a Microsoft Teams team associated with them.

2. **Body:** Provides information about the value of having a Microsoft Teams team attached to the shared workspaces, to help make people associated with them more effective at teamwork.

3. **Visualization:** The colored part of the donut chart reflects the percentage of workspaces that have a Microsoft Teams team attached to them. The percentage is calculated as follows:

- **Numerator:** The number of shared workspaces in your organization that had a Microsoft Teams team associated with them in the last 28 days
- **Denominator:** The number of shared workspaces in your org in the last 28 days

The number in the center of the donut chart represents the total number of shared workspaces that have a Microsoft Teams team associated with them.

4. **View related content:** Select this link to view help content.

Related content

[Microsoft 365 apps health – Technology experiences \(article\)](#)

[Communication – People experiences \(article\)](#)

[Content collaboration – People experiences \(article\)](#)

[Meetings – People experiences \(article\)](#)

[Mobility – People experiences \(article\)](#)

[Privacy controls for Productivity Score \(article\)](#)

Meetings – People experiences

6/3/2021 • 7 minutes to read • [Edit Online](#)

Productivity Score provides insights into your organization's digital transformation journey through its use of Microsoft 365 and the technology experiences that support it. Your organization's score reflects people and technology experience measurements and can be compared to benchmarks from organizations similar to yours. The meetings category is part of the people experiences measures. To learn more, check out the [Productivity Score overview](#) and read [Microsoft's Privacy Statement](#).

Prerequisites

To get started with Meetings insights, people in your organization need to be licensed for:

- Microsoft Teams

For more information, see [assign licenses to users](#).

After people have been active in Teams at least once in the last 28 days, you will start to see the insights.

Why your organization's meetings score matters

Meetings, where people explore ideas, plan, solve problems, and make decisions, are a fundamental pillar for organizational productivity. Research indicates that when people use online meeting tools effectively, they tend to save up to 104 minutes per week.

How we calculate the meetings score

We provide a primary insight in the experience that contains the key metrics for this category. Then, a scoring framework, detailed below, is used for these metrics to calculate your organization's score.

Primary insight

Microsoft Teams integrate with Outlook calendar and provides a host of capabilities to make your meetings more engaging and effective. The primary insight looks at all Microsoft Teams online meetings that were held in your organization. The Primary insight also tracks how many meetings follow at least one of the best practices for Teams meetings.

60% of meetings in your org include one or more meeting best practices

Meetings are more effective when everyone's engaged. Encourage people to turn on video to talk face-to-face, share screens to focus the conversation, and share files to help people absorb information. [How we calculate your score](#)

Meetings with best practices

36.1K/60.2K

Peer benchmark

[View resources about meetings](#)

1. **Header:** Shows the percentage of online meetings on Microsoft Teams held in the past 28 days that had video or screen sharing during the meeting.
2. **Body:** Provides more information on how following best practices for engagement during a meeting, such as use of video or screen sharing, can make meetings more effective.

3. Visualization (current state):

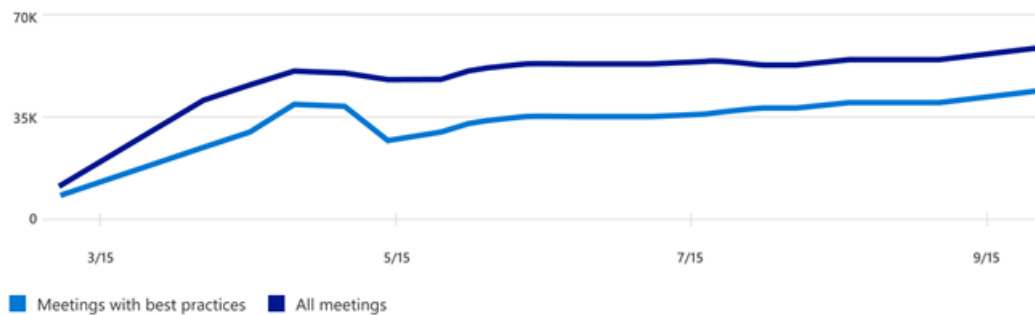
- In this horizontal bar chart, the blue (colored) portion represents the percentage shown in the header
- The fraction (numerator/denominator) is used for calculating the percentage shown in the header
 - Numerator: The number of online Microsoft Teams meetings including people from your organization who have used video or screen sharing.
 - Denominator: The number of online Microsoft Teams meetings including people from your organization that were held in the last 28 days.
- The peer benchmark value of the key metric is also shown as a percentage.

4. **Link to resources:** Select this link to view help content.

Trend visualization of the primary insight

The following chart shows the trend-lines of both the numerator and the denominator of the key metric from the primary insight. In other words, it shows the number of online Microsoft Teams meetings with best practices, such as video or screen sharing, and the total number of online Microsoft Teams meetings held over the last 180 days. Each data point on the line chart is an aggregate of activity for the last 28 days.

Number of meetings over time that include best practices



Scoring framework

The meetings score for your organization measures the degree to which online Microsoft Teams meetings in your organization followed best practices in the last 28 days. It is weighted based on the number of people in your org attending the meetings and the meetings' duration.

Explore more about meetings in your organization

We also provide you with supporting information to help you understand how people in your organization, as an aggregate, conduct meetings. These additional metrics don't directly contribute to your Productivity Score, but can help you create an action plan as part of your digital transformation.

Breakdown of how many meetings follow best practices

People use video in 35% of meetings 1

Turning video on and using screen sharing during meetings helps people feel more included and makes discussions more engaging. 2

Meetings with best practices in Microsoft Teams 1



[View related actions](#)

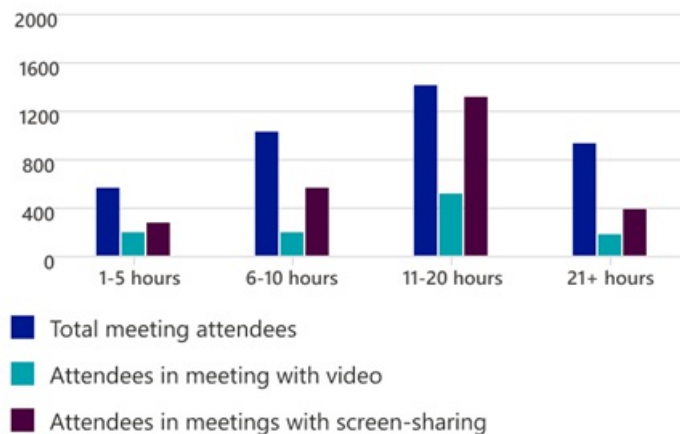
1. **Header:** Highlights the percentage of online Microsoft Teams meetings that use video best practices considered in the primary insight and scoring.
2. **Body:** Provides information on the value of using these practices during meetings to make them more engaging.
3. **Visualization:** The breakdown in the visualization is meant to represent the extent to which online Microsoft Teams meetings are following each of the following best practices:
 - **Video:** The colored portion and the fraction represent the percentage of online Microsoft Teams meetings that have video turned on. The fraction is constructed from:
 - Numerator: Online Microsoft Teams meetings held in the last 28 days that had video from at least one participant turned on.
 - Denominator: The total number of online Microsoft Teams meetings held in your organization in the last 28 days
 - **Screen sharing:** The colored portion and the fraction represent the percentage of online Microsoft Teams meetings in which people used the screen-sharing feature. The fraction includes:
 - Numerator: Online Microsoft Teams meetings held in the last 28 days that had at least one participant sharing their screen.
 - Denominator: The total number of online Microsoft Teams meetings conducted in your organization in the last 28 days

Distribution of time spent by people in meetings

30% of people spend over 20 hours a week in meetings 1

Help ensure that people make good use of the time they spend in meetings with tools that help them feel engaged and productive. 2

Attendees, by hours in meetings per week 3



[View related content](#) 4

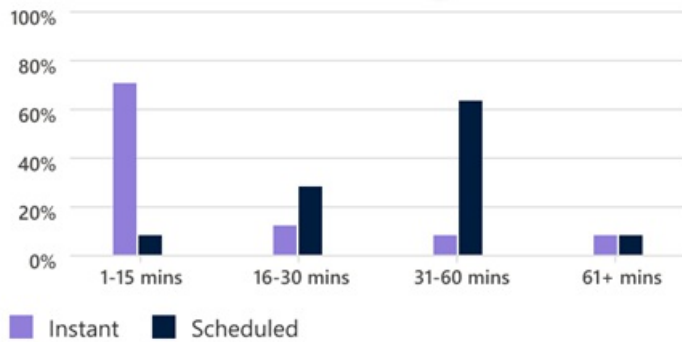
1. **Header:** Shows the percentage of people in your organization who attend online Microsoft Teams meetings for more than 20 hours per week on average, based on their activity in the last 28 days.
2. **Body:** Provides details on the value of using meeting best practices to make meetings engaged and productive
3. **Visualization:** Provides a view of people in your organization based on their average time spent per week in meetings within the last 28 days. The following information is provided for each category:
 - **Total meeting attendees:** Shows the number of people in your organization who attended meetings, based on the average meeting duration range, in the last 28 days. For example, the 6-10 hours category indicates the number of people who attended meetings for an average of that many hours per week in the last 28 days.
 - **Attendees in meetings with video:** For each category, this shows how many people in your organization were in any meeting with video in the last 28 days.
 - **Attendees in meetings with screen sharing:** For each category, this shows how many people were in a meeting that included screen sharing in the last 28 days.

Distribution of meeting length by type

82% of instant meetings are less than 30 minutes long 1

Instant meetings can help people quickly resolve issues and make decisions. 2

Percentage of instant and scheduled meetings, by meeting length 3



[View related actions](#)

1. **Header:** Shows the percentage of instant (not previously scheduled) online Microsoft Teams meetings in the last 28 days that are under 30 minutes long.
2. **Body:** Provides information about the value of using instant meetings to resolve issues quickly.
3. **Visualization:** Provides the distribution of length (in minutes) of instant and scheduled meetings that took place in your organization in the last 28 days. The distribution categorizes each meeting into 1-15 minutes, 16-30 minutes, 31-60 minutes, and greater than 60 minutes.

NOTE

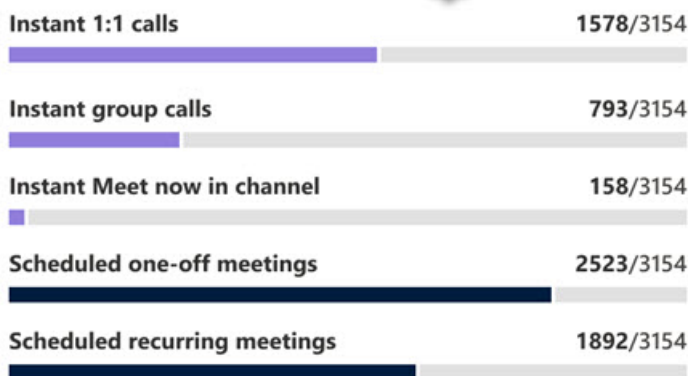
the scheduled meetings include all meetings that appeared on people's calendars. The instant meetings include calls, including both 1:1 and group calls, as well as meetings started using the "Meet now" feature in Microsoft Teams channels.

Use of different meeting types

5% of people participate in instant meetings from Microsoft Teams channels 1

Holding instant meetings from a Microsoft Teams channel creates transparency and helps with decision making. Encourage people to record these sessions to help keep coworkers informed. 2

Attendees, by meeting type 3



[View related actions](#)

1. **Header:** Highlights the percentage of instant online Microsoft Teams meetings over the preceding 28 days that are less than 30 minutes long.
2. **Body:** Provides information about the value of using "Meet now" in the Microsoft Teams channel feature.
3. **Visualization:** Shows what type of meetings are being attended by people who are attending any online Microsoft Teams meetings. Each meeting type is represented as a horizontal bar, where the colored portion and the fraction represent the following:
 - **Instant 1:1 calls:**
 - Numerator: The number of people attending 1:1 calls in the last 28 days
 - Denominator: The number of people attending any online Microsoft Teams meeting in the last 28 days
 - **Instant group calls:**
 - Numerator: The number of people attending group calls in the last 28 days
 - Denominator: The number of people attending any online Microsoft Teams meeting in the last 28 days
 - **Instant Meet now in channel:**
 - Numerator: The number of people using "Meet now" feature within Microsoft Teams channels (for instant meetings) in the last 28 days
 - Denominator: The number of people attending any online Microsoft Teams meeting in the last 28 days
 - **Scheduled one-off meetings:**
 - Numerator: The number of people attending one-off online Microsoft Teams meetings on their calendar (scheduled) in the last 28 days
 - Denominator: The number of people attending any online Microsoft Teams meeting in the last 28 days

- **Scheduled recurring meetings:**

- Numerator: The number of people attending instances of recurring meetings on their calendar (scheduled) in the last 28 days
- Denominator: The number of people attending any online Microsoft Teams meeting in the last 28 days

Related content

[Microsoft 365 apps health – Technology experiences](#) (article)

[Communication – People experiences](#) (article)

[Content collaboration – People experiences](#) (article)

[Mobility – People experiences](#) (article)

[Privacy controls for Productivity Score](#) (article)

[Teamwork – People experiences](#) (article)

Microsoft 365 Apps health – technology experiences

4/3/2021 • 4 minutes to read • [Edit Online](#)

Productivity Score provides insights into your organization's digital transformation journey through its use of Microsoft 365 and the technology experiences that support it. Your organization's score reflects people and technology experience measurements and can be compared to benchmarks from organizations similar to yours. The apps health category is part of the measurements that falls under technology experiences. To learn more, check out the [Productivity Score overview](#) and read [Microsoft's Privacy Statement](#).

Why your organization's Microsoft 365 apps health score matters

Your organizational productivity is dependent on healthy application environment. Devices running most current versions of Microsoft 365 apps on recommended channel are more secure and help people in your organization get the most out of the features in Microsoft 365.

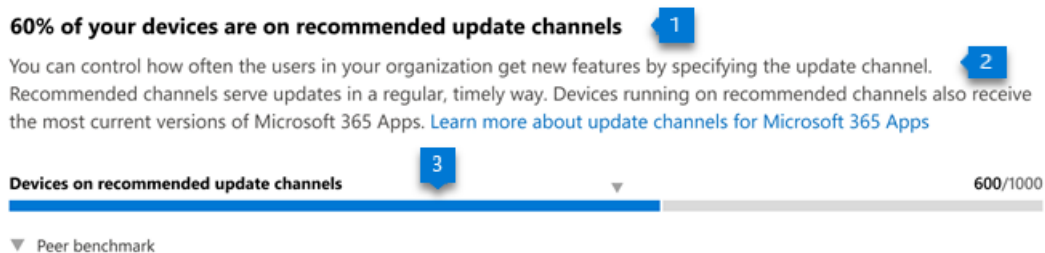
How we calculate the Microsoft 365 apps health score

We calculate your Microsoft 365 apps health score by measuring the number of devices on each update channel. We also determine whether the devices are running a supported version, and the most current release of Microsoft 365 apps.

We provide a primary insight in the experience that contains the key metrics for this category. Then, a scoring framework, detailed in the following sections, is used to calculate your score.

Primary insight

The primary insight is calculated from devices that are running Microsoft 365 Apps on recommended updated channel.



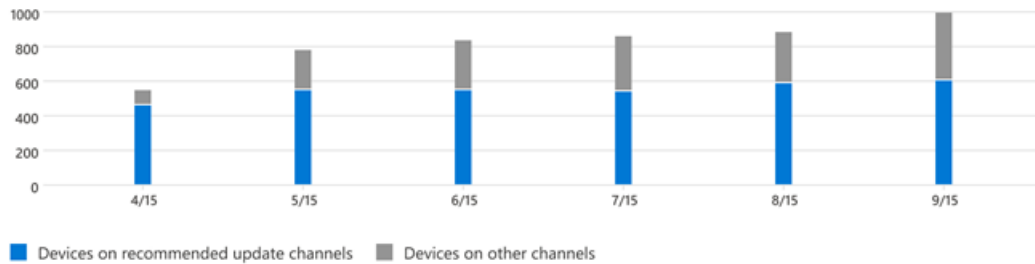
Information considered for this include Microsoft 365 apps channel, build, and version that is running on the device.

1. **Header:** Shows percentage of devices on recommended update channel
2. **Body:** Provides more information on how running the devices on recommended update channel will help getting latest update and running current versions on devices.
3. **Visualization (current state):**
 - Horizontal bars where the blue-colored portions represent the percentage of devices running recommended updated channel.
 - Highlight the (numerator/denominator) of the fraction used to calculate the percentage expressed in horizontal bars.
 - Peer Benchmark value for devices running on recommended updated channel is also shown as a percentage.

Trend visualization of the primary insight

The following chart shows the number of devices in the recommended update channel over the last 180 days. The data point on the line chart is an aggregate of activity for the last 28 days.

Number of devices on recommended update channels of Microsoft 365 Apps over time



Scoring framework

The Microsoft 365 apps health score measures whether devices are running Microsoft 365 apps on recommended channel and on latest versions.

Explore your organization Microsoft 365 app channels and versions

We also provide supporting information that helps you gain additional visibility into what channels and versions devices in your organization are currently running. These additional metrics do not contribute to your Productivity Score but can help you create an action plan to increase your Microsoft 365 apps health score by making sure devices run Microsoft 365 apps on recommended channels.

Devices on current channel and running supported versions

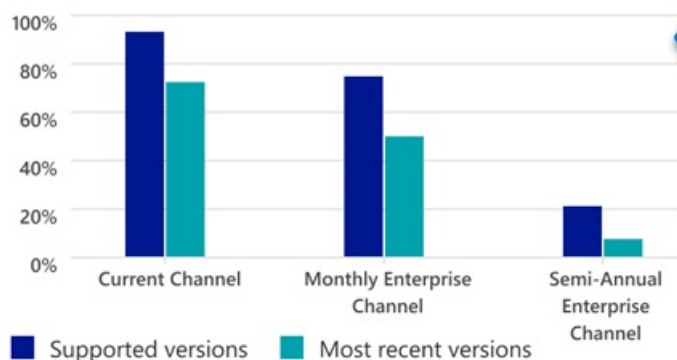
89% of devices on the Current Channel are running supported versions of Microsoft 365 Apps



We recommend Current Channel and Monthly Enterprise Channel, because they provide your users with the newest Office features and feature updates as soon as they're ready. Automatic updates are the easiest way to keep devices on recommended channels.



Percentage of devices, by update channel type ^①



[Learn more](#)



1. **Header:** Highlights the percentage of devices on the Current Channel are running supported versions of

Microsoft 365 Apps

2. **Body:** Provides information about the value of devices running Microsoft 365 apps on recommended channel.
3. **Visualization:** The breakdown in the visualization represents the extent to what percentage of devices on latest and supported versions of Microsoft 365 apps across different channel), as follows:
 - **Supported versions:** The blue bar represents the percentage of devices running on supported version of Microsoft 365 apps.
 - **Latest releases:** The teal color bar represents percentage of devices on latest releases.
4. **Learn more:** Select this link to view help content.

Devices running latest and supported versions

80% of devices are running supported Microsoft 365 Apps and 60% are running the most recent versions

1

People who have devices on recommended channels benefit from a more consistent cross-platform experience, better performance, and the latest intelligence and productivity features. Devices running unsupported versions of apps might be missing security updates and aren't eligible for Microsoft Support.

2

Devices running version type ⓘ

3



[Learn more](#)

4

1. **Header:** Highlights the percentage of devices running supported versions and devices running the most recent versions.
2. **Body:** Provides information about the value running devices on recommended channels and supported/latest versions.
3. **Visualization:** The breakdown in the visualization is meant to represent the extent to show how many devices running supported versions and most recent versions of Microsoft 365 apps):
 - **Supported versions:** The blue (colored) portion of the bar and the fraction (numerator/denominator) on the bar represents the percentage of devices running supported version of Microsoft 365 apps.
 - Numerator: The number of devices on supported versions of Microsoft 365 apps within the last 28 days
 - Denominator: The number of devices using Microsoft 365 apps within the last 28 days
 - **Most recent versions:** The teal (colored) portion of the bar and the fraction (numerator/denominator) on the bar represents the percentage of devices running recent versions of Microsoft 365 apps.
 - Numerator: The number of devices on recent versions of Microsoft 365 apps within the last 28 days
 - Denominator: The number of devices using Microsoft 365 apps within the last 28 days
4. **Learn more:** Select this link to view help content.

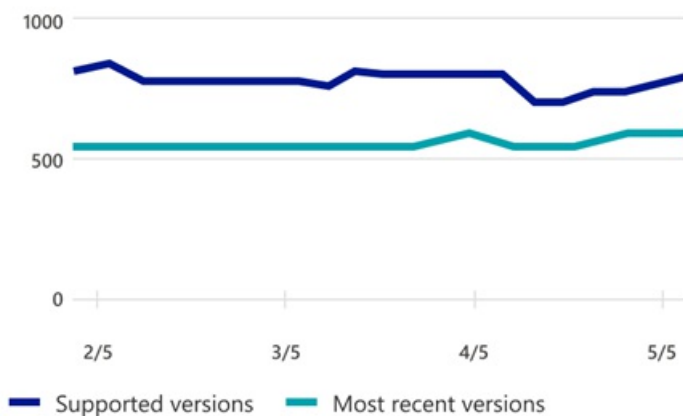
Trend visualization of the devices

This chart shows the trend-line of the devices running supported versions and latest versions of Microsoft 365 apps over the last 180 days.

Number of devices running supported or the most recent versions of Microsoft 365 Apps over time

Devices in all update channels should be running supported apps when automatic updates are on. If automatic updates are turned off, devices will eventually have unsupported builds.

Devices running version type over time ⓘ



[Learn more](#)

Devices in your organization

This section helps you act on the metrics you want to focus on by providing relevant information to all the metrics for Microsoft 365 apps health - technology experiences.

The following columns are presented in the table at the channel/version level:

- **Channel** : Current Microsoft 365 apps channel on the devices.
- **Status**: Microsoft 365 apps support state of the devices based on current channel and version.
- **Versions**: Current Microsoft 365 apps versions on the devices.
- **# of devices**: Number of devices.

Related content

[Communication – People experiences](#) (article)

[Content collaboration – People experiences](#) (article)

[Meetings – People experiences](#) (article)

[Mobility – People experiences](#) (article)

[Privacy controls for Productivity Score](#) (article)

[Teamwork – People experiences](#) (article)

Change your organization's address, technical contact, and more

7/12/2021 • 3 minutes to read • [Edit Online](#)

You can make changes to your organization profile, such as your organization name, address, phone, and technical contact. **You must be a global admin to update this information.**

To change the address associated with your bill or subscription, see [Change your billing addresses for Microsoft 365 for business](#).

Edit organization information

IMPORTANT

You can't change the country or region for your subscription. That's because the country or region where your organization is headquartered determines which services are available to you, the taxes and billing currency, and the location of the data center. To change your organization's country or region, sign up for a new account, choose the desired country or region, and purchase a new subscription.

To change other information on your company's profile page:

1. In the admin center, go to the **Settings** > **Org settings** page.
2. On the **Organization profile** tab, select **Organization information**.
3. Update your organization's information, then select **Save changes**. Be sure to fill in all required fields marked with an * to enable saving your changes.

An explanation of each field is provided below.

What do these fields mean?

FIELD	DESCRIPTION
-------	-------------

FIELD	DESCRIPTION
Name	<p>The name entered here is what users will see on the following pages:</p> <p>Sign-in page: If your users have set up other Microsoft accounts with their business or school email address, they may see the organization name on the sign-in page. This helps them distinguish between their work or school account and their other accounts, so they can identify which one to use when they sign in.</p> <p>Organization profile link and page: The link to your organization's profile displays the organization name.</p> <p>Yammer navigation: In Yammer, the left navigation uses the organization name as the name of the home Yammer network.</p> <p>OneDrive sync client: The organization name is shown in File Explorer on Windows and Finder on Mac, the file paths, the OneDrive activity center, the tooltip of the OneDrive cloud icon, and the OneDrive settings window. Currently, updating the organization name does not update it for configured clients.</p> <p>MS Teams: Organization Switcher in Teams displays the organization Name</p>
Address, City, State/Province, Postal code	<p>The address entered here is what you will see on your bill, under Sold To: The Sold To address on your bill is the same as your organization address on your profile page (see Understand your bill or invoice for Microsoft 365 for business).</p>
Country or region	<p>This is the country or region where the company is headquartered. The selected country or region determines which services are available to you, the taxes and billing currency for your country or region, and the location of the data center closest to you (see Microsoft Office license restrictions).</p> <p>NOTE: Once selected, the country or region cannot be changed. If you want to change the selection, you'll have to cancel your subscription and sign up again. For help with this process, contact support.</p>
Phone	<p>This is the primary number for your company. It's usually the number of your company headquarters.</p>
Technical contact	<p>This is the email address for the primary technical person who administers your Microsoft 365 subscription. This is the person who will receive communications about Microsoft 365 service status.</p>
Preferred language	<p>The preferred language determines the language for all communications that are sent from Microsoft to your organization. When you sign up, this setting determines the language used by SharePoint Online, which your users see on your team site. If you change the language preference setting after you sign up, all future communications are sent in the most recent language selected.</p> <p>NOTE: The language used by SharePoint Online can't be changed.</p>

Change your alternate email address

As an admin, you can change your alternate email address for resetting passwords.

1. Go to the [Microsoft 365 admin center](#).
2. In the header, select your profile icon, then select **View account**.
3. On the left, select **Security info**.
4. In the Email section, select **Change**
5. Edit the address in the **Alternate email** box, then select **Next**.
6. Enter the code sent to the alternate email address and select **OK** to verify the change. To learn about changing other profile information, see [Change your contact preferences](#) or [Change your display language](#).

Email signatures

You can change your email signature in Outlook Web App. For more information, see [Mail settings](#).

Related content

[Send email from a different address](#) (article)

[Change a user name and email address](#) (article)

[Configure email forwarding in Microsoft 365](#) (article)

Update your admin phone number and email address

8/13/2021 • 2 minutes to read • [Edit Online](#)

This article explains how you, the admin, can change your business phone and email address in Microsoft 365.

If you're looking for how to change your company's profile information, such as company name and address, company phone number, and technical contact information, see [Change your organization's address, technical contact email, and other information](#).

For more information about changing user contact information or removing former employees, see [Related content](#).

To update your phone number and email address

Use the **Security Info** page to change your mobile phone number and alternate email address. The alternate email address is used for important notifications, such as resetting your admin password (not your computer admin password).

1. Browse to the [Microsoft 365 admin center](#).
2. In the header, select your profile icon > **My account** > **Security Info**.
3. In the **Security info** tab, select **Add Method** > **Phone** > **Alternate Phone** or **Email** to add details. To update your mobile, phone, and alternate email address details, select **Change**. Make sure you use something other than your Microsoft email address for your alternate email address.

IMPORTANT

The alternate email address and the mobile phone number are needed for resetting your admin password (not your computer admin password).

4. When you are finished, select **Save**.

For answers to billing questions, see:

- [Change your billing addresses for Microsoft 365 for business](#)
- [Manage payment methods](#)

Related content

[Change a user name and email address](#) (video)

[Add a new employee](#) (video)

[Remove a former employee](#) (video)

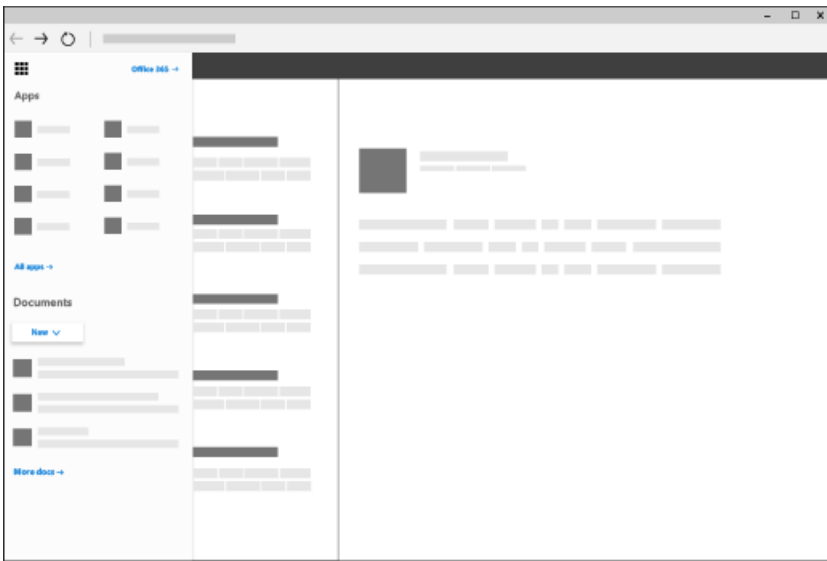
[Access and back up a former user's data](#) (article)

Add custom tiles to the app launcher

7/12/2021 • 2 minutes to read • [Edit Online](#)

In Microsoft 365, you can quickly and easily get to your email, calendars, documents, and apps using the App launcher ([learn more](#)). These are apps you get with Microsoft 365 as well as custom apps that you add from the [SharePoint Store](#) or [Azure AD](#).

You can add your own custom tiles to the app launcher that point to SharePoint sites, external sites, legacy apps, and more. The custom tile appears under the app launcher's **All** apps, but you can pin it to the **Home** apps and instruct your users to do the same. This makes it easy to find the relevant sites, apps, and resources to do your job. In the below example, a custom tile called "Contoso Portal" is used to access an organization's SharePoint intranet site.



Add a custom tile to the app launcher

1. Sign in to the admin center as a Global Administrator, go to **Settings** > **Org Settings**, and choose the **Organization profile** tab.
2. On the **Organization profile** tab, choose **Custom app launcher tiles**.
3. Select **Add a custom tile**.
4. Enter a **Tile name** for the new tile. The name will appear in the tile.
5. Enter a **URL of website** for the tile. This is the location where you want your users to go when they select the tile on the app launcher. Use HTTPS in the URL.

TIP

If you're creating a tile for a SharePoint site, navigate to that site, copy the URL, and paste it here. The URL of your default team site looks like this: `https://<company_name>.sharepoint.com`

6. Enter a **URL of the image** for the tile. The image appears on the My apps page and app launcher.

TIP

The image should be 60x60 pixels and be available to everyone in your organization without requiring authentication.

7. Enter a **Description** for the tile. You see this when you select the tile on the My apps page and select **App details**.
8. Select **Save changes** to create the custom tile.

Your custom tile now appears in the app launcher on the **All** tab for you and your users.

NOTE

If you don't see the custom tile created in the previous steps, make sure you have an Exchange Online mailbox assigned to you and you've signed into your mailbox at least once. These steps are required for custom tiles in Microsoft 365.

Edit or delete a custom tile

1. In the admin center, go to the **Settings > Org Settings > Organization profile** tab.
2. On the **Organization profile** page, next to **Add custom tiles for your organization**, select **Edit**.
3. Update the **Tile name**, **URL**, **Description**, or **Image URL** for the custom tile (see [Add a custom tile to the app launcher](#)).
4. Select **Update > Close**.

To delete a custom tile, from the **Custom tiles** window, select the tile, select **Remove tile > Delete**.

Next steps

In addition to adding tiles to the app launcher, you can add app launcher tiles to the navigation bar ([learn more](#)). To customize the look and feel of Microsoft 365 to match your organization's brand, see [Customize the Microsoft 365 theme](#).

Related content

[Pin apps to your users' app launcher](#) (article)

[Upgrade your Microsoft 365 for business users to the latest Office client](#) (article)

[Manage add-ins in the admin center](#) (article)

Pin apps to your users' app launcher

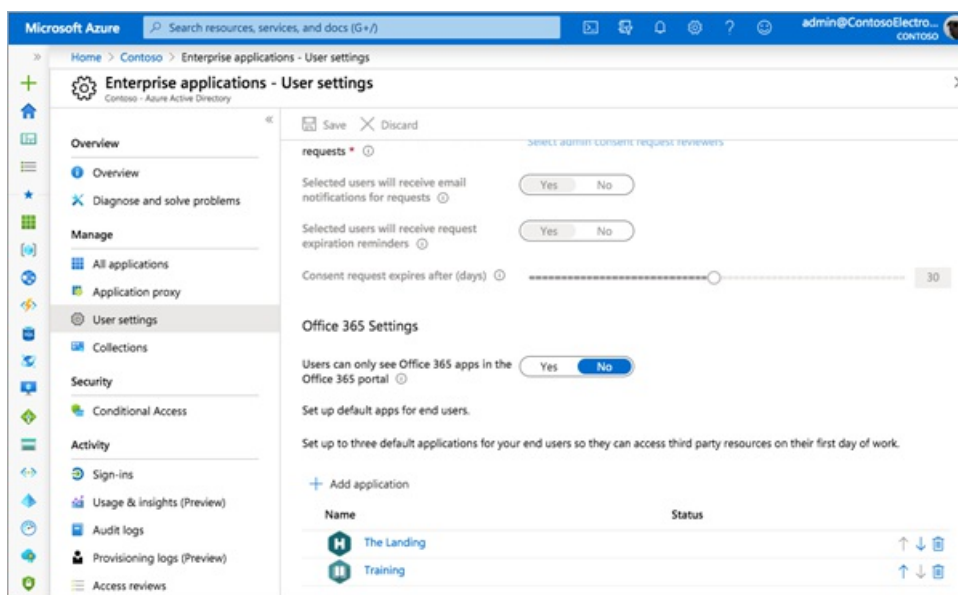
4/3/2021 • 2 minutes to read • [Edit Online](#)

You can use controls in the Azure Active Directory portal to pin up to three apps to Office.com and the app launcher for all the users in your organization. You can also organize groups of applications. Any app you add can later be unpinned by the user at any time. To pin an app for your users, you must be a Cloud application administrator, or Application administrator in Azure Active Directory, or a Global administrator in Office 365. For more information about admin roles, see [admin roles in Azure Active Directory](#) and [admin roles in Microsoft 365](#).

For more information about the app launcher and Office.com, see [meet the app launcher](#) and [updates to office.com and the-Office 365 app launcher](#) blog article.

Use the Azure Active Directory portal to pin apps

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. In the left nav, choose **Show all**, and under **Admin centers**, choose **Azure Active Directory**.
3. In **Azure Active Directory**, choose **Enterprise applications > User settings**.
4. In the **Office 365 Settings** section, choose **Add application**.
5. Choose the applications you want to pin to the users' app launcher, and then choose **Add**.



Pin a custom app

NOTE

The user interface will indicate if you need need to purchase additional Azure AD licenses to use this feature. For more information see [Azure Active Directory pricing](#).

1. In **Azure Active Directory**, choose **Enterprise applications > New application** on the top of the **All applications** page.
2. On the **Add an application** page, choose **Non-gallery application** or **Create your own application** if you are in the preview version of Azure Active Directory.
3. Type a name for the application and then assign user in the **Users and groups** tab.

4. Use the **Properties** tab to upload an icon for the app.
5. To assign a URL to the app, in the **Single sign-on** tab, choose **Linked** and then enter a URL.
6. Choose **Save**.

Create application collections

You can also create application collections for the users in your organization. For instructions, see [create collections on the My Apps portal in the Azure portal](#).

Upgrade your Microsoft 365 for business users to the latest Office client

6/14/2021 • 4 minutes to read • [Edit Online](#)

Office 2010 reaches end-of-support

Office 2010 reached its end of support on October 13, 2020. Microsoft will no longer provide the following:

- Technical support for issues
- Bug fixes for issues that are discovered
- Security fixes for vulnerabilities that are discovered

See [Office 2010 end of support roadmap](#) for more information.

Is this the right topic for you?

If you're the admin responsible for the Microsoft 365 for business subscription in your organization, you're in the right place. Admins are typically responsible for tasks like managing users, resetting passwords, managing Office installs and adding or removing licenses.

If you're not an admin and you have a [Microsoft 365 Family](#) product, see [How do I upgrade Office](#) for information about upgrading your older, home use version of Office.

Get ready to upgrade to Microsoft 365

As an admin, you control what version of Office people in your organization can install. We highly recommend that you help users in your organization running older versions of Office such as Office 2010, Office 2013, or Office 2016 upgrade to the latest version to take advantage of its security and productivity improvements.

Upgrade steps

The steps below will guide you through the process of upgrading your users to the latest Office desktop client. We recommend you read through these steps before beginning the upgrade process.

Step 1 - Check system requirements

[Check the system requirements](#) for Office to make sure your devices are compatible with the latest version of Office. For example, newer versions of Office can't be installed on computers running Windows XP or Windows Vista.

TIP

If you have users in your organization running older versions of Windows on their PCs or laptops, we recommend upgrading to Windows 10. Windows 7 has reached end of support. Read [Support for Windows 7 ends in January 2020](#) for more info.

Check out the [Windows 10 system requirements](#) to see if you can upgrade their operating systems.

Check application compatibility

To ensure a successful upgrade, we recommend identifying your Office applications--including VBA scripts,

macros, third-party add-ins, and complex documents and spreadsheets--and assessing their compatibility with the latest version of Office.

For example, if you're using third-party add-ins with your current Office install, contact the manufacture to make sure they're compatible with the latest version of Office.

Step 2 - Check your existing subscription plan

Some Microsoft 365 plans don't include the full desktop versions of Office and the steps to upgrade are different if your plan doesn't include Office.

Not sure which subscription plan you have? See [What Microsoft 365 for business subscription do I have?](#)

If your existing plan includes Office, move on to [Step 3 - Uninstall Office](#).

If your existing plan doesn't include Office, then select from the options below:

Upgrade options for plans that don't include Office

Option 1: Switch Office subscriptions

Switch to a subscription that includes Office. See [Switch to a different Microsoft 365 for business plan](#).

Option 2: Buy individual, one-time purchases of Office, or buy Office through a volume license

- Buy an individual, one-time purchase of Office. See [Office Home & Business](#) or [Office Professional](#)
- OR
- Buy multiple copies of Office through a volume license. See, [Compare suites available through volume licensing](#).

Step 3 - Uninstall Office

Before installing the latest version of Office, we recommend you uninstall all older versions of Office. However, if you change your mind about upgrading Office, note the following instances where you won't be able to reinstall Office after uninstalling it.

We recommend if you have third-party add-ins, contact the manufacturer to see if there's an update that will work with the latest version of Office.

TIP

If you run into issues while uninstalling Office, you can use the Microsoft Support and Recovery Assistant tool to help you remove Office: [Download and run the Microsoft Support and Recovery Assistant](#).

Select the version of Office you want to uninstall

- [From a PC](#)
- [From a Mac](#)

Known issues trying to reinstall older versions of Office after an uninstall

Office through a volume license If you no longer have access to the source files of these volume license versions of Office, you won't be able to reinstall it.

Office pre-installed on your computer If you no longer have a disc or product key (if Office came with one) you won't be able to reinstall it.

Non-supported subscriptions If your copy of Office was obtained through discontinued subscriptions, such

as Office 365 Small Business Premium or Office 365 Mid-size Business, you won't be able to install an older version of Office unless you have the product key that came with your subscription.

If you'd prefer to install your older version of Office side-by-side with the latest version, you can see a list of versions where this is supported in, [Install and use different versions of Office on the same PC](#). A side-by-side installation might be the right choice for you, if for example, you've installed third-party add-ins you're using with your older version of Office and you're not yet sure they're compatible with the latest version.

Step 4 - Assign Office licenses to users

If you haven't already done so, assign licenses to any users in your organization who need to install Office, see [Assign licenses to users in Microsoft 365 for business](#).

Step 5 - Install Office

After you've verified the users you want to upgrade all have licenses, the final step is to have them install Office, see [Download and install or reinstall Office on your PC or Mac](#).

TIP

If you don't want your users installing Office themselves, see [Manage software download settings in Office 365](#). You can use the [Office Deployment Tool](#) to download the Office software to your local network and then deploy Office by using the software deployment method you typically use.

Test and deploy Microsoft 365 Apps by partners in the Integrated apps portal

8/13/2021 • 18 minutes to read • [Edit Online](#)

The Microsoft 365 admin center gives you the flexibility to deploy single store apps, custom business line of apps and Microsoft 365 partner apps from a single location. The location can be accessed in the Microsoft Admin center settings, in Integrated apps. The ability to find, test, and fully deploy purchased and licensed apps by Microsoft partners from the Integrated apps portal provides the convenience and benefits your organization requires to keep business services updated regularly and running efficiently.

For additional information about purchasing and licensing Microsoft 365 apps from partners for your organization, see [Manage and deploy Microsoft 365 Apps from the Microsoft 365 admin center](#).

For more info on how partners create these apps, see [How to plan a SaaS offer for the commercial marketplace](#)

The Integrated apps portal is only accessible to global admins and available to world-wide customers only. This feature is not available in sovereign and government clouds.

The Integrated apps portal displays a list of apps, which includes single apps and Microsoft 365 apps from partners which are deployed your organization. Only web apps, SPFx apps, Office add-ins and Teams apps are listed. For web apps, you can see two kinds of apps.

- SaaS apps that are available in [appsource.microsoft.com](#), and can be deployed by admins giving consent on behalf of the organization.
- SAML gallery apps that are linked with office add-ins.

Manage apps in the Integrated apps portal

You can manage testing and deployment of purchased and licensed Microsoft 365 Apps from partners.

1. In the admin center, select **Settings**, and then select **Integrated apps**.
2. Choose an app with **Status** of **More apps available** to open the **Manage** pane. The status of **more apps available** lets you know that there are more integrations from the ISVs that aren't yet deployed.
3. On the **Overview** tab, select **Deploy**. Some apps require you to add users before you can select Deploy.
4. Select **Users**, choose **Is this a test deployment**, and then choose **Entire organization**, **Specific users/groups** or **Just me**. You can also choose **Test deployment** if you prefer to wait to deploy the app to the entire organization. Specific users or groups can be a Microsoft 365 group, a security group, or a distribution group.
5. Select **Update** and then **Done**. You can now select Deploy on the Overview tab.
6. Review the app information, and then select **Deploy**.
7. Select **Done** on the Deployment completed page and review the details of the test or full deployment on the **Overview** tab.
8. If the app has a status of **Update pending**, you can click on the app to open the Manage pane and update the app.

Find published apps for testing and full deployment

You can find, test, and fully deploy published apps that don't already appear in the list on the Integrated apps page. By purchasing and licensing the apps from the admin center, you can add Microsoft and Microsoft partner apps to your list from a single location.

1. In the admin center, in the left nav, choose **Settings**, and then choose **Integrated apps**.
2. Select **Get apps** to get a view of the apps.
3. On the **Microsoft 365 Apps** published apps page, select the app you want to deploy by choosing **Get it now**. The apps displayed primarily are Word, PowerPoint, Excel, Outlook add-ins, Teams app and SharePoint apps (built on SharePoint Framework technology). Accept the permissions and select **Continue**.
4. Select **Deploy** at the top of the page next to the message that refers to waiting to be deployed.

If the app selected is linked to a SaaS offer by an ISV, all the other apps that are part of this linked offer will appear on the Configuration page. If you choose to deploy of all of the apps, select **Next**. Otherwise, select **Edit**, and choose which apps you want deployed. Some apps require you to add users before you can select **Deploy**.

5. Select **Add users**, choose **Is this a test deployment**, and then choose **Entire organization** or **Specific users/groups** or **Just me**.

Specific users/groups can be a Microsoft 365 group, a security group, or a distributed group. You can also choose **Test deployment** if you prefer to wait to deploy the app to the entire organization.

6. Select **Next** to get to the **Accept permission request** page. The app capabilities and permissions of each of the apps are listed. If the app needs consent, select **Accept permissions**. Only a global administrator can give consent.
7. Select **Next** to review the deployment and choose **Finish deployment**. You can view the deployment from the **Overview** tab by choosing **View this deployment**. In the Microsoft 365 admin center, you can see the status of each deployed app and the date you deployed the app.

NOTE

If an app was previously deployed from somewhere other than the Integrated Apps portal, the **Deployment Type** is **Custom**.

Unsupported scenarios

You won't be able to deploy a single store app or Microsoft 365 Apps by partner from Integrated apps portal for the following scenarios.

- The same add-in is linked to more than one SaaS offer.
- The SaaS offer is linked to add-ins, but it does not integrate with Microsoft Graph and no AAD App ID is provided.
- The SaaS offer is linked to add-ins, but AAD App ID provided for Microsoft Graph integration is shared across multiple SaaS offers.

Upload custom line-of-business apps for testing and full deployment

1. In the admin center, in the left nav, choose **Settings** and then **Integrated apps**.
2. Select **Upload custom apps**. Only a custom line of apps for Word, PowerPoint, Excel and Outlook is supported.

3. Upload the manifest file from your device or add a URL link. Some apps require you to add users before you can select Deploy.
4. Select **Add users**, choose **Is this a test Deployment**, and choose **Entire organization** or **Specific users/groups** or **Just me**.

Specific users/groups can be a Microsoft 365 group, a security group, or a distributed group. You can also choose **Test deployment** if you want to wait to deploy the app to the entire organization.
5. Select **Next** to get to the **Accept permission request** page. The app capabilities and permissions of the apps are listed. If the app needs consent, select **Accept permissions**. Only a global administrator can give consent.
6. Select **Next** to review the deployment and choose **Finish deployment**. You can view the deployment from the **Overview** tab by choosing **View this deployment**.

Prepare to deploy add-ins in Integrated apps

Office add-ins help you personalize your documents and streamline the way you access information on the web (see [Start using your Office Add-in](#)).

Add-ins provides the following benefits:

- When the relevant Office application starts, the add-in automatically downloads. If the add-in supports add-in commands, the add-in automatically appears in the ribbon within the Office application.
- Add-ins no longer appear for users if the admin turns off or deletes the add-in, or if the user is removed from Azure Active Directory or from a group that the add-in is assigned to.

Add-ins are supported in three desktop platforms Windows, Mac and Online Office apps. It is also supported in iOS and Android (Outlook Mobile Add-ins Only).

It can take up to 24 hours for an add-in to show up for client for all users.

Today both Exchange Admins and Global Admins can deploy add-ins from Integrated apps.

Before you begin

Deployment of add-ins requires that the users are using Microsoft 365 Enterprise licenses (E3/E5/F3) or Microsoft 365 Business licenses (Business Basic, Business Standard, Business Premium). The users also need to be signed into Office using their organizational ID) and have Exchange Online and active Exchange Online mailboxes. Your subscription directory must either be in, or federated to Azure Active Directory.

Deployment doesn't support the following:

- Add-ins that target Word, Excel, or PowerPoint in Office 2013
- An on-premises directory service
- Add-in Deployment to an Exchange On-prem Mailbox
- Deployment of Component Object Model (COM) or Visual Studio Tools for Office (VSTO) add-ins.
- Deployments of Microsoft 365 that do not include Exchange Online such as Microsoft 365 Apps for Business and Microsoft 365 Apps for Enterprise.

Office Requirements

For Word, Excel, and PowerPoint add-ins, your users must be using one of the following:

- On a Windows device, Version 1704 or later of Microsoft 365 Enterprise licenses (E3/E5/F3) or Microsoft 365 Business licenses (Business Basic, Business Standard, Business Premium).
- On a Mac, Version 15.34 or later.

For Outlook, your users must be using one of the following:

- Version 1701 or later of Microsoft 365 Enterprise licenses (E3/E5/F3) or Microsoft 365 Business licenses (Business Basic, Business Standard, Business Premium).
- Version 1808 or later of Office Professional Plus 2019 or Office Standard 2019.
- Version 16.0.4494.1000 or later of Office Professional Plus 2016 (MSI) or Office Standard 2016 (MSI).

NOTE

MSI versions of Outlook show admin-installed add-ins in the appropriate Outlook ribbon, not the "My add-ins" section.

- Version 15.0.4937.1000 or later of Office Professional Plus 2013 (MSI) or Office Standard 2013 (MSI).
- Version 16.0.9318.1000 or later of Office 2016 for Mac.
- Version 2.75.0 or later of Outlook mobile for iOS.
- Version 2.2.145 or later of Outlook mobile for Android.

Exchange Online requirements

Microsoft Exchange stores the add-in manifests within your organization's tenant. The admin deploying add-ins and the users receiving those add-ins must be on a version of Exchange Online that supports OAuth authentication.

Check with your organization's Exchange admin to find out which configuration is in use. OAuth connectivity per user can be verified by using the [Test-OAuthConnectivityPowerShell](#) cmdlet.

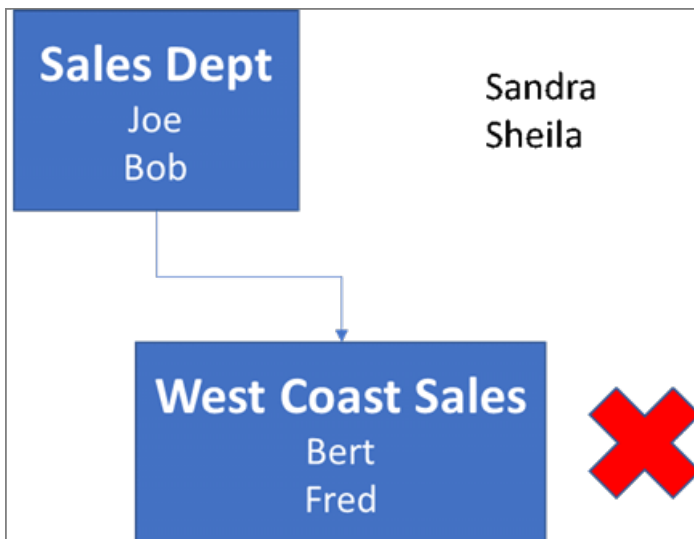
User and group assignments

The deployment of add-in is currently supported to the majority of groups supported by Azure Active Directory, including Microsoft 365 groups, distribution lists, and security groups. Deployment supports users in top-level groups or groups without parent groups, but not users in nested groups or groups that have parent groups.

NOTE

Non-mail enabled security groups are not currently supported.

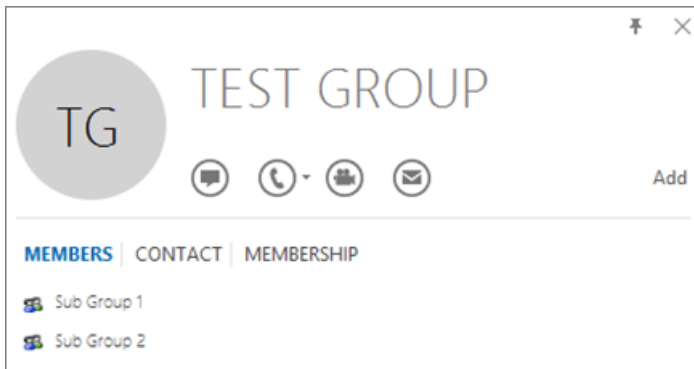
In the following example, Sandra, Sheila, and the Sales Department group are assigned to an add-in. Because the West Coast Sales Department is a nested group, Bert and Fred aren't assigned to an add-in.



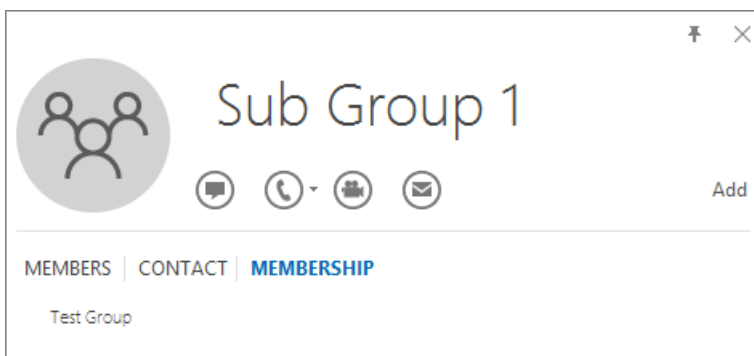
Find out if a group contains nested groups

The easiest way to detect if a group contains nested groups is to view the group contact card within Outlook. If

you enter the group name within the **To** field of an email and then select the group name when it resolves, it will show you if it contains users or nested groups. In the example below, the **Members** tab of the Outlook contact card for the Test Group shows no users and only two sub groups.



You can do the opposite query by resolving the group to see if it's a member of any group. In the example below, you can see under the **Memberships** tab of the Outlook contact card that Sub Group 1 is a member of the Test Group.



Note that you can use the Azure Active Directory Graph API to run queries to find the list of groups within a group. For more information, see [Operations on groups | Graph API reference](#).

Recommended approach for deploying Office add-ins

To roll out add-ins by using a phased approach, we recommend the following:

1. Roll out the add-in to a small set of business stakeholders and members of the IT department. You can turn on the flag **Is this a test deployment**. If the deployment is successful, move to step 2.
2. Roll out the add-in to more individuals within the business. Again, evaluate the results and, if successful, continue with full deployment.
3. Perform a full rollout to all users. Turn off the flag from **Is this a Test deployment**.

Depending on the size of the target audience, you can add or remove roll-out steps.

Deploy an Office add-in using the admin center

1. In the admin center, select **Settings**, then select **Integrated apps**.
2. Select **Get apps** at the top of the page. AppSource will load in an embedded format. Either search for an add-in or find it through clicking on Product on the left nav. If the add-in has been linked by the ISV to a SaaS app or other apps and add-ins and if the SaaS app is a paid app then you will be shown a dialog box to either buy the license or Deploy. Irrespective of whether you have bought the license or not you can go ahead with the deployment. Select **Deploy**.
3. You will see the **Configuration** page where all the apps are listed. If you don't have permissions or the

right access to deploy the app, the respective information will be highlighted. You can select the apps you want to deploy. By selecting **Next**, you will view the **Users** page. If the add-in hasn't been linked by the ISV, you will be routed to the Users page.

4. Select **Everyone**, **Specific users/groups**, or **Just me** to specify whom the add-in is deployed to. Use the Search box to find specific users or groups. If you are testing the add-in, select **Is this a test deployment**.
5. Select **Next**. All the app capabilities and permissions are displayed in a single pane along with certification info if the app has Microsoft 365 certification. Selecting the certification logo lets the user see more details about the certification.
6. Review, and then select **Finish deployment**.
7. A green "tick" icon appears when the add-in is deployed. Follow the on-page instructions to test the add-in.

NOTE

Users might need to relaunch Office to view the add-in icon on the app ribbon. Outlook add-ins can take up to 24 hours to appear on app ribbons.

It's good practice to inform users and groups that the deployed add-in is available. Consider sending an email that describes when and how to use the add-in. Include or link to help content or FAQs that might help users if they have problems with the add-in.

Considerations when assigning an add-in to users and groups

Global admins and Exchange admins can assign an add-in to everyone or to specific users and groups. Each option has implications:

- **Everyone** This option assigns the add-in to every user in the organization. Use this option sparingly and only for add-ins that are truly universal to your organization.
- **Users** If you assign an add-in to an individual user, and then deploy the add-in to a new user, you must first add the new user.
- **Groups** If you assign an add-in to a group, users who are added to the group are automatically assigned the add-in. When a user is removed from a group, the user loses access to the add-in. In either case, no additional action is required from the admin.
- **Just me** If you assign an add-in to just yourself, the add-in is assigned to only your account, which is ideal for testing the add-in.

The right option for your organization depends on your configuration. However, we recommend making assignments by using groups. As an admin, you might find it easier to manage add-ins by using groups and controlling the membership of those groups rather than assigning individual users each time. In some situations, you might want to restrict access to a small set of users by making assignments to specific users by assigning users manually.

More about Office add-ins security

Office add-ins combine an XML manifest file that contains some metadata about the add-in, but most importantly points to a web application which contains all the code and logic. Add-ins can range in their capabilities. For example, add-ins can:

- Display data.

- Read a user's document to provide contextual services.
- Read and write data to and from a user's document to provide value to that user.

For more information about the types and capabilities of Office add-ins, see [Office Add-ins platform overview](#), especially the section "Anatomy of an Office Add-in."

To interact with the user's document, the add-in needs to declare what permission it needs in the manifest. A five-level JavaScript API access-permissions model provides the basis for privacy and security for users of task pane add-ins. The majority of the add-ins in the Office Store are level ReadWriteDocument with almost all add-ins supporting at least the ReadDocument level. For more information about the permission levels, see [Requesting permissions for API use in content and task pane add-ins](#).

When updating a manifest, the typical changes are to an add-in's icon and text. Occasionally, add-in commands change. However, the permissions of the add-in do not change. The web application where all the code and logic for the add-in runs can change at any time, which is the nature of web applications.

Updates for add-ins happen as follows:

- **Line-of-business add-in:** In this case, where an admin explicitly uploaded a manifest, the add-in requires that the admin upload a new manifest file to support metadata changes. The next time the relevant Office applications start, the add-in will update. The web application can change at any time.
- **Office Store add-in:** When an admin selected an add-in from the Office Store, if an add-in updates in the Office Store, the next time the relevant Office applications start, the add-in will update. The web application can change at any time.

NOTE

For Word, Excel and PowerPoint use a [SharePoint App Catalog](#) to deploy add-ins to users in an on-premises environment with no connection to Microsoft 365 and/or support for SharePoint add-ins required. For Outlook use Exchange control panel to deploy in an on-premises environment without a connection to Microsoft 365.

Add-in states

An add-in can be in either the **On** or **Off** state.

STATE	HOW THE STATE OCCURS	IMPACT
Active	Admin uploaded the add-in and assigned it to users or groups.	Users and groups assigned to the add-in see it in the relevant clients.
Turned off	Admin turned off the add-in.	Users and groups assigned to the add-in no longer have access to it. If the add-in state is changed to Active, the users and groups will have access to it again.
Deleted	Admin deleted the add-in.	Users and groups assigned the add-in no longer have access to it.

Consider deleting an add-in if no one is using it anymore. For example, turning off an add-in might make sense if an add-in is used only during specific times of the year.

Manage an Office add-in using the admin center

Post deployment, admins can also manage user access to add-ins.

1. In the admin center, select **Settings**, then select **Integrated apps**.
2. On the Integrated apps page, it will display a list of apps will be either single add-ins or add-ins that have been linked with other apps.
3. Select an app with **Status of More apps available** to open the **Manage** pane. The status of **more apps available** lets you know that there are more integrations from the ISVs that aren't yet deployed.
4. On the **Overview** tab, select **Deploy**. Some apps require you to add users before you can select Deploy.
5. Select **Users**, select **Is this a test deployment**, and then select either **Entire organization**, **Specific users/groups** or **Just me**. You can also select **Test deployment** if you prefer to wait to deploy the app to the entire organization. Specific users or groups can be a Microsoft 365 group, a security group, or a distribution group.
6. Select **Update** and then select **Done**. You can now select **Deploy** on the **Overview** tab.
7. Review the app information, and then select **Deploy**.
8. Select **Done** on the **Deployment completed** page, and review the details of the test or full deployment on the **Overview** tab.
9. If the app has a status of **Update pending**, you can click on the app to open the **Manage** pane and update the app.
10. To just update users, select the **Users** tab and make the appropriate change. Select **Update** after making your changes.

Delete an add-in

You can also delete an add-in that was deployed.

1. In the admin center, select **Settings**, then select **Integrated apps**.
2. Select any row to display the management pane.
3. Select the **Configuration** tab.
4. Select the add-in that you want to delete and then select **Remove**.

NOTE

If the add-in has been deployed by another admin, then the Remove button will be disabled. Only the admin who has deployed the app or a global admin can delete the add-in.

Scenarios where Exchange admin cannot deploy an add-in

There are two cases in which an Exchange Admin won't be able to deploy an add-in:

- If an add-in needs permission to MS Graph APIs and needs consent from a global admin.
- If an add-in is linked to two or more add-ins and webapps, and at least one of these add-ins is deployed by another admin (exchange/global) and the user assignment is not uniform. We only allow deployment of add-ins when the user assignment is the same for all the already deployed apps.

Frequently asked questions

Which administrator role do I need to access Integrated apps?

Only global administrators can access Integrated Apps. Integrated apps won't show up in the left nav for other administrators.

Why do I see Add-in in the left nav under Setting but not Integrated apps?

There could be a few reasons:

- The logged in administrator is an Exchange administrator.

- The customer is in sovereign cloud and Integrated apps experience is available to sovereign cloud customers yet.

What apps can I deploy from Integrated apps?

Integrated apps allow deployment of Web Apps, Teams app, Excel, PowerPoint, Word, Outlook add-ins, and SPFx apps. For add-ins, Integrated apps support deployment to Exchange online mailboxes and not on-premises Exchange mailboxes.

Can administrators delete or remove apps?

Yes. Global administrators can delete or remove apps.

- Select an app from the list view. On the **Configuration** tab, select which apps to remove.

Is Integrated apps available in sovereign cloud?

No. Integrated apps aren't available to sovereign cloud customers.

Is Integrated apps available in government clouds?

No. Integrated apps aren't available to government cloud customers.

Determine if Centralized Deployment of add-ins works for your organization

8/11/2021 • 5 minutes to read • [Edit Online](#)

Centralized Deployment is the recommended and most feature-rich way for most customers to deploy Office add-ins to users and groups within your organization. If you're an admin, use this guidance to determine if your organization and users meet the requirements so that you can use Centralized Deployment.

Centralized Deployment provides the following benefits:

- A Global admin can assign an add-in directly to a user, to multiple users via a group, or to everyone in the organization.
- When the relevant Office application starts, the add-in automatically downloads. If the add-in supports add-in commands, the add-in automatically appears in the ribbon within the Office application.
- Add-ins no longer appear for users if the admin turns off or deletes the add-in, or if the user is removed from Azure Active Directory or from a group that the add-in is assigned to.

Centralized Deployment supports three desktop platforms Windows, Mac and Online Office apps. Centralized Deployment also supports iOS and Android (Outlook Mobile Add-ins Only).

It can take up to 24 hours for an add-in to show up for client for all users.

Before you begin

Centralized deployment of add-ins requires that the users are using Microsoft 365 Enterprise SKUs: E3/E5/F3 or Business SKUs: Business Basic, Business Standard, Business Premium (and are signed into Office using their organizational ID), and have Exchange Online and active Exchange Online mailboxes. Your subscription directory must either be in, or federated to Azure Active Directory. You can view specific requirements for Office and Exchange below, or use the [Centralized Deployment Compatibility Checker](#).

Centralized Deployment doesn't support the following:

- Add-ins that target Word, Excel, or PowerPoint in Office 2013
- An on-premises directory service
- Add-in Deployment to an Exchange On-Prem Mailbox
- Add-in deployment to SharePoint
- Teams apps
- Deployment of Component Object Model (COM) or Visual Studio Tools for Office (VSTO) add-ins.
- Deployments of Microsoft 365 that do not include Exchange Online such as SKUs: Microsoft 365 Apps for Business and Microsoft 365 Apps for Enterprise.

Office Requirements

- For Word, Excel, and PowerPoint add-ins, your users must be using one of the following:
 - On a Windows device, Version 1704 or later of Microsoft 365 Enterprise SKUs: E3/E5/F3 or Business SKUs: Business Basic, Business Standard, Business Premium.
 - On a Mac, Version 15.34 or later.
- For Outlook, your users must be using one of the following:

- Version 1701 or later of Microsoft 365 Enterprise SKUs: E3/E5/F3 or Business SKUs: Business Basic, Business Standard, Business Premium.
- Version 1808 or later of Office Professional Plus 2019 or Office Standard 2019.
- Version 16.0.4494.1000 or later of Office Professional Plus 2016 (MSI) or Office Standard 2016 (MSI)*
- Version 15.0.4937.1000 or later of Office Professional Plus 2013 (MSI) or Office Standard 2013 (MSI)*
- Version 16.0.9318.1000 or later of Office 2016 for Mac
- Version 2.75.0 or later of Outlook mobile for iOS
- Version 2.2.145 or later of Outlook mobile for Android

*MSI versions of Outlook show admin-installed add-ins in the appropriate Outlook ribbon, not the "My add-ins" section.

Exchange Online requirements

Microsoft Exchange stores the add-in manifests within your organization's tenant. The admin deploying add-ins and the users receiving those add-ins must be on a version of Exchange Online that supports OAuth authentication.

Check with your organization's Exchange admin to find out which configuration is in use. OAuth connectivity per user can be verified by using the [Test-OAuthConnectivity](#) PowerShell cmdlet.

Centralized Deployment Compatibility Checker

Using the Centralized Deployment Compatibility Checker, you can verify whether the users on your tenant are set up to use Centralized Deployment for Word, Excel and PowerPoint. The Compatibility Checker is not required for Outlook support. Download the [compatibility checker](#).

Run the compatibility checker

1. Start an elevated PowerShell.exe window.
2. Run the following command:

```
Import-Module 0365CompatibilityChecker
```

3. Run the `Invoke-CompatibilityCheck` command:

```
Invoke-CompatibilityCheck
```

This command prompts you for *TenantDomain* (for example, *TailspinToysIncorporated.onmicrosoft.com*) and *TenantAdmin* credentials (use your global admin credentials), and then requests consent.

NOTE

Depending on the number of users in your tenant, the checker could complete in minutes or hours.

When the tool finishes running, it produces an output file in comma-separated (.csv) format. The file is saved to `C:\windows\system32` by default. The output file contains the following information:

- User Name
- User ID (User's email address)
- Centralized Deployment ready - If the remaining items are true
- Office plan - The plan of Office they are licensed for

- Office Activated - If they have activated Office
- Supported Mailbox - If they are on an OAuth-enabled mailbox

NOTE

Multifactor authentication is not supported when using the Central Deployment PowerShell module. The module only works with Basic authentication.

User and group assignments

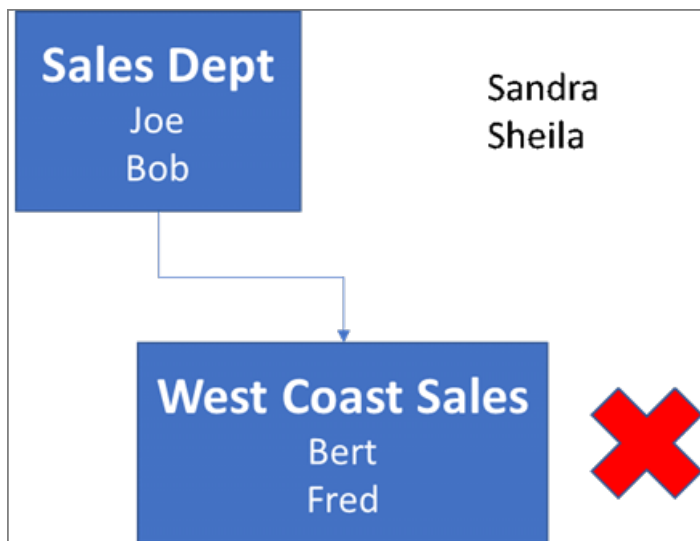
The Centralized Deployment feature currently supports the majority of groups supported by Azure Active Directory, including Microsoft 365 groups, distribution lists, and security groups.

NOTE

Non-mail enabled security groups are not currently supported.

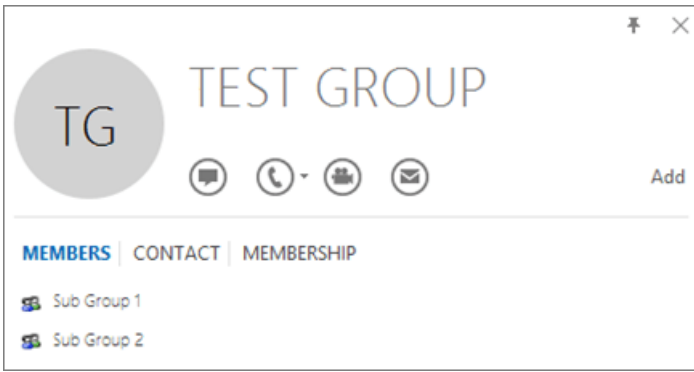
Centralized Deployment supports assignments to individual users, groups, and everyone in the tenant. Centralized Deployment supports users in top-level groups or groups without parent groups, but not users in nested groups or groups that have parent groups.

Take a look at the following example where Sandra, Sheila, and the Sales Department group are assigned to an add-in. Because the West Coast Sales Department is a nested group, Bert and Fred aren't assigned to an add-in.

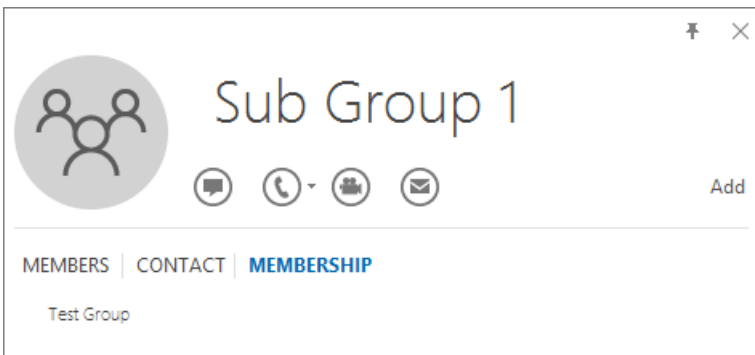


Find out if a group contains nested groups

The easiest way to detect if a group contains nested groups is to view the group contact card within Outlook. If you enter the group name within the **To** field of an email and then select the group name when it resolves, it will show you if it contains users or nested groups. In the example below, the **Members** tab of the Outlook contact card for the Test Group shows no users and only two sub groups.



You can do the opposite query by resolving the group to see if it's a member of any group. In the example below, you can see under the **Membership** tab of the Outlook contact card that Sub Group 1 is a member of the Test Group.



Alternately, you can use the Azure Active Directory Graph API to run queries to find the list of groups within a group. For more information, see [Operations on groups | Graph API reference](#).

Contacting Microsoft for support

If you or your users encounter problems loading the add-in while using Office apps for the web (Word, Excel, etc.), which were centrally deployed, you may need to contact Microsoft support ([learn how](#)). Provide the following information about your Microsoft 365 environment in the support ticket.

PLATFORM	DEBUG INFORMATION
Office	Charles/Fiddler logs Tenant ID (learn how) CorrelationID. View the source of one of the office pages and look for the Correlation ID value and send it to support: <pre><input name=" **wdCorrelationId**" type="hidden" value=" **{BC17079E-505F-3000-C177-26A8E27EB623}**"></pre> <pre><input name="user_id" type="hidden" value="1003bffd96933623"></form></pre>
Rich clients (Windows, Mac)	Charles/Fiddler logs Build numbers of the client app (preferably as a screenshot from File/Account)

Related content

- [Deploy add-ins in the admin center](#) (article)
- [Manage add-ins in the admin center](#) (article)
- [Centralized Deployment FAQ](#) (article)
- [Upgrade your Microsoft 365 for business users to the latest Office client](#) (article)

Deploy add-ins in the admin center

8/13/2021 • 6 minutes to read • [Edit Online](#)

Office add-ins help you personalize your documents and streamline the way you access information on the web (see [Start using your Office Add-in](#)). As an admin, you can deploy Office add-ins for the users in your organization by using the Centralized Deployment feature in the [Microsoft 365 admin center](#). Centralized Deployment is the recommended and most feature-rich way for most admins to deploy add-ins to users and groups within an organization.

For more information on how to determine if your organization can support Centralized Deployment, see [Determine if Centralized Deployment of add-ins works for your organization](#).

To learn more about managing add-ins after deployment, see [Manage add-ins in the admin center](#)

NOTE

For Word, Excel and PowerPoint use a [SharePoint App Catalog](#) to deploy add-ins to users in an on-premises environment with no connection to Microsoft 365 and/or support for SharePoint add-ins required. For Outlook use Exchange control panel to deploy in an on-premises environment without a connection to Microsoft 365.

Recommended approach for deploying Office add-ins

To roll out add-ins by using a phased approach, we recommend the following:

1. Roll out the add-in to a small set of business stakeholders and members of the IT department. If the deployment is successful, move to step 2.
2. Roll out the add-in to more individuals within the business. Again, evaluate the results and, if successful, continue with full deployment.
3. Perform a full rollout to all users.

Depending on the size of the target audience, you can add or remove roll-out steps.

Deploy an Office add-in using the admin center

Before you begin, see [Determine if Centralized Deployment of add-ins works for your organization](#).

1. In the admin center, go to the **Settings > Add-ins** page. If you don't see the **Add-in** Page, go to the **Settings > Integrated apps > Add-ins** page.
2. Select **Deploy Add-in** at the top of the page, and then select **Next**.

NOTE

You can also deploy add-ins in the admin center through [Integrated Apps](#). Integrated Apps is visible to Global and Exchange administrators. If you don't see the above steps, go to the Centralized Deployment section by going to **Settings > Integrated apps**. On the top of the **Integrated apps** page, choose **Add-ins**.

3. Select an option and follow the instructions.
4. If you selected the option to add an add-in from the Office Store, make your add-in selection.

You can view available add-ins by categories: **Suggested for you**, **Rating**, or **Name**. Only free add-ins are available from the Office Store. Paid add-ins aren't supported currently. After you select an add-in, accept the terms and conditions to proceed.

NOTE

With the Office Store option, updates and enhancements are automatically deployed to users.

5. On the next page, select **Everyone**, **Specific users/groups**, or **Just me** to specify who the add-in is deployed to. Use the Search box to find specific users or groups.

NOTE

To learn about other states that apply to an add-in, see [Add-in states](#).

6. Select **Deploy**.
7. A green tick appears when the add-in is deployed. Follow the on-page instructions to test the add-in.

NOTE

Users might need to relaunch Office to view the add-in icon on the app ribbon. Outlook add-ins can take up to 24 hours to appear on app ribbons.

8. When finished, select **Next**. If you've deployed to just yourself, you can select **Change who has access to add-in** to deploy to more users.

If you've deployed the add-in to other members of your organization, follow the instructions to announce the deployment of the add-in.

It's good practice to inform users and groups that the deployed add-in is available. Consider sending an email that describes when and how to use the add-in. Include or link to Help content or FAQs that might help users if they have problems with the add-in.

Considerations when assigning an add-in to users and groups

Global admins and Exchange admins can assign an add-in to everyone or to specific users and groups. Each option has implications:

- **Everyone** This option assigns the add-in to every user in the organization. Use this option sparingly and only for add-ins that are truly universal to your organization.
- **Users** If you assign an add-in to an individual user, and then deploy the add-in to a new user, you must first add the new user.
- **Groups** If you assign an add-in to a group, users who are added to the group are automatically assigned the add-in. When a user is removed from a group, the user loses access to the add-in. In either case, no additional action is required from the admin.
- **Just me** If you assign an add-in to just yourself, the add-in is assigned to only your account, which is ideal for testing the add-in.

The right option for your organization depends on your configuration. However, we recommend making assignments by using groups. As an admin, you might find it easier to manage add-ins by using groups and controlling the membership of those groups rather than assigning individual users each time. In some situations, you might want to restrict access to a small set of users by making assignments to specific users by

assigning users manually.

More about Office add-ins security

Office add-ins combine an XML manifest file that contains some metadata about the add-in, but most importantly points to a web application which contains all the code and logic. Add-ins can range in their capabilities. For example, add-ins can:

- Display data.
- Read a user's document to provide contextual services.
- Read and write data to and from a user's document to provide value to that user.

For more information about the types and capabilities of Office add-ins, see [Office Add-ins platform overview](#), especially the section "Anatomy of an Office Add-in."

To interact with the user's document, the add-in needs to declare what permission it needs in the manifest. A five-level JavaScript API access-permissions model provides the basis for privacy and security for users of task pane add-ins. The majority of the add-ins in the Office Store are level ReadWriteDocument with almost all add-ins supporting at least the ReadDocument level. For more information about the permission levels, see [Requesting permissions for API use in content and task pane add-ins](#).

When updating a manifest, the typical changes are to an add-in's icon and text. Occasionally, add-in commands change. However, the permissions of the add-in do not change. The web application where all the code and logic for the add-in runs can change at any time, which is the nature of web applications.

Updates for add-ins happen as follows:

- **Line-of-business add-in:** In this case, where an admin explicitly uploaded a manifest, the add-in requires that the admin upload a new manifest file to support metadata changes. The next time the relevant Office applications start, the add-in will update. The web application can change at any time.

NOTE

Admin does not need to remove a LOB Add-in for doing an update. In the Add-ins section, Admin can simply click on the LOB Add-in and choose the **Update Button** in the bottom right corner. Update will work only if the version of the new add-in is greater than that of the existing add-in.

- **Office Store add-in:** When an admin selected an add-in from the Office Store, if an add-in updates in the Office Store, the add-in will update later in Centralized Deployment. The next time the relevant Office applications start, the add-in will update. The web application can change at any time.

Related content

[Manage add-ins in the admin center](#) (article)

[Build your first Word task pane add-in](#) (article)

[Minors and acquiring add-ins from the store](#) (article) \ [Use Centralized Deployment PowerShell cmdlets to manage add-ins](#) (article)

[Troubleshoot: User not seeing add-ins](#) (article)

Manage add-ins in the admin center

7/23/2021 • 4 minutes to read • [Edit Online](#)

Office add-ins help you personalize your documents and streamline the way you access information on the web (see [Start using your Office add-in](#)).

After an admin deploys add-ins for users in an organization, the admin can turn add-ins off or on, edit, delete, and manage access to the add-ins.

For more information about installing add-ins from the admin center, see [Deploy add-ins in the admin center](#).

Add-in states

An add-in can be in either the **On** or **Off** state.

STATE	HOW THE STATE OCCURS	IMPACT
Active	Admin uploaded the add-in and assigned it to users or groups.	Users and groups assigned to the add-in see it in the relevant clients.
Turned off	Admin turned off the add-in.	Users and groups assigned to the add-in no longer have access to it. If the add-in state is changed to Active , the users and groups will have access to it again.
Deleted	Admin deleted the add-in.	Users and groups assigned the add-in no longer have access to it.

Consider deleting an add-in if no one is using it anymore. For example, turning off an add-in might make sense if an add-in is used only during specific times of the year.

Delete an add-in

You can also delete an add-in that was deployed.

1. In the admin center, go to the **Settings > Services & add-ins** page.

NOTE

You can also deploy add-ins in the admin center through [Integrated Apps](#). Integrated Apps is visible to Global and Exchange administrators. If you don't see the above steps, go to the Centralized Deployment section by going to **Settings > Integrated apps**. On the top of the **Integrated apps** page, choose **Add-ins**.

2. Select the deployed add-in.
3. Click on **Delete Add-In**. Remove the Add-in button on the bottom-right corner.
4. Validate your selections, and choose **Remove add-in**.

Edit add-in access

Post deployment, admins can also manage user access to add-ins.

1. In the admin center, go to the **Settings > Services & add-ins** page.

NOTE

You can also deploy add-ins in the admin center through [Integrated Apps](#). Integrated Apps is visible to Global and Exchange administrators. If you don't see the above steps, go to the Centralized Deployment section by going to **Settings > Integrated apps**. On the top of the **Integrated apps** page, choose **Add-ins**.

2. Select the deployed add-in.
3. Click on **Edit** under **Who has Access**.
4. Save the changes.

Prevent add-in downloads by turning off the Office Store across all clients (Except Outlook)

NOTE

Outlook add-in installation is managed by a [different process](#).

As an organization you may wish to prevent the download of new Office add-ins from the Office Store. This can be used in conjunction with Centralized Deployment to ensure that only organization-approved add-ins are deployed to users within your organization.

To turn off add-in acquisition

1. In the admin center, go to the **Settings > Services & add-ins** page.

NOTE

You can also deploy add-ins in the admin center through [Integrated Apps](#). Integrated Apps is visible to Global and Exchange administrators. If you don't see the above steps, go to the Centralized Deployment section by going to **Settings > Integrated apps**. On the top of the **Integrated apps** page, choose **Add-ins**.

2. Select **User owned apps and services**.
3. Clear the option to let users access the Office store.

This will prevent all users from acquiring the following add-ins from the store.

- Add-ins for Word, Excel, and PowerPoint 2016 from:
 - Windows
 - Mac
 - Office
- Acquisitions starting within **AppSource**
- Add-ins within Microsoft 365

A user who tries to access the store will see the following message: **Sorry, Microsoft 365 has been configured to prevent individual acquisition of Office Store add-ins.**

Support for turning off the Office Store is available in the following versions:

- Windows: 16.0.9001 - Currently available.

- Mac: 16.10.18011401 - Currently available.
- iOS: 2.9.18010804 - Currently available.
- The web - Currently available.

This does not prevent an administrator from using Centralized Deployment to assign an add-in from the Office Store.

NOTE

Add-ins such as Visio Data Visualizer, Bing Maps, and People Graph will still show up in the ribbon, even if an admin has disabled the Store. To remove these links, administrators must disable the Store through Group Policy Object (GPO).

To prevent a user from signing in with a Microsoft account, you can restrict logon to use only the organizational account. For more information, see [Identity, authentication, and authorization in Office 2016](#).

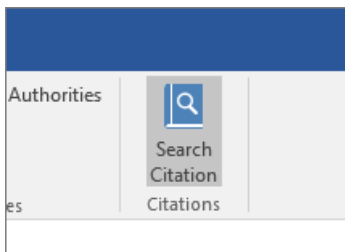
NOTE

Preventing users from accessing the office store will also prevent them from [Sideloaded Office Add-ins for testing from a network share](#).

More about the end-user experience with add-ins

After you deploy an add-in, your end users can start using it in their Office applications (see [Start using your Office Add-in](#)). The add-in appears on all platforms that the add-in supports.

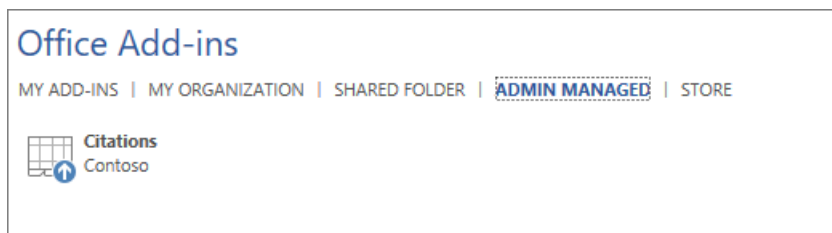
If the add-in supports add-in commands, the commands appear on the Office ribbon. In the following example, the command **Search Citation** appears for the **Citations** add-in.



If the deployed add-in doesn't support add-in commands or if you want to view all deployed add-ins, you can view them via **My Add-ins**.

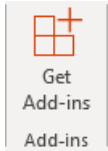
In Word 2016, Excel 2016, or PowerPoint 2016

1. Select **Insert > My Add-ins**.
2. Select the **Admin Managed** tab in the Office Add-ins window.
3. Double-click the add-in you deployed earlier (in this example, **Citations**).



In Outlook

1. On the **Home** ribbon, select **Get Add-ins**.



2. Select **Admin-managed** in the left nav.

Related content

[Deploy add-ins in the admin center](#) (article)

Learn more about creating and building [Office Add-ins](#) (article)

[Use Centralized Deployment PowerShell cmdlets to manage add-ins](#) (article)

[Troubleshoot: User not seeing add-ins](#) (article)

[Minors and acquiring add-ins from the Microsoft Store](#) (article)

Manage Industry news

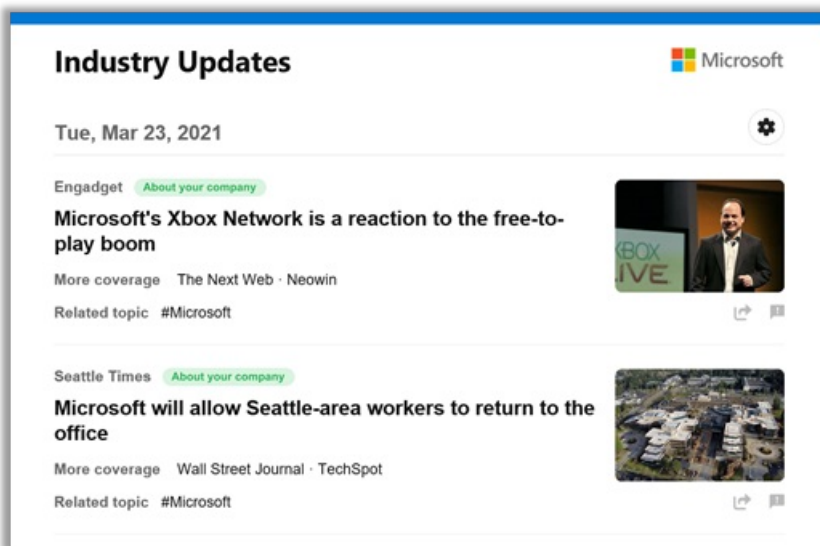
7/12/2021 • 3 minutes to read • [Edit Online](#)

To provide your users with up-to-date news headlines about your industry and info from your organization, use the News service to enable a customized news feed for your organization. You can also enable a daily Industry Updates email, and manage settings for the Bing homepage and Microsoft Edge new tab page.

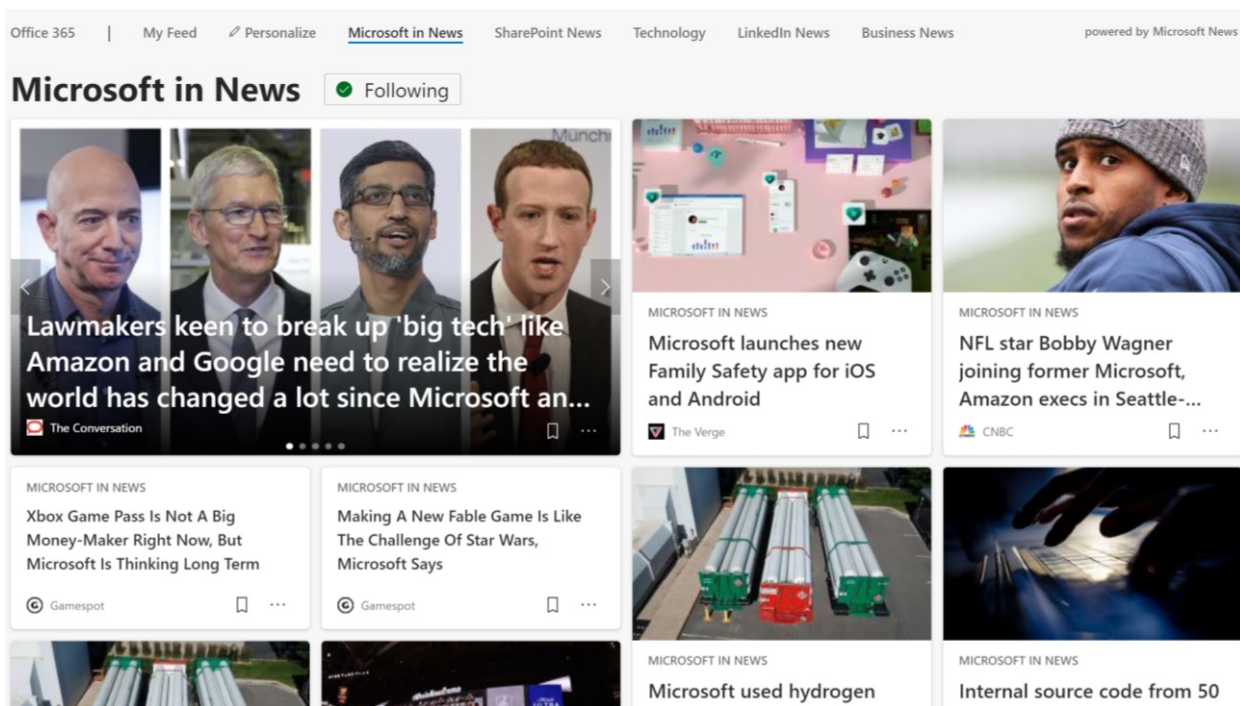
What your users will see

You have the option to send your users a daily Industry Updates email with headlines and links to full articles. Users can customize their email updates by following additional topics, choosing when the update is delivered, excluding articles behind paywalls, and selecting the number of articles they want to see.

Signed-in users who go to the Bing homepage see your industry's news feed under the personalized info for your organization.



They can also see company, industry, and internal news or personalized work information on their Microsoft Edge new tab page.



News settings

As an admin, you control the News feed settings for your organization, including the selected industry and the Bing homepage, the Microsoft Edge new tab page (Starting with the release of Edge 87), and the email experiences.

1. In the Microsoft 365 admin center, go to **Settings > Org settings > Services > News**.
2. In the **News** panel, click the **General** tab.
3. In the **Industry** list, select your organization's industries. This determines the general news that appears in your organization news feed. Microsoft may pre-select an industry using information from your account. You can remove or add industries by updating the **Industry** list.
4. In the **Topics** field, enter topics that you want see news articles about. Your users can't change these topics.
5. You can block articles containing keywords in the **Exclude content** field. For example, to avoid articles containing the keyword "bake" from showing up in the news feed, add the keyword "bake" in the **Exclude content** field. Avoid including general terms (the, it, and, etc.); they can block relevant content from appearing in your enterprise news feeds.
6. Select **Save**. It may take up to 24 hours for changes to appear.

Industry updates in email

You can send a daily email update with relevant industry news to your users' inboxes. To set daily email updates for users:

1. In the Microsoft 365 admin center, go to **Settings > Org settings > Services > News**.
2. In the **News** panel, click the **Industry Updates** tab.
3. Select **Send daily email updates** to send an email to your users.
4. To give users the ability to customize the news they get in their email updates, select **Allow users to customize their own topics**.

Bing homepage

You can customize the Bing homepage to include news about your industry.

1. In the Microsoft 365 admin center, go to **Settings > Org settings > Services > News**.
2. In the **News** panel, click the **Bing homepage** tab, and select **Include on Bing homepage**.

The industry news appears under the personalized info from your organization on Bing.com.

Microsoft Edge new tab page

When your users sign in to Microsoft Edge (release 87 or higher) with a valid work or school account, they can see news tailored to your organization.

1. In the Microsoft 365 admin center, go to **Settings > Org settings > Services > News**.
2. In the **News** panel, click **Microsoft Edge new tab page**.
3. Select **Allow Office 365 content on the new tab page**. When enabled, users can customize their new tab to show information from Office 365, including recommended and recent files, along with frequently used SharePoint sites and other information.
4. Select **Show company information and industry news on the new tab page**. News articles about your organization and industry appear for users that choose to see articles on their new tab.

Related articles

- [Microsoft Search](#)
- [Manage your data and service](#)

Manage Office Scripts settings

7/28/2021 • 3 minutes to read • [Edit Online](#)

[Office Scripts](#) allows users to automate tasks by recording, editing, and running scripts in Excel on the web. Office Scripts works with Power Automate, and users run scripts on workbooks by using the Excel Online (Business) connector. Microsoft 365 admins can manage Office Scripts settings from the Microsoft 365 admin center.

Before you begin

- To manage Office Scripts settings, you must be a Global admin. For more information, see [About admin roles](#).
- Ensure users in your organization have a valid license for a Microsoft 365 or Office 365 commercial or EDU plan that includes access to Office desktop apps, such as one of the following plans:
 - Microsoft 365 Business Standard
 - Microsoft 365 Apps for business
 - Microsoft 365 Apps for enterprise
 - Office 365 E3
 - Office 365 E5
 - Office 365 A3
 - Office 365 A5

Manage availability of Office Scripts and sharing of scripts

1. In the Microsoft 365 admin center, go to the **Settings** > **Org settings** > **Services** tab.
2. Select **Office Scripts**.
3. Office Scripts is turned on by default, and everyone in your organization can access and use the feature and share scripts. To turn off Office Scripts for your organization, clear the **Let users automate their tasks in Excel on the web** check box.
4. If you previously turned off Office Scripts for your organization and you want to turn it back on, select **Let users automate their tasks in Excel on the web**, and then specify who can access and use the feature:
 - To allow all users in your organization to access and use Office Scripts, leave **Everyone** (the default) selected.
 - To allow only members of a specific group to access and use Office Scripts, select **Specific group**, and then enter the name or email alias of the group to add it to the allow list. You may add only one group to the allow list, and it must be one of the following types:
 - Microsoft 365 group
 - Distribution group
 - Security group
 - Mail-enabled security group

To learn more about the different types of groups, see [Compare groups](#).

- To allow users with access to Office Scripts to share their scripts with others in your organization, select **Let users with access to Office Scripts share their scripts with others in the organization**. Sharing scripts outside of an organization is not allowed.

NOTE

If you later turn off script sharing for your organization, users will still be able to run previously-shared scripts.

- Specify which users with access to Office Scripts can share their scripts:
 - To allow all users with access to Office Scripts to share their scripts, leave **Everyone** (the default) selected.
 - To allow only members of a specific group with access to Office Scripts to share their scripts, select **Specific group**, and then enter the name or email alias of the group to add it to the allow list. You may add only one group to the allow list, and it must be one of the following types:
 - Microsoft 365 group
 - Distribution group
 - Security group
 - Mail-enabled security groupTo learn more about the different types of groups, see [Compare groups](#).
- To allow users to run their Office Scripts inside Power Automate flows, select **Let users with access to Office Scripts run their scripts with Power Automate**. This allows users to add flow steps with the [Excel Online \(Business\) Connector's Run script](#) option.
 - To allow all users with access to Office Scripts to use their scripts in flows, leave **Everyone** (the default) selected.
 - To allow only members of a specific group with access to Office Scripts to use their scripts in flows, select **Specific group**, and then enter the name or email alias of the group to add it to the allow list. You may add only one group to the allow list, and it must be one of the following types:
 - Microsoft 365 group
 - Distribution group
 - Security group
 - Mail-enabled security groupTo learn more about the different types of groups, see [Compare groups](#).
 - To learn more about using Office Scripts with Power Automate, see [Run Office Scripts with Power Automate](#).

- Select **Save**.

It can take up to 48 hours for changes to Office Scripts settings to take effect.

Next steps

Because Office Scripts works with Power Automate, we recommend that you review your existing data loss prevention (DLP) policies to ensure your organization's data remains protected while users use Office Scripts. For more information, see [Data loss prevention \(DLP\) policies](#).

Related content

[Office Scripts technical documentation](#) (link page)

[Introduction to Office Scripts in Excel](#) (article)

[Sharing Office Scripts in Excel for the Web](#) (article)

[Record, edit, and create Office Scripts in Excel on the web](#) (article)

Find your partner or reseller

4/3/2021 • 2 minutes to read • [Edit Online](#)

As an admin, you can work with a partner to purchase, activate, and renew Microsoft 365 subscriptions through a Microsoft Open Volume Licensing program.

Not sure if Open Volume Licensing is for you? Check out the [Microsoft Open Programs overview](#).

Find a new partner or reseller

If you're ready to buy or renew Microsoft 365 through Open Volume Licensing, or you simply want more information about working with a partner, choose an option below.

- [Search for a partner using Microsoft PinPoint](#)
- [Call Microsoft Volume Licensing](#)

Find contact information for a partner you've worked with in the past

NOTE

In some cases, you can find information in the Microsoft 365 admin center for partners you've worked with in the past. Keep in mind that this information may be out of date. As a best practice, we recommend contacting the person or department responsible for purchasing in your organization to find out which partner you should work with.

Get partner info in the admin center

1. In the admin center, go to the **Settings** > [Partner relationships](#) page.
2. If you have a partner, the partner's name and relationship to your organization will be listed here. To view partner contact information (phone number and email address), select the partner name.

More resources

[Microsoft Volume Licensing Service Center training and resources](#)

For Microsoft partners

[Help for partners](#)

Set up the Standard or Targeted release options

8/13/2021 • 4 minutes to read • [Edit Online](#)

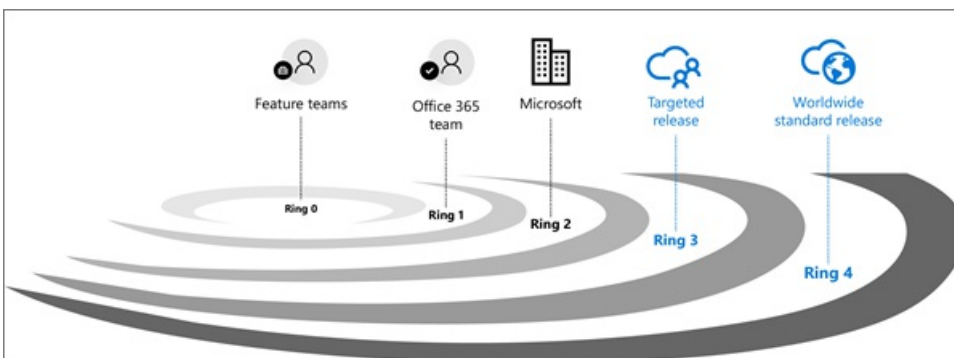
IMPORTANT

The Microsoft 365 updates described in this article apply to Microsoft 365, SharePoint Online, and Exchange Online. These release options are targeted, best effort ways to release changes to Microsoft 365 but cannot be guaranteed at all times or for all updates. They do not apply to Microsoft 365 Apps, Skype for Business, Microsoft Teams, and related services. For information about release options for Microsoft 365 Apps, see [Overview of update channels for Microsoft 365 Apps](#).

With Microsoft 365, you receive new product updates and features as they become available instead of doing costly updates every few years. You can manage how your organization receives these updates. For example, you can sign up for an early release so that your organization receives updates first. You can designate that only certain individuals receive the updates. Or, you can remain on the default release schedule and receive the updates later. This article explains the different release options and how you can use them for your organization.

How it works - release validation

Any new release is first tested and validated by the feature team, then by the entire Microsoft 365 feature team, followed by all of Microsoft. After internal testing and validation, the next step is a **Targeted release** (formerly known as First release) to customers who opt in. At each release ring, Microsoft collects feedback and further validates quality by monitoring key usage metrics. This series of progressive validation is in place to make sure the worldwide-release is as robust as possible. The releases are pictured in the following figure.



For significant updates, customers are initially notified by the [Microsoft 365 Roadmap](#). As an update gets closer to rolling out, it is communicated through your [Microsoft 365 Message center](#).

NOTE

You need a Microsoft 365 or Azure AD account to access your Message center through the [admin center](#). Microsoft 365 home plan users do not have an admin center.

Standard release

This is the default option where you and your users receive the latest updates when they're released broadly to all customers.

A good practice is to leave the majority of users in **Standard release** and IT Pros and power users in **Targeted**

release to evaluate new features and prepare teams to support business users and executives.

NOTE

If you switch from targeted release back to standard release track, your users may lose access to features that haven't reached standard release yet.

Targeted release

With this option, you and your users can be the first to see the latest updates and help shape the product by providing early feedback. You can choose to have individuals or the entire organization receive updates early.

IMPORTANT

Large or complex updates may take longer than others so that no users are adversely affected. There is no guarantee on the exact timeline of a release.

Targeted release for entire organization

If you [Set up the release option in the admin center](#) for this option, all your users will get the Targeted release experience. For organizations with more than 300 users, we recommend using a test subscription for this option. For test subscription information, please reach out to your Microsoft contact.

Targeted release for selected users

If you [Set up the release option in the admin center](#) for this option, you can define specific users, usually power users, to receive early access to features and functionality.

Benefits of Targeted release

Targeted release allows admins, change managers, or anyone else responsible for Microsoft 365 updates to prepare for the upcoming changes by letting them:

- Test and validate new updates before they are released to all the users in the organization.
- Prepare user notification and documentation before updates are released worldwide.
- Prepare internal help-desk for upcoming changes.
- Go through compliance and security reviews.
- Use feature controls, where applicable, to control the release of updates to end users.

Set up the release option in the admin center

You can change how your organization receives Microsoft 365 updates by following these steps. You have to be a global admin in Microsoft 365 to opt in.

IMPORTANT

It can take up to 24 hours for the below changes to take effect in Microsoft 365. If you opt out of targeted release after enabling it, your users may lose access to features that haven't reached the scheduled release yet.

1. In the admin center, go to the **Settings > Org Setting**, and under the **Organization profile tab**, choose **Release preferences**.
2. To disable targeted release, select **Standard release**, then select **Save changes**.

3. To enable targeted release for all users in your organization, select **Targeted release for everyone**, then select **Save changes**.
4. To enable targeted release for some people in your organization, select **Targeted release for selected users**, then select **Save changes**.
5. Choose **Select users** to add users one at a time, or **Upload users** to add them in bulk.
6. When you're done adding users, select **Save changes**.

Next steps

Discover how to [manage messages](#) in your [Microsoft 365 Message center](#) to get notifications about upcoming Microsoft 365 updates and releases.

Related content

[Join the Office Insider Program](#) (article)

Manage which Office features appear in What's New

8/13/2021 • 2 minutes to read • [Edit Online](#)

When an important Office feature is released, users will get a message about it when they choose **Help > What's New** in their Office app on Windows.

You can control which of these feature messages your users are shown by using the **What's new in Office** feature in the Microsoft 365 admin center. If you decide to hide a feature message to your users, you can always come back later and decide to show it to them.

NOTE

- Hiding a feature message from your users doesn't disable the feature in the Office app.
- You must be assigned either the Global admin role or the Office apps admin role to use the **What's new in Office** feature.

Show or hide new features

1. In the Microsoft 365 admin center, under **Settings**, choose **Org settings**, select the **Services** tab, and then select **What's new in Office**.
2. When you click on the feature name, a fly-out panel appears with the following information:
 - A short description of the feature.
 - A link to an article to learn more about the feature.
 - The Office applications that the feature appears in.
 - The first version (release) that the feature is available in for that channel.
3. Choose **Hide from users**. Or, if you previously hid the feature, choose **Show to users**.

You can also select multiple features on the **Manage which Office features appear in What's New** page, and then choose either **Hide** or **Show**.

NOTE

- If a feature is available in multiple Office apps, setting the feature to **Hidden** hides the feature message in all of those Office apps.
- All feature messages are shown to users by default. This is the default status for all features, and the status only changes if you have chosen to hide or show a feature message.
- You can also get to the **What's new in Office** feature from the Microsoft 365 Apps admin center (<https://config.office.com>). The feature is found under **Customization > What's New Management**.

List of features

You can filter which features appear on the **Manage which Office features appear in What's New** page. You can filter by channel, application, or status, or by some combination of them.

New features appear on the page based on the following schedule:

CHANNEL	DATE	TAKE ACTION
Current	15th of the month	1 - 3 weeks before the monthly release
Monthly Enterprise	First of the month	Two weeks before the major release that brings new features
Semi-Annual Enterprise (Preview)	Sept 1 and March 1	2 weeks before the major release that brings new features
Semi-Annual Enterprise	Jan 1 and July 1	2 weeks before the major release that brings new features

For more information about when new versions are released to each update channel, see [Update history for Microsoft 365 Apps \(listed by date\)](#).

Add the "What's new in Office" card to the admin center home page

1. On the Microsoft 365 admin page, choose **Add card** on top of the page
2. Locate **Manage which Office features appear in What's New** in the list and choose it.
3. Once the card is on your home page, you can choose **What's new in Office** to [show or hide the features](#) for your organization.

Related articles

[Office What's New management is now generally available](#)

Microsoft 365 usage analytics

8/3/2021 • 11 minutes to read • [Edit Online](#)

Use Microsoft 365 usage analytics within Power BI to gain insights on how your organization is adopting the various services within Microsoft 365. You can visualize and analyze Microsoft 365 usage data, create custom reports and share the insights within your organization. You can also gain insights into how specific regions or departments are using Microsoft 365.

Microsoft 365 usage analytics gives you access to a pre-built dashboard that provides a cross-product view of the last 12 months and contains a number of pre-built reports. Each report provides you with specific usage insights. User-specific information is available for the last full calendar month.

The [data model](#) that powers the template app includes user attributes from Active Directory, enabling the ability to pivot in certain reports. The following Active Directory attributes are included: location, department, and organization.

See [Enable Microsoft 365 usage analytics](#) to start collecting data.

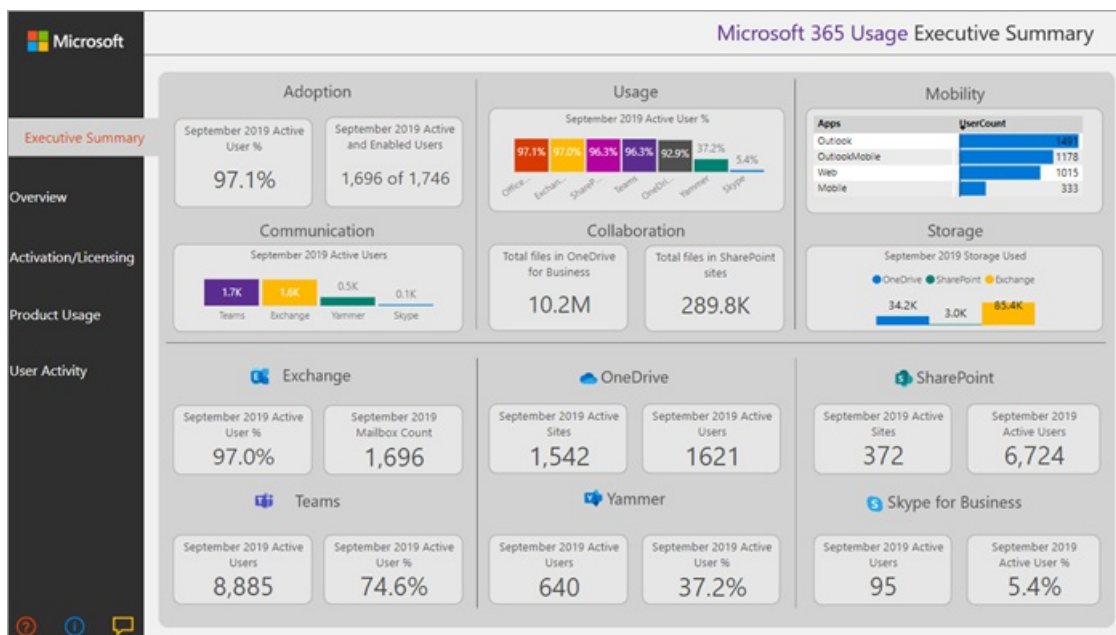
Microsoft 365 usage analytics contains a number of reports detailed in the following sections.

You can access detailed reports for each area by selecting the data tables. You can view all pre-built reports by selecting the tabs at the bottom of the site. For more detailed instructions, read [Navigating and utilizing the reports](#) and [Customizing the reports](#).

Executive summary

The executive summary is a high-level, at-a-glance view of Microsoft 365 for Business adoption, usage, mobility, communication, collaboration, and storage reports, and is meant for business decision makers. It provides a view into how some individual services are being used, based on all the users who have been enabled and those who are active. All values of the month shown on the report refer to the latest complete month.

This summary lets you quickly understand usage patterns in Office and how and where your employees are collaborating.



Overview

The Microsoft 365 overview report contains the following reports. You can view them by choosing the tab on top of the report page. All values of the month shown on the top section of the report refer to the latest complete month.

- **Adoption** – Offers an all-up summary of adoption trends. Use the reports in this section to learn how your users have adopted Microsoft 365, as well as how overall usage of the individual services has changed month over month. You can see how many users are enabled, how many people in your organization are actively using Microsoft 365, how many are returning users, and how many are using the product for the first time.
- **Usage** – Offers a drill-down view into the volume of active users and the key activities for each product for the last 12 months. Use the reports in this section to learn how people in your organization are using Microsoft 365.
- **Communication** – You can see at a glance whether people in your organization prefer to stay in touch by using Teams, Yammer, email, or Skype calls. You can observe if there are shifts in patterns in the use of communication tools among your employees.
- **Collaboration** – See how people in your organization use OneDrive and SharePoint to store documents and collaborate with each other, and how these trends evolve month over month. You can also see how many users shared documents internally or externally and how many users used SharePoint sites or OneDrive accounts, broken out by owners and other collaborators.
- **Storage** – Use this report to track cloud storage for mailboxes, OneDrive, and SharePoint sites.
- **Mobility** – Track which clients and devices people use to connect to email, Teams, Skype, or Yammer.

Activation and licensing

The activation and license page offers reports on Microsoft 365 activation; that is, how many users have downloaded and activated Office apps and how many licenses have been assigned by your organization. The month value towards the top refers to the current month, and the metrics reflect values aggregated from the beginning of the month to the current date.

- **Activation** – Track service plan (for example, Microsoft 365 Apps for enterprise, Project, and Visio) activations in your organization. Each person with an Office license can install products on up to five devices. You can also use reports in this section to see the devices on which people have installed Office apps. Note that to activate a plan, a user must install the app and sign in with their account.
- **Licensing** – This report contains an overview of license types, the count of users who were assigned each license type, and the license assignment distribution for each month. The month value towards the top refers to the current month, and the metrics reflect values aggregated from the beginning of the month to the current date.

Product usage

This report contains a separate report for each Microsoft 365 service, including Exchange, Microsoft 365 groups, OneDrive, SharePoint, Skype, Teams, and Yammer. Each report contains total enabled vs. total active user reports, counts of entities such as mailboxes, sites, groups, and accounts, as well as activity type reports where appropriate. All values of the month shown on the top section of the report refer to the latest complete month.

User activity

User activity reports are available for certain individual services. These reports provide user-level detail usage

data joined with Active Directory attributes. In addition, the Department Adoption report lets you slice by Active Directory attributes so that you can see active users across all individual services. All metrics are aggregated for the latest complete month. To view the content date, navigate to the table page and select UserActivity table where the value under TimeFrame provides the reporting period.

FAQ

Is this template app going to be available through purchase or will it be free?

It is not free, you will need a Power BI Pro license. For details see [prerequisites](#) for installing, customizing, and distributing a template app.

To share the dashboards with others, please see more at [Share dashboards and reports](#).

Is the Usage Summary Reports Reader role enough to view the usage analytics?

The Usage Summary Reports Reader role only allows access to tenant level aggregates in Microsoft 365 usage analytics. We recommend the Reports Reader or Usage Summary Reports Reader role to anyone who's responsible for change management and adoption, but is not necessarily an IT administrator.

Who can connect to Microsoft 365 usage analytics?

You have to be either a **Global admin**, **Exchange admin**, **Skype for Business admin**, **SharePoint admin**, **Global reader** or **Report reader** in order to establish the connection to the template app. See [About admin roles](#) for more information.

Who can customize the usage analytics reports?

Only the user who made the initial connection to the template app can customize the reports or create new reports in the Power BI web interface. See [Customizing the reports in Microsoft 365 usage analytics](#) for instructions.

Can I only customize the reports from the Power BI web interface?

In addition to customizing the reports from the Power BI web interface, users can also use Power BI Desktop to connect directly to the Microsoft 365 reporting service to build their own reports.

How can I get the pbbit file that this dashboard is associated with?

You can access to the pbbit file from the [Microsoft Download center](#).

Who can view the dashboards and reports?

If you connected to the template app, you can share it with anybody by using the [sharing functionality](#). Power BI licensing requires that both the user sharing and the user with whom a dashboard is shared have Power BI Pro or Power BI Premium.

Can anyone share the dashboard, or does it have to be the person who connected to the dashboard?

When sharing the dashboard, you can either allow users to re-share the dashboard with others or not. You can set this option at the time of sharing.

Is it possible to work on and customize the same template app with a group of people?

Yes. To enable a group of admins to work together on the same template app, you can leverage the app workspace functionality of Power BI, for more information, see [How should I collaborate and share dashboards and reports?](#)

For which timeframe is data available?

The majority of the reports display data for the previous 12 months. However, some of the charts may show less history since the data collection for different products and reports were started at different times and thus data for the full 12 months might not be available. All the reports will eventually build up to 12 months of history. Reports that show user level details show data for the previous complete month.

What data is included in the template app?

The data in the template app currently covers the same set of activity metrics available in the [Activity Reports](#). As reports are added to the activity reports, they will be added to the template app in a future release.

How does the data in the template app differ from the data in the usage reports?

The underlying data you see in the template app matches the data you see in the activity reports in the Microsoft 365 admin center. The key differences are that in the admin center data is available for the last 7/30/90/180 days while the template app presents data on a monthly basis for up to 12 months.

In addition, user level details in the template app are only available for the last complete month for users who were assigned a product license and performed an activity.

When should I use the template app and when the usage reports?

The [Activity Reports](#) are a good starting point to understand usage and adoption of Microsoft 365. The template app combines the Microsoft 365 usage data and your organization's Active Directory information and enables admins to analyze the data set using the visual analytics capabilities of Power BI. This enables admins to not just visualize and analyze Microsoft 365 usage data, but also slice it by Active Directory properties such as departments, location etc. They can also create custom reports and share the insights within their organization.

How often is the data refreshed?

When you connect to the template app for the first time, it will automatically populate with your data for the previous 12 months. After that, the template app data will refresh weekly. Customers can choose to modify the refresh schedule if their use of this data demands a different update rhythm.

The back-end Microsoft 365 service will refresh data on a daily basis and provides data that is between 5-8 days latent from the current date.

The **Content date** column in each dataset represents the freshness date of the data in the template app.

How is an active user defined?

The definition of active user is the same as the definition of [active user](#) in the activity reports.

What SharePoint site collections are included in the SharePoint reports?

The current version of the template app includes file activity from SharePoint team sites and SharePoint group sites.

Which groups are included in the Microsoft 365 Groups usage report?

The current version of the template app includes usage from Outlook groups, Yammer groups, and SharePoint groups. It does not include groups related to Microsoft Teams or Planner.

When will an updated version of the template app become available?

Major changes to the template app will be released twice a year which may include new reports or new data. Minor changes to the reports may be released on a more frequent basis.

Is it possible to integrate the data from the template app into existing solutions?

The data in the template app can be retrieved through the Microsoft 365 APIs (in preview). When they ship to production they will be merged within the [Microsoft Graph reporting APIs](#).

Are there plans to expand the template app to show usage data from other Microsoft products?

This is considered for future improvements. Check the [Microsoft 365 Roadmap](#) for updates.

How can I pivot by company information in Active Directory?

Company information is included one of the Active Directory fields in the template app and you can see it as a pre-built filter in the **Product User** activity reports. It is available as column in the **UserState** table.

Is it possible to bring in additional fields from Active Directory?

Additional customization on this data is possible by connecting to the [Microsoft Graph reporting APIs](#) to pull additional fields from Azure Active Directory and join to the dataset.

Is it possible to aggregate the information in the template app across multiple subscriptions?

At this time, the template app is for a single subscription, as it is associated with the credentials that was used to initially connect to it.

Is it possible to see usage by plan (i.e. E1, E3)?

In the template app, usage is represented at the per product level. Data about the various subscriptions that are assigned to users are provided, however it is not possible to correlate user activity to the subscription assigned to user.

Is it possible to integrate other data sets into the template app?

You can use Power BI Desktop to connect to the Microsoft 365 APIs (in preview) to bring additional data sources to combine with the template app data.

For more information see the [Customize document](#).

Is it possible to see the "Top Users" reports for a specific timeframe?

All user level reports present aggregated data for the previous month.

Will the template app be localized?

This is currently not on the roadmap.

I have a specific question about the data I'm seeing for my organization. Who can I reach out to?

You can use the feedback button in the admin center activity overview page, or you can open a [support case](#) to get help with the template app.

How can partners access the data?

If a partner has delegated admin rights, he or she can connect to the template app on behalf of their customer.

Can I hide identifiable information such as user, group, and site names in reports?

Yes, see [Make the collected data anonymous](#).

Related content

[Enable Microsoft 365 usage analytics](#) (article)

[Navigate and utilize the reports in Microsoft 365 usage analytics](#) (article)

[Review usage reports in Microsoft 365](#) (video)

Enable Microsoft 365 usage analytics

8/13/2021 • 3 minutes to read • [Edit Online](#)

Microsoft 365 usage analytics is not yet available for Microsoft 365 US Government Community.

Before you begin

To get started with Microsoft 365 usage analytics you must first make the data available in the [Microsoft 365 admin center](#), then initiate the template app in Power BI.

Get Power BI

If you don't already have Power BI, you can [sign up for Power BI Pro](#). Select **Try free** to sign up for a trial, or **Buy now** to get Power BI Pro.

You can also expand **Products** to buy a version of Power BI.

NOTE

You need a Power BI Pro license to install, customize, and distribute a template app. For more information, please see [Prerequisites](#).

To share your data, both you and the people who you share the data with, need a Power BI Pro license, or the content needs to be in a workspace in a [Power BI premium service](#).

Enable the template app

To enable the template app, you have to be a **Global administrator**.

See [about admin roles](#) for more information.


1. In the admin center, go to the **Settings > Org settings > Services** tab.
2. On the **Services** tab, select **Reports**.
3. On the Reports panel that opens, set **Make report data available to Microsoft 365 usage analytics for Power BI** to **On > Save**.

The data collection process will complete in two to 48 hours depending on the size of your tenant. The **Go to Power BI** button will be enabled (no longer gray) when data collection is complete.

Start the template app

To start the template app, you have to be either a **global administrator**, **report reader**, **Exchange administrator**, **Skype for Business administrator**, or **SharePoint administrator**.

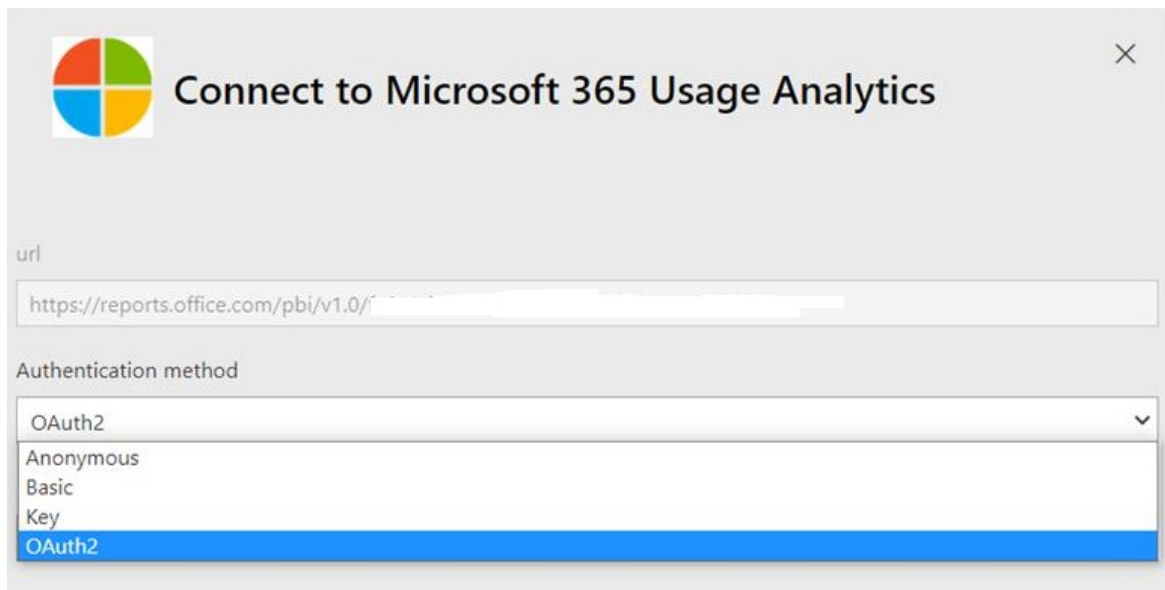
1. Copy the tenant ID and select **Go to Power BI**.
2. When you get to Power BI, sign in. Then **Select Apps->Get apps** from the navigation menu.
3. In the **Apps** tab, type Microsoft 365 in the search box and then select **Microsoft 365 usage analytics > Get it now**.



Microsoft 365 Usage Analytics
By Megan Bowen
Power BI
Analyze usage and adoption trends of Microsoft 365 services in your organization

[Get it now](#)

4. Once the app is installed. Select the tile to open it.
5. Select **Explore app** to view the app with sample data. Choose **Connect** to connect the app to your organization's data.
6. Choose **Connect**, on the **Connect to Microsoft 365 usage analytics** screen, then type in the tenant ID (without dashes) you copied in step (1), and select **Next**.
7. On the next screen, select **OAuth2** as the **Authentication method** > **Sign in**. If you choose any other authentication method, the connection to the template app will fail.



url

<https://reports.office.com/pbi/v1.0/>

Authentication method

OAuth2

Anonymous

Basic

Key

OAuth2

8. After the template app is instantiated the Microsoft 365 usage analytics dashboard will be available in Power BI on the web. The initial loading of the dashboard will take between 2 to 30 minutes.

Tenant level aggregates will be available in all reports after opting in. **User-level details will only become available around the 5th of the next calendar month after opting in.** This will impact all reports under User Activity (See [Navigate and utilize the reports in Microsoft 365 usage analytics](#) for tips on how to view and use these reports).

Make the collected data anonymous

To make the data that is collected for all reports anonymous, you have to be a global administrator. This will hide identifiable information such as user, group and site names in reports and in the template app .

1. In the admin center, go to the **Settings** > **Org Settings**, and under **Services** tab, choose **Reports**.

2. Select **Reports**, and then choose to **Display anonymous identifiers**. This setting gets applied both to the usage reports as well as to the template app.
3. Select **Save changes**.

Related content

[About usage analytics](#) (article)

[Get the latest version of usage analytics](#) (article)

[Navigate and utilize the reports in Microsoft 365 usage analytics](#) (article)

Get the latest version of Microsoft 365 usage analytics

4/3/2021 • 2 minutes to read • [Edit Online](#)

The template app may be refreshed with new data or new visualizations several times per year. Your existing instance will continue to work, but if you would like to get the latest version, a new instance must be created and any customizations must be applied to the new instance. See [Enable Microsoft 365 usage analytics](#).

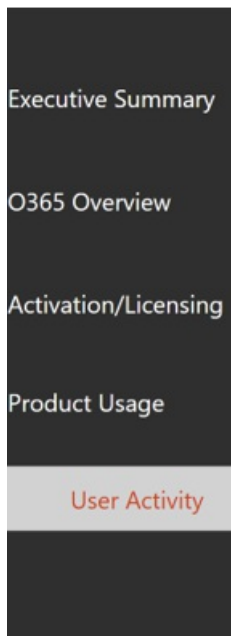
Navigate and utilize the reports in Microsoft 365 usage analytics

4/3/2021 • 2 minutes to read • [Edit Online](#)

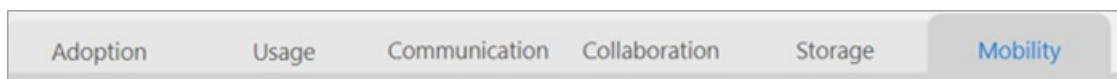
The dashboard provides you with a quick overview of the main usage and adoption metrics. By selecting the top-level metrics, you can access reports that provide more details and insights. Each report tab contains data visualizations specific to an aspect of usage and adoption for your organization. The data collected is explained in the title of each report and a tile appears that contains further information about the visualizations on the report tab that you are viewing.

To get started with your reports, here are some tips:

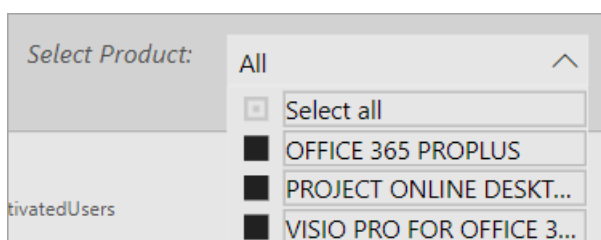
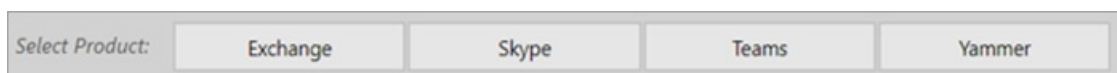
- Use the navigation tabs on the left or on a related metric on the **Executive Summary** page to navigate to each top-level report.



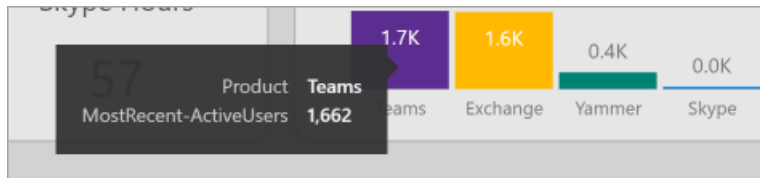
- Use the navigation tabs at the top of each top-level report to navigate to different reports within that level.



- Many reports contain a slicer where you can filter on the product, AAD attribute, or activity that you want to view. These can be either single-select or multi-select.

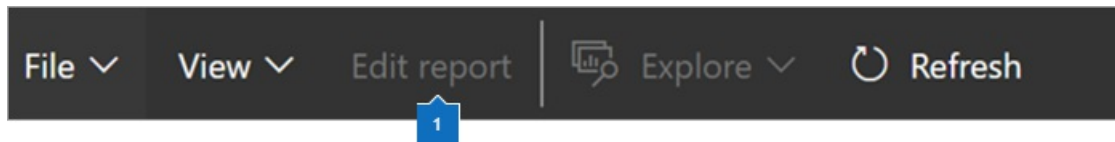


- Hover over data points to view a callout that contains details.




The user who has instantiated the template app will have the ability to customize the report to their needs. To customize the template app:

- Select **Edit report** at the top of the report.



- Create your own visuals by using the underlying [datasets](#).
- Use PowerBI Desktop to bring in your own data sources.

To share your reports, just select the share button  at the top of the page.

To learn how to customize the reports, see [Customizing the reports in Microsoft 365 usage analytics](#).

You can find lots of additional information in the Power BI help documentation:

- [Power BI basic concepts](#)

Learn about dashboard, datasets, reports, and other Power BI concepts.

- [Get started with Power BI](#)

Learn the basic functionality in Power BI. Find links to how to use Power BI Desktop.

- [Share dashboards and reports](#)

Learn how to share reports with your colleagues or people outside your organization. You can also share the report or a filtered version of the report.

Active user in Microsoft 365 usage reports

4/3/2021 • 2 minutes to read • [Edit Online](#)

Active user in usage reports

An active user of Microsoft 365 products for [Microsoft 365 usage analytics](#) and the [Activity Reports in the admin center](#) is defined as follows.

PRODUCT	DEFINITION OF AN ACTIVE USER	NOTES
Exchange Online	Any user who has performed any of the following actions: Mark as read, send messages, create appointments, send meeting requests, accept (as tentative) or decline meeting requests, cancel meetings.	No calendar information is represented, this will be added in an upcoming update.
SharePoint Online	Any user who has interacted with a file by creating, modifying, viewing, deleting, sharing internally or externally, or synchronizing to clients on any site or viewed a page on any site.	The active user metric for SharePoint Online in the Microsoft 365 Usage Analytics template app only reflect users who did file activity against a SharePoint Team site or a Group site. The template app will be updated to synchronize the definition to the same as that on the usage reports in the admin center.
OneDrive for Business	Any user who has interacted with a file by creating, modifying, viewing, deleting, sharing internally or externally, or synchronizing to clients.	
Yammer	Any user who has read, posted, or liked a message on Yammer.	
Skype for Business	Any user who has participated in a peer-to-peer session (including instant messaging, audio and video calls, application sharing, and file transfers) or who has organized or participated in a conference.	
Office	Any user who has activated their Microsoft 365 Pro Plus, Visio Pro or Project Pro subscription on at least one device.	
Microsoft 365 Groups	Any group member that has mailbox activity (if a message has been sent to the group)	This definition will be enhanced with group site file activity and Yammer group activity (file activity on group site and message posted to Yammer group associated with the group.) This data is currently not available in the Microsoft 365 Usage Analytics template app

PRODUCT	DEFINITION OF AN ACTIVE USER	NOTES
Microsoft Teams	Any user who has participated in chat messages, private chat messages, calls, meetings or other activity. Other activity is defined as the number of other team activities by the user some of which include, and not limited to: liking messages, apps, working on files, searching, following teams and channel and favoriting them.	

Adoption Metrics

[Microsoft 365 usage analytics](#) contains additional adoption metrics related to active users to show adoption of the products over time. These metrics are valid for the month, year, and product selected and are defined as follows.

METRIC	DESCRIPTION
EnabledUsers	Number of users enabled to use the product in the month.
ActiveUsers	Number of users active in the month.
MoMReturningUsers	Number of users active in the month that were also active in the preceding month.
FirstTimeUsers	Number of users active in the month that had never used the service before.
CumulativeActiveUsers	Number of users active in the month plus any preceding month.
ActiveUsers(%)	Percent of users, rounded to the nearest tenth, active in the month compared to the number of users enabled in that month.
MoMReturningUsers(%)	Percent of users, rounded to the nearest tenth, active in the month that were also active in the preceding month compared to the number of active users.

MoMReturningUsers, FirstTimeUsers, & CumulativeActiveUsers were reset starting January 1st 2018 with the inclusion of Microsoft Teams.

Customize the reports in Microsoft 365 usage analytics

7/2/2021 • 4 minutes to read • [Edit Online](#)

Microsoft 365 usage analytics provides a dashboard in Power BI that offers insights into how users adopt and use Microsoft 365. The dashboard is just a starting point to interact with the usage data. The reports can be customized for more personalized insights.


You can also use the Power BI desktop to further customize your reports by connecting them to other data sources to gain richer insights about your business.

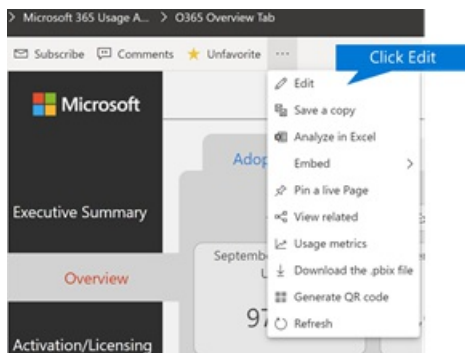
Customizing reports in the browser

The following two examples show how to modify an existing visual and how to create a new visual.

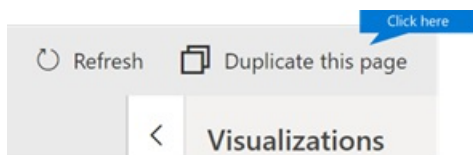
Modify an existing visual

This example shows how to modify the **Activation** tab within the **Activation/Licensing** report.

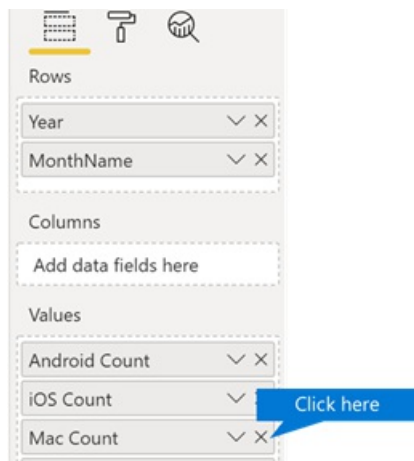
1. Within the **Activation/Licensing** report, select the **Activation** tab.
2. Enter the edit mode by choosing the **Edit** button on the top through the  button.



3. On the top right, choose **Duplicate this page**.





4. In the bottom right, choose any of the bar-charts showing the count of users activating based on the OS such as Android, iOS, Mac, etc.
5. In the **Visualizations** area to the right, in order to remove **Mac Count** from the visual, select the X next to it.



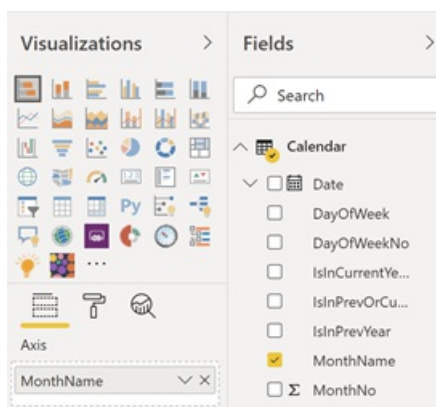
Create a new visual

The following example shows how to create a new visual to track new Yammer users on monthly basis.

1. Go to the **Product Usage** report using the left nav and select the **Yammer** tab.
2. Switch to edit mode by choosing  and **Edit**.
3. At the bottom of the page, select the  to create a new page.
4. In the **Visualizations** area to the right, choose the **Stacked bar chart** (top row, first from left).



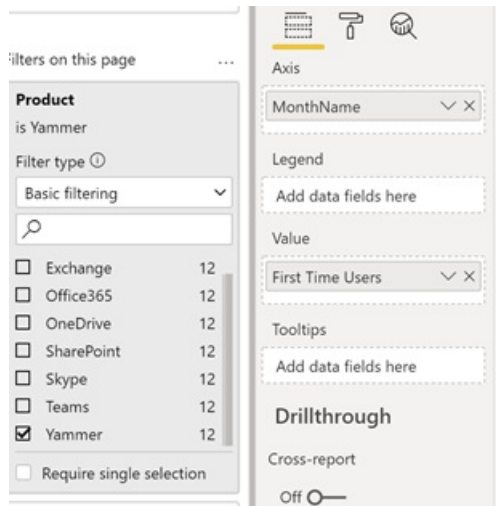
5. Select the bottom right of that visualization and drag to make it larger.
6. In the **Fields** area to the right, expand the **Calendar** table.
7. Drag **MonthName** to the fields area, directly below the **Axis** heading in the **Visualizations** area.



8. In the **Fields** area to the right, expand the **TenantProductUsage** table.
9. Drag **FirstTimeUsers** to the fields area, directly below the **Value** heading.

10. Drag **Product** to the **Filters** area, directly below the **Visual level filters** heading.

11. In the **Filter Type** area that appears, select the **Yammer** check box.



12. Just below the list of visualizations, choose the **Format** icon .

13. Expand Title and change the **Title Text** value to **First-Time Yammer Users by Month**.

14. Change the **Text Size** value to **12**.

15. Change the title of the new page by editing the name of the page on bottom right.

16. Save out the report by Clicking on **Reading View** on top and then **Save**.

Customizing the reports in Power BI Desktop

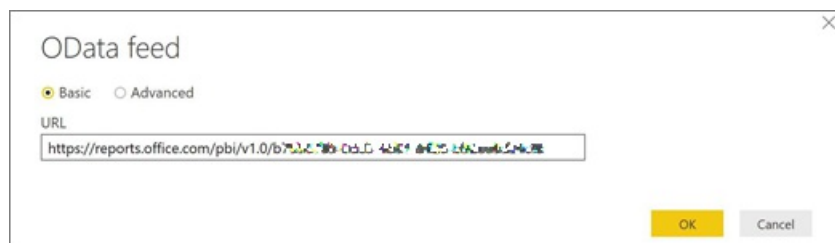
For most customers modifying the reports and chart visuals in Power BI web will be sufficient. For some however, there may be a need to join this data with other data sources to gain richer insights contextual to their own business, in which case they can customize and build additional reports using Power BI Desktop. You can download [Power BI Desktop](#) for free.

Use the reporting APIs

You can start by connecting directly to the ODATA reporting APIs from Microsoft 365 that power these reports.

1. Go to **get data > Other > ODATA Feed > Connect**.
2. In the URL window enter "https://reports.office.com/pbi/v1.0/<tenantid>"

NOTE: The reporting APIs are in preview and are subject to change until they go into production.



3. Enter your Microsoft 365 (organization or school) admin credentials to authenticate to Microsoft 365 when prompted.

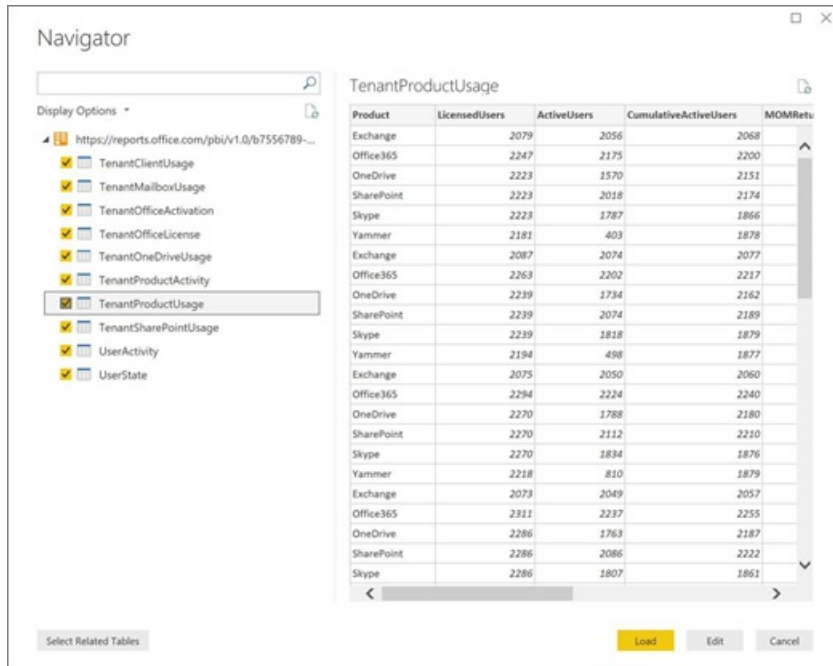
See the [FAQ](#) for more information about who is allowed to access the Microsoft 365 Adoption template app reports.

4. Once the connection is authorized, you will see the Navigator window that shows the datasets available

to connect to.

Select all and choose **Load**.

This will download the data into your Power BI Desktop. Save this file and then you can start creating the reports you need.

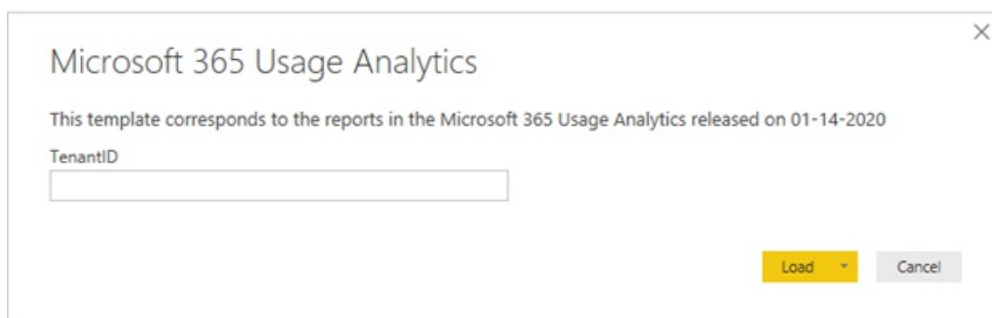


Use the Microsoft 365 usage analytics template

You can also use the Power BI template file that corresponds to the Microsoft 365 usage analytics reports as a starting point to connect to the data. The advantage of using the pbix file is that it has the connection string already established. You can also take advantage of all the custom measures that are created, on top of the data that the base schema returns and build on it further.

You can download the Power BI template file from the [Microsoft Download Center](#). After you download the Power BI template file, follow these steps to get started:

1. Open the pbix file.
2. Enter your tenant id value in the dialog.



3. Enter your admin credentials to authenticate to Microsoft 365 when prompted.

for more information about who is allowed to access the Microsoft 365 usage analytics reports.

Once authorized, the data will be refreshed in the Power BI file.

Data load may take some time, once complete, you can save the file as a .pbix file and continue to customize the reports or bring an additional data source into this report.

4. Follow [Getting started with Power BI](#) documentation to understand how to build reports, publish them to

the Power BI service, and share with your organization. Following this path for customization and sharing may require additional Power BI licenses. See Power BI [licensing guidance](#) for details.

Connect to Microsoft 365 Government Community Cloud (GCC) data with Usage Analytics

8/4/2021 • 2 minutes to read • [Edit Online](#)

Use the following procedures to connect to your data with the Microsoft 365 Usage Analytics report in a Microsoft 365 Government Community Cloud (GCC) tenant.

NOTE

These instructions are specifically for Microsoft 365 GCC tenants.

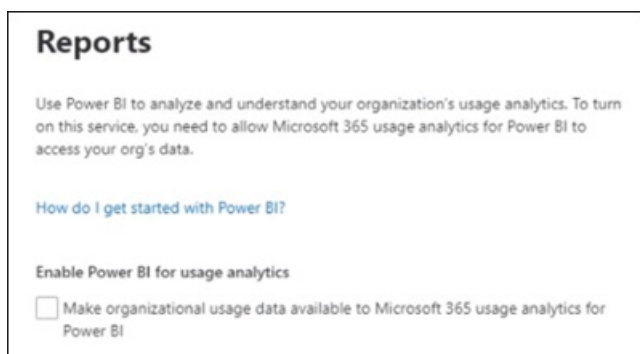
Before you begin

To initially configure Microsoft 365 Usage Analytics:

- You need to be a Microsoft 365 Global admin to enable data collection.
- You need the [Power BI Desktop](#) application to use the template file.
- You need a [Power BI Pro license](#) or Premium capacity to publish and view the report.

Step 1: Make you organization's data available for the Microsoft 365 Usage Analytics report

1. In the Microsoft 365 admin center, expand the navigation menu, select **Reports**, then select **Usage**.
2. On the **Usage Reports** page, in the Microsoft 365 Usage Analytics section, select **Get Started**.
3. Under **Enable Power BI for usage analytics**, select **Make organizational usage data available to Microsoft usage analytics for Power BI**, and then select **Save**.



This will start a process to make your organizations data accessible for this report, and you will see a message stating that **We're getting your data ready for Microsoft 365 usage analytics**. Note that this process can take 24 hours to complete.

4. When your organizations data is ready, refreshing the page will show a message stating that your data is now available, and will also provide your **tenant ID** number. You will need to use the tenant ID in a later step when you attempt to connect to your tenant data.

Microsoft 365 usage analytics

Get the most from your subscription. Analyze and explore usage data in Power BI.

[How do I use Microsoft 365 usage analytics?](#)

✔ Your data is now available. Use tenant ID 477798de-ea8d-475e-8dab-8d7448ded0a2 in Power BI to instantiate Microsoft 365 usage analytics. Please choose "oAuth2" as your authentication method. ✕

[Go to Power BI](#)

IMPORTANT

When your data is available, do not select **Go to Power BI**, which will take you to the Power BI Marketplace. The template app for this report required by GCC tenants is not available in the Power BI Marketplace.

Step 2: Download the Power BI template, connect to your data, and publish the report

Microsoft 365 GCC users can download and use the Microsoft 365 Usage Analytics report template file to connect to their data. You will need Power BI Desktop to open and use the template file.

NOTE

Currently, a template app for the Microsoft 365 Usage Analytics report is not available for GCC tenants in the Power BI Marketplace.

1. After downloading the [Power BI template](#), open it using Power BI Desktop.
2. When prompted for a **TenantID**, enter the tenant ID you received when you prepared your organization's data for this report in step 1. Then select **Load**. It will take several minutes for your data to load.

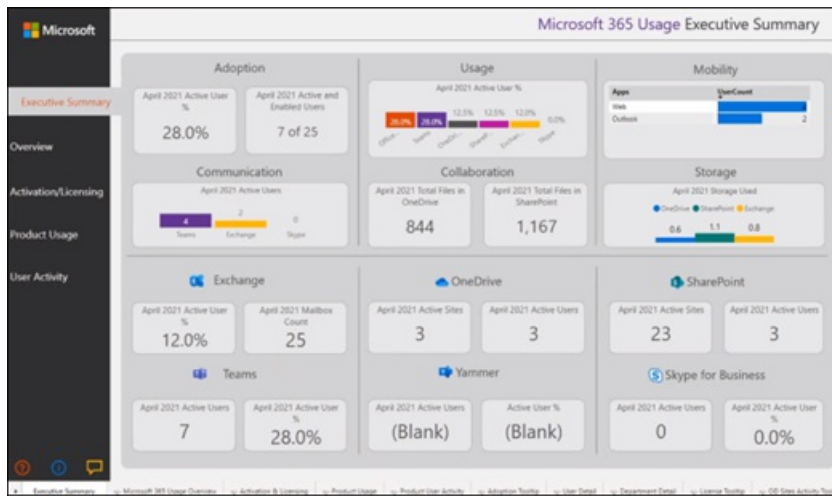
Microsoft 365 Usage Analytics

This template corresponds to the reports in the Microsoft 365 Usage Analytics released on 02-13-2021

TenantID

[Load](#) [Cancel](#)

3. When loading completes, your report will display, and you will see an executive summary of your data.



4. Save your changes to the report.
5. Select **Publish** in the Power BI Desktop menu to publish the report to the Power BI Online service where it can be viewed. This requires either a Power BI Pro license or Power BI Premium capacity. As part of the [publish process](#), you will need to select a destination to publish to an available workspace in the Power BI Online Service.

Related content

[About usage analytics](#)

[Get the latest version of usage analytics](#)

[Navigate and utilize the reports in Microsoft 365 usage analytics](#)

Microsoft 365 usage analytics data model

4/3/2021 • 18 minutes to read • [Edit Online](#)

Data for the Microsoft 365 usage analytics tables

Microsoft 365 usage analytics connects to an API that exposes a multidimensional data model. The APIs that Microsoft 365 usage analytics uses to generate its data are from the various, generally-available, Graph APIs. The function of the Microsoft 365 usage analytics API by itself is not generally available.

NOTE

For more information, see [Working with Microsoft 365 usage reports in Microsoft Graph](#).

This API provides information about the monthly trend of usage of the various Microsoft 365 services. For the exact data returned by the API refer to the table in the following section.

Data tables returned by the Microsoft 365 Reporting API

TABLE NAME	INFORMATION IN THE TABLE	DATE RANGE
Tenant Product Usage	Contains monthly totals of enabled, active users, month-over-month retained users, first-time users, and the cumulative active users.	Contains monthly aggregated data for a rolling 12-month period including the current partial month.
Tenant Product Activity	Contains monthly totals of activities and active user count for various activities within the products. See active user definition for information about the activities within a product that are returned in this data table.	Contains monthly aggregated data for a rolling 12-month period including the current partial month.
Tenant Office Licenses	Contains data about number of Microsoft Office subscriptions assigned to users	Contains end-of-month state data for a rolling 12-month period including the current partial month.
Tenant Mailbox Usage	Contains data about the user's mailbox, for total mailbox count and how storage is used.	Contains end-of-month state data for a rolling 12-month period including the current partial month.
Tenant Client Usage	Contains data about the number of users actively using specific client/devices to connect to Exchange Online, Skype for Business and Yammer.	Contains monthly aggregated data for a rolling 12-month period including the current partial month.
Tenant SharePoint Online Usage	Contains data about the SharePoint sites, covering Team or Groups sites such as total number of sites, number of documents on site, file count by activity type and storage used.	Contains end-of-month state data for a rolling 12-month period including the current partial month.

TABLE NAME	INFORMATION IN THE TABLE	DATE RANGE
Tenant OneDrive for Business Usage	Contains data about the OneDrive accounts such as number of accounts, number of documents across OneDrives, storage used, file count by activity type.	Contains end-of-month state data for a rolling 12-month period including the current partial month.
Tenant Microsoft 365 Groups Usage	Contains data about Microsoft 365 Groups usage including Mailbox, SharePoint, and Yammer.	Contains end-of-month state data for a rolling 12-month period including the current partial month.
Tenant Office Activation	Contains data about number of Office subscription activations, count of activation per device (Android/iOS/Mac/PC), activations by service plan, for example, Microsoft 365 Apps for enterprise, Visio, Project.	Contains end-of-month state data for a rolling 12-month period including the current partial month.
User State	Contains metadata about users, including user display name, products assigned, location, department, title, company. This data is about users who were assigned a license during the last complete month. Every user is uniquely represented by a user ID.	This data is about users that had a license assigned during the last complete month.
User Activity	Contains per-user level information about activity performed by licensed users. See active user definition for information about the activities within a product that are returned in this data table.	This data is about users that performed an activity in any of the services during the last complete month.

Expand the following sections to see the detailed information for each data table.

Data table - User State

This table provides user level details for all users that have a license assigned to them during the last complete month. It brings in data from the Azure Active Directory.

COLUMN NAME	COLUMN DESCRIPTION
UserId	Unique user ID that represents a user and enables joining with other data tables within the data set.
Timeframe	Month value for which this table has data for.
UPN	User principal name, uniquely identifies the user to be able to join with other external data sources.
DisplayName	User's display name.
IDType	ID type is set to 1 if the user is a Yammer user who connects by using their Yammer ID or 0 if they connect to Yammer by using their Microsoft 365 ID. Value is 1 to represent that this user connects to Yammer with their Yammer ID and not their Microsoft 365 ID

COLUMN NAME	COLUMN DESCRIPTION
HasLicenseEXO	Set to true if user is assigned a license and enabled to use Exchange.
HasLicenseODB	Set to true if user is assigned a license and enabled to use OneDrive for Business.
HasLicenseSPO	Set to true if user is assigned a license and enabled to use SharePoint Online.
HasLicenseYAM	Set to true if user is assigned a license and enabled to use Yammer.
HasLicenseSFB	Set to true if user is assigned a license and enabled to use Skype For Business.
HasLicenseTeams	Set to true if user is assigned a license and enable to use Microsoft Teams.
Company	Company data represented in Azure Active Directory for this user.
Department	Department data represented in Azure Active Directory for this user.
LocationCity	City data represented in Azure Active Directory for this user.
LocationCountry	Country data represented in Azure Active Directory for this user.
LocationState	State data represented in Azure Active Directory for this user.
LocationOffice	User's office.
Title	Title data represented in Azure Active Directory for this user.
Deleted	True if the user has been deleted from Microsoft 365 in that last complete month.
DeletedDate	Date when the user was deleted from Microsoft 365.
YAM_State	States of the user in the Yammer system, can be active, deleted, or suspended.
YAM_ActivationDate	Date the user entered the state of being active in Yammer.
YAM_DeletionDate	Date the user entered the state of being deleted in Yammer.
YAM_SuspensionDate	Date the user entered the state of being suspended in Yammer.

Data table - User Activity

This table contains data about each user who had an activity in any of the services in the previous month.

COLUMN NAME	COLUMN DESCRIPTION
UserID	Unique user ID that represents a user and enables joining with other data tables within the data set.
IDType	ID type is set to 1 if the user is a Yammer user who connects by using their Yammer ID or 0 if they connect to Yammer by using their Microsoft 365 ID. Value is 1 to represent that this user connects to Yammer with their Yammer ID and not their Microsoft 365 ID
Timeframe	Month value for which this table represents data for.
EXO_EmailSent	Number of emails sent.
EXO_EmailReceived	Number of emails received.
EXO_EmailRead	Number of emails read activity the user performed, it could be multiple times reading an already read email, or an email received previously.
EXO_AppointmentCreated	Number of appointments created.
EXO_MeetingAccepted	Number of meetings accepted.
EXO_MeetingCancelled	Number of meetings canceled.
EXO_MeetingDeclined	Number of meetings declined.
EXO_MeetingSent	Number of meetings sent.
ODB_FileViewedModified	Number of files this user interacted with on any OneDrive for Business (for example, created, updated, deleted, viewed, or downloaded).
ODB_FileSynched	Number of files this user synchronized on any OneDrive for Business.
ODB_FileSharedInternally	Number of files this user shared internally from any OneDrive for Business, or with users within groups (that might include external users).
ODB_FileSharedExternally	Number of files this user shared externally from any OneDrive for Business.
ODB_AccessByOwner	Number of files the user interacted with that reside on their own OneDrive for Business.
ODB_AccessOthers	Number of files this user interacted with which reside on another user's OneDrive for Business.
SPO_GroupFileViewedModified	Number of files with this user interacted on any group site.
SPO_GroupFileSynched	Number of files this user synchronized on any group site.

COLUMN NAME	COLUMN DESCRIPTION
SPO_GroupFileSharedInternally	The count of files that have been shared with users within the organization, or with users within groups (that might include external users).
SPO_GroupFileSharedExternally	Number of files this user shared externally from any group site.
SPO_GroupAccessByOwner	Number of files the user interacted with that reside on a group site that they own.
SPO_GroupAccessByOthers	Number of files the user interacted with that reside on a group site that another user owns.
SPO_OtherFileViewedModified	Number of files with which this user interacted on any other site.
SPO_OtherFileSynched	Number of files this user synchronized from any other site.
SPO_OtherFileSharedInternally	Number of files this user shared internally from any other site, or with users within groups (that might include external users).
SPO_OtherFileSharedExternally	Number of files this user shared externally from any other site.
SPO_OtherAccessedByOwner	Number of sites the user interacted with that reside on other site that they own.
SPO_OtherAccessedByOthers	Number of sites the user interacted with that reside on other site that another user owns.
SPO_TeamFileViewedModified	Number of files with which this user interacted on any team site.
SPO_TeamFileSynched	Number of files this user synchronized from any team site.
SPO_TeamFileSharedInternally	Number of files this user shared internally from any team site, or with users within groups (that might include external users).
SPO_TeamFileSharedExternally	Number of files this user shared externally from any team site.
SPO_TeamAccessByOwner	Number of files the user interacted with that reside on a team site that they own.
SPO_TeamAccessByOthers	Number of files the user interacted with that reside on a team site that another user owns.
Teams_ChatMessages	Number of chat messages sent.
Teams_ChannelMessage	Number of messages posted to channels.

COLUMN NAME	COLUMN DESCRIPTION
Teams_CallParticipate	Number of calls the user participated in.
Teams_MeetingParticipate	Number of meetings the user joined.
Teams_HasOtherAction	Boolean value if the user performed other actions in Microsoft Teams.
YAM_MessagePost	Number of Yammer messages this user posted.
YAM_MessageLiked	Number of Yammer messages this user liked.
YAM_MessageRead	Number of Yammer messages this user read.
SFB_P2PSummary	Number of peer-to-peer sessions this user took part in.
SFB_ConfOrgSummary	Number of conference sessions this user organized.
SFB_ConfPartSummary	Number of conference sessions this user participated in.

NOTE

Teams_HasOtherAction means user is considered active but has a zero value for the Chat Messages, 1:1 calls, Channel Messages, Total Meetings, and Meetings organized.

Data table - Tenant Product Usage

This table provides month-over-month adoption data in terms of enable, active, returning, and first-time users for each product within Microsoft 365. The Microsoft 365 values represent active usage in either of the products.

COLUMN NAME	COLUMN DESCRIPTION
Product	Name of products for which the usage information is summarized. Microsoft 365 value in the product column represents activity across any of the products
Timeframe	Month value. There will be one row per product per month for the last 12 months including the current partial month.
EnabledUsers	Number of users enabled to use the product for the time-frame value, if a user was enabled for portion of the month, they are still counted.
ActiveUsers	Number of users who performed an intentional activity in the product for the time-frame value. A user is counted as active for a product in a particular month, if they have performed one of the key activities in the product. The key activities are available in the Tenant Product Activity table.
CumulativeActiveUsers	Number of users who are enabled to use a product and have used the product up to the timeframe month at least once since data collection started in the new usage system.

COLUMN NAME	COLUMN DESCRIPTION
MoMReturningUsers	Number of users who are active in the timeframe month and also were active in the previous month.
FirstTimeUsers	Number of users who became active in the timeframe for the first time since data collection in the new usage system. A user is counted as a first-time user in a particular month, if we detect their activity for the first time since the beginning of data collection in this new reporting system. Once counted as a first-time user, even if this user has a large gap in their activity they will never be counted again as a first-time user
Content Date	If timeframe shows current month, this value will represent the latest date of the current month for which data is available. If Timeframe shows previous month, this value will represent the last date of the timeframe month.

Data table - Tenant Product Activity

This table provides monthly totals of activity and active user count for various activities within the products.

COLUMN NAME	COLUMN DESCRIPTION
Timeframe	Month value. There will be one row per product per month for the last 12 months including the current partial month.
Product	Name of the product within Microsoft 365 for which usage data is available.
Activity	Name of the activity in a product that is used to showcase active use of product.
ActivityCount	This is the total number of actions counted for each activity performed within the product across all active users. Note: For SharePoint Online and OneDrive for Business activities, this value represents the number of distinct documents with which users interacted with.
ActiveUserCount	Number of users who performed the activity within the product.
TotalDurationInMinute	Amount of duration in minutes across all active users who used audio or video session in an applicable Skype for Business activity.
Content Date	If timeframe shows current month, this value will represent the latest date of the current month for which data is available. If Timeframe shows previous month, this value will represent the last date of the timeframe month.

Data table - Tenant Mailbox Usage

This table consists of summary data across all licensed Exchange Online users who have a user mailbox. It contains end of month state across all user mailboxes. The data in this table is not additive across multiple months. Latest month's data in this table represents the most recent state.

COLUMN NAME	COLUMN DESCRIPTION
TotalMailboxes	Number of user mailboxes for Microsoft 365 subscription.
IssueWarningQuota	Total quota for issuing warning across all users' mailboxes.
ProhibitSendQuota	Total quota for prohibit send across all user mailboxes.
ProhibitSendReceiveQuota	Total quota for prohibit send receive quota across all user mailboxes.
TotalItemBytes	Amount of storage used across all user mailboxes in bytes.
MailboxesNoWarning	Number of user mailboxes that were under the storage warning limit.
MailboxesIssueWarning	Number of user mailboxes that were issued a warning for storage quota.
MailboxesExceedSendQuota	Number of user mailboxes that have exceeded the send quota.
MailboxesExceedSendReceiveQuota	Number of user mailboxes that have exceeded the send/receive quota.
DeletedMailboxes	Number of users mailboxes deleted in the timeframe.
Timeframe	Month value.
Content Date	If timeframe shows current month, this value will represent the latest date of the current month for which data is available. If Timeframe shows previous month, this value will represent the last date of the timeframe month.

Data table - Tenant Client Usage

This table provides month-over-month summary data about the clients that the users are using to connect to Exchange Online, Skype for Business and Yammer. This table does not yet have client use data for SharePoint Online and OneDrive for Business.

COLUMN NAME	COLUMN DESCRIPTION
Product	Name of the product within Microsoft 365 for which client usage data is available.
ClientId	Name of each device used to connect to product.
UserCount	Number of users that used each of the clients for each product.
Timeframe	Month value

COLUMN NAME	COLUMN DESCRIPTION
Content Date	If timeframe shows current month, this value will represent the latest date of the current month for which data is available. If Timeframe shows previous month, this value will represent the last date of the timeframe month.

Data table - Tenant SharePoint Online Usage

This table consists of month over month summary data about the usage or activity of SharePoint Online sites. This only covers Team Sites and Group sites. The end of month state of SharePoint Online sites is represented in this column, for example, if a user created a five documents and used 10 MB for total storage, and then deleted some files, and added more files so that at the end of month state for files is seven total that use five MB of storage, the value of represented in this table is end of month state. This table is hidden to avoid duplicate count of aggregations and is used as a source to create two reference tables.

COLUMN NAME	COLUMN DESCRIPTION
SiteType	Site type value (any/team/group) (any represents either of these 2 sites types).
TotalSites	Number of sites that existed at the end of the timeframe.
DocumentCount	Total number of documents that existed on the site at the end of the timeframe.
Diplansed	Total storage used summed across all sites at the end of the timeframe.
ActivityType	Number of sites that recorded the various types of file activity (any/active files/ files shared EXT/INT/files synched). Represents any of the file activity that was performed.
SitesWithOwnerActivities	Number of active sites, where the site owner performed a particular file activity on their own sites. You can get the site owner from the PowerShell command get-sposite . This is the person who is responsible for the site.
SitesWithNonOwnerActivities	Number of active sites summed up for the month, where the users other than the site owner performed a particular file activity on sites. You can get the site owner from the PowerShell command get-sposite . This is the person who is responsible for the site.
ActivityTotalSites	Number of sites that recorded any activity during the timeframe. If a site that had activity earlier in the timeframe, and was deleted by the end of the timeframe, it would still be counted in the active site total for that timeframe.
Timeframe	This column has the date value. Used as Many to one relationship for Calendar table.

COLUMN NAME	COLUMN DESCRIPTION
Content Date	If timeframe shows current month, this value will represent the latest date of the current month for which data is available. If Timeframe shows previous month, this value will represent the last date of the timeframe month.

Data table - Tenant OneDrive Usage

This table provides data about the OneDrive accounts such as number of accounts, number of documents across OneDrive accounts, storage used, file count by activity type. The end of month state of OneDrive for Business accounts is represented in this table. For example, if a user created a Five documents that used 10 MB of storage, and then deleted a few and added more files so that at the end of month they have seven files that use Five MB of storage, then the end of the month value is represented in this table at the end of the month.

COLUMN NAME	COLUMN DESCRIPTION
SiteType	Value is "OneDrive".
TotalSites	Number of OneDrive for Business accounts that existed at the end of the timeframe.
DocumentCount	Total number of documents that existed across all OneDrive for Business accounts at the end of the timeframe
Diplansed	Total storage used summed across all OneDrive account at the end of the timeframe.
ActivityType	Number of accounts that recorded the various types of file activity (any/active files/ files shared EXT/INT/files synched). Any represents any of the file activity was performed
SitesWithOwnerActivities	Number of active OneDrive for Business accounts, where the account owner performed a particular file activity on their own account.
SitesWithNonOwnerActivities	Count of OneDrive for Business accounts where file activity was performed by users other than the owner of the account.
ActivityTotalSites	Number of OneDrive for Business accounts that recorded any activity during the timeframe. If a OneDrive for Business account had activity earlier in the timeframe, and was deleted by the end of the timeframe, it would still be counted in the active OneDrive for Business account for that timeframe.
Timeframe	This column has the date value. Used as Many to one relationship for Calendar table.
Content Date	If timeframe shows current month, this value will represent the latest date of the current month for which data is available. If Timeframe shows previous month, this value will represent the last date of the timeframe month.

Data table - Tenant Microsoft 365 Groups Usage

This table provides data about how Microsoft 365 Groups is used across the organization.

COLUMN NAME	COLUMN DESCRIPTION
TimeFrame	Month value. There will be one row per product per month for the last 12 months including the current partial month.
GroupType	Type of group (private/public/any).
TotalGroups	Number of groups in each group type.
ActiveGroups	Number of active groups.
MBX_TotalGroups	Number of mailbox groups.
MBX_ActiveGroups	Number of active mailbox groups.
MBX_TotalActivities	Number of mailbox activities.
MBX_TotalItems	Number of mailbox items.
MBX_StorageUsed	Quantity of mailbox storage used.
SPO_TotalGroups	Number of SharePoint groups.
SPO_ActiveGroups	Number of active SharePoint groups.
SPO_FileAccessedActiveGroups	Number of SharePoint groups that have file accessed activities.
SPO_FileSyncedActiveGroups	Number of SharePoint groups that have file synchronized activities.
SPO_FileSharedInternallyActiveGroups	Number of SharePoint groups that have shared activities internally, or with groups (that might include external users).
SPO_FileSharedExternallyActiveGroups	Number of SharePoint groups which have shared externally activities.
SPO_TotalActivities	Number of SharePoint activities.
SPO_FileAccessedActivities	Number of SharePoint file accessed activities.
SPO_FileSyncedActivities	Number of SharePoint file synchronized activities.
SPO_FileSharedInternallyActivities	Number of SharePoint file shared activities internally, or with groups (that might include external members).
SPO_FileSharedExternallyActivities	Number of SharePoint file shared externally activities.
SPO_TotalFiles	Number of SharePoint files.
SPO_ActiveFiles	Number of active SharePoint files.

COLUMN NAME	COLUMN DESCRIPTION
SPO_StorageUsed	Quantity of SharePoint storage used.
YAM_TotalGroups	Number of Yammer groups.
YAM_ActiveGroups	Number of active Yammer groups.
YAM_LikedActiveGroups	Number of Yammer groups which have like activities.
YAM_PostedActiveGroups	Number of Yammer groups which have post activities.
YAM_ReadActiveGroups	Number of Yammer groups which have read activities.
YAM_TotalActivities	Number of Yammer activities.
YAM_LikedActivities	Number of Yammer like activities.
YAM_PostedActivities	Number of Yammer post activities.
YAM_ReadActivites	Number of Yammer read activities.

Data table - Tenant Office Activation

The table provides data about the number of Office subscription activations across the service plans, for example, Microsoft 365 Apps for enterprises, Visio, Project. It also provides data about number of activations per device (Android/iOS/Mac/PC).

COLUMN NAME	COLUMN DESCRIPTION
ServicePlanName	List of the service plan name values and counts of activations by devices, as depicted by below columns.
TotalEnabled	Number of users enabled per service plan name by the end of the timeframe.
TotalActivatedUsers	Number of users that have activated each service plan t by the end of the timeframe.
AndroidCount	Number of activations per service plan for Android device by the end of the timeframe.
iOSCount	Number of activations per service plan for iOS device by the end of the timeframe.
MacCount	Number of activations per service plan for MAC device by the end of the timeframe.
PcCount	Number of activations per service plan for PC device by the end of the timeframe.
WinRtCount	Number of activations per service plan for Windows Mobile device by the end of the timeframe.

COLUMN NAME	COLUMN DESCRIPTION
Timeframe	This column has the date value. Used as Many to one relationship for Calendar table.
Content Date	If timeframe shows current month, this value will represent the latest date of the current month for which data is available. If Timeframe shows previous month, this value will represent the last date of the timeframe month.

Troubleshooting Microsoft 365 usage analytics

5/7/2021 • 4 minutes to read • [Edit Online](#)

Explore the following list of error messages to get help with the most common issues with Microsoft 365 usage analytics.

We are unable to process your request. You have to first subscribe to this data from the Microsoft 365 admin center

Error Code: 422

Where you will see this message: In Power BI when you are connecting to the Microsoft 365 Usage Analytics template app or when directly calling the Microsoft 365 Reporting APIs.

Cause: Before you can connect to the app, you have to subscribe to the data from the Microsoft 365 admin center. If this step isn't done first, you won't be able to connect to the template app, even if you provide your Microsoft 365 tenant ID.

To fix this error: To subscribe to the data, go to the admin center > **Reports** > **Usage** and locate the Microsoft 365 usage analytics tile on the main dashboard page. Select the **Get started** button and then in the **Reports** pane that opens, turn the **Make data available to Microsoft 365 usage analytics for Power BI** setting on and **Save**.

We are processing your data

Where you will see this message: In the **Microsoft 365 usage analytics** tile on the **Usage** dashboard in the Microsoft 365 admin center.

Cause: When you [opt in to seeing data in the template app](#) from the Microsoft 365 admin center, the Microsoft 365 system starts generating historical usage data for your organization. Depending on the size of your tenant, this step could take anywhere between 2 hours to 48 hours.

To fix this: Just be patient, but if the message does not change to **Your data is ready** after 3 days, [contact Microsoft 365 for business support](#).

We are unable to process your request at this time. We are still preparing the data for your organization

Error Code: 423

Where you will see this message: In Power BI, when you are connecting to the Microsoft 365 Usage Analytics template app or when directly calling the Microsoft 365 Reporting APIs.

Cause: When you [opt in to seeing data in the template app](#) from the admin center, the Microsoft 365 system starts generating historical usage data for your organization. Depending on the size of your tenant, this step could take anywhere between two hours to 48 hours.

To fix this: Just be patient, but if the message does not change to **Your data is ready** even 3 days since initiation, [contact Microsoft 365 for business support](#).

The tenant ID you provided is not in the correct format

Error Code: 400

Where you will see this message: In Power BI, when you are connecting to the Microsoft 365 Usage Analytics template app or when directly calling the Microsoft 365 Reporting APIs.

Cause: The tenant ID is a guid and has to be in the format of xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. If you enter any other string in the tenant input box, you will get this error.

To fix this error: Go to the admin center > **Reports** > [Usage](#) and locate the Microsoft 365 usage analytics tile on the main dashboard page. The tenant ID is listed on the tile. You can copy it from here and paste it in the dialog box for connecting to the template app.

The tenant ID you provided is not recognized by our system

Error Code: 404

Where you will see this message: In Power BI when you are connecting to the Microsoft 365 Usage Analytics template app or when directly calling the Microsoft 365 Reporting APIs.

Cause: The tenant ID you provided is not valid or does not exist.

To fix this error: Go to the admin center > **Reports** > [Usage](#) and locate the Microsoft 365 usage analytics tile on the main dashboard page. The tenant ID is listed on the tile. You can copy it from here and paste it in the dialog box for connecting to the template app.

Please re-enter your credentials to sign in to Power BI again

Error Code: 302

Where you will see this message: In Power BI when you are connecting to the Microsoft 365 Usage Analytics template app or when directly calling the Microsoft 365 Reporting APIs.

Cause: The authorization code failed and may require you to enter your credentials again.

To fix this error: Sign out of Power BI, and then sign in again.

You do not have the right authorization to access to this data. To be able to gain access to the data from this service you need to be either a global admin or any one of the product admins

Error Code: 403

Where you will see this message: In Power BI when you are connecting to the Microsoft 365 Usage Analytics template app or when directly calling the Microsoft 365 Reporting APIs.

Cause: The authorization code failed because the user who tried connecting to the template app does not have the right level of authorization to access this data.

To fix this error: Provide the credentials of a user who is either a **Global admin**, **Exchange admin**, **Skype for Business admin**, **SharePoint admin**, **Global reader** or **Report reader** to connect to the template app. See [About admin roles](#) for more information.

Refresh failed

Where you will see this message: Email from Power BI or failed status in the refresh history.

Cause: Sometimes the credentials of the user who connected to the template app are reset, and not updated in the connection settings of the template app causing the user to see refresh failure errors.

To fix this error: In Power BI, find the dataset corresponding to the Microsoft 365 Usage Analytics template app, select **schedule refresh** and provide your admin credentials.

If that doesn't work, clear the cache, and re-create the template app.

Top 10 ways to secure Microsoft 365 for business plans

7/12/2021 • 14 minutes to read • [Edit Online](#)

If you are a small or medium-size organization using one of Microsoft's business plans and your type of organization is targeted by cyber criminals and hackers, use the guidance in this article to increase the security of your organization. This guidance helps your organization achieve the goals described in the Harvard Kennedy School [Cybersecurity Campaign Handbook](#).

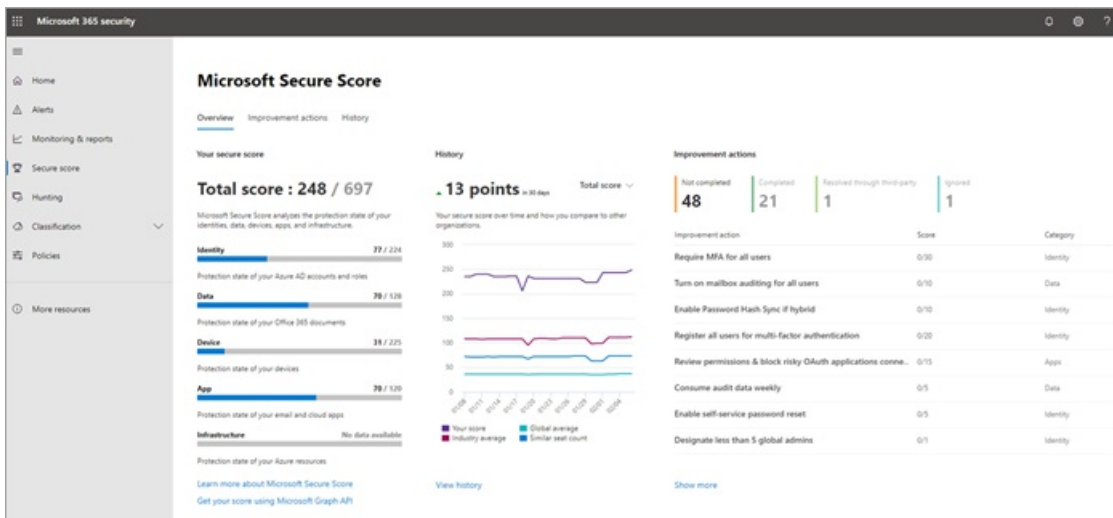
Microsoft recommends that you complete the tasks listed in the following table that apply to your service plan.

NUMBER	TASK	MICROSOFT 365 BUSINESS STANDARD	MICROSOFT 365 BUSINESS PREMIUM
1	Set up multi-factor authentication	✓	✓
2	Train your users	✓	✓
3	Use dedicated admin accounts	✓	✓
4	Raise the level of protection against malware in mail	✓	✓
5	Protect against ransomware	✓	✓
6	Stop auto-forwarding for email	✓	✓
7	Use Office Message Encryption		✓
8	Protect your email from phishing attacks		✓
9	Protect against malicious attachments and files with Safe Attachments		✓
10	Protect against phishing attacks with Safe Links		✓

If you have Microsoft Business Premium, the quickest way to setup security and begin collaborating safely is to follow the guidance in this library: [Microsoft 365 for smaller businesses and campaigns](#). This guidance was developed in partnership with the Microsoft Defending Democracy team to protect all small business customers against cyber threats launched by sophisticated hackers.

Before you begin, check your [Microsoft 365 Secure Score](#) in the Microsoft 365 security center. From a centralized dashboard, you can monitor and improve the security for your Microsoft 365 identities, data, apps,

devices, and infrastructure. You are given points for configuring recommended security features, performing security-related tasks (such as viewing reports), or addressing recommendations with a third-party application or software. With additional insights and more visibility into a broader set of Microsoft products and services, you can feel confident reporting about your organization's security health.



1: Set up multi-factor authentication

Using multi-factor authentication is one of the easiest and most effective ways to increase the security of your organization. It's easier than it sounds - when you log in, multi-factor authentication means you'll type a code from your phone to get access to Microsoft 365. This can prevent hackers from taking over if they know your password. Multi-factor authentication is also called 2-step verification. Individuals can add 2-step verification to most accounts easily, for example, to their Google or Microsoft accounts. Here's how to [add two-step verification to your personal Microsoft account](#).

For businesses using Microsoft 365, add a setting that requires your users to log in using multi-factor authentication. When you make this change, users will be prompted to set up their phone for two-factor authentication next time they log in. To see a training video for how to set up MFA and how users complete the set up, see [set up MFA](#) and [user set up](#).

To set up multi-factor authentication, you turn on Security defaults:

For most organizations, Security defaults offer a good level of additional sign-in security. For more information, see [What are security defaults?](#)

If your subscription is new, Security defaults might already be turned on for you automatically.

You enable or disable security defaults from the **Properties** pane for Azure Active Directory (Azure AD) in the Azure portal.

1. Sign in to the [Microsoft 365 admin center](#) with global admin credentials.
2. In the left nav choose **Show All** and under **Admin centers**, choose **Azure Active Directory**.
3. In the **Azure Active Directory admin center** choose **Azure Active Directory > Properties**.
4. At the bottom of the page, choose **Manage Security defaults**.
5. Choose **Yes** to enable security defaults or **No** to disable security defaults, and then choose **Save**.

After you set up multi-factor authentication for your organization, your users will be required to set up two-step verification on their devices. For more information, see [Set up 2-step verification for Microsoft 365](#).

For full details and complete recommendations, see [Set up multi-factor authentication for users](#).

2: Train your users

The Harvard Kennedy School [Cybersecurity Campaign Handbook](#) provides excellent guidance on establishing a strong culture of security awareness within your organization, including training users to identify phishing attacks.

In addition to this guidance, Microsoft recommends that your users take the actions described in this article: [Protect your account and devices from hackers and malware](#). These actions include:

- Using strong passwords
- Protecting devices
- Enabling security features on Windows 10 and Mac PCs

Microsoft also recommends that users protect their personal email accounts by taking the actions recommended in the following articles:

- [Help protect your Outlook.com email account](#)
- [Protect your Gmail account with 2-step verification](#)

3: Use dedicated admin accounts

The administrative accounts you use to administer your Microsoft 365 environment include elevated privileges. These are valuable targets for hackers and cyber criminals. Use admin accounts only for administration. Admins should have a separate user account for regular, non-administrative use and only use their administrative account when necessary to complete a task associated with their job function. Additional recommendations:

- Be sure admin accounts are also set up for multi-factor authentication.
- Before using admin accounts, close out all unrelated browser sessions and apps, including personal email accounts.
- After completing admin tasks, be sure to log out of the browser session.

4: Raise the level of protection against malware in mail

Your Microsoft 365 environment includes protection against malware, but you can increase this protection by blocking attachments with file types that are commonly used for malware. To bump up malware protection in email, view a [short training video](#), or complete the following steps:

1. Go to <https://protection.office.com> and sign in with your admin account credentials.
2. In the Security & Compliance Center, in the left navigation pane, under **Threat management**, choose **Policy > Anti-Malware**.
3. Double-click the default policy to edit this company-wide policy.
4. Select **Settings**.
5. Under **Common Attachment Types Filter**, select **On**. The file types that are blocked are listed in the window directly below this control. You can add or delete file types later, if needed.
6. Select **Save**.

For more information, see [Anti-malware protection in EOP](#).

5: Protect against ransomware

Ransomware restricts access to data by encrypting files or locking computer screens. It then attempts to extort money from victims by asking for "ransom," usually in form of cryptocurrencies like Bitcoin, in exchange for access to data.

You can protect against ransomware by creating one or more mail flow rules to block file extensions that are commonly used for ransomware, or to warn users who receive these attachments in email. A good starting point is to create two rules:

- Warn users before opening Office file attachments that include macros. Ransomware can be hidden inside macros, so we'll warn users to not open these files from people they do not know.
- Block file types that could contain ransomware or other malicious code. We'll start with a common list of executables (listed in the table below). If your organization uses any of these executable types and you expect these to be sent in email, add these to the previous rule (warn users).

To create a mail transport rule, view a [short training video](#), or complete the following steps:

1. Go to the [Exchange admin center](#).
2. In the **mail flow** category, select **rules**.
3. Select **+**, and then **Create a new rule**.
4. Select ******** at the bottom of the dialog box to see the full set of options.
5. Apply the settings in the following table for each rule. Leave the rest of the settings at the default, unless you want to change these.
6. Select **Save**.

SETTING	WARN USERS BEFORE OPENING ATTACHMENTS OF OFFICE FILES	BLOCK FILE TYPES THAT COULD CONTAIN RANSOMWARE OR OTHER MALICIOUS CODE
Name	Anti-ransomware rule: warn users	Anti-ransomware rule: block file types
Apply this rule if . . .	Any attachment . . . file extension matches . . .	Any attachment . . . file extension matches . . .
Specify words or phrases	Add these file types: dotm, docm, xlsx, sltm, xla, xlam, xll, pptm, potm, ppam, ppsm, sldm	Add these file types: ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh, exe, pif
Do the following . . .	Prepend a disclaimer	Block the message . . . reject the message and include an explanation
Provide message text	Do not open these types of files— unless you were expecting them— because the files may contain malicious code and knowing the sender isn't a guarantee of safety.	

TIP

You can also add the files you want to block to the Anti-malware list in [step 4](#).

For more information, see:

- [Ransomware: how to reduce risk](#)
- [Restore your OneDrive](#)

6: Stop auto-forwarding for email

Hackers who gain access to a user's mailbox can exfiltrate mail by configuring the mailbox to automatically forward email. This can happen even without the user's awareness. You can prevent this from happening by configuring a mail flow rule.

To create a mail transport rule:

1. Go to the [Exchange admin center](#).
2. In the **mail flow** category, select **rules**.
3. Select **+**, and then **Create a new rule**.
4. Select **More options** at the bottom of the dialog box to see the full set of options.
5. Apply the settings in the following table. Leave the rest of the settings at the default, unless you want to change these.
6. Select **Save**.

SETTING	REJECT AUTO-FORWARD EMAILS TO EXTERNAL DOMAINS
Name	Prevent auto forwarding of email to external domains
Apply this rule if ...	The sender . . . is external/internal . . . Inside the organization
Add condition	The recipient . . . is external/internal . . . Outside the organization
Add condition	The message properties . . . include the message type . . . Auto-forward
Do the following ...	Block the message . . . reject the message and include an explanation.
Provide message text	Auto-forwarding email outside this organization is prevented for security reasons.

7: Use Office Message Encryption

Office Message Encryption is included with Microsoft 365. It's already set up. With Office Message Encryption, your organization can send and receive encrypted email messages between people inside and outside your organization. Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services. Email message encryption helps ensure that only intended recipients can view message content.

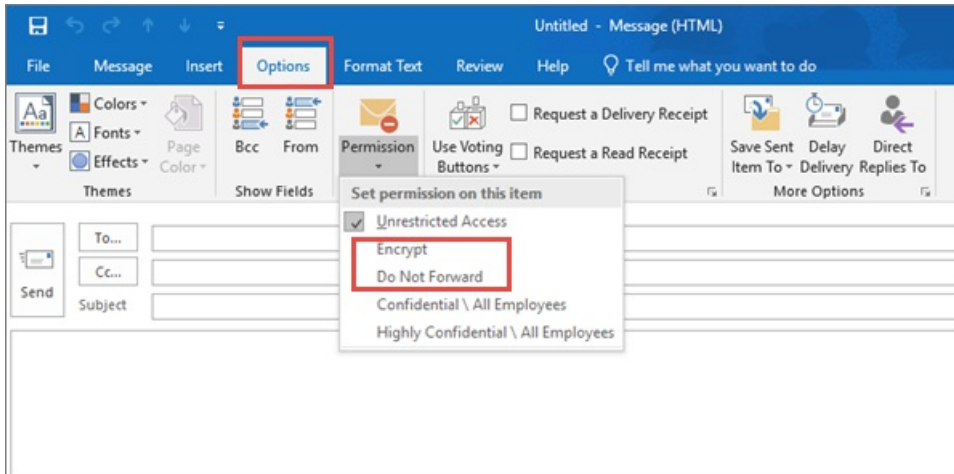
Office Message Encryption provides two protection options when sending mail:

- Do not forward
- Encrypt

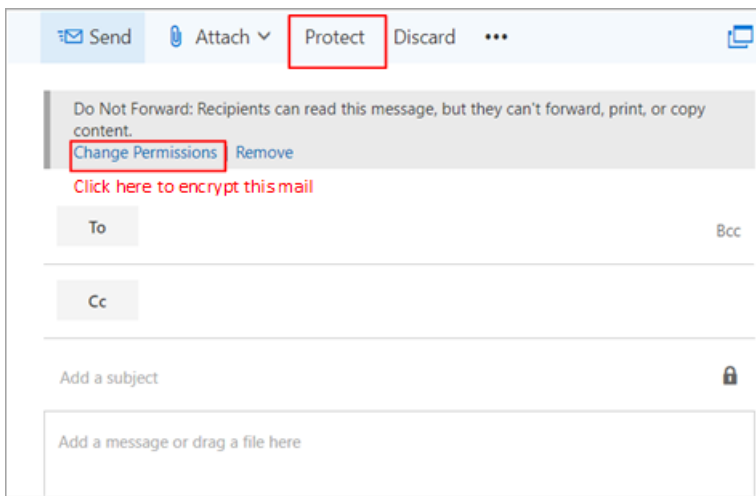
Your organization might have configured additional options that apply a label to email, such as Confidential.

To send protected email

In Outlook for PC, select **Options** in the email, and then choose **Permissions**.



In Outlook.com, select **Protect** in the email. The default protection is **Do not forward**. To change this to encrypt, select **Change Permissions > Encrypt**.



To receive encrypted email

If the recipient has Outlook 2013 or Outlook 2016 and a Microsoft email account, they'll see an alert about the item's restricted permissions in the Reading pane. After opening the message, the recipient can view the message just like any other.

If the recipient is using another email client or email account, such as Gmail or Yahoo, they'll see a link that lets them either sign in to read the email message or request a one-time passcode to view the message in a web browser. If users aren't receiving the email, have them check their Spam or Junk folder.

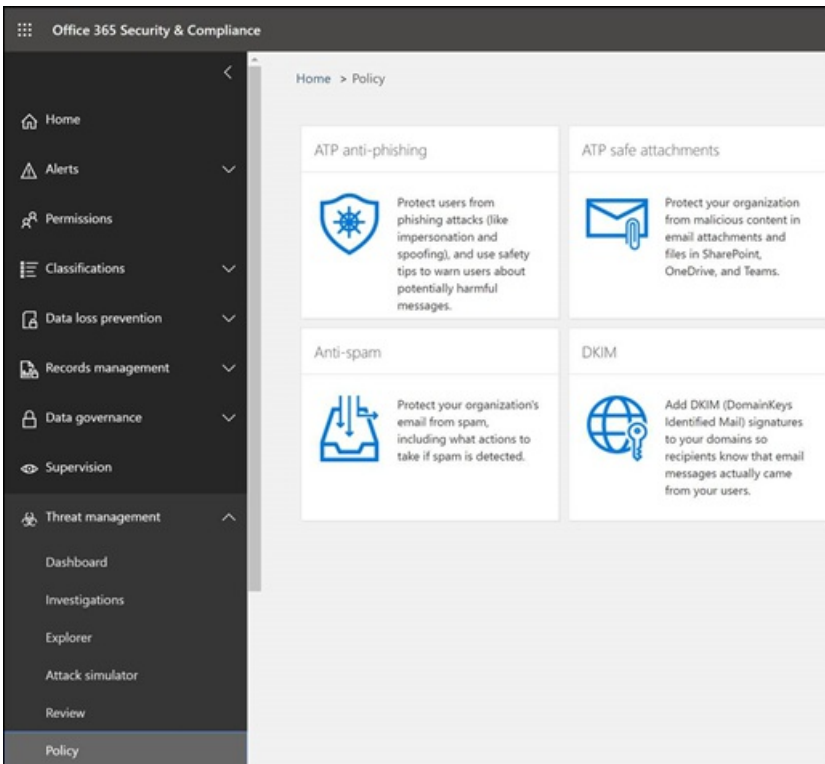
For more information, see [Send, view, and reply to encrypted messages in Outlook for PC](#).

8. Protect your email from phishing attacks

If you've configured one or more custom domains for your Microsoft 365 environment, you can configure targeted anti-phishing protection. Anti-phishing protection, a part of Microsoft Defender for Office 365, can help

protect your organization from malicious impersonation-based phishing attacks and other phishing attacks. If you haven't configured a custom domain, you do not need to do this.

We recommend that you get started with this protection by creating a policy to protect your most important users and your custom domain.



To create an anti-phishing policy in Defender for Office 365, view a [short training video](#), or complete the following steps:

1. Go to <https://protection.office.com>.
2. In the Security & Compliance Center, in the left navigation pane, under **Threat management**, select **Policy**.
3. On the Policy page, select **Anti-phishing**.
4. On the Anti-phishing page, select **+ Create**. A wizard launches that steps you through defining your anti-phishing policy.
5. Specify the name, description, and settings for your policy as recommended in the chart below. See [Learn about anti-phishing policy in Microsoft Defender for Office 365 options](#) for more details.
6. After you have reviewed your settings, select **Create this policy** or **Save**, as appropriate.

SETTING OR OPTION	RECOMMENDED SETTING
Name	Domain and most valuable campaign staff
Description	Ensure most important staff and our domain are not being impersonated.
Add users to protect	Select + Add a condition, The recipient is . Type user names or enter the email address of the candidate, campaign manager, and other important staff members. You can add up to 20 internal and external addresses that you want to protect from impersonation.

SETTING OR OPTION	RECOMMENDED SETTING
Add domains to protect	Select + Add a condition , The recipient domain is . Enter the custom domain associated with your Microsoft 365 subscription, if you defined one. You can enter more than one domain.
Choose actions	If email is sent by an impersonated user: select Redirect message to another email address , and then type the email address of the security administrator; for example, securityadmin@contoso.com. If email is sent by an impersonated domain: select Quarantine message .
Mailbox intelligence	By default, mailbox intelligence is selected when you create a new anti-phishing policy. Leave this setting On for best results.
Add trusted senders and domains	For this example, don't define any overrides.
Applied to	Select The recipient domain is . Under Any of these , select Choose . Select + Add . Select the check box next to the name of the domain, for example, contoso.com, in the list, and then select Add . Select Done .

For more information, see [Set up anti-phishing policies in Defender for Office 365](#).

9: Protect against malicious attachments and files with Safe Attachments

People regularly send, receive, and share attachments, such as documents, presentations, spreadsheets, and more. It's not always easy to tell whether an attachment is safe or malicious just by looking at an email message. Microsoft Defender for Office 365 includes Safe Attachment protection, but this protection is not turned on by default. We recommend that you create a new rule to begin using this protection. This protection extends to files in SharePoint, OneDrive, and Microsoft Teams.

To create an Safe attachment policy, view a [short training video](#), or complete the following steps:

1. Go to <https://protection.office.com> and sign in with your admin account.
2. In the Security & Compliance Center, in the left navigation pane, under **Threat management**, select **Policy**.
3. On the Policy page, select **Safe Attachments**.
4. On the Safe attachments page, apply this protection broadly by selecting the **Turn on ATP for SharePoint, OneDrive, and Microsoft Teams** check box.
5. Select **+** to create a new policy.
6. Apply the settings in the following table.
7. After you have reviewed your settings, select **Create this policy** or **Save**, as appropriate.

SETTING OR OPTION	RECOMMENDED SETTING
Name	Block current and future emails with detected malware.
Description	Block current and future emails and attachments with detected malware.
Save attachments unknown malware response	Select Block - Block the current and future emails and attachments with detected malware.
Redirect attachment on detection	Enable redirection (select this box) Enter the admin account or a mailbox setup for quarantine. Apply the above selection if malware scanning for attachments times out or error occurs (select this box).
Applied to	The recipient domain is . . . select your domain.

For more information, see [Set up anti-phishing policies in Defender for Office 365](#).

10: Protect against phishing attacks with Safe Links

Hackers sometimes hide malicious websites in links in email or other files. Safe Links, part of Microsoft Defender for Office 365, can help protect your organization by providing time-of-click verification of web addresses (URLs) in email messages and Office documents. Protection is defined through Safe Links policies.

We recommend that you do the following:

- Modify the default policy to increase protection.
- Add a new policy targeted to all recipients in your domain.

To get to Safe Links, view a [short training video](#), or complete the following steps:

1. Go to <https://protection.office.com> and sign in with your admin account.
2. In the Security & Compliance Center, in the left navigation pane, under **Threat management**, select **Policy**.
3. On the Policy page, select **Safe Links**.

To modify the default policy:

1. On the Safe links page, under **Policies that apply to the entire organization**, double-click the **Default** policy.
2. Under **Settings that apply to content across Office 365**, enter a URL to be blocked, such as *example.com*, and select +.
3. Under **Settings that apply to content except email**, select **Office 365 applications**, **Do not track when users click safe links**, and **Do not let users click through safe links to original URL**.
4. Select **Save**.

To create a new policy targeted to all recipients in your domain:

1. On the Safe links page, under **Policies that apply to specific recipients**, select + to create a new policy.

2. Apply the settings listed in the following table.

3. Select **Save**.

SETTING OR OPTION	RECOMMENDED SETTING
Name	Safe links policy for all recipients in the domain
Select the action for unknown potentially malicious URLs in messages	Select On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.
Apply real-time URL scanning for suspicious links and links that point to files	Select this box.
Applied to	The recipient domain is . . . select your domain.

For more information, see [Safe Links in Microsoft Defender for Office 365](#).

Related content

[Multi-factor authentication for Microsoft 365](#) (article)

[Manage and monitor priority accounts](#) (article)

[Microsoft 365 Reports in the admin center](#) (video)

Multifactor authentication for Microsoft 365

8/13/2021 • 5 minutes to read • [Edit Online](#)

Passwords are the most common method of authenticating a sign-in to a computer or online service, but they are also the most vulnerable. People can choose easy passwords and use the same passwords for multiple sign-ins to different computers and services.

To provide an additional level of security for sign-ins, you must use multifactor authentication (MFA), which uses both a password, which should be strong, and an additional verification method based on:

- Something you have with you that is not easily duplicated, such as a smart phone.
- Something you uniquely and biologically have, such as your fingerprints, face, or other biometric attribute.

The additional verification method is not employed until after the user's password has been verified. With MFA, even if a strong user password is compromised, the attacker does not have your smart phone or your fingerprint to complete the sign-in.

MFA support in Microsoft 365

By default, both Microsoft 365 and Office 365 support MFA for user accounts using:

- A text message sent to a phone that requires the user to type a verification code.
- A phone call.
- The Microsoft Authenticator smart phone app.

In both cases, the MFA sign-in is using the "something you have with you that is not easily duplicated" method for the additional verification. There are multiple ways in which you can enable MFA for Microsoft 365 and Office 365:

- With security defaults
- With Conditional Access policies
- For each individual user account (not recommended)

These ways are based on your Microsoft 365 plan.

PLAN	RECOMMENDATION	TYPE OF CUSTOMER
All Microsoft 365 plans	Use security defaults, which require MFA for all user accounts. You can also configure per-user MFA on individual user accounts, but this is not recommended.	Small business
Microsoft 365 Business Premium Microsoft 365 E3 Azure Active Directory (Azure AD) Premium P1 licenses	Use Conditional Access policies to require MFA for user accounts based on group membership, apps, or other criteria.	Small business to enterprise
Microsoft 365 E5 Azure AD Premium P2 licenses	Use Azure AD Identity Protection to require MFA based on sign-in risk criteria.	Enterprise

PLAN	RECOMMENDATION	TYPE OF CUSTOMER

Security defaults

Security defaults is a new feature for Microsoft 365 and Office 365 paid or trial subscriptions created after October 21, 2019. These subscriptions have security defaults turned on, which:

- Requires all of your users to use MFA with the Microsoft Authenticator app.
- Blocks legacy authentication.

Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.

Security defaults ensure that all organizations have a basic level of security for user sign-in that is enabled by default. You can disable security defaults in favor of MFA with Conditional Access policies.

You enable or disable security defaults from the **Properties** pane for Azure AD in the Azure portal.

Directory properties

Name *

Country or region

United States

Location

United States datacenters

Notification language

Directory ID



Technical contact

Global privacy contact

Privacy statement URL

Access management for Azure resources

MOD Administrator (admin@M365x436900.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)

Yes

No

[Manage Security defaults](#)

You can use security defaults with any Microsoft 365 plan.

For more information, see this [overview of security defaults](#).

Conditional Access policies

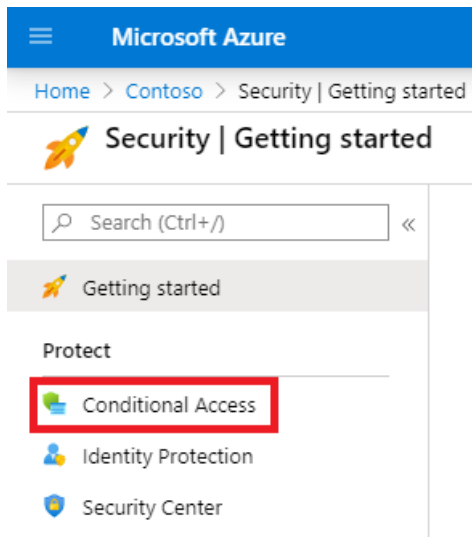
Conditional Access policies are a set of rules that specify the conditions under which sign-ins are evaluated and allowed. For example, you can create a Conditional Access policy that states:

- If the user account name is a member of a group for users that are assigned the Exchange, user, password, security, SharePoint, or global administrator roles, require MFA before allowing access.

This policy allows you to require MFA based on group membership, rather than trying to configure individual user accounts for MFA when they are assigned or unassigned from these administrator roles.

You can also use Conditional Access policies for more advanced capabilities, such as requiring MFA for specific apps or that the sign-in is done from a compliant device, such as your laptop running Windows 10.

You configure Conditional Access policies from the **Security** pane for Azure AD in the Azure portal.



You can use Conditional Access policies with:

- Microsoft 365 Business Premium
- Microsoft 365 E3 and E5
- Azure AD Premium P1 and Azure AD Premium P2 licenses

For small businesses with Microsoft 365 Business Premium, you can easily use Conditional Access policies with the following steps:

1. Create a group to contain the user accounts that require MFA.
2. Enable the **Require MFA for global admins** policy.
3. Create a group-based Conditional Access policy with these settings:
 - Assignments > Users and groups: The name of your group from Step 1 above.
 - Assignments > Cloud apps or actions: All cloud apps.
 - Access controls > Grant > Grant access > Require multi-factor authentication.
4. Enable the policy.
5. Add a user account to the group created in Step 1 above and test.
6. To require MFA for additional user accounts, add them to the group created in Step 1.

This Conditional Access policy allows you to roll out the MFA requirement to your users at your own pace.

Enterprises should use [Common Conditional Access policies](#) to configure the following policies:

- [Require MFA for administrators](#)
- [Require MFA for all users](#)
- [Block legacy authentication](#)

For more information, see this [overview of Conditional Access](#).

Azure AD Identity Protection

With Azure AD Identity Protection, you can create an additional Conditional Access policy to [require MFA when sign-in risk is medium or high](#).

You can use Azure AD Identity Protection and risk-based Conditional Access policies with:

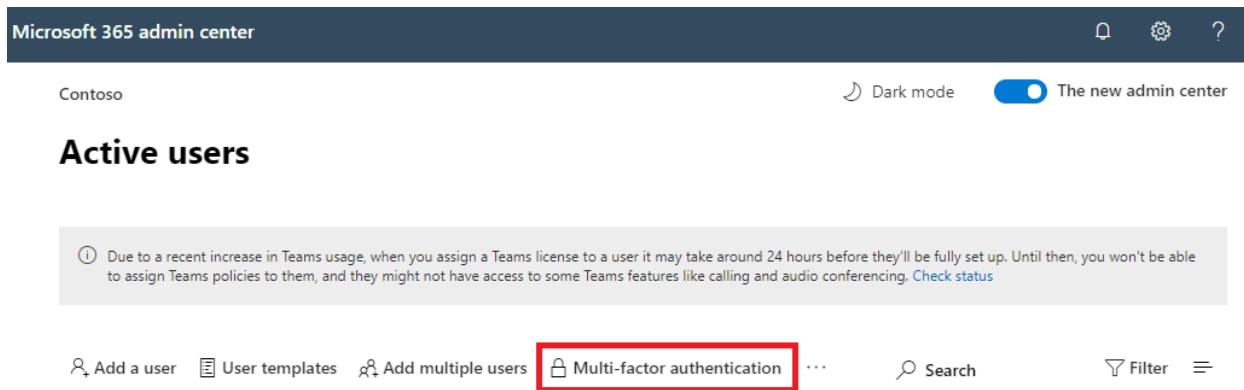
- Microsoft 365 E5
- Azure AD Premium P2 licenses

For more information, see this [overview of Azure AD Identity Protection](#).

Legacy per-user MFA (not recommended)

You should be using either security defaults or Conditional Access policies to require MFA for your user account sign-ins. However, if either of these cannot be used, Microsoft strongly recommends MFA for user accounts that have administrator roles, especially the global administrator role, for any size subscription.

You enable MFA for individual user accounts from the [Active users](#) pane of the Microsoft 365 admin center.



After being enabled, the next time the user signs in, they will be prompted to register for MFA and to choose and test the additional verification method.

Using these methods together

This table shows the results of enabling MFA with security defaults, Conditional Access policies, and per-user account settings.

ITEM	ENABLED	DISABLED	SECONDARY AUTHENTICATION METHOD
Security defaults	Can't use Conditional Access policies	Can use Conditional Access policies	Microsoft Authenticator app
Conditional Access policies	If any are enabled, you can't enable security defaults	If all are disabled, you can enable security defaults	User-specified during MFA registration
Legacy per-user MFA (not recommended)	Overrides security defaults and Conditional Access policies requiring MFA at each sign in	Overridden by security defaults and Conditional Access policies	User-specified during MFA registration

If security defaults are enabled, all new users are prompted for MFA registration and the use of the Microsoft Authenticator app at their next sign-in.

Ways to manage MFA settings

There are two ways to manage MFA settings.

In the Azure portal, you can:

- Enable and disable security defaults
- Configure Conditional Access policies

In the Microsoft 365 admin center, you can configure per-user and service [MFA settings](#).

Next steps

[Set up MFA for Microsoft 365](#)

Related content

[Turn on multifactor authentication](#) (video)

[Turn on multifactor authentication for your phone](#) (video)

Set up multifactor authentication

8/13/2021 • 3 minutes to read • [Edit Online](#)

Based on your understanding of [multifactor authentication \(MFA\)](#) and its support in Microsoft 365, it's time to set it up and roll it out to your organization.

IMPORTANT

If you purchased your subscription or trial after October 21, 2019, and you're prompted for MFA when you sign in, [security defaults](#) have been automatically enabled for your subscription.

Before you begin

- You must be a Global admin to manage MFA. For more information, see [About admin roles](#).
- If you have legacy per-user MFA turned on, [Turn off legacy per-user MFA](#).
- If you have Office 2013 clients on Windows devices, [turn on Modern Authentication for Office 2013 clients](#).
- Advanced: If you have third-party directory services with Active Directory Federation Services (AD FS), set up the Azure MFA Server. See [advanced scenarios with Azure AD Multifactor Authentication and third-party VPN solutions](#) for more information.

Turn Security defaults on or off

For most organizations, Security defaults offer a good level of additional sign-in security. For more information, see [What are security defaults?](#)

If your subscription is new, Security defaults might already be turned on for you automatically.

You enable or disable security defaults from the **Properties** pane for Azure Active Directory (Azure AD) in the Azure portal.

1. Sign in to the [Microsoft 365 admin center](#) with global admin credentials.
2. In the left nav choose **Show All** and under **Admin centers**, choose **Azure Active Directory**.
3. In the **Azure Active Directory admin center** choose **Azure Active Directory > Properties**.
4. At the bottom of the page, choose **Manage Security defaults**.
5. Choose **Yes** to enable security defaults or **No** to disable security defaults, and then choose **Save**.

If you have been using [baseline Conditional Access policies](#), you will be prompted to turn them off before you move to using security defaults.

1. Go to the [Conditional Access - Policies page](#).
2. Choose each baseline policy that is **On** and set **Enable policy** to **Off**.
3. Go to the [Azure Active Directory - Properties page](#).
4. At the bottom of the page, choose **Manage Security defaults**.
5. Choose **Yes** to enable security defaults and **No** to disable security defaults, and then choose **Save**.

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional

actions before a user is granted access to an application or service.

IMPORTANT

Turn off both per-user MFA and Security defaults before you enable Conditional Access policies.

Conditional Access is available for customers who have purchased Azure AD Premium P1, or licenses that include this, such as Microsoft 365 Business Premium, and Microsoft 365 E3. For more information, see [create a Conditional Access policy](#).

Risk-based conditional access is available through Azure AD Premium P2 license, or licenses that include this, such as Microsoft 365 E5. For more information, see [risk-based Conditional Access](#).

For more information about the Azure AD P1 and P2, see [Azure Active Directory pricing](#).

Turn on Modern authentication for your organization

For most subscriptions modern authentication is automatically turned on, but if you purchased your subscription before August 2017, it is likely that you will need to turn on Modern Authentication in order to get features like Multifactor Authentication to work in Windows clients like Outlook.

1. In the [Microsoft 365 admin center](#), in the left nav choose **Settings** > **Org settings**.
2. Under the **Services** tab, choose **Modern authentication**, and in the **Modern authentication** pane, make sure **Enable Modern authentication** is selected. Choose **Save changes**.

Turn off legacy per-user MFA

If you have previously turned on per-user MFA, you must turn it off before enabling Security defaults.

1. In the Microsoft 365 admin center, in the left nav choose **Users** > **Active users**.
2. On the **Active users** page, choose **Multi-factor authentication**.
3. On the multi-factor authentication page, select each user and set their Multi-Factor auth status to **Disabled**.

Next steps

- [How to register for their additional verification method](#)
- [What is: Multifactor Authentication](#)
- [How to sign-in after registration](#)
- [How to change their additional verification method](#)

Related content

[Turn on multifactor authentication](#) (video)

[Turn on multifactor authentication for your phone](#) (video)

Manage and monitor priority accounts

7/2/2021 • 3 minutes to read • [Edit Online](#)

In every Microsoft 365 organization, there are people that are essential, like executives, leaders, managers, or other users who have access to sensitive, proprietary, or high priority information.

To help your organization protect these accounts, you can now designate specific users as priority accounts and leverage app-specific features that provide them with extra protection. In the future, more apps and features will support priority accounts, and to start with, we've announced two capabilities: **priority account protection** and **premium mail flow monitoring**.

- **Priority account protection** - Microsoft Defender for Office 365 (formerly Office 365 Advanced Threat Protection) supports priority accounts as tags that can be used in filters in alerts, reports, and investigations. For more information, check out [User tags in Microsoft Defender for Office 365](#).

A natural question is, "Aren't all users a priority? Why not designate all users as priority accounts?" Yes, all users are a priority, but priority account protection offers the following additional benefits:

- **Additional heuristics:** Our analysis of mail flow in the Microsoft datacenters indicates that mail flow patterns for company executives are different than the average employee. Priority account protection offers additional heuristics that are specifically tailored to company executives that wouldn't benefit a regular employee.
- **Additional visibility in reporting:** In effect, information for all users (or all affected users) is already available in alerts, reports, and investigations. The priority accounts tag as a filter allows you to specifically target your investigations.
- **Premium Mail Flow Monitoring** - Healthy mail flow can be critical to business success, and delivery delays or failures can have a negative impact on the business. You can choose a threshold for failed or delayed emails, receive alerts when that threshold is exceeded, and view a report of email issues for priority accounts. For more information, check out [Email issues for priority accounts report in the modern EAC](#)

For security best practices for priority accounts, see [Security recommendations for priority accounts](#).

Before you begin

The **Priority account protection** feature that's described in this topic is available only to organizations that meet the following requirements:

- Microsoft Defender for Office 365 Plan 2, including those with Office 365 E3, Office 365 E5, Microsoft 365 E5, or Microsoft 365 E5 Security.

The **Premium Mail Flow Monitoring** feature that's described in this topic is available only to organizations that meet the following requirements:

- Your organization needs to have a license count of at least 5,000, from either one of, or a combination of the following products: Office 365 E3, Microsoft 365 E3, Office 365 E5, Microsoft 365 E5. For example, your organization can have 3,000 Office 365 E3 licenses and 2,500 Microsoft 365 E5, for a total of 5,500 licenses from the qualifying products.
- Your organization needs to have at least 50 monthly active Exchange Online users.

NOTE

You can monitor up to 250 priority accounts.

When you apply priority account protection to a mailbox, you should also apply priority account protection to users who have access to the mailbox (for example, the CEO and the CEO's executive assistant who manages the CEO's calendar).

Add priority accounts from the Setup page

Add priority accounts from the **Setup page**.

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Go to **Setup > Organizational knowledge**, and choose **View** under **Monitor your most important accounts**.
3. Select **Get Started** or **Manage**.
4. On the **Add Priority accounts** page, in the search field, type the name or email address of the person you want to add to the priority accounts list. You can also set your email threshold for failed or delayed emails and get a weekly report of issues for priority accounts.
5. Select the user and choose **Save**.

You can also add priority accounts from the Active users page.

Add priority accounts from Active users page

Add priority accounts from the Active users page.

1. Go to the admin center at <https://admin.microsoft.com>.
2. Go to **Users > Active users** and select the three dots (more actions) at the top of the page. Select **Manage priority accounts**.
3. Select **Add accounts**, and on the **Add Priority accounts** page, in the search field, type the name of the person you want to add to the priority accounts list.
4. Select the user and choose **Save**.

Remove a user from the priority accounts list

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com>.
2. Go to **Setup > Organizational knowledge**, and choose **View** under **Monitor your most important accounts**.
3. On the **Monitor your most accounts** page, choose **Priority accounts** under **Manage this feature**.
4. On the **Priority accounts** page, select the user or users you want to remove from the list and choose, **Remove accounts**.

Related topics

[Using Priority Accounts in Microsoft 365](#)

Enable Modern Authentication for Office 2013 on Windows devices

7/12/2021 • 2 minutes to read • [Edit Online](#)

To enable modern authentication for any Windows devices that have Office 2013 installed, you need to set specific registry keys.

Enable modern authentication for Office 2013 clients

NOTE

Modern authentication is already enabled for Office 2016 clients, you do not need to set registry keys for Office 2016.

To enable modern authentication for any devices running Windows (for example on laptops and tablets), that have Microsoft Office 2013 installed, you need to set the following registry keys. The keys have to be set on each device that you want to enable for modern authentication:

REGISTRY KEY	TYPE	VALUE
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\EnableADAL	REG_DWORD	1
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Version	REG_DWORD	1

Once you have set the registry keys, you can set Office 2013 devices apps to use [multifactor authentication \(MFA\)](#) with Microsoft 365.

If you're currently signed-in with any of the client apps, you need to sign out and sign back in for the change to take effect. Otherwise, the MRU and roaming settings will be unavailable until the ADAL identity is established.

Disable modern authentication on devices

To disable modern authentication on a device, set the following registry keys on the device:

REGISTRY KEY	TYPE	VALUE
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\EnableADAL	REG_DWORD	0

Related content

[Sign in to Office 2013 with a second verification method](#) (article)

[Outlook prompts for password and doesn't use Modern Authentication to connect to Office 365](#) (article)

Prerequisites for protecting data on devices with Microsoft 365 for business

5/1/2021 • 2 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

The first step in setting up your organization with Microsoft 365 for business is to make sure you can meet the prerequisites.

Requirements for setting up your organization with Microsoft 365 for business

- Windows devices must be running Windows 7 Professional, Windows 8 Pro, or Windows 8.1 Pro.

[Upgrade Windows devices to Windows Pro Creators Update](#)

If you're running Windows 10 Home, then you must **purchase** Windows 10 Pro. See [upgrade Windows 10 Home to Windows 10 Pro](#) for instructions.

- Remove devices from mobile management solutions (Mobile Iron, AirWatch, and so on). You'll enroll all the people in your organization in Microsoft 365 for business mobile management.
- Apple iOS 8.0 and later.

Google Android 4.0 and later (including Samsung KNOX Standard 4.0 and higher). For more information, see [Intune supported devices](#).

- If you have existing Office applications on user computers, read [prepare for Office client installation](#) to understand steps you might need to take before you can set up Microsoft 365 for business to install Office 2016 on user computers.

Microsoft 365 Business Premium security and compliance features

4/30/2021 • 4 minutes to read • [Edit Online](#)

Microsoft 365 Business Premium offers simplified security features to help safeguard your data on PCs, phones, and tablets.

Microsoft 365 admin center security features

You can manage many of the Microsoft 365 Business Premium security features in the admin center, which gives you a simplified way to turn these features on or off. In the admin center, you can do the following:

- [Set application management settings for Android or iOS devices](#) .

These settings include deleting files from an inactive device after a set period, encrypting work files, requiring that users set a PIN, and so on.

- [Set application protection settings for Windows 10 devices](#) .

These settings can be applied to company data on both company-owned, or personally owned devices.

- [Set device protection settings for Windows 10 devices](#) .

You can enable [BitLocker](#) encryption to help protect data in case a device is lost or stolen, and enable [Windows Exploit Guard](#) to provide advanced protection against ransomware.

- [Remove company data from devices](#)

You can remotely wipe company data if a device is lost, stolen, or an employee leaves your company.

- [Reset Windows 10 devices to their factory settings](#) .

You can reset any Windows 10 devices that have device protection settings applied to them.

Additional security features

Advanced features in Microsoft 365 Business Premium are available to help you protect your business against cyber-threats and safeguard sensitive information.

- [Microsoft Defender for Office 365](#)

Microsoft Defender for Office 365 helps guard your business against sophisticated phishing and ransomware attacks designed to compromise employee or customer information. Features include:

- Sophisticated attachment scanning and AI-powered analysis to detect and discard dangerous messages.
- Automatic checks of links in email to assess if they're part of a phishing scheme. This keeps you safe from accessing unsafe websites.

- [The full capabilities of Intune in the Azure portal](#)

Accessing the Intune admin center in the Azure portal allows you to set up additional security features, such as management of MacOS devices, iPhone, and Android devices, along with advanced device management for Windows, that aren't available through Microsoft 365 admin center.

- Same [Conditional Access](#) as Azure AD Premium P1 plan

Conditional Access can help protect your organization from sign-in risk, access attempts from an unexpected network or locale, access attempts from risky device types, and so on. Conditional Access policies are enforced after the first authentication is completed, and it uses signals from the first authentication event to determine if the attempted access should be approved, denied, or if more proof (such as a second form of identification) is required.

The conditional access features included are:

- Access based on username, group, and role
- Access [based on an app](#)
- [Access based on location](#); only allow access from trusted IP ranges or specific countries
- Require MFA for access
- Block access to apps that use [legacy authentication](#)
- Require apps to use [Intune app protection](#)
- Custom authentication such as MFA with third-party providers, for example DUO.

Other features:

- [Self-service password reset](#) for hybrid Azure AD

Compliance features

Your Microsoft 365 Business Premium subscription includes features that help you maintain compliance and regulatory standards.

- [Learn about data loss prevention](#) (DLP).

You can set up DLP to automatically detect sensitive information, like credit card numbers, social security numbers, and so on, to prevent their inadvertent sharing outside your company.

- [Exchange Online Archiving](#)

Exchange Online Archiving license enables messages to be easily archived with continuous data backup. It stores all of a user's emails, including deleted items, in case they're needed later for discovery or restoration. Additionally, you can use different retention policies to preserve email data for litigation holds, eDiscovery, or to meet compliance requirements.

- [Sensitivity labels](#)

Microsoft 365 Business Premium includes all the features of [Azure Information Protection Plan 1](#). With this plan, you can create **Sensitivity labels** that allow you to control access to sensitive information in email and documents, with controls like "Do not forward" and "Do not copy." You can also classify sensitive information as "Confidential" and specify how classified information can be shared outside and inside the business. Enterprise-grade encryption is easy to apply to email and documents to keep your information private. You can also install the Azure Information Protection client add-in for Office apps. For more information, see [Azure Information Protection unified labeling client](#). For Sensitivity labels, install the `AzInfoProtection_UL.exe`.

You can manage these features in the Security & Compliance center and the Intune admin center. Over time the simplified controls will be added to the Microsoft 365 admin center.

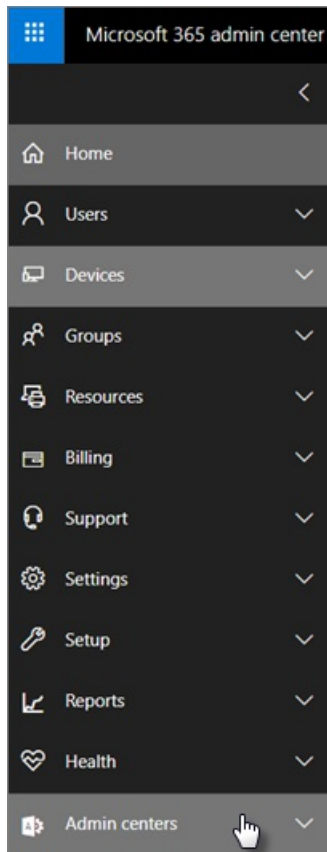
FAQ

Are these security features available in all markets?

Yes, these features are available in all markets where Microsoft 365 Business Premium is sold.

How do I find the Security & Compliance center?

1. [Sign in to Microsoft 365 Business Premium](#) by using your admin credentials.
2. In the left nav, locate **Admin centers** and expand it.



3. Choose **Security & Compliance** to go to Security & compliance center.

Increase threat protection

6/14/2021 • 9 minutes to read • [Edit Online](#)

This article helps you increase the protection in your Microsoft 365 subscription to protect against phishing, malware, and other threats. These recommendations are appropriate for organizations with an increased need for security, like law offices and health care clinics.

Before you begin, check your Office 365 Secure Score. Office 365 Secure Score analyzes your organization's security based on your regular activities and security settings, and assigns a score. Begin by taking note of your current score. To increase your score, complete the actions recommended in this article. The goal isn't to achieve the maximum score, but to be aware of opportunities to protect your environment that don't negatively affect productivity for your users.

For more information, see [Microsoft Secure Score](#).

Raise the level of protection against malware in mail

Your Office 365 or Microsoft 365 environment includes protection against malware. You can increase this protection by blocking attachments with file types that are commonly used for malware. To increase malware protection in email:

1. Go to <https://protection.office.com> and sign in with your admin account credentials.
2. In the Security & Compliance Center, in the left navigation pane, under **Threat management**, choose **Policy > Anti-Malware**.
3. Double-click the default policy to edit this company-wide policy.
4. Select **Settings**.
5. Under **Common Attachment Types Filter**, select **On**. The file types that are blocked are listed in the window directly below this control. Make sure that you add these file types:

```
ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh, exe, pif
```

If necessary, you can add or delete file types later.

6. Select **Save**.

For more information, see [Anti-malware protection in EOP](#).

Protect against ransomware

Ransomware restricts access to data by encrypting files or locking computer screens. It then attempts to extort money from victims by asking for "ransom," usually in the form of cryptocurrencies like Bitcoin, in exchange for access to data.

To protect against ransomware, create one or more mail flow rules to block file extensions that are commonly used for ransomware. (You added these rules in the [raise the level of protection against malware in mail](#) step.) You can also warn users who receive these attachments in email.

In addition to the files that you blocked in the previous step, it's a good practice to create a rule to warn users before opening Office file attachments that include macros. Ransomware can be hidden inside macros, so warn users not to open these files from people they don't know.

To create a mail transport rule:

1. Go to the admin center at <https://admin.microsoft.com>, and choose **Admin centers** > **Exchange**.
2. In the **mail flow** category, select **rules**.
3. Select **+**, and then select **Create a new rule**.
4. Select **More options** at the bottom of the dialog box to see the full set of options.
5. Apply the settings in the following table for the rule. Use the default values for the rest of the settings, unless you want to change them.
6. Select **Save**.

SETTING	WARN USERS BEFORE OPENING ATTACHMENTS OF OFFICE FILES
Name	Anti-ransomware rule: warn users
Apply this rule if . . .	Any attachment . . . file extension matches . . .
Specify words or phrases	Add these file types: dotm, docm, xlsx, sltm, xla, xlam, xll, pptm, potm, ppam, ppsm, sldm
Do the following . . .	Notify the recipient with a message
Provide message text	Do not open these types of files from people you do not know because they might contain macros with malicious code.

For more information, see:

- [Ransomware: how to reduce risk](#)
- [Restore your OneDrive](#)

Stop auto-forwarding for email

Hackers who gain access to a user's mailbox can steal mail by setting the mailbox to automatically forward email. This can happen even without the user's awareness. To prevent this from happening, configure a mail flow rule.

To create a mail transport rule, either watch [this short video](#) or follow these steps:

1. In the Microsoft 365 admin center, select **Admin centers** > **Exchange**.
2. In the **mail flow** category, select **rules**.
3. Select **+**, and then select **Create a new rule**.
4. To see all the options, select **More options** at the bottom of the dialog box.
5. Apply the settings in the following table. Use the default values for the rest of the settings, unless you want to change them.
6. Select **Save**.

SETTING	WARN USERS BEFORE OPENING ATTACHMENTS OF OFFICE FILES
Name	Prevent auto forwarding of email to external domains
Apply this rule if ...	The sender . . . is external/internal . . . Inside the organization
Add condition	The message properties . . . include the message type . . . Auto-forward
Do the following ...	Block the message . . . reject the message and include an explanation.
Provide message text	Auto-forwarding email outside this organization is prevented for security reasons.

Protect your email from phishing attacks

If you've configured one or more custom domains for your Office 365 or Microsoft 365 environment, you can configure targeted anti-phishing protection. Anti-phishing protection, part of Microsoft Defender for Office 365, can help protect your organization from malicious impersonation-based phishing attacks and other phishing attacks. If you haven't configured a custom domain, you don't need to do this.

We recommend that you get started with this protection by creating a policy to protect your most important users and your custom domain.

To create an anti-phishing policy in Microsoft Defender for Office 365, watch [this short training video](#), or complete the following steps:

1. Go to <https://protection.office.com>.
2. In the Security & Compliance Center, in the left navigation pane, under **Threat management**, choose **Policy**.
3. On the **Policy** page, choose **Anti-phishing**.
4. On the **Anti-phishing** page, select + **Create**. A wizard launches that steps you through defining your anti-phishing policy.
5. Specify the name, description, and settings for your policy as recommended in the following table. For more details, see [Learn about anti-phishing policy in Microsoft Defender for Office 365 options](#).
6. After you've reviewed your settings, choose **Create this policy** or **Save**, as appropriate.

SETTING OR OPTION	RECOMMENDED SETTING
Name	Domain and most valuable campaign staff
Description	Ensure most important staff and our domain are not being impersonated.
Add users to protect	Select + Add a condition, The recipient is . Type user names or enter the email address of the candidate, campaign manager, and other important staff members. You can add up to 20 internal and external addresses that you want to protect from impersonation.

SETTING OR OPTION	RECOMMENDED SETTING
Add domains to protect	Select + Add a condition, The recipient domain is . Enter the custom domain associated with your Microsoft 365 subscription, if you defined one. You can enter more than one domain.
Choose actions	If email is sent by an impersonated user: Choose Redirect message to another email address , and then type the email address of the security administrator; for example, <i>Alice@contoso.com</i> . If email is sent by an impersonated domain: Choose Quarantine message .
Mailbox intelligence	By default, mailbox intelligence is selected when you create a new anti-phishing policy. Leave this setting On for best results.
Add trusted senders and domains	Here you can add your own domain, or any other trusted domains.
Applied to	Select The recipient domain is . Under Any of these , select Choose . Select + Add . Select the check box next to the name of the domain, for example, <i>contoso.com</i> , in the list, and then select Add . Select Done .

Protect against malicious attachments and files with Safe Attachments

People regularly send, receive, and share attachments, such as documents, presentations, spreadsheets, and more. It's not always easy to tell whether an attachment is safe or malicious just by looking at an email message. Microsoft Defender for Office 365 includes Safe Attachment protection, but this protection is not turned on by default. We recommend that you create a new rule to begin using this protection. This protection extends to files in SharePoint, OneDrive, and Microsoft Teams.

To create an Safe Attachment policy, either watch [this short video](#), or complete the following steps:

1. Go to <https://protection.office.com>, and sign in with your admin account.
2. In the Security & Compliance Center, in the left navigation pane, under **Threat management**, choose **Policy**.
3. On the Policy page, choose **Safe Attachments**.
4. On the Safe attachments page, apply this protection broadly by selecting the **Turn on ATP for SharePoint, OneDrive, and Microsoft Teams** check box.
5. Select + to create a new policy.
6. Apply the settings in the following table.
7. After you have reviewed your settings, choose **Create this policy** or **Save**, as appropriate.

SETTING OR OPTION	RECOMMENDED SETTING
Name	Block current and future emails with detected malware.

SETTING OR OPTION	RECOMMENDED SETTING
Description	Block current and future emails and attachments with detected malware.
Save attachments unknown malware response	Select Block - Block the current and future emails and attachments with detected malware.
Redirect attachment on detection	Enable redirection (select this box) Enter the admin account or a mailbox setup for quarantine. Apply the above selection if malware scanning for attachments times out or error occurs (select this box).
Applied to	The recipient domain is . . . select your domain.

For more information, see [Set up anti-phishing policies in Microsoft Defender for Office 365](#).

Protect against phishing attacks with Safe Links

Hackers sometimes hide malicious websites in links in email or other files. Safe Links, part of Microsoft Defender for Office 365, can help protect your organization by providing time-of-click verification of web addresses (URLs) in email messages and Office documents. Protection is defined through Safe Links policies.

We recommend that you do the following:

- Modify the default policy to increase protection.
- Add a new policy targeted to all recipients in your domain.

To set up Safe Links, watch [this short training video](#), or complete the following steps:

1. Go to <https://protection.office.com>, and sign in with your admin account.
2. In the Security & Compliance Center, in the left navigation pane, under **Threat management**, choose **Policy**.
3. On the Policy page, choose **Safe Links**.

To modify the default policy:

1. On the Safe links page, under **Policies that apply to the entire organization**, select the **Default** policy.
2. Under **Settings that apply to content except email**, select **Microsoft 365 Apps for enterprise, Office for iOS and Android**.
3. Select **Save**.

To create a new policy targeted to all recipients in your domain:

1. On the Safe links page, under **Policies that apply to the entire organization**, select **+** to create a new policy.
2. Apply the settings listed in the following table.
3. Select **Save**.

SETTING OR OPTION	RECOMMENDED SETTING
Name	Safe links policy for all recipients in the domain
Select the action for unknown potentially malicious URLs in messages	Select On - URLs will be rewritten and checked against a list of known malicious links when user clicks on the link.
Use Safe Attachments to scan downloadable content	Select this box.
Applied to	The recipient domain is . . . select your domain.

For more information, see [Safe Links](#).

Go to Intune admin center

1. Sign in to [Azure portal](#).
2. Select **All services** and type in *Intune* in the **Search Box**.
3. Once the results appear, select the start next to **Microsoft Intune** to make it a favorite and easy to find later.

In addition to the admin center, you can use Intune to enroll and manage your organization's devices. For more information, see [Capabilities by enrollment method for Windows devices](#) and [Enrollment options for devices managed by Intune](#).

Threats detected by Microsoft Defender Antivirus

3/24/2021 • 3 minutes to read • [Edit Online](#)

Microsoft Defender Antivirus protects your Windows devices from software threats, such as viruses, malware, and spyware.

- Viruses typically spread by attaching their code to other files on your device or network and can cause infected programs to work incorrectly.
- Malware includes malicious files, applications, and code that can cause damage and disrupt normal use of devices. Also, malware can allow unauthorized access, use system resources, steal passwords and account information, lock you out of your computer and ask for ransom, and more.
- Spyware collects data, such as web-browsing activity, and sends the data to remote servers.

To provide threat protection, Microsoft Defender Antivirus uses several methods. These methods include cloud-delivered protection, real-time protection, and dedicated protection updates.

- Cloud-delivered protection helps provide near-instant detection and blocking of new and emerging threats.
- Always-on scanning uses file- and process-behavior monitoring and other techniques (also known as *real-time protection*).
- Dedicated protection updates are based on machine learning, human and automated big-data analysis, and in-depth threat resistance research.

To learn more about malware and Microsoft Defender Antivirus, see the following articles:

- [Understanding malware & other threats](#)
- [How Microsoft identifies malware and potentially unwanted applications](#)
- [Next-generation protection in Windows 10](#)

What happens when a non-Microsoft antivirus solution is used?

Microsoft Defender Antivirus is part of the operating system and is enabled on devices that are running Windows 10. However, if you're using a non-Microsoft antivirus solution and you aren't using [Microsoft Defender for Endpoint](#), then Microsoft Defender Antivirus automatically goes into disabled mode.

When in disabled mode, users and customers can still use Microsoft Defender Antivirus for scheduled or on-demand scans to identify threats; however, Microsoft Defender Antivirus will no longer:

- be used as the default antivirus app.
- actively scan files for threats.
- remediate, or resolve, threats.

If you uninstall the non-Microsoft antivirus solution, Microsoft Defender Antivirus will automatically go into active mode to protect your Windows devices from threats.

TIP

- If you're using Microsoft 365, consider using Microsoft Defender Antivirus as your primary antivirus solution. Integration can provide better protection. See [Better together: Microsoft Defender Antivirus and Office 365](#).
- Make sure to keep Microsoft Defender Antivirus up to date, even if you're using a non-Microsoft antivirus solution.

What to expect when threats are detected

When threats are detected by Microsoft Defender Antivirus, the following things happen:

- Users receive [notifications in Windows](#).
- Detections are listed in the [Windows Security app](#) on the **Protection history** page.
- If you've [secured your Windows 10 devices](#) and [enrolled them in Intune](#), and your organization has 800 or fewer devices enrolled, you'll see threat detections and insights in the [Microsoft 365 admin center](#) on the **Threats and antivirus** page, which you can access from the **Microsoft Defender Antivirus** card on the **Home** page (or from the navigation pane by selecting **Health > Threats & antivirus**).

If your organization has more than 800 devices enrolled in Intune, you'll be prompted to view threat detections and insights from [Microsoft Endpoint Manager](#) instead of from the **Threats and antivirus** page.

NOTE

The **Microsoft Defender Antivirus** card and **Threats and antivirus** page are being rolled out in phases, so you may not have immediate access to them.

In most cases, users don't need to take any further action. As soon as a malicious file or program is detected on a device, Microsoft Defender Antivirus blocks it and prevents it from running. Plus, newly detected threats are added to the antivirus and antimalware engine so that other devices and users are protected, as well.

If there's an action a user needs to take, such as approving the removal of a malicious file, they'll see that in the notification they receive. To learn more about actions that Microsoft Defender Antivirus takes on a user's behalf, or actions users might need to take, see [Protection History](#). To learn how to manage threat detections as an IT professional/admin, see [Review detected threats and take action](#).

To learn more about different threats, visit the [Microsoft Security Intelligence Threats site](#), where you can perform the following actions:

- View current information about top threats.
- View the latest threats for a specific region.
- Search the threat encyclopedia for details about a specific threat.

Related content

[Secure Windows 10 devices](#) (article)

[Evaluate Microsoft Defender Antivirus](#) (article)

[How to turn on real-time and cloud-delivered antivirus protection](#) (article)

[How to turn on and use Microsoft Defender Antivirus from the Windows Security app](#) (article)

[How to turn on Microsoft Defender Antivirus by using Group Policy](#) (article)

[How to update your antivirus definitions](#) (article)

[How to submit malware and non-malware to Microsoft for analysis](#) (article)

Review detected threats and take action

3/17/2021 • 5 minutes to read • [Edit Online](#)

As soon as a malicious file or software is detected, Microsoft Defender Antivirus blocks it and prevents it from running. And with cloud-delivered protection turned on, newly detected threats are added to the antivirus and antimalware engine so that your other devices and users are protected, as well.

Microsoft Defender Antivirus detects and protects against the following kinds of threats:

- Viruses, malware, and web-based threats on devices
- Phishing attempts
- Data theft attempts

As an IT professional/admin, you can view information about threat detections across [Windows 10 devices that are enrolled in Intune](#) in the Microsoft 365 admin center. You'll see summary information, such as:

- How many devices need antivirus protection
- How many devices are not in compliance with security policies
- How many threats are currently active, mitigated, or resolved

You have several options to view specific information about threat detections and devices:

- The **Active devices** page in the [Microsoft 365 admin center](#). See [Manage threat detections on the Active devices page](#) in this article.
- The **Active threats** page in the [Microsoft 365 admin center](#). See [Manage threat detections on the Active threats page](#) in this article.
- The **Antivirus** page in [Microsoft Endpoint Manager](#). See [Manage threat detections in Microsoft Endpoint Manager](#) in this article.

To learn more, see [Threats detected by Microsoft Defender Antivirus](#).

Manage threat detections on the **Active devices** page

The following procedure applies to customers who have Microsoft 365 Business Premium.

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com> and sign in.
2. In the navigation page, select **Devices** > **Active devices**. You'll see a list of active devices and details, such as protection status, antivirus (AV) protection state, and the number of active threats detected.
3. Select a device to view more details about that device and available actions. A flyout opens with recommendations and available actions, such as **Update policy**, **Update antivirus**, **Run quick scan**, **Run full scan**, and more.

Manage threat detections on the **Active threats** page

The following procedure applies to customers who have Microsoft 365 Business Premium. [Windows 10 devices must be secured](#) and [enrolled in Intune](#).

NOTE

The **Microsoft Defender Antivirus** card and **Active threats** page are being rolled out in phases, so you may not have immediate access to them.

1. Go to the Microsoft 365 admin center at <https://admin.microsoft.com> and sign in.
2. On the **Microsoft Defender Antivirus** card, select **View active threats**. (Alternatively, in the navigation pane, select **Health > Threats & antivirus**.)
3. On the **Active threats** page, select a detected threat to learn more about it. A flyout opens with details about that threat, including which devices are affected.
4. On the flyout, select a device to view available actions, such as **Update policy**, **Update antivirus**, **Run quick scan**, and more.

Actions you can take

When you view details about specific threats or devices, you'll see recommendations and one or more actions you can take. The following table describes actions that you might see.

ACTION	DESCRIPTION
Configure protection	Your threat protection policies need to be configured. Select the link to go to your policy configuration page. Need help? See Manage device security with endpoint security policies in Microsoft Intune .
Update policy	Your antivirus and real-time protection policies need to be updated or configured. Select the link to go to the policy configuration page. Need help? See Manage device security with endpoint security policies in Microsoft Intune .
Run quick scan	Starts a quick antivirus scan on the device, focusing on common locations where malware might be registered, such as registry keys and known Windows startup folders.
Run full scan	Starts a full antivirus scan on the device, focusing on common locations where malware might be registered, and including every file and folder on the device. Results are sent to Microsoft Endpoint Manager .
Update antivirus	Requires the device to get security intelligence updates for antivirus and antimalware protection.
Restart device	Forces a Windows 10 device to restart within five minutes. IMPORTANT: The device owner or user is not automatically notified of the restart and could lose unsaved work.

Manage threat detections in Microsoft Endpoint Manager

You can use Microsoft Endpoint Manager to manage threat detections. Windows 10 devices must be [enrolled in](#)

Intune (part of Microsoft Endpoint Manager).

1. Go to the Microsoft Endpoint Manager admin center at <https://endpoint.microsoft.com> and sign in.
2. In the navigation pane, select **Endpoint security**.
3. Under **Manage**, select **Antivirus**. You'll see several tabs, such as **Summary**, **Windows 10 unhealthy endpoints**, and **Windows 10 detected malware**.
4. Review the information on the available tabs, and then take any needed action.

For example, suppose that devices are listed on the **Windows 10 detected malware** tab. When you select a device, you'll have certain actions available, such as **Restart**, **Quick Scan**, **Full Scan**, **Sync**, or **Update signatures**. Select an action for that device.

The following table describes the actions you might see in Microsoft Endpoint Manager.

ACTION	DESCRIPTION
Restart	Forces a Windows 10 device to restart within five minutes. IMPORTANT: The device owner or user is not automatically notified of the restart and could lose unsaved work.
Quick Scan	Starts a quick antivirus scan on the device, focusing on common locations where malware might be registered, such as registry keys and known Windows startup folders. Results are sent to Microsoft Endpoint Manager .
Full Scan	Starts a full antivirus scan on the device, focusing on common locations where malware might be registered, and including every file and folder on the device. Results are sent to Microsoft Endpoint Manager .
Sync	Requires a device to check in with Intune (part of Microsoft Endpoint Manager). When the device checks in, the device receives any pending actions or policies assigned to the device.
Update signatures	Requires the device to get security intelligence updates for antivirus and antimalware protection.

TIP

For more information, see [Remote actions for devices](#).

How to submit a file for malware analysis

If you have a file that you think was missed or wrongly classified as malware, you can submit that file to Microsoft for malware analysis. Users and IT admins can submit a file for analysis. Visit <https://www.microsoft.com/wdsi/filesubmission>.

Set up compliance features

5/1/2021 • 2 minutes to read • [Edit Online](#)

Your Microsoft 365 Business Premium comes with features to protect your data and devices, and help you keep your and your customers' sensitive information secure.

Set up DLP features

See [Create a DLP policy from a template](#) for an example on how to set up a policy to protect against protect loss of personal data.

DLP comes with many ready-to-use policy templates for many different locales. For example, Australia Financial Data, Canada Personal Information Act, U.S. Financial Data, and so on. See [What the DLP policy templates include](#) for a full list. All of these templates can be enabled similar to the PII template example.

Set up email retention with Exchange Online Archiving

Exchange Online Archiving license features help maintain compliance and regulatory standards by preserving email content for eDiscovery. It also helps reduce your risk if there is a lawsuit, and provides a way to recover data after a security breach or when you need to recover deleted items. You can use litigation hold to preserve all of a user's content, or use retention policies to customize what you want to preserve.

Litigation hold: You can preserve all mailbox content including deleted items by putting a user's entire mailbox on litigation hold.

To place a mailbox on litigation hold, in the Admin center:

1. In the left nav, go to **Users > Active users**.
2. Select a user whose mailbox you want to place on litigation hold. In the user pane, expand **Mail settings**, and next to **More settings**, choose **Edit Exchange properties**.
3. On the mailbox page for the user, choose **** mailbox features **** on the left nav, and then choose the **Enable** link under **Litigation hold**.
4. In the **litigation hold** dialog box, you can specify the litigation hold duration in the **Litigation hold duration** field. Leave the field empty if you want to place an infinite hold. You can also add notes and direct the mailbox owner to a website you might have to explain more about the litigation hold. > **Save**.

Retention: You can enable customized retention policies, for example, to preserve for a specific amount of time or delete content permanently at the end of the retention period. To learn more, see [Overview of retention policies](#).

Set up Sensitivity labels

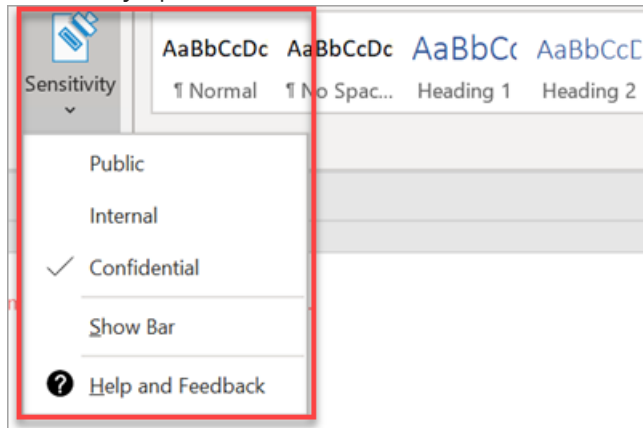
Sensitivity labels come with Azure Information Protection (AIP) Plan 1, and help you classify, and optionally protect your documents and emails, by applying labels. Labels can be applied automatically by administrators who define rules and conditions, manually by users, or by using a combination where users are given recommendations.

To set up Sensitivity labels, view [create and manage sensitivity labels](#) video.

Install the Azure Information Protection client manually

To manually install the AIP client:

1. Download **AzinfoProtection_UL.exe** from [Microsoft download center](#).
2. You can verify that the installation worked by viewing a Word document and making sure that the **Sensitivity** option is available on the **Home** tab.



For more information, see [Install the client](#).

GDPR simplified: A guide for your small business

6/14/2021 • 17 minutes to read • [Edit Online](#)

Using Microsoft 365 for business to help you to mitigate and manage GDPR compliance

The General Data Protection Regulation (GDPR) is a European Union (EU) regulation that mandates how an organization should handle personal data. If your business sells to, provides services to, or employs citizens of the European Union, then the [GDPR](#) will affect you.

As a small business admin, you are probably asking yourself "how do I get started"? This may be especially true if your business does not handle personal data as a core business activity, or if GDPR is totally new to you.

You can get started by reviewing this article, which is aimed at helping you understand what the GDPR is, why it came about, and how Microsoft 365 for business can help your organization comply with the GDPR.

It also includes answers to common questions about GDPR that small businesses may have, and highlights steps a small business can take to prepare for GDPR.

IMPORTANT

The Microsoft 365 solutions and recommendations in this article are tools and resources that can help you manage and protect your data, but are not a guarantee of GDPR compliance. It is up to you to assess your own compliance status. Consult with your own legal and/or professional advisors when needed.

A quick overview of the GDPR

The GDPR is an EU regulation that updates and expands the earlier Data Protection Directive (DPD) first enacted in 1995. The GDPR is concerned with the privacy of an individual's data, be that individual a client, customer, employee, or business partner. The GDPR's goal is to strengthen personal data protection for EU citizens, whether they reside in the EU or elsewhere. The regulation sets out expectations and advises on how to achieve them. Organizations must have measures in place that satisfy the requirements of the GDPR.

The GDPR is all about data and how it's used. Think of data as having a life cycle. The cycle starts when you collect data, continues as you store it and use it (processing), and ends when you completely delete it from your systems.

The GDPR is concerned with the following types of data:

- **Personal data:** If you can link data to an individual and identify them, then that data is considered personal with respect to the GDPR. Examples of personal data include name, address, date of birth, and IP address. The GDPR considers even encoded information (also known as "pseudonymous" information) to be personal data, regardless of how obscure or technical the data is, if the data can be linked to an individual.
- **Sensitive personal data** This is data that adds more details to personal data. Examples include religion, trade union membership, ethnic origin, and so on. Sensitive personal data also includes biometric data and DNA. Under GDPR, sensitive data has more stringent protection rules than personal data.

GDPR terms

You'll see some terms referred to frequently in the GDPR. It's important to understand these terms.

Consent

The GDPR states: "The processing of personal data should be designed to serve mankind." The GDPR hopes to achieve this goal by using consent when processing personal data. That could be the simple act of asking your customers if they want to receive email messages from your company. It also means no more opt-out check boxes on your website when you want to use data for marketing. You must take explicit consent using a "clear affirmative act". And, you will need to also keep records of when a consent is taken or revoked.

Data subject rights

The GDPR establishes data subject rights, which means that, with respect to their personal data, customers, employees, business partners, clients, contractors, students, suppliers, and so forth have the right to:

- **Be informed about their data:** You must inform individuals about your use of their data.
- **Have access to their data:** You must give individuals access to any of their data that you hold (for example, by using account access or in some manual manner).
- **Ask for data rectification:** Individuals can ask you to correct inaccurate data.
- **Ask for data to be deleted:** Also known as the 'right to erasure', this right allows an individual to request that any of their personal data a company has collected is deleted across all systems that use it or share it.
- **Request restricted processing:** An individual can ask that you suppress or restrict their data. However, it is only applicable under certain circumstances.
- **Have data portability:** An individual can ask for their data to be transferred to another company.
- **Object:** An individual can object to their data being used for various uses including direct marketing.
- **Ask not to be subject to automated decision-making, including profiling:** The GDPR has strict rules about using data to profile people and automate decisions based on that profiling.

Steps to prepare for GDPR

This section describes steps a small business can take to help it get ready for GDPR. Much of the information for these steps was provided through [Seven steps for businesses to get ready for the General Data Protection Regulation](#), a publication provided through the Publications Office of the European Union.

A good way for a small business to get started with GDPR is to make sure to apply the following key principles when collecting personal data:

- Collect personal data with clearly defined purposes for what you are using it for, and don't use them for anything else. For example, if you tell your clients to give you their email addresses so they can get your new offers or promotions, you can only use their email addresses for only that specific purpose.
- Don't collect more data than you need. For example, if your business requires a mailing address for you to deliver goods, you need a customer's address and a name, but you don't need to know the person's marital status.

Step 1: Know the personal data that you collect and use within your business, and the reasons you need it

As a small business, one of the first steps you should take is to make an inventory of the personal data you collect and use within your business, and why it is needed. This includes data on both your employees and your customers.

For example, you may need your employee's personal data based on the employment contract and for legal reasons (for example, reporting taxes to the Internal Revenue Service).

As another example, you may manage lists of individual customers to send them notices about special offers, if

they have consented to this.

Microsoft 365 features that can help

[Microsoft Information Protection in Microsoft 365](#) can help you discover, classify, and protect sensitive information in your company. You can use trainable classifiers to help you identify and label document types that contain personal data.

Step 2: Inform your customers, employees, and other individuals when you need to collect their personal data

Individuals must know that you process their personal data and for which purpose. For example, if a customer needs to create a customer profile to access your business's online site, make sure you state specifically what you intend to do with their information.

But there is no need to inform individuals when they already know how you will use the data. For example, when they provide you a home address for a delivery they ordered.

You also have to be able to inform individuals on request about the personal data you hold on them and give them access to their data. Being organized with your data makes it easier to provide to them, if needed.

Step 3: Keep personal data for only as long as necessary

For employees data, keep it as long as the employment relationship remains and for related legal obligations. For customer data, keep it as long as the customer relationship lasts and for related legal obligations (for example, tax purposes). Delete the data when it is no longer needed for the purposes for which you collected it.

Microsoft 365 features that can help

[Retention policies and labels](#) can be used to help you keep personal data for a certain time and delete it when it's no longer needed.

Step 4: Secure the personal data you are processing

If you store personal data on an IT system, limit the access to the files containing the data, for example, by a strong password. Regularly update the security settings of your system.

NOTE

The GDPR does not prescribe the use of any specific IT system, but make that the system has the appropriate level of security. See [GDPR Article 32: Security of Processing](#) for more information.

If you store physical documents with personal data, make sure that they are not accessible by unauthorized persons.

If you choose to store personal data in the cloud, such as through Microsoft 365, you have security features such as the ability to help you to manage permissions to files and folders, centralized secure locations to save your files (OneDrive or SharePoint document libraries), and data encryption when sending or retrieving your files.

Microsoft 365 features that can help

You can use [Microsoft Data Loss Prevention \(DLP\)](#) to help to protect your business's sensitive information. You can [set up a DLP policy](#) that uses the [GDPR template](#).

Step 5: Keep documentation on your data processing activities

Prepare a short document explaining what personal data you hold and for what reasons. You might be required to make the documentation available to your national data protection authority if needed.

Such documents should include the information listed below.

INFORMATION	EXAMPLES
-------------	----------

INFORMATION	EXAMPLES
The purpose of data processing	Alerting customers about special offers such as providing home delivery; paying suppliers; salary and social security coverage for employees
The types of personal data	Contact details of customers; contact details of suppliers; employee data
The categories of data subjects concerned	Employees; customers; suppliers
The categories of recipients	Labor authorities; tax authorities
The storage periods	Employees' personal data until the end of the employment contract (and related legal obligations); customers' personal data until the end of the client/contractual relationship
The technical and organizational security measures to protect the personal data	IT system solutions regularly updated; secured location; access control; data encryption; data backup
Whether personal data is transferred to recipients outside the EU	Use of a processor outside the EU (for example, storage in the cloud); data location of the processor; contractual commitments

You can find Microsoft's contractual commitments with regard to the GDPR in the [Microsoft Online Services Data Protection Addendum](#), which provides Microsoft's privacy and security commitments, data processing terms and GDPR Terms for Microsoft-hosted services to which customers subscribe under a volume licensing agreement.

Step 6: Make sure your subcontractors respect the rules

If you sub-contract processing of personal data to another company, only use a service provider who guarantees the processing in compliance with the requirements of the GDPR (for instance, security measures).

Step 7: Assign someone to oversee personal data protection

To better protect personal data, organizations might have to appoint a **Data Protection Officer (DPO)**. However, you may not need to designate a Data Protection Officer if processing of personal data isn't a core part of your business, or if you are a small business. For example, if your business only collects data on your customers for home delivery, you should not need to appoint a DPO. Even if you need to make use of a DPO, these duties might be assigned to an existing employee in addition to his/her other tasks. Or you could choose to hire an external consultant for this duty as needed.

You normally don't need to carry out a [Data Protection Impact Assessment](#). This is reserved for businesses that pose more risk to personal data (for example, if they do a large-scale monitoring of a publicly accessible area, such as video-surveillance).

If you are a small business managing employee wages and a list of clients, you typically do not need to do a Data Protection Impact Assessment.

Common small business questions about the GDPR

I'm a sole proprietor - do I really have to worry about the GDPR?

The GDPR is about the data you process, not the number of employees you have. It affects companies of all sizes, even sole proprietors. However, companies with fewer than 250 employees do have some exemptions, such as reduced record keeping, but only if you are sure the data processing doesn't affect the individual's rights

and is occasional processing.

As an example, processing of non-personal data would be exempt or need reduced measures. However, if you process any data that is seen as "special category sensitive data", even if it only occasionally, you will have to record this data processing. The definition of "occasional processing" is vague, but it's meant to apply to data that is used once or rarely.

You should also make sure that personal data that you collect is protected. This means that you need to encrypt it and make sure that access to it is controlled using at least a password. Keeping your customer data on a spreadsheet on your desktop with no protection won't meet GDPR expectations.

How can I tell if our company website is GDPR compliant?

The first question to ask yourself is: Do you collect personal data anywhere on your site? For example, you might have a contact form that asks for a name and email address. If you want to send marketing emails, make sure you add an 'opt-in' checkbox that explains exactly what you will use the data for. Only if the recipient checks that box can you use their personal data for marketing purposes.

Also, check that the database that stores the data is protected. Your web hosting company or cloud storage vendor will be able to advise on this. If you use Microsoft 365 for business, storage of data is GDPR-compliant.

My company is outside Europe. Does the GDPR really affect us?

The GDPR is a regulation that protects EU citizens. If your company deals with EU citizens now, or you hope to in the future, you will be affected. This applies to both citizens living in an EU State and those living elsewhere.

Consider the following examples:

- A U.S. company that hires cars to EU citizens will need to satisfy GDPR requirements when they collect and process the customer's data. The company will be required to take consent when they take the customer's data and ensure that the data is stored securely. They will also need to make sure the customer can apply all of their data subject rights.
- An Australian company sells products online, and its users set up online accounts. GDPR data subject rights and consent will be applied to EU citizens who open an account. The company will need to make sure the customer can apply all of their data subject rights.
- An international charity collects data about donors and uses it to send out updates and requests for donations. The GDPR states: "...the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest." However, the responsibility is on the organization to prove their interests override those of the data subject. The company (or in this case, the charitable organization) should always get informed, explicit, opt-in consent.

The GDPR also applies if customer data moves across borders. If you use cloud computing for data storage, you will need to make sure the service is fully GDPR-compliant. It can get complicated if data storage is in locations that have a poor record of data protection. If you use Microsoft 365 for business, we have the correct legal documentation in place to cover GDPR requirements.

Sure, I collect data, but some other company stores it. Does that get me off the hook?

Under the GDPR, if you collect data you are affected to some extent. The GDPR has the concept of a data processor and a data controller:

- **Data Controller:** An individual or organization (you can have joint controllers) that decides how, what, and why data is collected. They may store it using another company's cloud servers. For example, a website that collects customer data is a controller.
- **Data Processor:** An individual or organization that stores data on behalf of the controller(s) and processes these data upon request. For example, Microsoft 365 Apps for business data storage acts as a processor and is fully GDPR compliant.

An organization or system can act as both a controller and a processor. Microsoft 365 for business can act as both and complies with the GDPR.

Can I still send out marketing emails to my old customers?

You need to make sure your customers, even ones that you've had for years, have consented to use their data for marketing. You may have previously captured consent, as well as a record to show it. If so, you're all set to continue marketing. If not, you need to get permission from the customer to continue marketing to them. This usually involves sending an email asking customers to go to your site and select an option to consent to receive future emails.

Do I have to worry about the GDPR when I recruit new employees? What about current employees?

The GDPR doesn't just affect customer data; it extends to employee data, too. New recruits are often located using social media platforms such as LinkedIn. Make sure that you don't store any potential recruit data without their express permission.

As for existing employees and new employee contracts, a signature at the end of a contract does not necessarily assume consent, especially when a non-affirmative clause is used in a contract. In this case, you must capture consent in an explicit manner associated with the clause. What this means depends on your employee contract, but you can use "legitimate interest" in some cases and add an employee data processing notice to make sure your employees are aware of what you will do with their data.

Satisfy privacy concerns using Microsoft 365 for business

Becoming compliant with the GDPR is about making sure that personal data is protected. The GDPR has a concept known as Privacy by Design and Default. This means that data protection should be "baked in" to a system and a product so that satisfying privacy concerns is second nature.

Like their larger counterparts, a small business needs convenience without sacrificing security. Microsoft 365 for business is designed for companies of fewer than 300 employees. Small companies can use Microsoft cloud-based tools to improve business productivity. With Microsoft 365 for business, a small business can manage emails, documentation, and even meetings and events. It also has built-in security measures and device management, which are vital for GDPR compliance.

Microsoft 365 for business can help you with the GDPR process in the following ways:

- **Discover:** An important step to GDPR compliance is knowing what data you have.
- **Manage:** Controlling access to data and managing its use is an integral part of GDPR. Microsoft 365 for business protects business data based on policies you want to apply to devices. Device management is vital in an age where employees work remotely. Microsoft 365 for business includes device management features that makes sure data is protected across all devices. For example, you can specify that all Windows 10 devices in your business are protected via Windows Defender.
- **Protect:** Microsoft 365 for business is designed for security. Its device management and data protection controls work across your business network, including remote devices, to help keep data secure. Microsoft 365 for business offers controls such as privacy settings in Office applications and encryption of documents. With Microsoft 365 for business, you can perform GDPR compliance monitoring to make sure you have the right level of protection set.
- **Report:** The GDPR places a lot of emphasis on reporting. Even a business with a single employee, if that business processes large amounts of data, is required to document and report on their procedures. Microsoft 365 for business takes the headache out of reporting requirements for smaller organizations.

Tools such as audit logs allow you to track and report on data movement. Reports include classifying the data you collect and store, what you do with the data, and transfers of the data.

Customers, employees, and clients are becoming more aware of the importance of data privacy and now expect a company or organization to respect that privacy. Microsoft 365 for business provides you with the tools to achieve and maintain GDPR compliance without a massive upheaval to your business.

Next steps

To get ready for the GDPR, here are some suggestions for next steps to take:

- Evaluate your GDPR program with [Accountability Readiness Checklists](#).
- Investigate [Microsoft 365 for business](#) as a solution for achieving and maintaining compliance with GDPR.

IMPORTANT

Get legal advice appropriate for your company or organization.

Additional resources

[Microsoft Trust Center overview of the GDPR](#)

The Official Microsoft Blog: [Microsoft commitment to GDPR](#)

European Commission sites:

- [Data protection](#)
- [2018 reform of EU data protection rules](#)

Options for protecting your devices and app data

4/3/2021 • 2 minutes to read • [Edit Online](#)

You have several ways to secure your organizations devices and data on them with Microsoft 365 for business and enterprise. You can use the following stand-alone plans:

- Intune (a part of Microsoft Endpoint Management)
- Azure Active Directory Premium plans.
- Basic Mobility and Security (included in most Microsoft 365 for business and enterprise plans) Or use the subscriptions that include some, or all of the previous standalone plans.
- A Microsoft 365 Business Premium subscription, which includes security and threat protection for small business under 300 users.
- Microsoft 365 Enterprise plans that include advanced security and threat protection.

Device management options

- **Basic Mobility and Security** is offered with most Microsoft 365 plans, and is the only built-in choice offered for Microsoft 365 Business Standard and Microsoft 365 Business Basic. For more information, see [availability of Basic Mobility and Security](#).

If you have either Microsoft 365 Business Basic or Microsoft 365 Business Standard, you can also purchase Intune if your organization has more complex security needs.

- **Microsoft Intune** is a stand-alone plan that is also included with some Microsoft 365 for business or enterprise plans. If you have Intune either as a stand-alone or a part of your subscription, it provides ability to fine-tune your device and app-data management. For more information on availability with Microsoft 365, see [availability of Intune](#).

Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You control how your organization's devices are used, including mobile phones, tablets, and laptops. You can also configure specific policies to control applications. For more information, see [Microsoft Intune documentation](#).

- **Azure Active Directory (AD) Premium** plans are standalone plans that also come with some of the Microsoft 365 for business and enterprise plans. For more information, see [Azure AD pricing](#).

Azure AD Premium P1 and Azure AD Premium P2 allow you to set conditional access features, self-service password reset, etc. For more information on the capabilities of the Premium plans, see [Azure AD pricing](#) page.

- **Microsoft 365 Business Premium** includes Intune and Azure Active Directory Premium P1 and Office 365 Advanced Threat Protection.

Microsoft 365 Business Premium offers a set of policy templates for securing your devices and app data. It offers a good level of security and threat protection for most businesses under 300 users. For more information, see [set up Microsoft 365 Business Premium in the setup wizard, secure Windows 10 computers](#), and [Microsoft 365 Business Premium security and compliance features](#).

- **Microsoft 365 for enterprise** subscriptions include Microsoft Intune and E5 also includes the Azure AD premium plans 1 and 2.

Microsoft 365 E5 offers the highest level of security and threat protection of all the Microsoft 365 subscriptions. For more information, see [Microsoft 365 for enterprise overview](#).

View and manage policies and devices

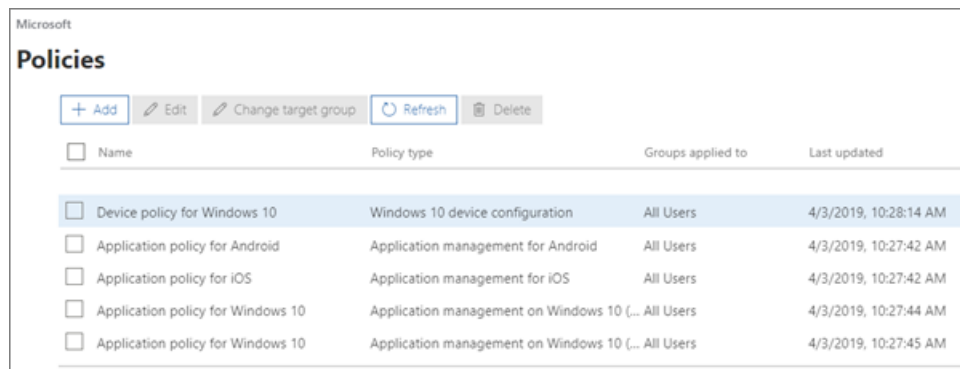
4/3/2021 • 2 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

View and edit device policies

1. Go to the admin center at <https://admin.microsoft.com>.
2. On the left nav, choose **Devices** > **Policies**.

On this page, you can create, edit, change target group, or delete a policy.

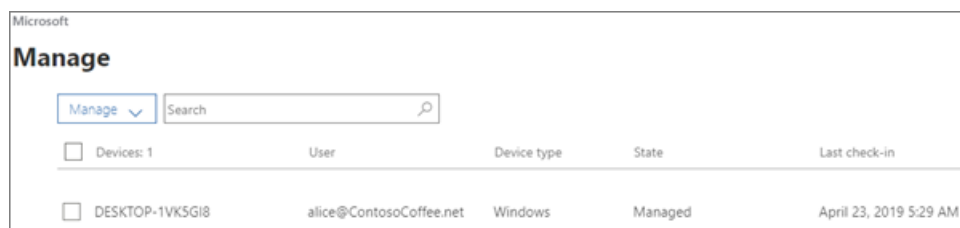


<input type="checkbox"/>	Name	Policy type	Groups applied to	Last updated
<input checked="" type="checkbox"/>	Device policy for Windows 10	Windows 10 device configuration	All Users	4/3/2019, 10:28:14 AM
<input type="checkbox"/>	Application policy for Android	Application management for Android	All Users	4/3/2019, 10:27:42 AM
<input type="checkbox"/>	Application policy for iOS	Application management for iOS	All Users	4/3/2019, 10:27:42 AM
<input type="checkbox"/>	Application policy for Windows 10	Application management on Windows 10 (... All Users	All Users	4/3/2019, 10:27:44 AM
<input type="checkbox"/>	Application policy for Windows 10	Application management on Windows 10 (... All Users	All Users	4/3/2019, 10:27:45 AM

View and manage devices

1. On the left nav, choose **Devices** > **Manage**.

On this page, you can select one or more devices and remove company data. For Windows 10 devices that you have set device protections settings for, you can also choose to reset the device to factory settings.



<input type="checkbox"/>	Devices: 1	User	Device type	State	Last check-in
<input type="checkbox"/>	DESKTOP-1VKSGI8	alice@ContosoCoffee.net	Windows	Managed	April 23, 2019 5:29 AM

Remove company data from devices

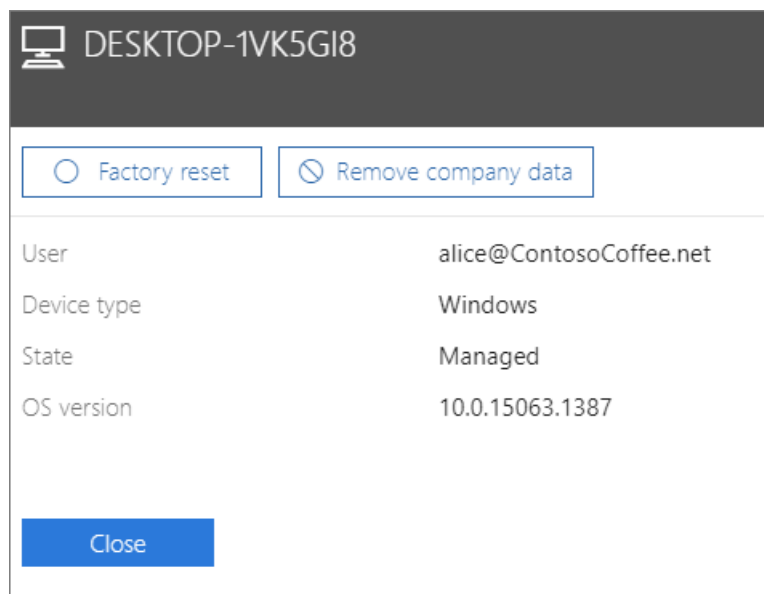
4/3/2021 • 2 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

Remove company data

You can use Microsoft 365 for business to remove company data that your users have on their [devices](#) or [Windows PCs](#) that are protected by Microsoft 365. **If you remove company data from a device, you cannot restore it later.**

1. Go to the admin center at <https://admin.microsoft.com>.
2. On the left nav, choose **Devices** > **Manage**.
3. On the **Manage** page, choose or search for a user who's data you want to remove, and choose the name.
4. On the next pane, select the device or devices from the **Devices** list. On the device pane that opens, you can choose to reset the device to factory settings or remove company data, depending on the device type.



5. On the confirmation pane, choose **Confirm** > **Close**.

Reset Windows 10 devices to their factory settings

4/3/2021 • 2 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

A factory reset reverts a device to the original settings it had when the device was purchased. All apps and data on the device that were installed after purchase are removed. You can use Microsoft 365 for business to factory reset Windows 10 devices you manage.

1. Go to the admin center at <https://admin.microsoft.com>.
2. In the left nav, choose **Devices > Manage**.
3. On the **Manage** page, check the checkbox next to the device you want to remove data from and then, in the **Manage** drop-down choose **Factory reset**.
4. On the **Are you sure you want to factory reset the devices below** pane, choose **Confirm > Close**.

How do protection features in Microsoft 365 Business Premium map to Intune settings

4/3/2021 • 6 minutes to read • [Edit Online](#)

Android and iOS application protection settings

The following table details how the Android and iOS application policy settings map to Intune settings.

To find the Intune setting, sign in with your Microsoft 365 Business Premium admin credentials, and go to **Admin centers**, and then **Intune**.

IMPORTANT

A Microsoft 365 Business Premium subscription gives you a license to modify all the Intune settings. See [Introduction to Intune to get started](#).

Select the Policy name you want — for example, Application policy for Android — and then choose **Policy settings**.

Under **Protect work files when devices are lost or stolen**

ANDROID OR IOS APPLICATION POLICY SETTING	INTUNE SETTING(S)
Delete work files from an inactive device after	Offline interval (days) before app data is wiped
Force users to save work files to OneDrive for Business Note that only OneDrive for Business is allowed	Select which storage services corporate data can be saved to

Under **Manage how user access Office files in mobile devices**

ANDROID OR IOS APPLICATION POLICY SETTING	INTUNE SETTING(S)
Delete work files from an inactive device after	Offline interval (days) before app data is wiped
Force users to save work files to OneDrive for Business Note that only OneDrive for Business is allowed	Select which storage services corporate data can be saved to
Encrypt work files	Encrypt app data
Under Manage how user access Office files in mobile devices	
Require a PIN or fingerprint to access Office apps	Require PIN to access This also sets: Allow simple PIN to Yes Pin Length to 4 Allow fingerprint instead of PIN to Yes Disable app PIN when device PIN is managed to No

ANDROID OR IOS APPLICATION POLICY SETTING	INTUNE SETTING(S)
Reset PIN when login fails this many times (this is disabled if PIN isn't required)	Number of attempts before PIN reset
Require users to sign in again after Office apps have been idle for (this is disabled if PIN isn't required)	Recheck the access requirements after (minutes) This also sets: Timeout is set to minutes This is same number of minutes you set in Microsoft 365 Business. Offline grace period is set to 720 minutes by default
Deny access to work files on jailbroken or rooted devices	Block managed apps from running on jailbroken or rooted devices
Allow users to copy content from Office apps into personal apps	Restrict cut, copy, and paste with other apps If the Microsoft 365 Business Premium option is set to On , then these three options are also set to All Apps in Intune: Allow app to transfer data to other apps Allow app to receive data from other apps Restrict cut, copy, and paste with other apps If the Microsoft 365 Business option is set to On , then all the Intune options are set to: Allow app to transfer data to other apps is set to Policy managed apps Allow app to receive data from other apps is set to All Apps Restrict cut, copy, and paste with other apps is set to Policy Managed apps with Paste-In

Windows 10 app protection settings

The following table details how the Windows 10 application policy settings map to Intune settings.

To find the Intune setting, sign in with your Microsoft 365 Business Premium admin credentials, and go to [Azure portal](#). Select **More services**, and type Intune into the Filter. Select **Intune App Protection > App Policy**.

IMPORTANT

A Microsoft 365 Business Premium subscription gives you a license to modify only the Intune settings that map to the settings available in Microsoft 365 Business Premium.

To explore the available settings, select the policy name you want, and then choose **General**, **Assignments**, **Allowed apps**, **Exempt apps**, **Required settings**, or **Advanced settings** from the left navigation pane.

WINDOWS 10 APPLICATION POLICY SETTING	INTUNE SETTING(S)
Encrypt work files	Advanced settings > Data protection: Revoke encryption keys on unenroll and Revoke access to protected data device enrolls to MDM are both set to On .
Prevent users from copying company data to personal files.	Required settings > Windows Information Protection mode. On in Microsoft 365 Business Premium maps to: Hide Overrides , Off in Microsoft 365 Business Premium maps to: Off .

WINDOWS 10 APPLICATION POLICY SETTING	INTUNE SETTING(S)
Office documents access control	<p>If this is set to On in Microsoft 365 Business Premium, then Advanced settings > Access, Use Windows Hello for Business as a method for signing into Windows is set to On, with the following additional settings:</p> <p>Set the minimum number of characters required for the PIN is set to 4.</p> <p>Configure the use of uppercase letters in the Windows Hello for Business PIN is set to Do not allow use of upper case letters for PIN.</p> <p>Configure the use of lowercase letters in the Windows Hello for Business PIN is set to Do not allow use of lower case letters for PIN.</p> <p>Configure the use of special characters in the Windows Hello for Business PIN is set to Do not allow the use of special characters in PIN.</p> <p>Specify the period of time (in days) that a PIN can be used before the system requires the user to change is set to 0.</p> <p>Specify the number of past PINs that can be associated to a user account that can't be reused is set to 0.</p> <p>Number of authentication failures allowed before the device will be wiped is set to same as in Microsoft 365 Business (5 by default).</p> <p>Maximum amount of time (in minutes) allowed after the device is idle that will cause the device to become PIN or password locked is set to same as in Microsoft 365 Business.</p>
Enable recovery of protected data	Advanced settings > Data protection: Show the enterprise data protection icon and Use Azure RMS for WIP are set to On .
Protect additional company cloud locations	Advanced settings > Protected domains and Cloud resources show domains and SharePoint sites.
Files used by these apps are protected	The list of protected apps is listed in Allowed apps .

Windows 10 device protection settings

The following table details how the Windows 10 device configuration settings map to Intune settings.

To find the Intune setting, sign in with your Microsoft 365 Business Premium admin credentials, and go to [Azure portal](#), then select **More services**, and type in Intune into the **Filter**, select **Intune > Device configuration > Profiles**. Then select **Device policy for Windows 10 > Properties > Settings**.

WINDOWS 10 DEVICE POLICY SETTING	INTUNE SETTING(S)
Help protect PCs from viruses and other threats using Windows Defender Antivirus	<p>Allow Real-time Monitoring = ON</p> <p>Allow Cloud Protection = ON</p> <p>Prompt Users for Samples Submission = Send Safe samples automatically (Default Non PII auto submit)</p>
Help protect PCs from web-based threats in Microsoft Edge	SmartScreen in Edge Browser settings is set to Required .

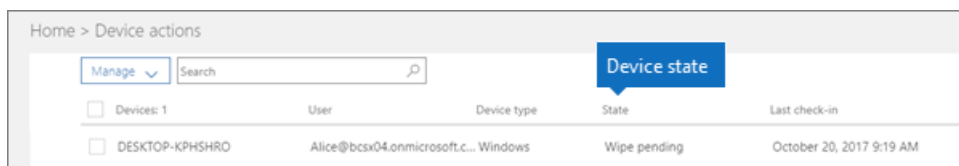
WINDOWS 10 DEVICE POLICY SETTING	INTUNE SETTING(S)
Turn off device screen when idle for (minutes)	Maximum minutes of inactivity until screen locks (minutes)
Allow users to download apps from Microsoft Store	Custom URI policy
Allow users to access Cortana	General > Cortana is set to block in Intune when set to off in Microsoft 365 Business Premium.
Allow users to receive Windows tips and advertisements from Microsoft	Windows spotlight , all blocked if this is set to off in Microsoft 365 Business Premium.
Keep Windows 10 devices up to date automatically	<p>This setting is in Microsoft Intune > Service updates - Windows 10 Update Rings, choose Update policy for Windows 10 devices, and then Properties > Settings. When the Microsoft 365 Business Premium setting is set to On, all the following settings are set:</p> <p>Service branch is set to CB (CBB when this is turned off in Microsoft 365 Business Premium).</p> <p>Microsoft product updates is set to Allow.</p> <p>Windows drivers is set to Allow.</p> <p>Automatic update behavior is set to Auto install at maintenance time with:</p> <p>After hours start is set to 6 AM.</p> <p>Active hours end is set to 10 PM.</p> <p>Quality update deferral period (days) is set to 0.</p> <p>Feature update deferral period (days) is set to 0.</p> <p>Delivery optimization download mode is set to HTTP blended with peering behind same NAT.</p>

Device states

4/3/2021 • 2 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

Devices in the **Device actions** list (Admin home > **Device actions**) can have the following states.



Devices	User	Device type	State	Last check-in
<input type="checkbox"/> DESKTOP-KPHSHRO	Alice@bcsx04.onmicrosoft.c...	Windows	Wipe pending	October 20, 2017 9:19 AM

STATUS	DESCRIPTION
Managed by Intune	Managed by Microsoft 365 Business Premium.
Retire pending	Microsoft 365 Business Premium is getting ready to remove company data from the device.
Retire in progress	Microsoft 365 Business Premium is currently removing company data from the device.
Retire failed	Remove company data action failed.
Retire canceled	Retire action was canceled.
Wipe pending	Waiting for factory reset to start.
Wipe in progress	Factory reset has been issued.
Wipe failed	Couldn't do factory reset.
Wipe canceled	Factory wipe was canceled.
Unhealthy	An action is pending (or in progress), but the device hasn't checked in for 30+ days.
Delete pending	Delete action is pending.
Discovered	Microsoft 365 Business Premium has detected the device.

Set or edit application protection settings for Windows 10 devices

4/3/2021 • 2 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

Edit an app management policy for Windows 10

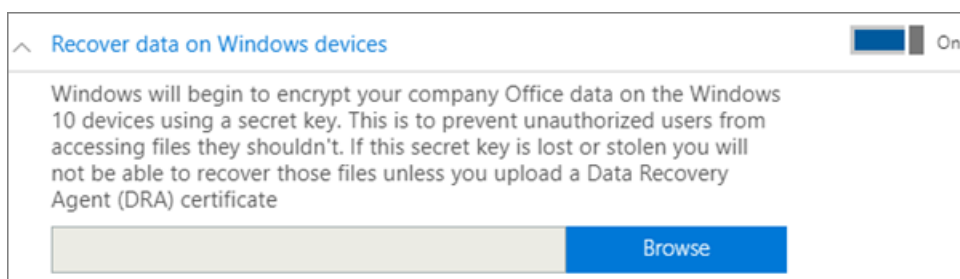
1. Go to the admin center at <https://admin.microsoft.com>.
2. On the left nav, choose **Devices** > **Policies** .
3. Choose an existing Windows app policy and then **Edit**.
4. Choose **Edit** next to a setting you want to change and then **Save**.

Create an app management policy for Windows 10

If your users have personal Windows 10 devices on which they perform work tasks, you can protect your data on those devices as well.

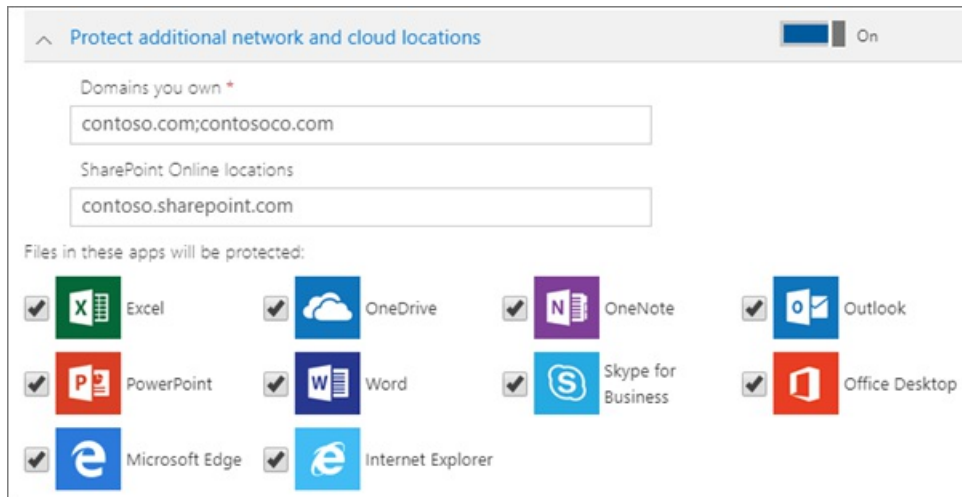
1. Go to the admin center at <https://admin.microsoft.com>.
2. On the left nav, choose **Devices** > **Policies** > **Add**.
3. On the **Add policy** pane, enter a unique name for this policy.
4. Under **Policy type**, choose **Application Management for Windows 10**.
5. Under **Device type**, choose either **Personal** or **Company Owned**.
6. The **Encrypt work files** is turned on automatically.
7. Set **Prevent users from copying company data to personal files and force them to save work files to OneDrive for Business** to **On** if you don't want the users to save work files on their PC.
8. Expand **Recover data on Windows devices**. We recommend that you turn it **On**. Before you can browse to the location of the Data Recovery Agent certificate, you have to first create one. For instructions, see [Create and verify an Encrypting File System \(EFS\) Data Recovery Agent \(DRA\) certificate](#).

By default, work files are encrypted using a secret key that is stored on the device and associated with the user's profile. Only the user can open and decrypt the file. However, if a device is lost or a user is removed, a file can be stuck in an encrypted state. An admin can use the Data Recovery Agent (DRA) certificate to decrypt the file.



9. Expand **Protect additional network and cloud locations** if you want to add additional domains or SharePoint Online locations to make sure that files in all the listed apps are protected. If you need to enter

more than one item for either field, use a semicolon (;) between the items.



10. Next decide **Who will get these settings?** If you don't want to use the default **All Users** security group, choose **Change**, choose the security groups who will get these settings > **Select**.
11. Finally, choose **Add** to save the policy, and assign it to devices.

Set app protection settings for Android or iOS devices

6/14/2021 • 3 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

Create an app management policy

1. Go to the admin center at <https://admin.microsoft.com>.
2. In the left nav, choose **Devices** > **Policies** > **Add**.
3. On the **Add policy** pane, enter a unique name for this policy.
4. Under **Policy type**, choose **Application Management for Android** or **Application Management for iOS**, depending on which set of policies you want to create.
5. Expand **Protect work files when devices are lost or stolen** and **Manage how users access Office files on mobile devices**. Configure the settings how you would like. **Manage how users access Office files on mobile devices** is **Off** by default, but we recommend that you turn it **On** and accept the default values. For more information, see [Available settings](#).

You can always use the **Reset default settings** link to return to the default setting.

+ Add policy

Policy name *

Enter a policy name

Policy type

Application Management for Android

^ Protect work files when devices are lost or stolen ⓘ On

Delete work files from an inactive device after days

Force users to save all work files to OneDrive for Business On

Encrypt work files On

[Restore default settings](#)

^ Manage how users access Office files on mobile devices ⓘ Off

Require a PIN or fingerprint to access Office apps Off

Reset PIN when login fails this many times

Require users to sign in again after Office apps have been idle for minutes

Deny access to work files on [jailbroken or rooted devices](#) Off

Allow users to copy content from Office apps into personal apps Off

- Next decide **Who will get these settings?** If you don't want to use the default **All Users** security group, choose **Change**, choose the security groups that get these settings > **Select**.
- Finally, choose **Done** to save the policy, and assign it to devices.

Edit an app management policy

- On the **Policies** card, choose **Edit policy**.
- On the **Edit policy** pane, choose the policy you want to change
- Choose **Edit** next to each setting to change the values in the policy. When you change a value, it's automatically saved in the policy.
- When you're finished, close the **Edit policy** pane.

Delete an app management policy

- On the **Policies** page, choose a policy and then **Delete**.
- On the **Delete policy** pane, choose **Confirm** to delete the policy or policies you chose.

Available settings

The following tables give detailed information about settings available to protect work files on devices and the settings that control how users access Office files from their mobile devices.

For more information, see [How do protection features in Microsoft 365 Business Premium map to Intune settings](#).

Settings that protect work files

The following settings are available to protect work files if a user's device is lost or stolen:

SETTING	DESCRIPTION
Delete work files from an inactive device after this many days	If a device isn't used for the number of days that you specify here, any work files stored on the device will be deleted automatically.
Force users to save all work files to OneDrive for Business	If this setting is On , the only available save location for work files is OneDrive for Business.
Encrypt work files	Keep this setting On so that work files are protected by encryption. Even if the device is lost or stolen, no one can read your company data.

Settings that control how users access Office files on mobile devices

The following settings are available to manage how users access Office work files:

SETTING	DESCRIPTION
Require a PIN or fingerprint to access Office apps	If this setting is On users must provide another form of authentication, in addition to their username and password, before they can use Office apps on their mobile devices.

SETTING	DESCRIPTION
Reset PIN when login fails this many times	To prevent an unauthorized user from randomly guessing a PIN, the PIN will reset after the number of wrong entries that you specify.
Require users to sign in again after Office apps have been idle for	This setting determines how long a user can be idle before they're prompted to sign in again.
Deny access to work files on jailbroken or rooted devices	Clever users may have a device that is jailbroken or rooted. This means that the user can modify the operating system, which can make the device more subject to malware. These devices are blocked when this setting is On .
Don't allow users to copy content from Office apps into personal apps	We do allow this by default, but if the setting is On , the user could copy information in a work file to a personal file. If the setting is Off , the user will be unable to copy information from a work account into a personal app or personal account.

Validate app protection settings on Android or iOS devices

7/8/2021 • 7 minutes to read • [Edit Online](#)

Follow the instructions in the following sections to validate app protection settings on Android or iOS devices.

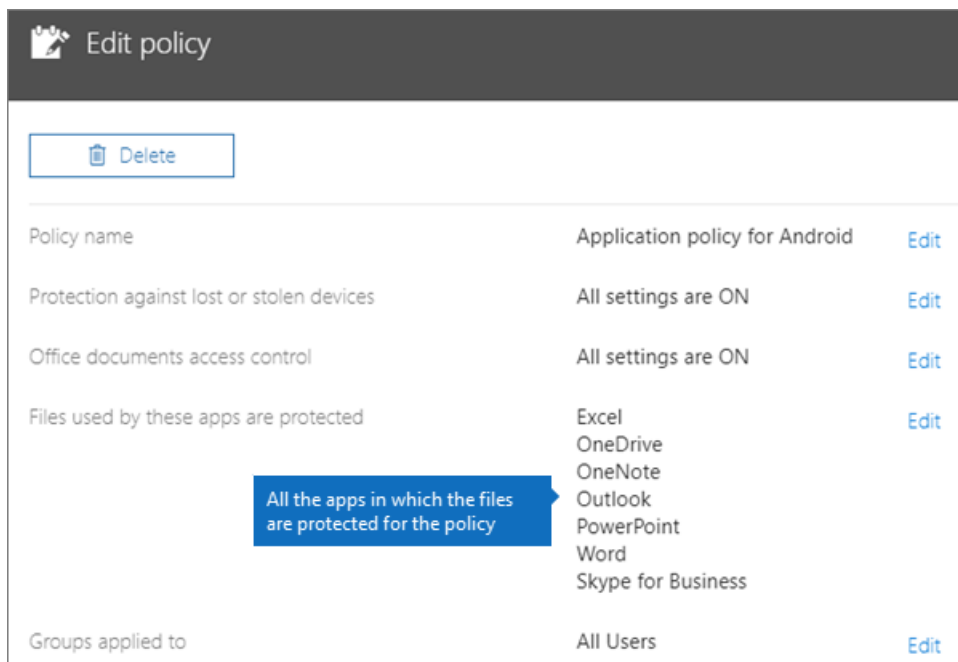
Android

Check that the app protection settings are working on user devices

After you [set app configurations for Android devices](#) to protect the apps, you can follow these steps to validate that the settings you chose work.

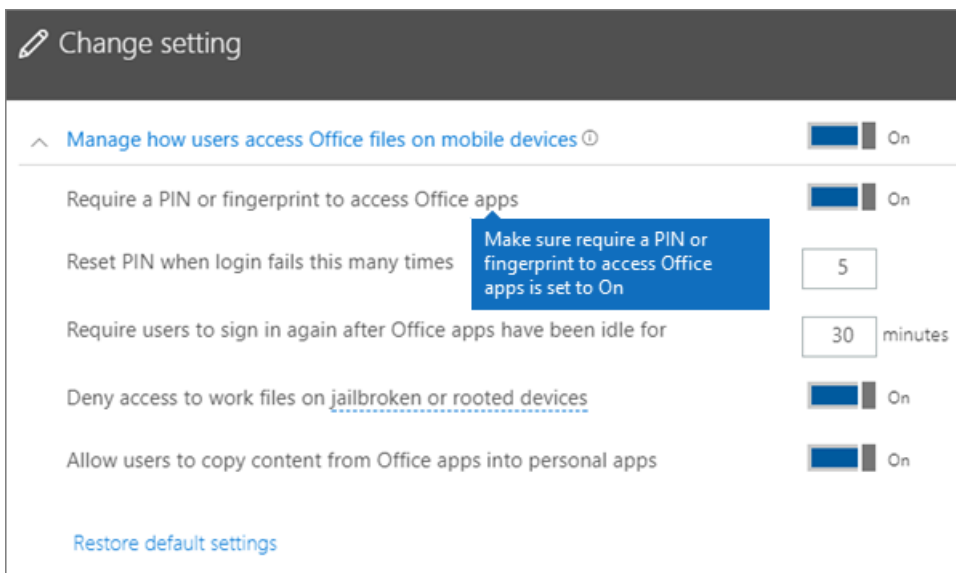
First, make sure that the policy applies to the app in which you're going to validate it.

1. In the Microsoft 365 Business Premium [admin center](#), go to **Policies > Edit policy**.
2. Choose **Application policy for Android** for the settings you created at setup, or another policy you created, and verify that it's enforced for Outlook, for example.

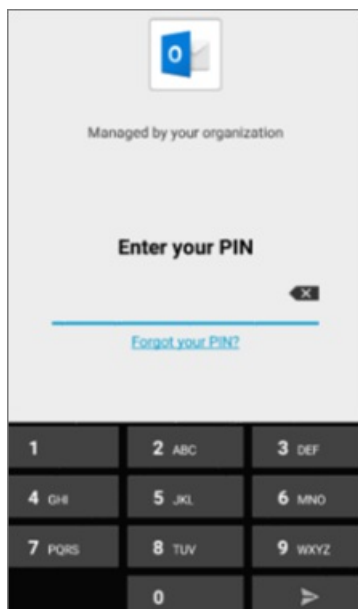


Validate Require a PIN or a fingerprint to access Office apps

In the **Edit policy** pane, choose **Edit** next to **Office documents access control**, expand **Manage how users access Office files on mobile devices**, and make sure that **Require a PIN or fingerprint to access Office apps** is set to **On**.



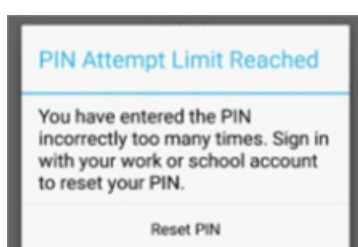
1. In the user's Android device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials.
2. You'll also be prompted to enter a PIN or use a fingerprint.



Validate Reset PIN after number of failed attempts

In the Edit policy pane, choose Edit next to Office documents access control, expand Manage how users access Office files on mobile devices, and make sure that Reset PIN after number of failed attempts is set to some number. This is 5 by default.

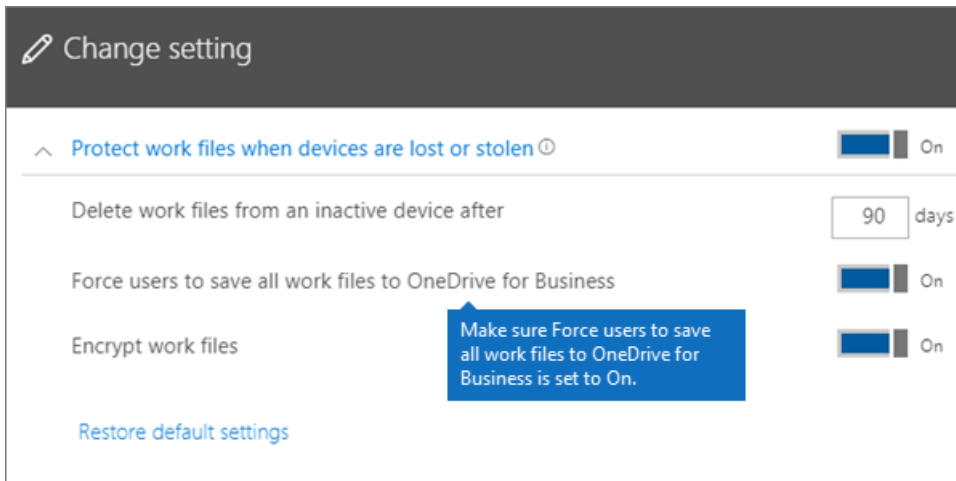
1. In the user's Android device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials.
2. Enter an incorrect PIN as many times as specified by the policy. You'll see a prompt that states **PIN Attempt Limit Reached** to reset the PIN.



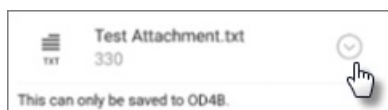
3. Press **Reset PIN**. You'll be prompted to sign in with the user's Microsoft 365 Business Premium credentials, and then required to set a new PIN.

Validate Force users to save all work files to OneDrive for Business

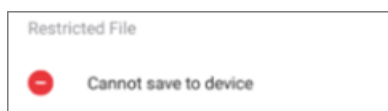
In the **Edit policy** pane, choose **Edit** next to **Protection against lost or stolen devices**, expand **Protect work files when devices are lost or stolen**, and make sure that **Force users to save all work files to OneDrive for Business** is set to **On**.



1. In the user's Android device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials, and enter a PIN if requested.
2. Open an email that contains an attachment and tap the down arrow icon next to the attachment's information.



You'll see **Cannot save to device** on the bottom of the screen.



NOTE

Saving to OneDrive for Business is not enabled for Android at this time, so you can only see that saving locally is blocked.

Validate Require user to sign in again if Office apps have been idle for a specified time

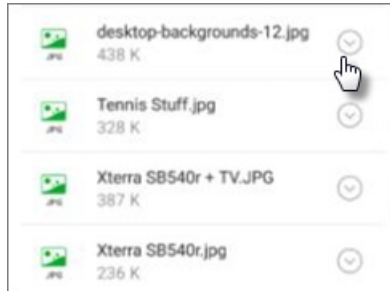
In the **Edit policy** pane, choose **Edit** next to **Office documents access control**, expand **Manage how users access Office files on mobile devices**, and make sure that **Require users to sign in again after Office apps have been idle for** is set to some number of minutes. This is 30 minutes by default.

1. In the user's Android device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials, and enter a PIN if requested.
2. You should now see Outlook's inbox. Let the Android device idle untouched for at least 30 minutes (or some other amount of time, longer than what you specified in the policy). The device will likely dim.
3. Access Outlook on the Android device again.
4. You'll be prompted to enter your PIN before you can access Outlook again.

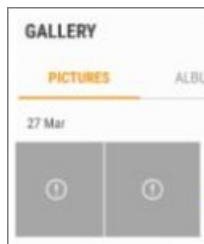
Validate Protect work files with encryption

In the **Edit policy** pane, choose **Edit** next to **Protection against lost or stolen devices**, expand **Protect work files when devices are lost or stolen**, and make sure that **Protect work files with encryption** is set to **On**, and **Force users to save all work files to OneDrive for Business** is set to **Off**.

1. In the user's Android device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials, and enter a PIN if requested.
2. Open an email that contains a few image file attachments.
3. Tap the down arrow icon next to the attachment's info to save it.



4. You may be prompted to allow Outlook to access photos, media, and files on your device. Tap **Allow**.
5. At the bottom of the screen, choose to **Save to Device** and then open the **Gallery** app.
6. You should see an encrypted photo (or more, if you saved multiple image file attachments) in the list. It may appear in the Pictures list as a gray square with a white exclamation point within a white circle in the center of the gray square.



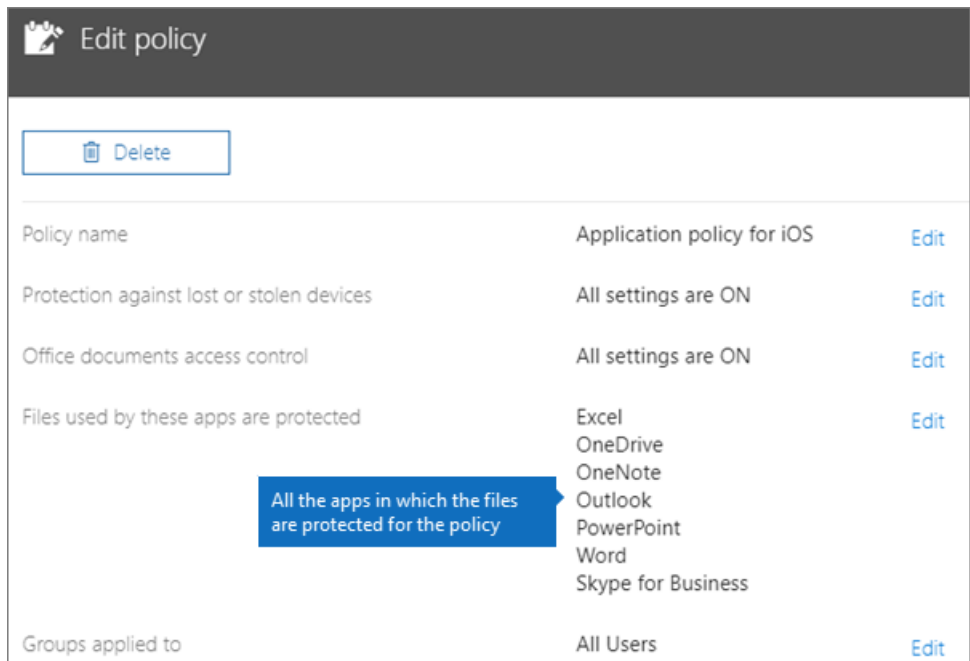
iOS

Check that the App protection settings are working on user devices

After you [set app configurations for iOS devices](#) to protect apps, you can follow these steps to validate that the settings you chose work.

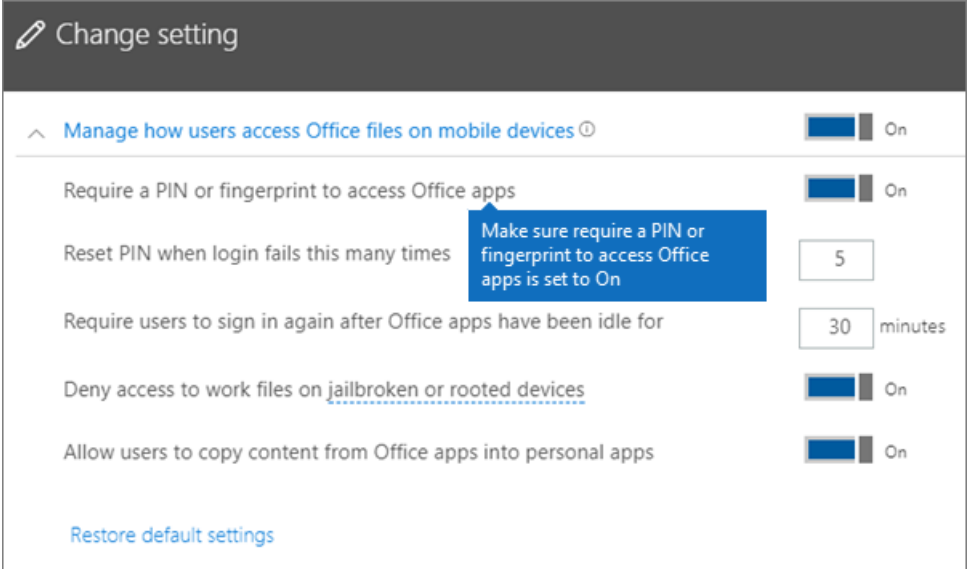
First, make sure that the policy applies to the app in which you're going to validate it.

1. In the Microsoft 365 Business Premium [admin center](#), go to **Policies > Edit policy**.
2. Choose **Application policy for iOS** for the settings you created at setup, or another policy you created, and verify that it's enforced for Outlook for example.

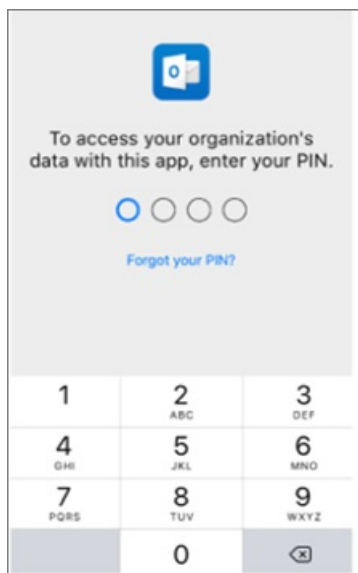


Validate Require a PIN to access Office apps

In the **Edit policy** pane, choose **Edit** next to **Office documents access control**, expand **Manage how users access Office files on mobile devices**, and make sure that **Require a PIN or fingerprint to access Office apps** is set to **On**.



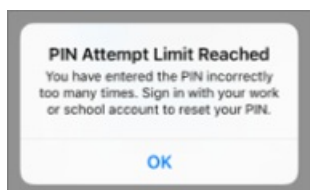
1. In the user's iOS device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials.
2. You'll also be prompted to enter a PIN or use a fingerprint.



Validate Reset PIN after number of failed attempts

In the Edit policy pane, choose Edit next to Office documents access control, expand Manage how users access Office files on mobile devices, and make sure that Reset PIN after number of failed attempts is set to some number. This is 5 by default.

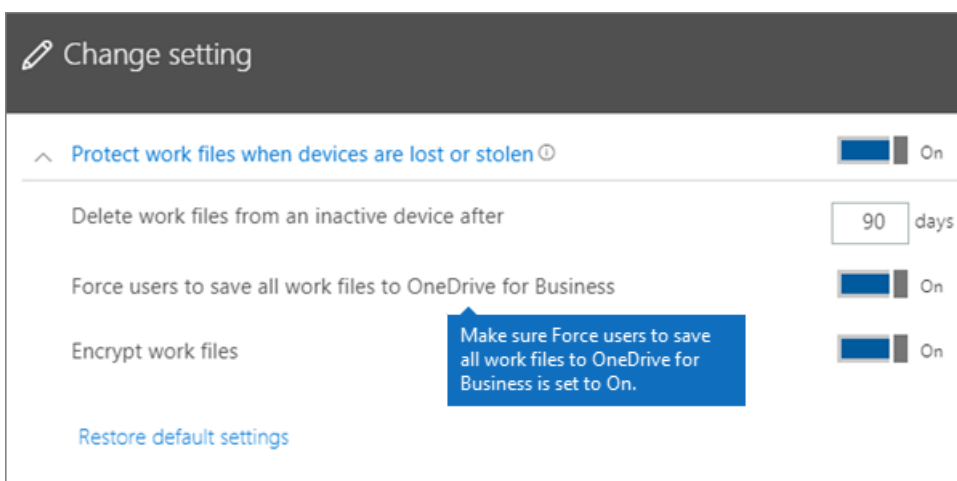
1. In the user's iOS device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials.
2. Enter an incorrect PIN as many times as specified by the policy. You'll see a prompt that states **PIN Attempt Limit Reached** to reset the PIN.



3. Press OK. You'll be prompted to sign in with the user's Microsoft 365 Business Premium credentials, and then required to set a new PIN.

Validate Force users to save all work files to OneDrive for Business

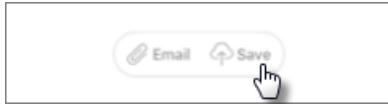
In the Edit policy pane, choose Edit next to Protection against lost or stolen devices, expand Protect work files when devices are lost or stolen, and make sure that Force users to save all work files to OneDrive for Business is set to On.



1. In the user's iOS device, open Outlook and sign in with the user's Microsoft 365 Business Premium

credentials, and enter a PIN if requested.

2. Open an email that contains an attachment, open the attachment and choose **Save** on the bottom of the screen.



3. You should only see an option for OneDrive for Business. If not, tap **Add Account** and select **OneDrive for Business** from the **Add Storage Account** screen. Provide the end user's Microsoft 365 Business Premium to sign in when prompted.

Tap **Save** and select **OneDrive for Business**.

Validate Require user to sign in again if Office apps have been idle for a specified time

In the **Edit policy** pane, choose **Edit** next to **Office documents access control**, expand **Manage how users access Office files on mobile devices**, and make sure that **Require users to sign in again after Office apps have been idle for** is set to some number of minutes. This is 30 minutes by default.

1. In the user's iOS device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials, and enter a PIN if requested.
2. You should now see Outlook's inbox. Let the iOS device untouched for at least 30 minutes (or some other amount of time, longer than what you specified in the policy). The device will likely dim.
3. Access Outlook on the iOS device again.
4. You'll be prompted to enter your PIN before you can access Outlook again.

Validate Protect work files with encryption

In the **Edit policy** pane, choose **Edit** next to **Protection against lost or stolen devices**, expand **Protect work files when devices are lost or stolen**, and make sure that **Protect work files with encryption** is set to **On**, and **Force users to save all work files to OneDrive for Business** is set to **Off**.

1. In the user's iOS device, open Outlook and sign in with the user's Microsoft 365 Business Premium credentials, and enter a PIN if requested.
 2. Open an email that contains a few image file attachments.
 3. Tap the attachment and then tap the **Save** option under it.
 4. Open **Photos** app from the home screen. You should see an encrypted photo (or more, if you saved multiple image file attachments) saved, but encrypted.
-

Edit or create device protection settings for Windows 10 PCs

6/14/2021 • 3 minutes to read • [Edit Online](#)

This article applies to Microsoft 365 Business Premium.

After you have set up default Windows protection settings on the Setup page, you can add new ones that apply to either all users, or a set of users. You can also edit any of the ones you have created.

Create protection settings for Windows 10 devices

View a video on how to secure Windows 10 devices with Microsoft 365 Business Premium:

1. Go to the admin center at <https://admin.microsoft.com>.
2. On the left nav, choose **Devices** > **Policies** > **Add**.
3. On the **Add policy** pane, enter a unique name for this policy.
4. Under **Policy type**, choose **Windows 10 Device Configuration**.
5. Expand **Secure Windows 10 Devices** > configure the settings how you would like. For more information, see [Available settings](#).

You can always use the **Reset default settings** link to return to the default setting.

+ Add policy

Policy name *

Policy type

Windows 10 device configuration ▾

^ Secure Windows 10 devices ⓘ On

Help protect PCs from viruses and other threats using Windows Defender Antivirus On

Help protect PCs from web-based threats in Microsoft Edge On

Use rules that reduce the attack surface of devices ⓘ On

Protect folders from threats such as ransomware ⓘ On

Prevent network access to potentially malicious content on the Internet ⓘ On

Help protect files and folders on PCs from unauthorized access with [BitLocker](#) On

Allow users to download apps from Microsoft Store On

Allow users to access Cortana On

Allow users to receive Windows tips and advertisements from Microsoft On

Keep Windows 10 devices up to date automatically On

Turn off device screen when idle for

5 minutes ▾

[Restore default settings](#)

Who will get these settings? [Change](#)

All Users

Add
Cancel

6. Next decide **Who will get these settings?** If you don't want to use the default **All users** security group, Choose **Change**, search for the security group who will get these settings > **Select**.

7. Finally, choose **Done** to save the policy, and assign it to devices.

Edit Windows 10 protection settings

1. Go to the admin center at <https://admin.microsoft.com>.
2. On the left nav, choose **Devices** > **Policies** .
3. Choose an existing Windows device policy and then **Edit**.
4. Choose **Edit** next to a setting you want to change and then **Save**.

Available settings

By default all settings are **On**. The following settings are available.

For more information, see [How do protection features in Microsoft 365 Premium map to Intune settings.](#)

SETTING	DESCRIPTION
Help protect PCs from viruses and other threats using Windows Defender Antivirus	Requires that Windows Defender Antivirus is turned on to protect PCs from the dangers of being connected to the internet.
Help protect PCs from web-based threats in Microsoft Edge	Turns on settings in Edge that help protect users from malicious sites and downloads.
Use rules that reduce the attack surface of devices	When turned On, attack surface reduction helps block actions and apps typically used by malware to infect devices. This setting is only available if Windows Defender Antivirus is set to On. See Reduce attack surfaces to learn more.
Protect folders from threats such as ransomware	This setting uses controlled folder access to protect company data from modification by suspicious or malicious apps, such as ransomware. These types of apps are blocked from making changes in protected folders. This setting is only available if Windows Defender Antivirus is set to On. See Protect folders with Controlled folder access to learn more.
Prevent network access to potentially malicious content on the Internet	Use this setting to block outbound user connections to low-reputation Internet locations that may host phishing scams, exploits, or other malicious content. This setting is only available if Windows Defender Antivirus is set to On . For more information, see Protect your network .
Help protect files and folders on PCs from unauthorized access with BitLocker	Bitlocker protects data by encrypting the computer hard drives and protect against data exposure if a computer is lost or stolen. For more information, see Bitlocker FAQ .
Allow users to download apps from Microsoft Store	Lets users download and install apps from the Microsoft Store. Apps include everything from games to productivity tools, so we leave this setting On , but you can turn it off for extra security.
Allow users to access Cortana	Cortana can be very helpful! Cortana can turn settings on or off for you, give directions, and make sure you're on time for appointments, so we keep this setting On by default.
Allow users to receive Windows tips and advertisements from Microsoft	Windows tips can be handy and help orient users when new features are released.
Keep Windows 10 devices up to date automatically	Makes sure that Windows 10 devices automatically receive the latest updates.
Turn off device screen when idle for this amount of time	Makes sure that company data is protected if a user is idle. A user may be working in a public location, like a coffee shop, and step away or be distracted for just a moment, leaving their device vulnerable to random glances. This setting lets you control how long the user can be idle before the screen shuts off.

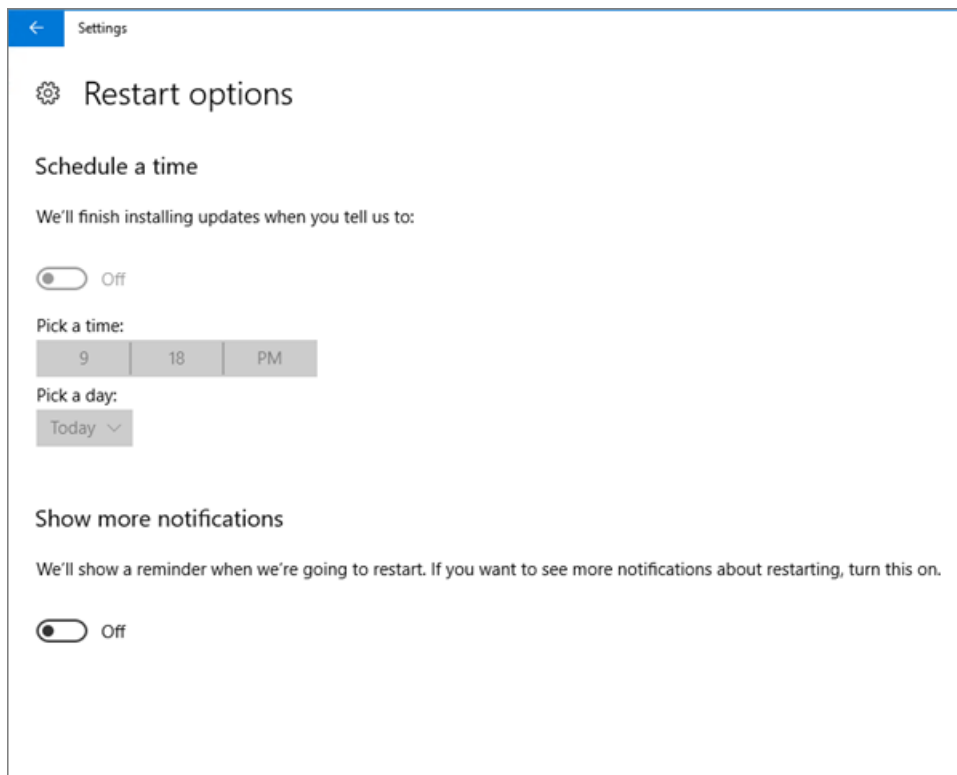
Validate device protection settings for Windows 10 PCs

6/14/2021 • 2 minutes to read • [Edit Online](#)

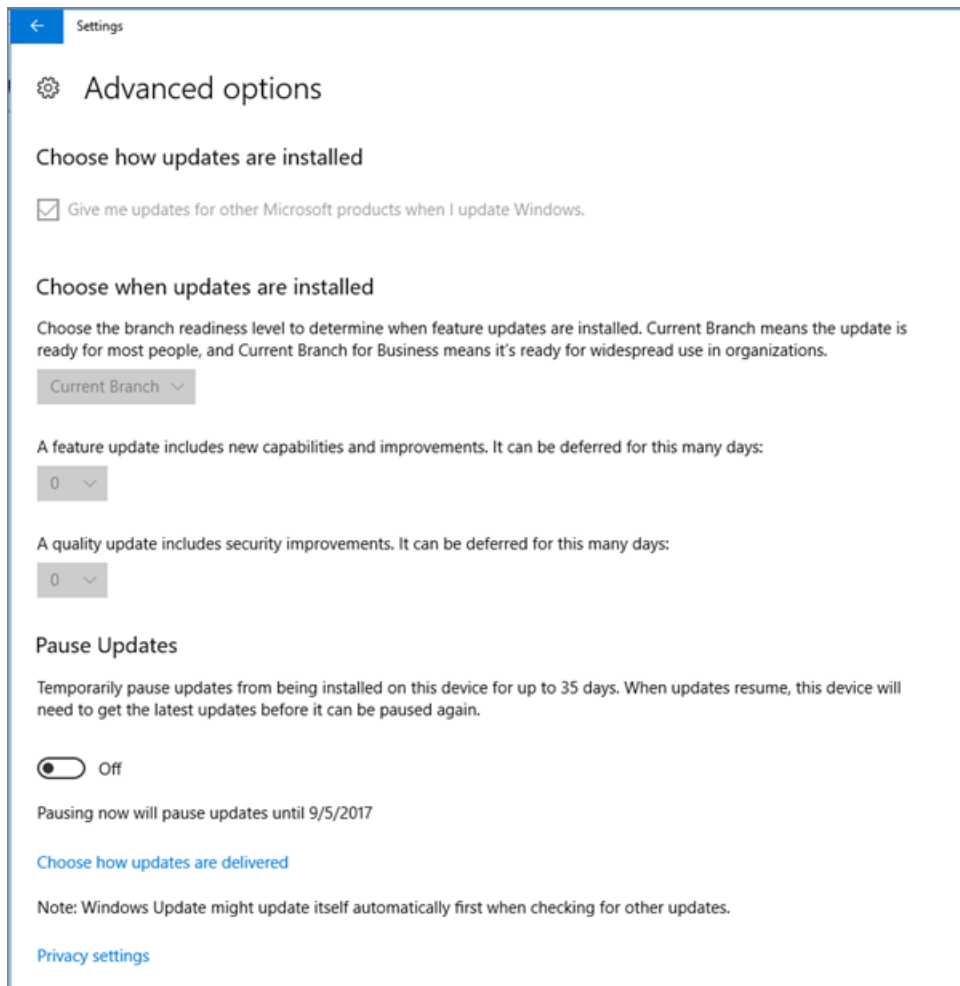
Verify that Windows 10 device policies are set

After you [set up devices policies](#), it may take up to a few hours for the policy to take effect on users' devices. You can confirm that the policies took effect by looking at various Windows Settings screens on the users' devices. Because the users won't be able to modify the Windows Update and Windows Defender Antivirus settings on their Windows 10 devices, many options will be grayed out.

1. Go to **Settings > Update & security > Windows Update > Restart options** and confirm that all settings are grayed out.

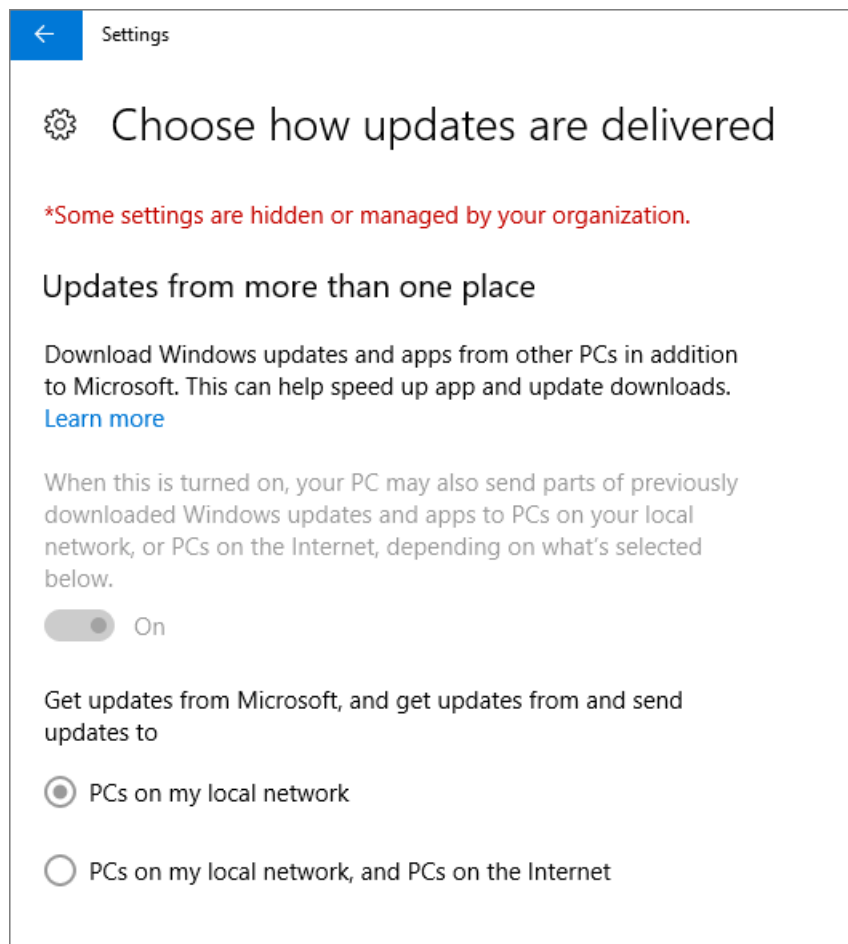


2. Go to **Settings > Update & security > Windows Update > Advanced options** and confirm that all settings are grayed out.

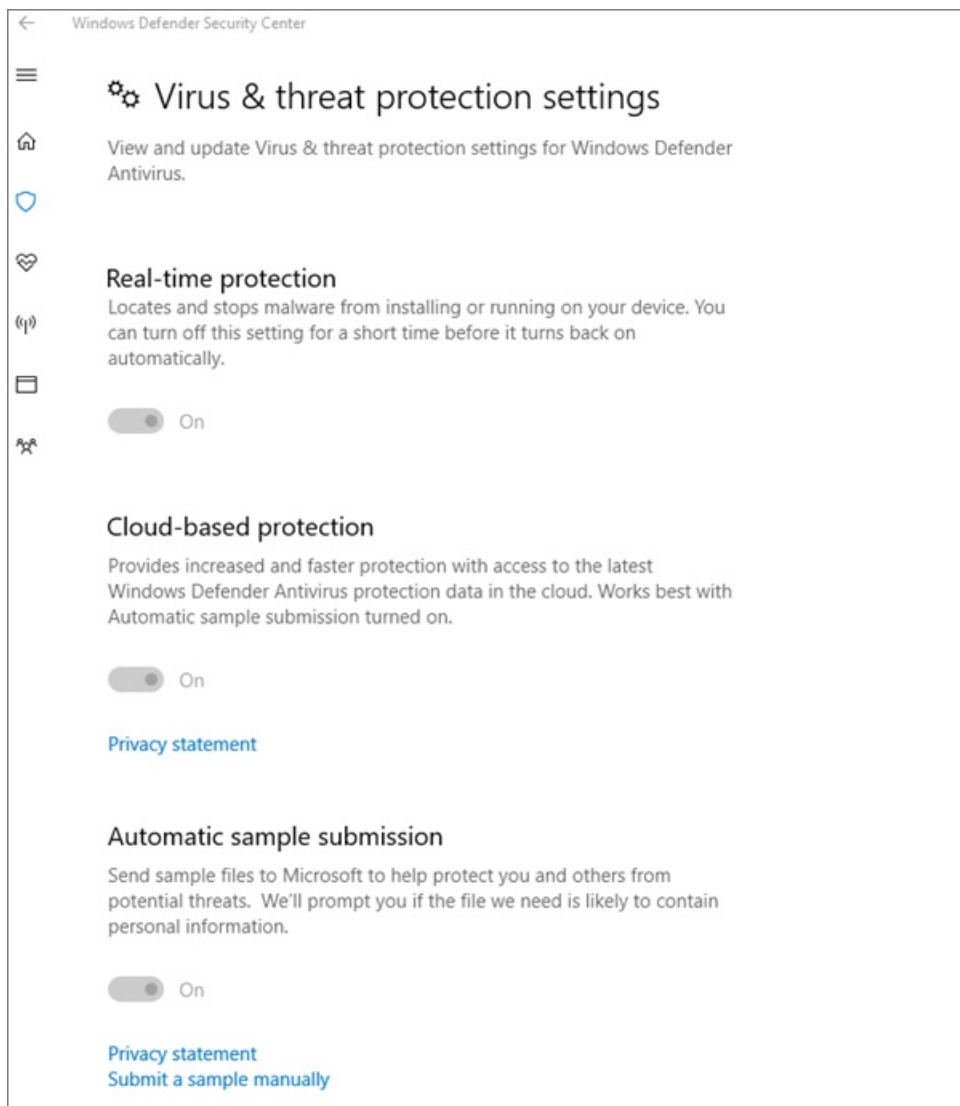


3. Go to **Settings > Update & security > Windows Update > Advanced options > Choose how updates are delivered.**

Confirm that you can see the message (in red) that some settings are hidden or managed by your organization, and all the options are grayed out.



4. To open the Windows Defender Security Center, go to **Settings > Update & security > Windows Defender > click Open Windows Defender Security Center > Virus & thread protection > Virus & threat protection settings.**
5. Verify that all options are grayed out.



Related Topics

[Microsoft 365 for business documentation and resources](#)

[Get started with Microsoft 365 for business](#)

[Manage Microsoft 365 for business](#)

[Set device configurations for Windows 10 PCs](#)

Use the step-by-step guide to add Autopilot devices and profile

7/12/2021 • 2 minutes to read • [Edit Online](#)

You can use Windows AutoPilot to set up **new** Windows 10 devices for your business so they're ready for use when you give them to your employees.

Device requirements

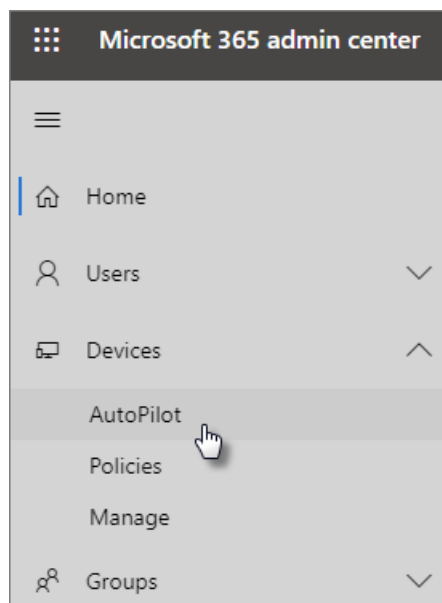
Devices must meet these requirements:

- Windows 10, version 1703 or later
- New devices that haven't been through Windows out-of-box experience

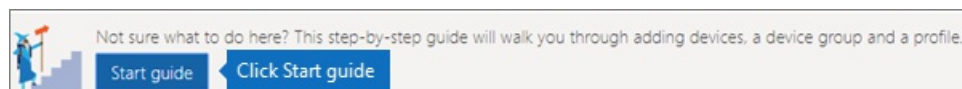
Use the setup guide to create devices and profiles

If you haven't created device groups or profiles yet, the best way to get started is by using the step-by-step guide. You can also [add devices](#) and [assign profiles](#) to them without using the guide.

1. Go to the admin center at <https://admin.microsoft.com>.
2. On the left navigation pane, choose **Devices > AutoPilot**.



3. On the **AutoPilot** page, click or tap **Start guide**.



4. On the **Upload .csv file with list of devices** page, browse to a location where you have the prepared .CSV file, then **Open > Next**. The file must have three headers:
 - Column A: Device Serial Number
 - Column B: Windows Product ID

- Column C: Hardware Hash

You can get this information from your hardware vendor, or you can use the [Get-WindowsAutoPilotInfo PowerShell script](#) to generate a CSV file.

For more information, see [Device list CSV-file](#). You can also download a sample file on the [Upload .csv file with list of devices](#) page.

NOTE

This script uses WMI to retrieve properties needed for a customer to register a device with Windows Autopilot. Note that it is normal for the resulting CSV file to not collect a Windows Product ID (PKID) value since this is not required to register a device and PKID being NULL in the output CSV is totally fine. Only the serial number and hardware hash will be populated.

4. On the **Assign a profile** page, you can either pick an existing profile or create a new one. If you don't have one yet, you'll be prompted to create one.

A profile is a collection of settings that can be applied to a single device or to a group of devices.

The default features are required and are set automatically. The default features are:

- Skip Cortana, OneDrive, and OEM registration.
- Create sign-in experience with your company brand.
- Connect your devices to Azure Active Directory accounts, and automatically enroll them to be managed by Microsoft 365 Business Premium.

For more information, see [About AutoPilot Profile settings](#).

5. The other settings are **Skip privacy settings** and **Don't allow user to become the local admin**. These are both set to **Off** by default.

Choose **Next**.

6. **You're done** indicates that the profile you created (or chose) will be applied to the device group you created by uploading the list of devices. The settings will be in effect when the device users sign in next. Choose **Close**.

Related content

[About AutoPilot Profile settings](#) (article)

[Options for protecting your devices and app data](#) (article)

Create and edit AutoPilot profiles

4/3/2021 • 2 minutes to read • [Edit Online](#)

Create a profile

A profile applies to a device, or a group of devices,

1. In the Microsoft 365 admin center, choose **Devices** > **AutoPilot**.
2. On the **AutoPilot** page, choose the **Profiles** tab > **Create profile**.
3. On the **Create profile** page, enter a name for the profile that helps you identify it, for example Marketing. Turn on the setting you want, and then choose **Save**. For more information about AutoPilot profile settings, see [About AutoPilot Profile settings](#).

Create profile

A profile is a collection of settings that can be applied to a single device or a device group.

Name your new profile

Marketing

AutoPilot default features (required) On

Skip Cortana, OneDrive and OEM registration
Sign-in experience with your company brand
MDM auto-enrollment with configured AAD accounts

Skip privacy settings On

Dont allow the user to become the local admin On

Save Cancel

Apply profile to a device

After you create a profile, you can apply it to a device or a group of devices. You can pick an existing profile in the [step-by-step guide](#) and apply it to new devices, or replace an existing profile for a device or group of devices.

1. On the **Prepare Windows** page, choose the **Devices** tab.
2. Select the check box next to a device name, and in the **Device** panel, choose a profile from the **Assigned profile** drop-down list > **Save**.

Assigned profile

None

Marketing

Test

None

Save Cancel

Edit, delete, or remove a profile

Once you've assigned a profile to a device, you can update it, even if you've already given the device to a user. When the device connects to the internet, it downloads the latest version of your profile during the setup process. If the user restores their device to its factory default settings, the device will again download the latest updates to your profile.

Edit a profile

1. On the **Prepare Windows** page, choose the **Profiles** tab.
2. Select the check box next to a device name, and in the **Profile** panel, update any of the available settings > **Save**.

If you do this before a user connects the device to the internet, then the profile gets applied to the setup process.

Delete a profile

1. On the **Prepare Windows** page, choose the **Profiles** tab.
2. Select the check box next to a device name, and in the **Profile** panel, select **Delete profile** > **Save**.

When you delete a profile, it gets removed from a device or a group of devices it was assigned to.

Remove a profile

1. On the **Prepare Windows** page, choose the **Devices** tab.
2. Select the check box next to a device name, and in the **Device** panel, choose **None** from the **Assigned profile** drop-down list > **Save**.

Create and edit AutoPilot devices

4/3/2021 • 2 minutes to read • [Edit Online](#)

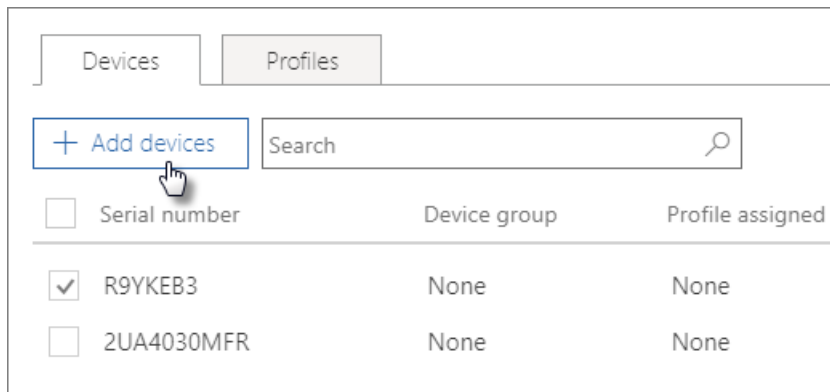
Upload a list of devices

You can use the [Step-by-step guide](#) to upload devices, but you can also upload devices in the **Devices** tab.

Devices must meet these requirements:

- Windows 10, version 1703 or later
- New devices that haven't been through Windows out-of-box experience

1. In the Microsoft 365 admin center, choose **Devices** > **AutoPilot**.
2. On the **AutoPilot** page, choose the **Devices** tab > **Add devices**.



3. On the **Add devices** panel, browse to a [Device list CSV file](#) that you prepared > **Save** > **Close**.

You can get this information from your hardware vendor, or you can use the [Get-WindowsAutoPilotInfo PowerShell script](#) to generate a CSV file.

Assign a profile to a device or a group of devices

1. On the **Prepare Windows** page, choose the **Devices** tab, and select the check box next to one or more devices.
2. On the **Device** panel, select a profile from the **Assigned profile** drop-down.

If you don't have any profiles yet, see [Create and edit AutoPilot profiles](#) for instructions.

About AutoPilot Profile settings

4/3/2021 • 2 minutes to read • [Edit Online](#)

AutoPilot profile settings

You can use AutoPilot profiles to control how Windows is installed on user devices. The profiles contain the following settings.

AutoPilot default features (required) that are set automatically:

SETTING	DESCRIPTION
Skip Cortana, OneDrive, and OEM registration	Skips the installation of consumer apps like Cortana and personal OneDrive. The device user can install these later as long as the user is a local admin on the device. The original manufacturer registration is skipped because the device will be managed by Microsoft 365 Business Premium.
Sign in experience with your company brand	If your company has a Add your company branding to Microsoft 365 Sign In page , the device user will get that experience when signing in.
MDM auto-enrollment with configured AAD accounts.	The user identity will be managed by Azure Active Directory, and users will sign in to Windows and Microsoft 365 with their Microsoft 365 Business Premium credentials.

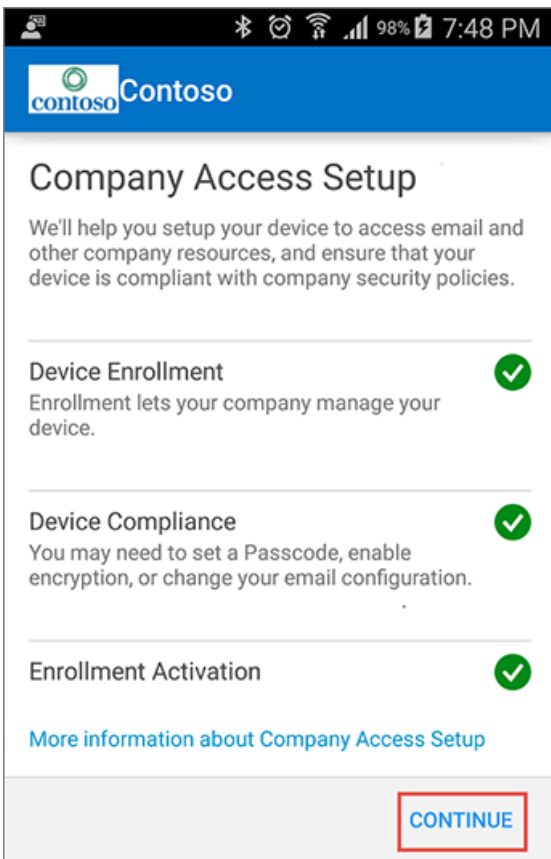
Optional settings:

SETTING	DESCRIPTION
Skip privacy settings (Off by default)	If this option is set to On , the device user will not see the license agreement for the device and Windows when he or she first signs in.
Don't allow the user to become the local admin	If this option is set to On , the device user will not be able to install any personal apps, such as Cortana.

Overview of Basic Mobility and Security for Microsoft 365

7/12/2021 • 2 minutes to read • [Edit Online](#)

You can manage and secure mobile devices when they're connected to your Microsoft 365 organization by using Basic Mobility and Security. Mobile devices like smartphones and tablets that are used to access work email, calendar, contacts, and documents play a big part in making sure that employees get their work done anytime, from anywhere. So it's critical that you help protect your organization's information when people use devices. You can use Basic Mobility and Security to set device security policies and access rules, and to wipe mobile devices if they're lost or stolen.



What types of devices can you manage?

You can use Basic Mobility and Security to manage many types of mobile devices like Windows Phone, Android, iPhone, and iPad. To manage mobile devices used by people in your organization, each person must have an applicable Microsoft 365 license and their device must be enrolled in Basic Mobility and Security.

To see what Basic Mobility and Security supports for each type of device, see [Capabilities of Basic Mobility and Security](#).

Setup steps for Basic Mobility and Security

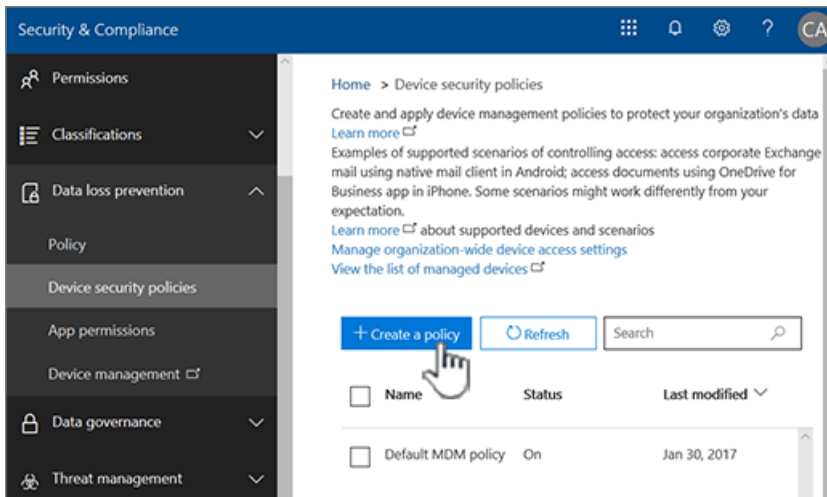
A Microsoft 365 global admin must complete the following steps to activate and set up Basic Mobility and Security. For detailed steps, follow the guidance in [Set up Basic Mobility and Security](#).

Here's a summary of the steps:

Step 1: Activate Basic Mobility and Security by following steps in the [Set up Basic Mobility and Security](#).

Step 2: Set up Basic Mobility and Security by, for example, creating an APNs certificate to manage iOS devices and adding a Domain Name System (DNS) record for your domain to support Windows phones.

Step 3: Create device policies and apply them to groups of users. When you do this, your users get an enrollment message on their device, and when they've completed enrollment, their devices are restricted by the policies you've set up for them. For more info, see [Enroll your mobile device using Basic Mobility and Security](#).



Device management tasks

After you've got Basic Mobility and Security set up and your users have enrolled their devices, you can manage the devices, block access, or wipe a device, if necessary. To learn more about some common device management tasks, including where to complete the tasks, see [Manage devices enrolled in Mobile Device Management for Microsoft 365](#).

Other ways to manage devices and apps

If you just need mobile app management (MAM), perhaps for people updating work projects on their own devices, Intune provides another option besides enrolling and managing devices. An Intune subscription allows you to set up MAM policies by using the Azure portal, even if people's devices aren't enrolled in Intune. For more info, see [App protection policies overview](#).

Related content

[Set up Basic Mobility and Security](#) (article)

[Enroll your mobile device using Basic Mobility and Security](#) (article)

[Manage devices enrolled in Mobile Device Management for Microsoft 365](#) (article)

[Get details about devices managed by Basic Mobility and Security](#) (article)

Choose between Basic Mobility and Security or Intune

8/9/2021 • 3 minutes to read • [Edit Online](#)

Microsoft Intune is a standalone product included with certain Microsoft 365 plans, while Basic Mobility and Security is part of the Microsoft 365 plans.

Availability of Basic Mobility and Security and Intune

Both Basic Mobility and Security and Intune are included in a variety of plans, described in the following table.

PLAN	BASIC MOBILITY AND SECURITY	MICROSOFT INTUNE
Microsoft 365 Apps	Yes	No
Microsoft 365 Business Basic	Yes	No
Microsoft 365 Business Standard	Yes	No
Office 365 E1	Yes	No
Office 365 E3	Yes	No
Office 365 E5	Yes	No
Microsoft 365 Business Premium	Yes	Yes
Microsoft 365 Firstline 3	Yes	Yes
Microsoft 365 Enterprise E3	Yes	Yes
Microsoft 365 Enterprise E5	Yes	Yes
Microsoft 365 Education A1	Yes	Yes
Microsoft 365 Education A3	Yes	Yes
Microsoft 365 Education A5	Yes	Yes
Microsoft Intune	No	Yes
Enterprise Mobility & Security E3	No	Yes
Enterprise Mobility & Security E5	No	Yes

NOTE

You can't start using Basic Mobility and Security if you're already using Microsoft Intune.

For details, see [Microsoft 365 and Office 365 platform service descriptions](#).

Differences in capabilities

Microsoft Intune and built-in Basic Mobility and Security both give you the ability to manage mobile devices in your organization, but there are key differences in capability, described in the following table.

NOTE

You can manage users and their mobile devices using both Intune and Basic Mobility and Security in the same Microsoft 365 Business Standard organization *by setting up Basic Mobility and Security first, and then adding Microsoft Intune*. This allows you to choose Basic Mobility and Security or the more feature-rich Intune solution. Assign an Intune license to enable the Intune features.

FEATURE AREA	FEATURE HIGHLIGHTS	BASIC MOBILITY AND SECURITY	MICROSOFT INTUNE
Device types	Managing different OS platforms and major management mode variants.	Windows iOS Android Android Samsung KNOX	Windows iOS Android Android Samsung KNOX mac OS, iPad OS
Device compliance	Set and manage security policies, like device level PIN lock and jailbreak detection.	Limitations on Android 9 and later devices. See details .	Yes
Conditional access based on device compliance	Prevent noncompliant devices from accessing corporate email and data from the cloud.	Not supported on Windows 10. Limited to controlling access to Exchange Online, SharePoint Online, and Outlook.	Yes
Device configuration	Configure device settings (for example, disabling the camera)	Limited set of settings.	Yes
Email profiles	Provision a native email profile on the device.	Yes	Yes
WiFi profiles	Provision a native WiFi profile on the device.	No	Yes
VPN profiles	Provision a native VPN profile on the device.	No	Yes
Mobile application management	Deploy your internal line-of-business apps and from apps stores to users.	No	Yes

FEATURE AREA	FEATURE HIGHLIGHTS	BASIC MOBILITY AND SECURITY	MICROSOFT INTUNE
Mobile application protection	Enable your users to securely access corporate information using the Office mobile and line-of-business apps they know, while ensuring security of data by helping to restrict actions like copy, cut, paste, and save as, to only those apps managed approved for corporate data. Works even if the devices are not enrolled to Basic Mobility and Security. See Protect app data using MAM policies.	No	Yes
Managed browser	Enable more secure web browsing using the Edge app.	No	Yes
Zero touch enrollment programs (AutoPilot)	Enroll large numbers of corporate-owned devices, while simplifying user setup.	No	Yes

In addition to features listed in the preceding table, Basic Mobility and Security and Intune both include a set of remote actions that send commands to devices over the internet. For example, you can remove Office data from an employee's device while leaving personal data in place (retire), remove Office apps from a employee's device (wipe), or reset a device to its factory settings (full wipe).

Basic Mobility and Security remote actions include retire, wipe and full wipe. For more information on Basic Mobility and Security actions, see [capabilities of Basic Mobility and Security](#).

With Intune you have the following set of actions:

- Autopilot reset (Windows only)
- [Bitlocker key rotation](#)(Windows only)
- [Use wipe, retire, or manually unenrolling the device](#)
- [Disable activation loc](#)(iOS only)
- [Fresh start](#)(Windows only)
- [Full scan](#)(Windows 10 only)
- [Locate device](#)(iOS only)
- [Lost mode](#)(iOS only)- [Quick scan](#)(Windows 10 only)
- [Remote control for Android](#)
- [Remote lock](#)
- [Rename device](#)
- [Reset passcode Restart](#)(Windows only)
- Update Windows Defender Security Intelligence (Windows only)
- Windows 10 PIN reset (Windows only)
- [Send custom notifications](#)(Android, iOS, iPad OS)
- [Synchronize device](#)

For more information on Intune actions, see [Microsoft Intune documentation](#).

Capabilities of Basic Mobility and Security

8/13/2021 • 7 minutes to read • [Edit Online](#)

Basic Mobility and Security can help you secure and manage mobile devices like iPhones, iPads, Androids, and Windows Phones used by licensed Microsoft 365 users in your organization. You can create mobile device management policies with settings that can help control access to your organization's Microsoft 365 email and documents for supported mobile devices and apps. If a device is lost or stolen, you can remotely wipe the device to remove sensitive organizational information.

Supported devices

You can use Basic Mobility and Security to secure and manage the following devices.

- iOS 11.0 or later versions
- Android 5.0 or later versions³
- Windows 8.1¹
- Windows 8.1 RT¹
- Windows 10²
- Windows 10 Mobile²

¹Access control for Windows 8.1 RT devices is limited to Exchange ActiveSync.

²Access control for Windows 10 requires a subscription that includes Azure AD Premium and the device needs to be joined to Azure Active Directory.

³After June 2020, Android versions later than 9 can't manage password settings except on Samsung Knox devices.

NOTE

Devices already enrolled with earlier OS versions continue to function although the capabilities might change without notice.

If people in your organization use mobile devices that aren't supported by Basic Mobility and Security, you might want to block Exchange ActiveSync app access to Microsoft 365 email for those devices, to help make your organization's data more secure. For steps to block Exchange ActiveSync, see [Manage device access settings in Basic Mobility and Security](#).

Access control for Microsoft 365 email and documents

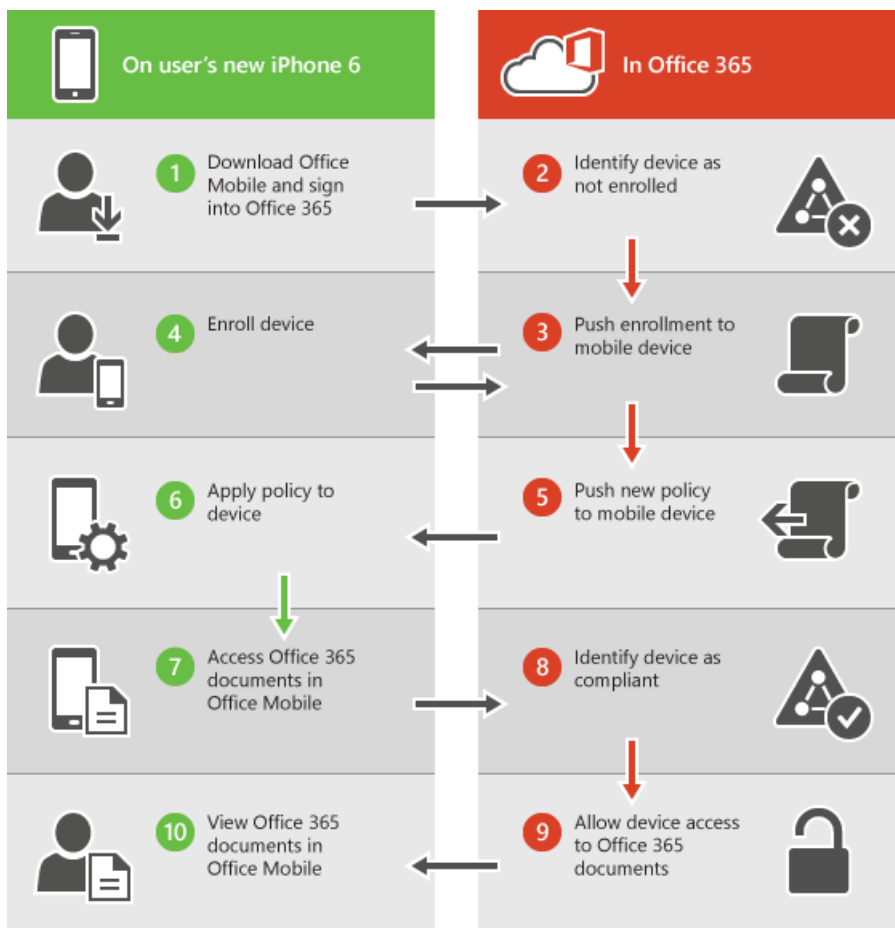
The supported apps for the different types of mobile devices in the following table prompt users to enroll in Basic Mobility and Security where there is a new mobile device management policy that applies to a user's device and the user hasn't previously enrolled the device. If a user's device doesn't comply with a policy, depending on how you set the policy up, a user might be blocked from accessing Microsoft 365 resources in these apps, or they might have access but Microsoft 365 reports a policy violation.

PRODUCT	IOS 10.0 OR LATER	ANDROID 5.0 OR LATER
Exchange Exchange ActiveSync includes built-in email and third-party apps, like TouchDown, that use Exchange ActiveSync Version 14.1 or later.	Mail	Email
OfficeandOneDrive for Business	Outlook OneDrive Word Excel PowerPoint	On phones and tablets: Outlook OneDrive Word Excel PowerPoint On phones only: Office Mobile

NOTE

- Support for iOS 10.0 and later versions includes iPhone and iPad devices.
- Management of BlackBerry OS devices isn't supported by Basic Security and Mobility. Use BlackBerry Business Cloud Services (BBCS) from BlackBerry to manage BlackBerry OS devices. BlackBerry devices running Android OS are supported as standard Android devices
- Users won't be prompted to enroll and won't be blocked or reported for policy violation if they use the mobile browser to access Microsoft 365 SharePoint sites, documents in Office Online, or email in Outlook Web App.

The following diagram shows what happens when a user with a new device signs in to an app that supports access control with Basic Mobility and Security. The user is blocked from accessing Microsoft 365 resources in the app until they enroll their device.



NOTE

Policies and access rules created in Basic Mobility and Security for Microsoft 365 Business Standard will override Exchange ActiveSync mobile device mailbox policies and device access rules created in the Exchange admin center. After a device is enrolled in Basic Mobility and Security for Microsoft 365 Business Standard, any Exchange ActiveSync mobile device mailbox policy or device access rule applied to the device will be ignored. To learn more about Exchange ActiveSync, see [Exchange ActiveSync in Exchange Online](#).

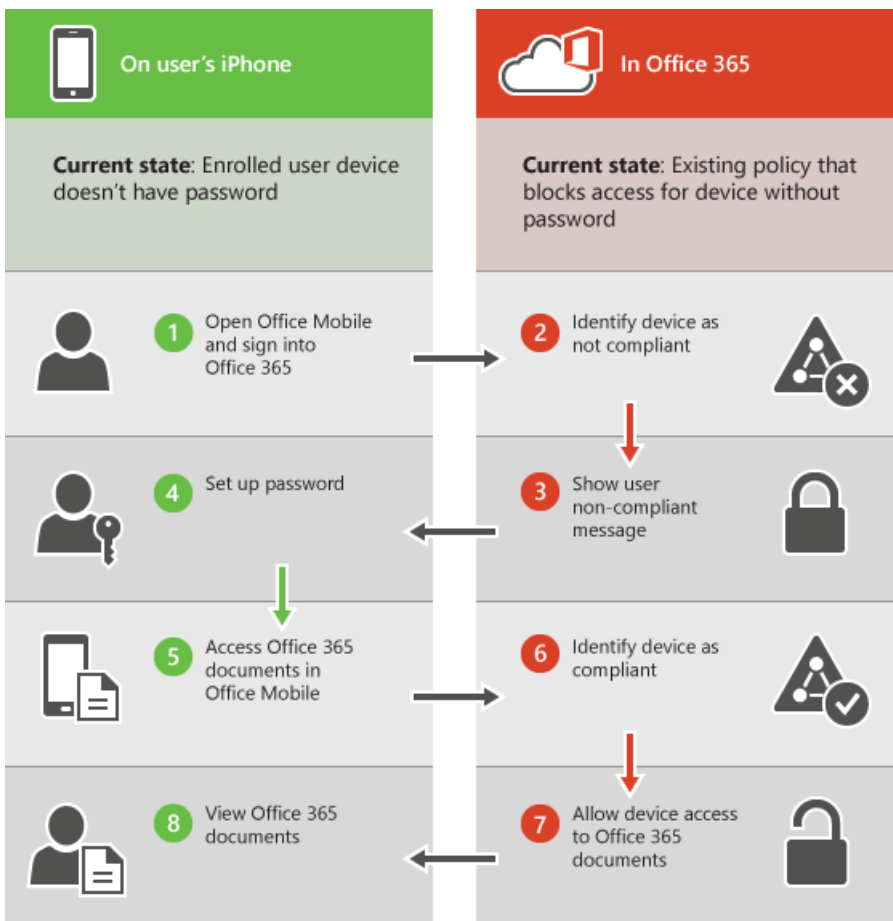
Policy settings for mobile devices

If you create a policy to block access with certain settings turned on, users are blocked from accessing Microsoft 365 resources when using a supported app that is listed in [Access control for Microsoft365 email and documents](#).

The settings that can block users from accessing Microsoft 365 resources are in these sections:

- Security
- Encryption
- Jail broken
- Managed email profile

For example, the following diagram shows what happens when a user with an enrolled device isn't compliant with a security setting in a mobile device management policy that applies to their device. The user signs in to an app that supports access control with Basic Mobility and Security. They are blocked from accessing Microsoft 365 resources in the app until their device complies with the security setting.



The following sections list the policy settings you can use to help secure and manage mobile devices that connect to your Microsoft 365 organization resources.

Security settings

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER	SAMSUNG KNOX
Require a password	Yes	Yes	Yes
Prevent simple password	Yes	No	No
Require an alphanumeric password	Yes	No	No
Minimum password length	Yes	Yes	Yes
Number of sign-in failures before device is wiped	Yes	Yes	Yes
Minutes of inactivity before device is locked	Yes	Yes	Yes
Password expiration (days)	Yes	Yes	Yes
Remember password history and prevent reuse	Yes	Yes	Yes

Encryption settings

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER	SAMSUNG KNOX
Require data encryption on devices ¹	No	Yes	Yes

¹With Samsung Knox, you can also require encryption on storage cards.

Jail broken setting

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER	SAMSUNG KNOX
Device cannot be jail broken or rooted	Yes	Yes	Yes

Managed email profile option

The following option can block users from accessing their Microsoft 365 email if they're using a manually created email profile. Users on iOS devices must delete their manually created email profile before they can access their email. After they delete the profile, a new profile is automatically created on the device. For instructions on how end users can get compliant, see [An existing email account was found](#).

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER	SAMSUNG KNOX
Email profile is managed	Yes	No	No

Cloud settings

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER	SAMSUNG KNOX
Require encrypted backup	Yes	No	No
Block cloud backup	Yes	No	No
Block document synchronization	Yes	No	No
Block photo synchronization	Yes	No	No
Allow Google backup	N/A	No	Yes
Allow Google account auto sync	N/A	No	Yes

System settings

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER	SAMSUNG KNOX
Block screen capture	Yes	No	Yes
Block sending diagnostic data from device	Yes	No	Yes

Application settings

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER	SAMSUNG KNOX
Block video conferences on device	Yes	No	No
Block access to application store	Yes	No	Yes
Require password when accessing application store	No	Yes	Yes

Device capabilities settings

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER	SAMSUNG KNOX
Block connection with removable storage	Yes	Yes	No
Block Bluetooth connection	Yes	Yes	No

Additional settings

You can set the following additional policy settings by using Security & Compliance Center PowerShell cmdlets. For more information, see [Security & Compliance Center PowerShell](#).

SETTING NAME	IOS 7.1 AND LATER	ANDROID 5 AND LATER
CameraEnabled	Yes	Yes
RegionRatings	Yes	No
MoviesRatings	Yes	No
TVShowsRating	Yes	No
AppsRatings	Yes	No
AllowVoiceDialing	Yes	No
AllowVoiceAssistant	Yes	No
AllowAssistantWhileLocked	Yes	No
AllowPassbookWhileLocked	Yes	No
MaxPasswordGracePeriod	Yes	No
PasswordQuality	No	Yes
SystemSecurityTLS	Yes	No
WLANEnabled	No	No

Settings supported by Windows

You can manage Windows 10 devices by enrolling them as mobile devices. After an applicable policy is deployed, users with Windows 10 devices will be required to enroll in Basic Mobility and Security the first time they use the built-in email app to access their Microsoft 365 email (requires Azure AD premium subscription).

The following settings are supported for Windows 10 devices that are enrolled as mobile devices. These settings won't block users from accessing Microsoft 365 resources.

Security settings

- Require an alphanumeric password
- Minimum password length
- Number of sign-in failures before device is wiped
- Minutes of inactivity before device is locked
- Password expiration (days)
- Remember password history and prevent reuse

NOTE

The following settings regulating passwords only control local Windows accounts. Windows accounts provided through join a domain or Azure Active Directory aren't affected by these settings.

System settings

Block sending diagnostic data from device.

Additional settings

You can set these additional policy settings by using PowerShell cmdlets:

- AllowConvenienceLogon
- UserAccountControlStatus
- FirewallStatus
- AutoUpdateStatus
- AntiVirusStatus
- AntiVirusSignatureStatus
- SmartScreenEnabled
- WorkFoldersSyncUrl

Remotely wipe a mobile device

If a device is lost or stolen, you can remove sensitive organizational data and help prevent access to your Microsoft 365 organization resources by doing a wipe from Security & Compliance center > **Data loss prevention** > **Device management**. You can do a selective wipe to remove only organizational data or a full wipe to delete all information from a device and restore it to its factory settings.

For more information, see [Wipe a mobile device in Basic Mobility and Security](#).

Related content

[Overview of Basic Mobility and Security for Microsoft 365](#) (article)

[Create device security policies in Basic Mobility and Security](#) (article)

Set up Basic Mobility and Security

7/12/2021 • 5 minutes to read • [Edit Online](#)

The built-in Basic Mobility and Security for Microsoft 365 helps you secure and manage users' mobile devices such as iPhones, iPads, Androids, and Windows phones. You can create and manage device security policies, remotely wipe a device, and view detailed device reports.

Have questions? For a FAQ to help address common questions, see [Basic Mobility and Security Frequently-asked questions \(FAQ\)](#). Be aware that you cannot use a delegated administrator account to manage Basic Mobility and Security. For more info, see [Partners: Offer delegated administration](#).

Device management is part of the Security & Compliance Center so you'll need to go there to kick off Basic Mobility and Security setup.

Activate the Basic Mobility and Security service

1. Sign in to Microsoft 365 with your global admin account.
2. Go to [Activate Basic Mobility and Security](#).

It can take some time to activate Basic Mobility and Security. When it finishes, you'll receive an email that explains the next steps to take.

Set up Mobile Device Management

When the service is ready, complete the following steps to finish setup.

Step 1: (Required) Configure domains for Basic Mobility and Security

If you don't have a custom domain associated with Microsoft 365 or if you're not managing Windows devices, you can skip this section. Otherwise, you'll need to add DNS records for the domain at your DNS host. If you've added the records already, as part of setting up your domain with Microsoft 365, you're all set. After you add the records, Microsoft 365 users in your organization who sign in on their Windows device with an email address that uses your custom domain are redirected to enroll in Basic Mobility and Security.

Need help setting up the records? Find your domain registrar and select the registrar name to go to step-by-step help for creating DNS record in the list provided in [Add DNS records to connect your domain](#). Use those instructions to create CNAME records described in [Simplify Windows enrollment without Azure AD Premium](#).

After you add the two CNAME records, go back to the Security & Compliance Center and go to **Data loss prevention** > **Device management** to complete the next step.

Step 2: (Required) Configure an APNs Certificate for iOS devices

To manage iOS devices like iPad and iPhones, you need to create an APNs certificate.

1. Sign in to Microsoft 365 with your global admin account.
2. In your browser type: <https://protection.office.com>.
3. Select **Data loss prevention** > **Device management**, and choose **APNs Certificate for iOS devices**.
4. On the **Apple Push Notification Certificate Settings** page, choose **Next**.
5. Select **Download your CSR file** and save the Certificate signing request to somewhere on your computer that you'll remember. Select **Next**.

6. On the **Create an APNs certificate** page:

- Select **Apple APNs Portal** to open the Apple Push Certificates Portal.
- Sign in with an Apple ID.

IMPORTANT

Use a company Apple ID associated with an email account that will remain with your organization even if the user who manages the account leaves. Save this ID because you'll need to use the same ID when it's time to renew the certificate.

- Select **Create a Certificate** and accept the **Terms of Use**.
- Browse to the Certificate signing request you downloaded to your computer from Microsoft 365 and select **Upload**.
- Download the APN certificate created by the Apple Push Certificate Portal to your computer.

TIP

If you're having trouble downloading the certificate, refresh your browser.

7. Go back to Microsoft 365 and select **Next**.

8. Browse to the APN certificate you downloaded from the Apple Push Certificates Portal.

9. Select **Finish**.

Step 3: (Recommended) Set up multi-factor authentication

MFA helps secure the sign in to Microsoft 365 for mobile device enrollment by requiring a second form of authentication. Users are required to acknowledge a phone call, text message, or app notification on their mobile device after correctly entering their work account password. They can enroll their device only after this second form of authentication is completed. After user devices are enrolled in Basic Mobility and Security, users can access Microsoft 365 resources with only their work account.

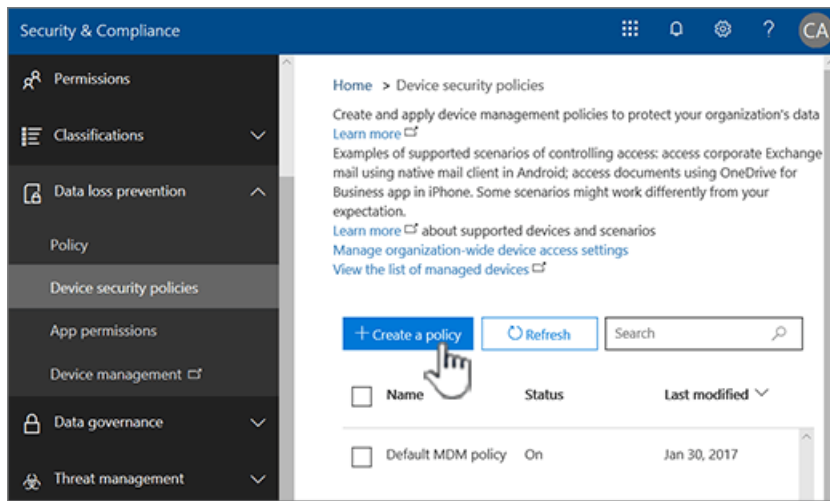
To learn how to turn on MFA in the Azure AD portal, see [Set up multi-factor authentication](#).

After you set up MFA, go back to the Security & Compliance Center and navigate to **Data loss prevention > Device management > Device policies** to complete the next step.

Step 4: (Recommended) Manage device security policies

The next step is to create and deploy device security policies to help protect your Microsoft 365 organization data. For example, you can help prevent data loss if a user loses their device by creating a policy to lock devices after five minutes of inactivity and wipe devices after three sign-in failures.

1. Sign in to Microsoft 365 with your global admin account.
2. Select [Activate Mobile Device Management](#). If the service is activated, instead the activation steps you'll see a link to [Manage Devices](#).
3. Go to **Device policies**.



4. Create and deploy device security policies appropriate for your organization following the steps in [Create device security policies in Basic Mobility and Security](#).

TIP

- When you create a new policy, you might want to set the policy to allow access and report policy violation where a user device isn't compliant with the policy. This allows you see how many mobile devices are impacted by the policy without blocking access to Microsoft 365.
- Before you deploy a new policy to everyone in your organization, we recommend you test it on the devices used by a small number of users.
- Also, before you deploy policies, let your organization know the potential impacts of enrolling a device in Basic Mobility and Security. Depending on how you set up the policies, devices that don't comply with policies (non-compliant devices) could be blocked from accessing Microsoft 365. Non-compliant devices might also have apps installed, photos, and other personal information which, on an enrolled device, could be deleted if the device is wiped. For more info, see [Wipe a mobile device in Basic Mobility and Security](#).

Make sure users enroll their devices

After you've created and deployed a mobile device management policy, each licensed Microsoft 365 user in your organization that the device policy applies receives an enrollment message the next time they sign into Microsoft 365 from their mobile device. They must complete the enrollment and activation steps before they can access Microsoft 365 email and documents. For more info, see [Enroll your mobile device using Basic Mobility and Security](#).

IMPORTANT

If a user's preferred language isn't supported by the enrollment process, users might receive enrollment notification and steps on their mobile devices in another language. Not all languages supported in Microsoft 365 are currently supported for the enrollment process on mobile devices.

Users with Android or iOS devices are required to install the Company Portal app as part of the enrollment process.

Related content

[Capabilities of Basic Mobility and Security](#) (article)

[Create device security policies in Basic Mobility and Security](#) (article)

Create device security policies in Basic Mobility and Security

7/12/2021 • 8 minutes to read • [Edit Online](#)

You can use Basic Mobility and Security to create device policies that help protect your organization information on Microsoft 365 from unauthorized access. You can apply policies to any mobile device in your organization where the user of the device has an applicable Microsoft 365 license and has enrolled the device in Basic Mobility and Security.

Before you begin

IMPORTANT

Before you can create a mobile device policy, you must activate and set up Basic Mobility and Security. For more info, see [Overview of Basic Mobility and Security](#).

- Learn about the devices, mobile device apps, and security settings that Basic Mobility and Security supports. See [Capabilities of Basic Mobility and Security](#).
- Create security groups that include Microsoft 365 users that you want to deploy policies to and for users that you might want to exclude from being blocked access to Microsoft 365. We recommend that before you deploy a new policy to your organization, you test the policy by deploying it to a small number of users. You can create and use a security group that includes just yourself or a small number Microsoft 365 users that can test the policy for you. To learn more about security groups, see [Create, edit, or delete a security group](#).
- To create and deploy Basic Mobility and Security policies in Microsoft 365, you need to be a Microsoft 365 global admin. For more info, see [Permissions in the Security & Compliance Center](#).
- Before you deploy policies, let your organization know the potential impacts of enrolling a device in Basic Mobility and Security. Depending on how you set up the policies, noncompliant devices can be blocked from accessing Microsoft 365 and data, including installed applications, photos, and personal information on an enrolled device, and data can be deleted.

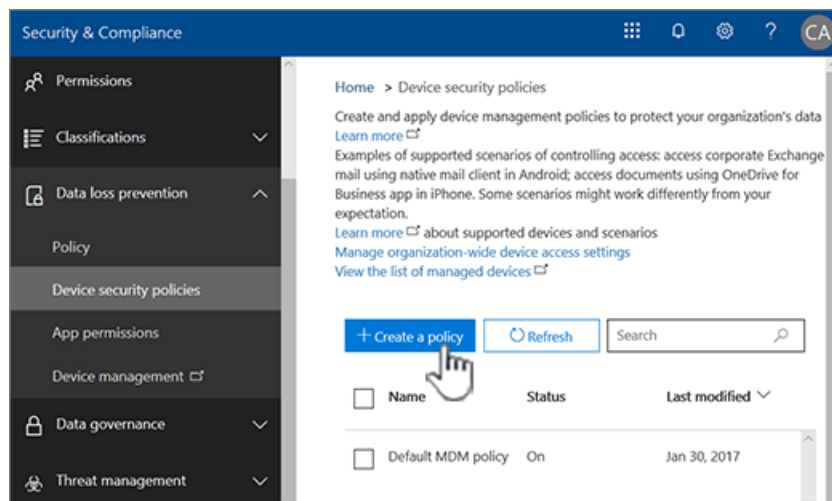
NOTE

Policies and access rules created in Basic Mobility and Security for Microsoft 365 Business Standard override Exchange ActiveSync mobile device mailbox policies and device access rules created in the Exchange admin center. After a device is enrolled in Basic Mobility and Security for Microsoft 365 Business Standard, any Exchange ActiveSync mobile device mailbox policy or device access rule applied to the device is ignored. To learn more about Exchange ActiveSync, see [Exchange ActiveSync in Exchange Online](#).

Step 1: Create a device policy and deploy to a test group

Before you can start, make sure you have activated and set up Basic Mobility and Security. For instructions, see [Overview of Basic Mobility and Security](#).

1. From your browser, type <https://protection.office.com/devicev2>.
2. Select **Create a policy**.



3. On the **Policy settings** page, specify the requirements you want applied to mobile devices in your organization.
4. **Require managing email profile:** When enabled, devices that don't have an email profile managed by Basic Mobility and Security are considered not compliant. A device can't have a managed email profile when it's not correctly targeted, or if the user manually set up the email account on the device. When you leave it **Not Enabled** (default), this setting isn't evaluated for compliance or non-compliance. For instructions on how users can get compliant when this option is selected, see [An existing email account was found](#).
5. On the **Do you want to apply this policy now?** page, choose the groups that you want to apply this policy to.
6. Select **Create this policy**.

The policy is pushed to the device of each user the policy applies to the next time they sign in to Microsoft 365 using their mobile device. If users haven't had a policy applied to their mobile device before, after you deploy the policy, they get a notification on their device that includes the steps to enroll and activate Basic Mobility and Security. For more info, see [Enroll your mobile device using Basic Mobility and Security](#). Until they complete enrollment in Basic Mobility and Security hosted by the Intune Service, access to email, OneDrive, and other services is restricted. After they complete enrollment by using the Intune Company Portal app, they can use the services and the policy is applied to their device.

Step 2: Verify that your policy works

After you've created a device policy, check that the policy works as you expect before you deploy it to your organization.

1. From your browser, type <https://protection.office.com/devicev2>.
2. Select **View the list of managed devices**.
3. Check the status of user devices that have the policy applied. You want the **State** of devices to be **Managed**.
4. You can also do a full or selective wipe on a device by clicking on **Factory reset** or **Remove company data** from **Manage** button after selecting a device. For instructions, see [Wipe a mobile device in Microsoft 365].

Step 3: Deploy a policy to your organization

After you've created a device policy and verified that it works as expected, deploy it to your organization.

1. From your browser type: <https://protection.office.com/devicev2>.
2. Select the policy you want to deploy, and choose **Edit** next to **Groups applied to**.
3. Search for a group to add and click on **Select**.

4. Select **Close** and **Change setting**.
5. Select **Close** and **Edit policy**.

The policy is pushed to the mobile device of each user the policy applies to the next time they sign in to Microsoft 365 from their mobile device. If users haven't had a policy applied to their mobile device, they get a notification on their device with steps to enroll and activate it for Basic Mobility and Security. After they've completed the enrollment, the policy is applied to their device. For more info, see [Enroll your mobile device using Basic Mobility and Security](#).

Step 4: Block email access for unsupported devices

To help secure your organization information, you should block app access to Microsoft 365 email for mobile devices that aren't supported by Basic Mobility and Security. For a list of supported devices, see [Supported devices](#).

To block app access:

1. From your browser, type <https://protection.office.com/devicev2>.
2. Select **Manage organization-wide device access settings**.
3. To block unsupported devices, choose **Block** under **If a device isn't supported by Basic Mobility and Security for Microsoft 365**, and then select **Save**.

Organization-wide device access settings

If a device isn't supported by MDM for Office 365, do you want to allow or block from using an Exchange account to access your organization's email? *

Allow

Block

[Learn more](#) about supported devices and scenarios

Are there any security groups you want to exclude from access control?

People in these security groups will always be able to use MDM for Office 365 to access their devices aren't compliant with the requirements specified in your device security policy

+ Add - Remove

Search

^ Groups (0)

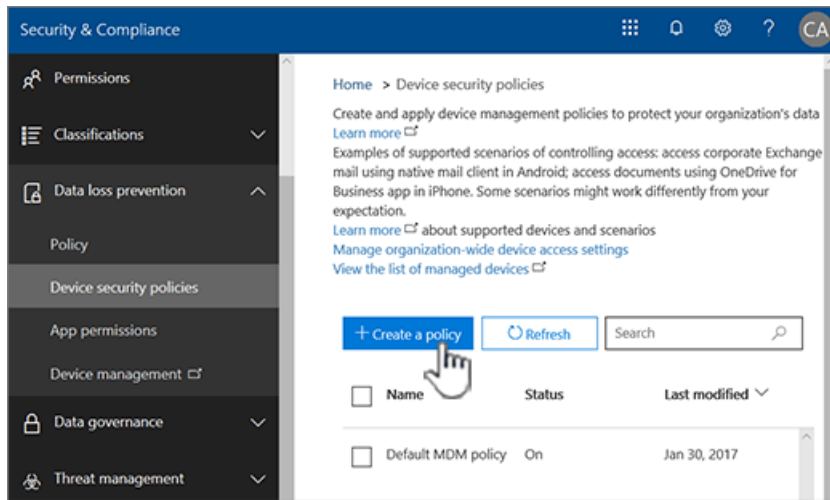
Save Cancel

Step 5: Choose security groups to be excluded from conditional access checks

If you want to exclude some people from conditional access checks on their mobile devices and you've created one or more security groups for those people, add the security groups here. The people in these groups won't have any policies enforced for their supported mobile devices. This is the recommended option if you no longer want to use Basic Mobility and Security in your organization.

1. From your browser, type <https://protection.office.com/devicev2>.

2. Select **Manage organization-wide device access settings**.

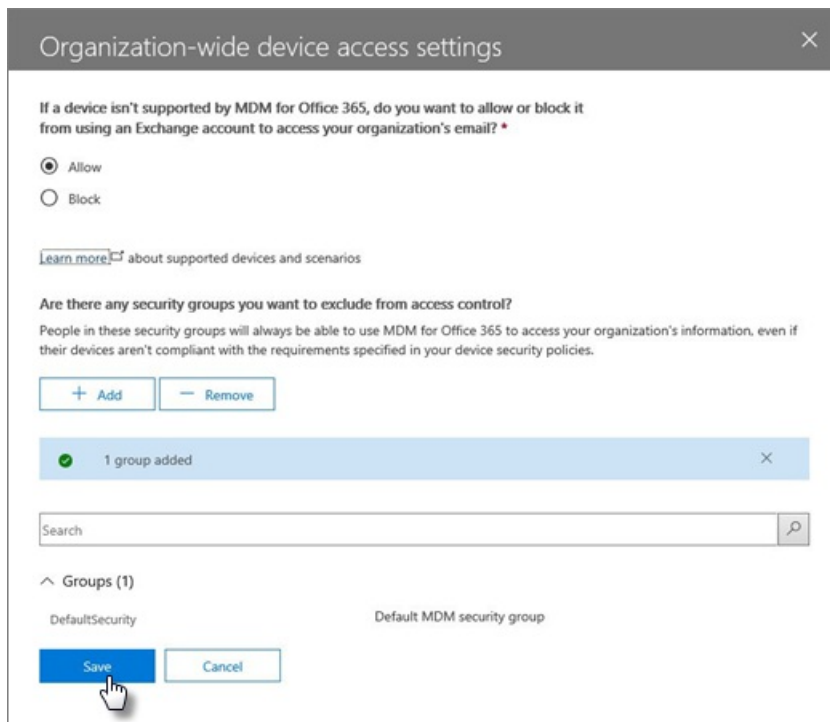


3. Select **Add** to add the security group that has users you want to exclude from having blocked access to Microsoft 365. When a user has been added to this list, they can access Microsoft 365 email when they are using an unsupported device.

4. Select the security group you want to use in the **Select group** panel.

5. Select the name, and then **Add > Save**.

6. On the **Organization-wide device access settings** panel, choose **Save**.



What is the impact of security policies on different device types?

When you apply a policy to user devices, the impact on each device varies somewhat among device types. See the following table for examples of the impact of policies on different devices.

SECURITY POLICY	ANDROID 4 AND LATER	SAMSUNG KNOX	IOS 6 AND LATER	NOTES
Require encrypted backup	No	Yes	Yes	iOS encrypted backup required.

SECURITY POLICY	ANDROID 4 AND LATER	SAMSUNG KNOX	IOS 6 AND LATER	NOTES
Block cloud backup	Yes	Yes	Yes	Block Google backup on Android (grayed out), cloud backup on iOS.
Block document synchronization	No	No	Yes	iOS: Block documents in the cloud.
Block photo synchronization	No	No	Yes	iOS (native): Block Photo Stream.
Block screen capture	No	Yes	Yes	Blocked when attempted.
Block video conference	No	No	Yes	FaceTime blocked on iOS, not on Skype or others.
Block sending diagnostic data	No	Yes	Yes	Block sending Google crash report on Android.
Block access to app store	No	Yes	Yes	App store icon missing on Android home page, disabled on Windows, missing on iOS.
Require password for app store	No	No	Yes	iOS: Password required for iTunes purchases.
Block connection to removable storage	No	Yes	N/A	Android: SD card is grayed out in settings, Windows notifies user, apps installed aren't available

SECURITY POLICY	ANDROID 4 AND LATER	SAMSUNG KNOX	IOS 6 AND LATER	NOTES
Block Bluetooth connection	See notes	See notes	Yes	We can't disable BlueTooth as a setting on Android. Instead, we disable all of the transactions that require BlueTooth: Advanced Audio Distribution, Audio/Video Remote Control, hands-free devices, headset, Phone Book Access, and Serial Port. A small toast message appears at the bottom of the page when any of these are used.

What happens when you delete a policy or remove a user from the policy?

When you delete a policy or remove a user from a group to which the policy was deployed, the policy settings, Microsoft 365 email profile and cached emails might be removed from the user's device. See the following table to see what is removed for the different device types.

WHAT'S REMOVED	IOS 6 AND LATER	ANDROID 4 AND LATER (INCLUDING SAMSUNG KNOX)
Managed email profiles ¹	Yes	No
Block cloud backup	Yes	No

¹ If the policy was deployed with the option **Email profile is managed** selected, the managed email profile and cached emails in that profile are deleted from the user device.

The policy is removed from the mobile device for each user the policy applies to the next time their device checks in with Basic Mobility and Security. If you deploy a new policy that applies to these user devices, they are prompted to re-enroll in Basic Mobility and Security.

You can also wipe a device either completely, or selectively wipe organizational information from the device. For more info, see [Wipe a mobile device in Basic Mobility and Security](#).

Related content

[Overview of Basic Mobility and Security](#) (article)

[Capabilities of Basic Mobility and Security](#) (article)

Create an APNs certificate for iOS devices

6/30/2021 • 2 minutes to read • [Edit Online](#)

To manage iOS devices such as iPads and iPhones in Basic Mobility and Security, create an APNs certificate.

1. Sign in to Microsoft 365 with your global admin account.
2. In your browser, type <https://protection.office.com/>.
3. Select **Data loss prevention** > **Device management**, and choose **APNs Certificate for iOS devices**.
4. On the **Apple Push Notification Certificate Settings** page, choose **Next**.
5. Select **Download** your CSR file and save the certificate signing request to somewhere on your computer that you'll remember. Select **Next**.
6. On the **Create an APNs certificate** page:
 - a. Select **Apple APNS Portal** to open the Apple Push Certificates Portal.
 - b. Sign in with an Apple ID.

IMPORTANT

Use a company Apple ID associated with an email account that will remain with your organization even if the user who manages the account leaves. Save this ID because you'll need to use the same ID when it's time to renew the certificate.

- c. Select **Create a Certificate** and accept the **Terms of Use**.
- d. Browse to the certificate signing request you downloaded to your computer from Microsoft 365, and select **Upload**.

Download the APNs certificate created by the Apple Push Certificate Portal to your computer.

TIP

If you're having trouble downloading the certificate, refresh your browser.

7. Go back to Microsoft 365, and select **Next** to get to the **Upload APNS certificate** page.
8. Browse to the APN certificate you downloaded from the Apple Push Certificates Portal.
9. Select **Finish**.

To complete setup, go back to the **Security & Compliance Center** > **Security policies** > **Device management** > **Manage settings**.

Manage device access settings in Basic Mobility and Security

6/30/2021 • 2 minutes to read • [Edit Online](#)

If you're using Basic Mobility and Security, there might be devices that you can't manage with Basic Mobility and Security. If so, you should block Exchange ActiveSync app access to Microsoft 365 email for mobile devices that aren't supported by Basic Mobility and Security. This helps secure your organization information across more devices.

Use these steps:

1. Sign in to Microsoft 365 with your global admin account.
2. In your browser, type:<https://protection.office.com>.

IMPORTANT

If this is the first time you're using Basic Mobility and Security for Microsoft 365 Business Standard, activate it here: [Activate Basic Security and Mobility](#). After you've activated it, manage your devices with [Office 365 Security & Compliance](#).

3. Go to **Data loss prevention > Device management > Device policies**, and select **Manage organization-wide device access settings**.
4. Select **Block**.

Organization-wide device access settings

If a device isn't supported by MDM for Office 365, do you want to allow or block from using an Exchange account to access your organization's email? *

Allow

Block

[Learn more](#) about supported devices and scenarios

Are there any security groups you want to exclude from access control?

People in these security groups will always be able to use MDM for Office 365 to access their devices aren't compliant with the requirements specified in your device security policy.

+ Add - Remove

Search

^ Groups (0)

Save Cancel

5. Select **Save**.

To learn what devices Basic Mobility and Security supports, see [Capabilities of Basic Mobility and Security](#).

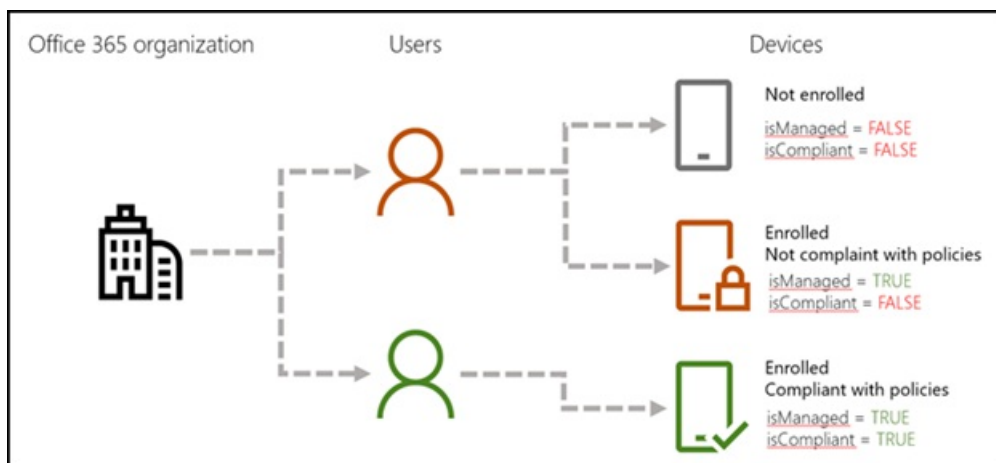
Get details about Basic Mobility and Security managed devices

6/30/2021 • 4 minutes to read • [Edit Online](#)

This article shows you how to use Windows PowerShell to get details about the devices in your organization that you set up for Basic Mobility and Security.

Here's a breakdown for the device details available to you.

DETAIL	WHAT TO LOOK FOR IN POWERSHELL
Device is enrolled in Basic Mobility and Security. For more info, see Enroll your mobile device using Basic Mobility and Security	The value of the <i>isManaged</i> parameter is: True = device is enrolled. False = device is not enrolled.
Device is compliant with your device security policies. For more info, see Create device security policies	The value of the <i>isCompliant</i> parameter is: True = device is compliant with policies. False = device is not compliant with policies.



NOTE

The commands and scripts in this article also return details about any devices managed by [Microsoft Intune](#).

Before you begin

There are a few things you need to set up to run the commands and scripts described in this article.

Step 1: Download and install the Azure Active Directory Module for Windows PowerShell

For more info on these steps, see [Connect to Microsoft 365 with PowerShell](#).

1. Go to [Microsoft Online Services Sign-In Assistant for IT Professionals RTW](#) and select **Download for Microsoft Online Services Sign-in Assistant**.
2. Install the Microsoft Azure Active Directory Module for Windows PowerShell with these steps:
 - a. Open an administrator-level PowerShell command prompt.
 - b. Run the `Install-Module MSOnline` command.

- c. If prompted to install the NuGet provider, type Y and press ENTER.
- d. If prompted to install the module from PSGallery, type Y and press ENTER.
- e. After installation, close the PowerShell command window.

Step 2: Connect to your Microsoft 365 subscription

1. In the Windows Azure Active Directory Module for Windows PowerShell, run the following command.

```
$UserCredential = Get-Credential
```

2. In the Windows PowerShell Credential Request dialog box, type the user name and password for your Microsoft 365 global admin account, and then select **OK**.
3. Run the following command.

```
Connect-MsolService -Credential $UserCredential
```

Step 3: Make sure you're able to run PowerShell scripts

NOTE

You can skip this step if you're already set up to run PowerShell scripts.

To run the `Get-MsolUserDeviceComplianceStatus.ps1` script, you need to enable the running of PowerShell scripts.

1. From your Windows Desktop, select **Start**, and then type `Windows PowerShell`. Right-click `Windows PowerShell`, and then select **Run as administrator**.
2. Run the following command.

```
Set-ExecutionPolicy RemoteSigned
```

3. When prompted, type `Y` and then press `Enter`.

Run the `Get-MsolDevice` cmdlet to display details for all devices in your organization

1. Open the Microsoft Azure Active Directory Module for Windows PowerShell.
2. Run the following command.

```
Get-MsolDevice -All -ReturnRegisteredOwners | Where-Object {$_.RegisteredOwners.Count -gt 0}
```

For more examples, see [Get-MsolDevice](#).

Run a script to get device details

First, save the script to your computer.

1. Copy and paste the following text into Notepad.

```

param (
    [PSObject[]]$users = @(),
    [Switch]$export,
    [String]$exportFileName = "UserDeviceComplianceStatus_" + (Get-Date -Format "yyMMdd_HHMMss") +
    ".csv",
    [String]$exportPath = [Environment]::GetFolderPath("Desktop")
)
[System.Collections.IDictionary]$script:schema = @{
    DeviceId = ''
    DeviceOSType = ''
    DeviceOSVersion = ''
    DeviceTrustLevel = ''
    DisplayName = ''
    IsCompliant = ''
    IsManaged = ''
    ApproximateLastLogonTimestamp = ''
    DeviceObjectId = ''
    RegisteredOwnerUpn = ''
    RegisteredOwnerObjectId = ''
    RegisteredOwnerDisplayName = ''
}
function createResultObject
{
    [PSObject]$resultObject = New-Object -TypeName PSObject -Property $script:schema
    return $resultObject
}
If ($users.Count -eq 0)
{
    $users = Get-MsolUser
}
[PSObject[]]$result = foreach ($u in $users)
{
    [PSObject]$devices = get-msoldevice -RegisteredOwnerUpn $u.UserPrincipalName
    foreach ($d in $devices)
    {
        [PSObject]$deviceResult = createResultObject
        $deviceResult.DeviceId = $d.DeviceId
        $deviceResult.DeviceOSType = $d.DeviceOSType
        $deviceResult.DeviceOSVersion = $d.DeviceOSVersion
        $deviceResult.DeviceTrustLevel = $d.DeviceTrustLevel
        $deviceResult.DisplayName = $d.DisplayName
        $deviceResult.IsCompliant = $d.GraphDeviceObject.IsCompliant
        $deviceResult.IsManaged = $d.GraphDeviceObject.IsManaged
        $deviceResult.DeviceObjectId = $d.ObjectId
        $deviceResult.RegisteredOwnerUpn = $u.UserPrincipalName
        $deviceResult.RegisteredOwnerObjectId = $u.ObjectId
        $deviceResult.RegisteredOwnerDisplayName = $u.DisplayName
        $deviceResult.ApproximateLastLogonTimestamp = $d.ApproximateLastLogonTimestamp
        $deviceResult
    }
}
If ($export)
{
    $result | Export-Csv -path ($exportPath + "\" + $exportFileName) -NoTypeInformation
}
Else
{
    $result
}

```

2. Save it as a Windows PowerShell script file by using the file extension.ps1; for example,Get-MsolUserDeviceComplianceStatus.ps1.

Run the script to get device information for a single user account

1. Open the Microsoft Azure Active Directory Module for Windows PowerShell.
2. Go to the folder where you saved the script. For example, if you saved it to C:\PS-Scripts, run the following command.

```
cd C:\PS-Scripts
```

3. Run the following command to identify the user you want to get device details for. This example gets details for bar@example.com.

```
$u = Get-MsolUser -UserPrincipalName bar@example.com
```

4. Run the following command to initiate the script.

```
.\Get-MsolUserDeviceComplianceStatus.ps1 -User $u -Export
```

The information is exported to your Windows Desktop as a CSV file. You can use additional parameters to specify the file name and path of the CSV.

Run the script to get device information for a group of users

1. Open the Microsoft Azure Active Directory Module for Windows PowerShell.
2. Go to the folder where you saved the script. For example, if you saved it to C:\PS-Scripts, run the following command.

```
cd C:\PS-Scripts
```

3. Run the following command to identify the group you want to get device details for. This example gets details for users in the FinanceStaff group.

```
$u = Get-MsolGroupMember -SearchString "FinanceStaff" | % { Get-MsolUser -ObjectId $_.ObjectId }
```

4. Run the following command to initiate the script.

```
.\Get-MsolUserDeviceComplianceStatus.ps1 -User $u -Export
```

The information is exported to your Windows Desktop as a CSV file. You can use additional parameters to specify the file name and path of the CSV.

Related topics

[Microsoft Connect Has Been Retired](#)

[Overview of Basic Mobility and Security](#)

[Get-MsolDevice](#)

Manage devices enrolled in Mobile Device Management in Microsoft 365

8/13/2021 • 2 minutes to read • [Edit Online](#)

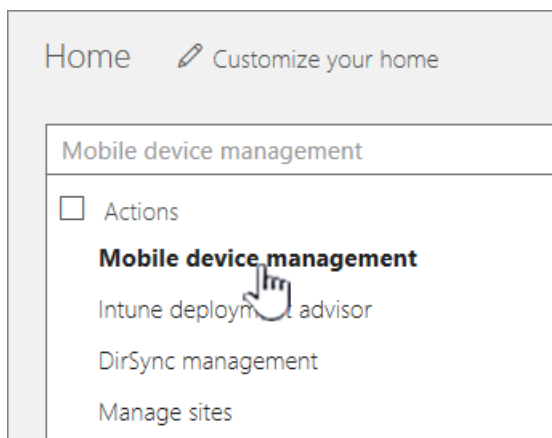
The built-in mobile device management for Microsoft 365 helps you secure and manage your users' mobile devices like iPhones, iPads, Androids, and Windows phones. The first step is to sign in to Microsoft 365 and set up Basic Mobility and Security. For more info, see [Set up Basic Mobility and Security](#).

After you've set it up, the people in your organization must enroll their devices in the service. For more info, see [Enroll your mobile device using Basic Mobility and Security](#). Then you can use Basic Mobility and Security to help manage devices in your organization. For example, you can use device security policies to help limit email access or other services, view devices reports, and remotely wipe a device. You'll typically go to the Security & Compliance Center to do these tasks. For more info, see [Microsoft 365 compliance center](#).

Device management tasks

To get to the device management panel, follow these steps:

1. Go to the [Microsoft 365 admin center](#).
2. Type Mobile Device Management into the search field, and select **Mobile Device Management** from the list of results.



3. Select **Let's get started**.

Manage mobile devices

After you've got Basic Mobility and Security set up, here are some ways you can manage the mobile devices in your organization.

TO DO THIS	DO THIS
Wipe a device	In the Device Management panel, select <i>device name</i> , then Full wipe to delete all information or Selective wipe to delete only organizational information on the device. For more info, see Wipe a mobile device in Basic Mobility and Security .

TO DO THIS	DO THIS
Block unsupported devices from accessing Exchange email using Exchange ActiveSync	In the Device Management panel, select Block .
Set up device policies like password requirements and security settings	In the Device Management panel, select Device security policies > Add + . For more info, see Create device security policies in Basic Mobility and Security .
View list of blocked devices	In the Device Management panel, under Select a view select Blocked .
Unblock noncompliant or unsupported device for a user or group of users	<p>Pick one of the following to unblock devices:</p> <ul style="list-style-type: none"> - Remove the user or users from the security group the policy has been applied to. Go to Microsoft 365 admin center > Groups, and then select group name. Select Edit members and admins. - Remove the security group the users are a member of from the device policy. Go to Security & Compliance Center > Security policies > Device security policies. Select device policy name, and then select Edit > Deployment. - Unblock all noncompliant devices for a device policy. Go to Security & Compliance Center > Security policies > Device security policies. Select device policy name and then select Edit > Access requirements. Select Allow access and report violation. - To unblock a noncompliant or unsupported device for a user or a group of users, go to Security & Compliance Center > Security policies > Device management > Manage device access settings. Add a security group with the members you want to exclude from being blocked access to Microsoft 365. For more info, see Create, edit, or delete a security group in the Microsoft 365 admin center.
Remove users so their devices are no longer managed by Basic Mobility and Security	<p>To remove the user, edit the security group that has device management policies for Basic Mobility and Security. For more info, see Create, edit, or delete a security group in the Microsoft 365 admin center.</p> <p>To remove Basic Mobility and Security from all your Microsoft 365 users, see Turn off Basic Mobility and Security.</p>

Live (v14)

Enroll your mobile device using Basic Mobility and Security

8/13/2021 • 2 minutes to read • [Edit Online](#)

Using your phone, tablet, and other mobile devices for work is a great way to stay informed and work on business projects while you're away from the office. Before you can use Microsoft 365 services with your device, you might need to first enroll it in Basic Mobility and Security for Microsoft 365 using Microsoft Intune Company Portal.

Organizations choose Basic Mobility and Security so that employees can use their mobile devices to securely access work email, calendars, and documents while the business secures important data and meets their compliance requirements. To learn more, see [Overview of Basic Mobility and Security for Microsoft 365](#). For more info, see [What information can my organization see when I enroll my device?](#).

IMPORTANT

When you enroll your device in Basic Mobility and Security for Microsoft 365, you might be required to set up a password, together with allowing the option for your work organization to wipe the device. A device wipe can be performed from the [Microsoft 365 admin center](#), for example, to remove all data from the device if the password is entered incorrectly too many times or if usage terms are broken.

Supported devices

Basic Mobility and Security for Microsoft 365 hosted by the Intune service works with most, but not all, mobile devices. The following are supported with Basic Mobility and Security:

- iOS 10.0 or later
- Android 4.4 or later
- Windows 8.1 and Windows 10 (Phone and PC)

If your device is not listed above, and you need to use it with Basic Mobility and Security, contact your work or school administrator.

TIP

If you're having trouble enrolling your device, see [Troubleshoot Basic Mobility and Security](#).

Set up your mobile device with Intune and Basic Mobility and Security

The Intune Company Portal enables a device to be managed by Microsoft 365 and Basic Mobility and Security.

iPhone or iPad

TIP

You won't be able to send and receive email until you complete this step.

Go to the Apple App Store, and download and install Intune Company Portal.

To connect and configure your iOS phone or tablet with the Company portal to Office 365, see [Set up iOS device access to your company resources](#).

Android phone or tablet

TIP

You won't be able to send and receive email until you complete this step.

Go to the Google Play store, and download and install Intune Company Portal.

To connect and configure your Android phone or tablet with the Company portal to Microsoft 365, see [Enroll your device with Company Portal](#).

Windows 8.1 and Windows 10

Go to the Microsoft Store, and download and install Intune Company Portal

To connect and configure your Windows phone or PC with the Company portal to Microsoft 365, see [Windows device enrollment in Intune Company Portal](#).

Next steps

After your device is enrolled in Basic Mobility and Security, you can start using Office apps on your device to work with email, calendar, contacts, and documents.

Privacy and security in Basic Mobility and Security

3/5/2021 • 2 minutes to read • [Edit Online](#)

Basic Mobility and Security is a cloud-based service powered by Microsoft Intune that helps you manage and secure mobile devices in your organization. After you activate Basic Mobility and Security, you can create mobile device management policies. These policies can then be deployed to mobile devices that have been enrolled by licensed Microsoft 365 users in your organization.

Microsoft Intune sends information to Microsoft 365 about the compliance status of each managed device, and then you can generate reports that show whether managed devices in your organization are compliant based upon the policies that were set. To learn more about Microsoft's commitment to the privacy and security, see the [Microsoft Trust Center](#).

Wipe a mobile device in Basic Mobility and Security

6/30/2021 • 3 minutes to read • [Edit Online](#)

You can use built-in Basic Mobility and Security for Microsoft 365 to remove only organizational information, or to perform a factory reset to delete all information from a mobile device and restore it to factory settings.

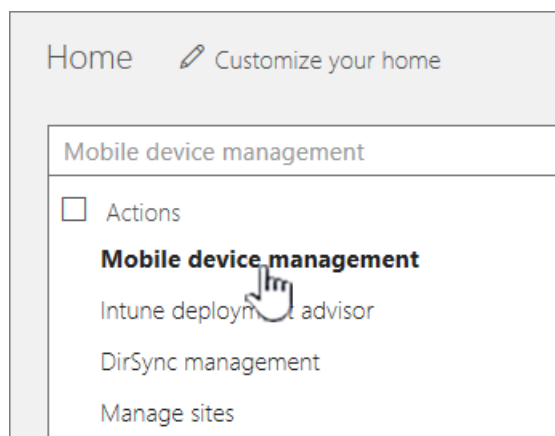
Before you begin

Mobile devices can store sensitive organizational information and provide access to your organization's Microsoft 365 resources. To help protect your organization's information, you can do Factory reset or Remove company data:

- **Factory reset:** Deletes all data on a user's mobile device, including installed applications, photos, and personal information. When the wipe is complete, the device is restored to its factory settings.
- **Remove company data:** Removes only organization data and leaves installed applications, photos, and personal information on a user's mobile device.
- **When a device is wiped (Factory Reset or Remove Company Data),** the device is removed from the list of managed devices.
- **Automatically reset a device:** You can set up a Basic Mobility and Security policy that automatically factory resets a device after the user unsuccessfully tries to enter the device password a specific number of times. To do this, follow the steps in [Create device security policies in basic mobility and security](#).
- **If you want to know the user experience** when you wipe their device, see [What's the user and device impact?](#).

Wipe a mobile device

1. Go to the [Microsoft 365 admin center](#).
2. Type Mobile Device Management into the search field, and select **Mobile Device Management** from the list of results.



3. Select **Manage devices**.
4. Select the device you want to wipe.
5. Select **Manage**.
6. Select the type of remote wipe you want to do.

- To do a full wipe and restore the device to its factory settings, select **Factory reset**.
- To do a selective wipe and delete only Microsoft 365 organization information, select **Remove company data**.
- To remove the device from your organization, select **Remove device**.

7. Select **Yes** to confirm.

How do I know it worked?

You no longer see the mobile device in the list of managed devices.

Why would you want to wipe a device?

Wipe a device for these reasons:

- Mobile devices like smartphones and tablets are becoming more full-featured all the time. This means it's easier for your users to store sensitive corporate information such as personal identification or confidential communications and access it on the go. If one of these mobile devices is lost or stolen, wiping the device can help prevent your organization's information from ending up in the wrong hands.
- When a user leaves the organization with a personal device that is enrolled in Basic Mobility and Security, you can help prevent organizational information from going with that user by performing a factory reset.
- If your organization provides mobile devices to users, you might need to reassign devices from time to time. Doing a Factory Reset on a device before assigning it to a new user helps ensure that any sensitive information from the previous owner is deleted.

What's the user and device impact?

The wipe is sent immediately to the mobile device and the device is marked as not compliant in Azure active directory. While all data is removed when a device is reset to factory defaults, the following table describes what content is removed for each device type when a device when you remove company data.

CONTENT IMPACT	IOS 10 AND LATER	ANDROID 5 AND LATER
Microsoft 365 app data is wiped if the device is protected by Intune App Protection policies. The apps aren't removed. For devices not protected by Mobile Application Management (MAM) policies, Outlook and OneDrive won't remove cached data. Note For applying Intune App protection policies you must have an Intune license.	Yes	Yes
Policy settings applied by Basic Mobility and Security to devices are no longer enforced; users can change the settings.	Yes	Yes
Email profiles created by Basic Mobility and Security are removed and cached email on the device is deleted.	Yes	N/A

NOTE

Company Portal app is available at the App Store for iOS and the Play Store for Android devices.

Turn off Basic Mobility and Security

6/30/2021 • 2 minutes to read • [Edit Online](#)

To effectively turn off Basic Mobility and Security, you remove groups of people defined by security groups from the device management policies, or remove the policies themselves.

- Remove groups of users by removing user security groups from the device policies you've created.
- Disable Basic Mobility and Security for everyone by removing all Basic Mobility and Security device policies.

These options remove Basic Mobility and Security enforcement for devices in your organization. Unfortunately, you can't simply "unprovision" Basic Mobility and Security after you've set it up.

IMPORTANT

Be aware of the impact on users' devices when you remove user security groups from policies or remove the policies themselves. For example, email profiles and cached emails might be removed, depending on the device. For more info, see [What happens when you delete a policy or remove a user from the policy?](#)

Remove user security groups from Basic Mobility and Security device policies

1. In your browser type:<https://protection.office.com/devicev2>.
2. Select a device policy, and select **Edit policy**.
3. On the **Deployment** page, select **Remove**.
4. Under **Groups**, select a security group.
5. Select **Remove**, and select **Save**.

Remove Basic Mobility and Security device policies

1. In your browser type:<https://protection.office.com/devicev2>.
2. Select a device policy, and then select **Delete policy**.
3. In the Warning dialog box, select **Yes**.

NOTE

For more steps to unblock devices if your organization devices are still in a blocked state, see the blog post [Removing Access Control from Mobile Device Management for Office 365](#).

Troubleshoot Basic Mobility and Security

3/5/2021 • 2 minutes to read • [Edit Online](#)

If you're running into issues when you try to enroll a device in Basic Mobility and Security, try the steps here to track down the problem. If the general steps don't fix the issue, see one of the later sections with specific steps for your device type.

Steps to try first

To start, check the following:

- Make sure that the device is not already enrolled with another mobile device management provider, such as Intune.
- Make sure that the device is set to the correct date and time.
- Switch to a different WIFI or cellular network on the device.
- For Android or iOS devices, uninstall and reinstall the Intune Company Portal app on the device.

iOS phone or tablet

- Make sure that you've set up an APNs certificate. For more info, see [Create an APNs Certificate for iOS devices](#).
- In **Settings > General > Profile (or Device Management)**, make sure that a Management Profile is not already installed. If it is, remove it.
- If you see the error message, "Device failed to enroll," sign in to Microsoft 365 and make sure that a license that includes Exchange Online has been assigned to the user who is signed in to the device.
- If you see the error message, "Profile failed to install," try one of the following:
 - Make sure that Safari is the default browser on the device, and that cookies are not disabled.
 - Reboot the device, and then navigate to portal.manage.microsoft.com. Sign in with your Microsoft 365 user ID and password, and attempt to install the profile manually.

Windows RT

- Make sure that your domain is set up in Microsoft 365 to work with Basic Mobility and Security. For more info, see [Set up Basic Mobility and Security](#).
- Make sure that the user is choosing **Turn On** rather than choosing **Join**.

Windows 10 PC

- Make sure that your domain is set up in Microsoft 365 to work with Basic Mobility and Security. For more info, see [Set up Basic Mobility and Security](#).
- Unless you have Azure Active Directory Premium, make sure that the user is choosing **Enroll in Device Management only** rather than choosing **Connect**.

Android phone or tablet

- Make sure the device is running Android 4.4 or later.
- Make sure that Chrome is up to date and is set as the default browser.
- If you see the error message, "We couldn't enroll this device," sign in to Microsoft 365 and make sure that a license that includes Exchange Online has been assigned to the user who is signed in to the device.
- Check the Notification Area on the device to see if any required end-user actions are pending, and if they are, complete the actions.

Share calendars with external users

8/13/2021 • 2 minutes to read • [Edit Online](#)

It's sometimes necessary for your users to schedule meetings with people outside your organization. To simplify the process of finding common meeting times, Microsoft 365 enables you to make calendars available to these people. These are people who need to see free and busy times for users in your organization, but don't have user accounts for your Microsoft 365 organization.

You can enable calendar sharing for all users in your organization in the Microsoft 365 admin center. Once sharing is enabled, your users can use Outlook Web App to share their calendars with anyone inside or outside the organization. People inside the organization can view the shared calendar along with their own calendar. People outside the organization will be sent a URL that they can use to view the calendar. Users in your organization decide when to share and how much to share.

NOTE

If you want to share calendars with an organization that uses Exchange Server 2013 (an on-premises solution), the Exchange administrator will need to set up an authentication relationship with the cloud. This is known as federation, and must meet minimum software requirements. See [Sharing](#) for more information.

Enable calendar sharing using the Microsoft 365 admin center

1. In the admin center, go to **Settings** > **Org settings**, and on the **Services tab**, select **Calendar**.
2. On the **Calendar** page, choose whether you want to let users share their calendars with people outside of your organization who have Microsoft 365 or Exchange. Choose whether you want to allow anonymous users (users without credentials) to access calendars via an email invitation.
3. Choose what type of calendar information to make available to users. You can allow all information, or limit it to time only or time, subject, and location only.

Invite people to access calendars

Once sharing is enabled, calendar owners can extend invitations to specific users. For instructions, see [Sharing your calendar in Outlook Web App](#).

Related content

[Turn external sharing on or off for a site](#) (article)

[Overview of the Microsoft 365 admin center](#) (video)

[Manage email and calendars](#) (link page)

Create a team with guests


4/3/2021 • 2 minutes to read • [Edit Online](#)

Try it!

You can use Microsoft Teams to work together on a project with your employees and people outside the business, like your clients.

1. In Teams, choose **Teams** in the left navigation, and then choose **Create team**.
2. In the **Create your team** box, enter a team name, provide a short description, choose a privacy setting, and then choose **Next**.
3. In the **Add members** box, enter the names of other employees in your organization. For outside guests, enter their email address.

If you get a message that you can't add a guest, visit the Teams and Skype admin center to turn on guest access.

4. Choose **Add** , and then choose **Close**.
5. At the bottom of the page, enter a short welcome message to your new team, and then choose **Send**  .

Your client will receive an email invitation from Teams, which will inform them that they need a free Microsoft account to join the team. They can create an account using their existing email address by following the instructions provided. They can then use Teams on the web or install the Teams app on their computer.

Schedule a Teams meeting with external users

5/28/2021 • 2 minutes to read • [Edit Online](#)

You can invite people from outside of your organization to a meeting without having to add them to Microsoft Teams. Here's how it works for your customers or partners when they [join a meeting without a Teams account](#).

Try it!

To schedule meetings with your employees, clients, External users and other guests, use Microsoft Teams.

1. In Microsoft Teams, in the left navigation, choose **Meetings**.
2. Choose **Schedule a meeting**.
3. In the **New meeting box**, enter a **Title** and **Location** for the meeting.
4. Enter a **Start** and **End** time and date.
5. In the **Details** box, enter a description of the meeting and any other details you want to add, such as a meeting agenda.
6. Under **Invite people**, enter the names of employees or clients that you want to invite.
7. If you see **Tentative** or **Busy** below any names, choose one of the **Free** times provided, or click **Scheduling assistant** for more options.
8. Choose **Schedule a meeting**.

Join a Teams meeting with guests

4/3/2021 • 2 minutes to read • [Edit Online](#)

With Microsoft Teams, you can easily join and participate in meetings with both internal and external users.

Try it!

1. In Microsoft Teams, choose **Calendar**, and find your meeting.
2. Select **Join**, decide whether you want your camera and microphone on or off, and select **Join Now**.
3. If you're an external guest, open the e-mail you received about the meeting and select **Join Microsoft Teams Meeting**.

If you don't want to download the app, choose **Join on the web** instead.

4. Enter your name and select **Join Now**.
5. Once everyone has arrived, you can start your meeting by sharing your desktop, a monitor, or an app like PowerPoint.
6. When the meeting is over, select **Hang up**.

Get support

7/26/2021 • 12 minutes to read • [Edit Online](#)

Watch: Get help or support

Need to speak to someone right away? Admins, have your account details ready when you call Support.

IMPORTANT

You must be an admin for a business subscription to use these support methods. If you're not a business admin, please use [this support page](#).

Start by [checking the current health of your services](#). You can view detailed information about current and past issues on the [Service health dashboard](#). If you're experiencing an issue that isn't listed, you can get support in one of the following ways:

Online support

Save time by starting your service request online. We'll help you find a solution or connect you to technical support.

1. Go to the admin center at <https://admin.microsoft.com>. If you get a message that says you don't have permission to access this page or perform this action, then you aren't an admin. (For more information, see [Who has admin permissions in my business?](#))
2. If the results don't help, select **Contact support**.
3. Enter a description of your issue, confirm your contact number and email address, select your preferred contact method, and then select **Contact me**. The expected wait time is indicated in the **Need help?** pane.

Phone support

Billing support is provided in English from 9 AM-5 PM (9 AM-6 PM in Australia), Monday-Friday.

Technical support is provided in English 24 hours a day, 7 days a week.

Admins, have your account details ready when you call.

NOTE

To better protect your organization, we added a PIN-based verification step to our existing phone-based verification process. If you contact us from a number that isn't registered with your organization profile, the Microsoft support representative sends a verification code to the registered email or phone number in your Microsoft 365 admin center profile. You must provide this code to the support representative to grant them access to your organization's account.

- In the United States, call 1 800 865 9408.
- In Australia, call 1 800 197 503.
- In Canada, call 1 800 865 9408.

- In the United Kingdom, call 0800 032 6417.

If your support phone number isn't listed above, use the drop-down menu below to find the number for your country or region.

With every subscription of Office 365 operated by 21Vianet, 21Vianet support provides technical, pre-sales, billing and subscription support. Support is available both online through the Office 365 operated by 21Vianet portal, and by telephone for both paid and trial subscriptions.

Authorized administrators can use the Office 365 operated by 21Vianet portal to submit service requests online and access support telephone numbers. For instructions, see [Contact support](#).

The Office 365 operated by 21Vianet technical support team troubleshoots only those issues that are related to Office 365 operated by 21Vianet. Issues that originate in customer networks fall outside of the Office 365 support boundaries, and in these cases, customers must work with their networking team for assistance.

Community and self-service support options

Self-service support is available for all Office 365 operated by 21Vianet users, and includes troubleshooting tools and videos, help articles and videos, as well as forums and wikis in the [Office 365 community](#). For more self-help resources, see [Learn about Office 365 operated by 21Vianet](#).

Pre-sales support

Pre-sales support for Office 365 operated by 21Vianet provides assistance on subscription features and benefits, plan comparisons, pricing and licensing, and helps to identify the right solution to meet your business needs. In addition, pre-sales support can help you find a Partner, and purchase and sign up for a trial. You can call during local business hours, Monday through Friday. Pre-sales support can be accessed using the same phone number as with technical support. For instructions, see [Contact support](#).

Billing and subscription management support

Assistance for billing and subscription management issues is available online or by telephone during China business hours (Beijing Time), Monday through Friday. Billing and subscription management support can be accessed using the same phone number and online service request process as with technical support. The support telephone number can be found on the Office 365 operated by 21Vianet portal. For instructions, see [Contact support](#).

Here are some examples of billing and subscription management issues:

- Signing up for a trial or purchasing a subscription
- Converting from a trial subscription to a paid subscription
- Understanding the bill
- Renewing a subscription
- Adding or removing licenses
- Canceling a paid subscription

Technical support

Technical support for Office 365 operated by 21Vianet subscriptions provides assistance with basic installation, setup, and general technical usage. Some examples of these issues are listed in the following table.

SUPPORT CATEGORY	EXAMPLES
Installation and setup	<p>Exchange Online</p> <ul style="list-style-type: none"> Office 365 mailbox migration Recipient configuration (mailbox permissions, configuring mail forwarding, configuring shared mailbox) Autodiscover configuration <p>SharePoint Online</p> <ul style="list-style-type: none"> Permissions and user groups Configuration of external users <p>Skype for Business Online</p> <ul style="list-style-type: none"> Installation and creating contacts <p>Microsoft 365 Apps for enterprise</p> <ul style="list-style-type: none"> Installation and setup
Configuration	<p>Service configuration issues</p> <ul style="list-style-type: none"> Single sign-on (SSO) Active Directory synchronization

NOTE

You can learn how to contact technical support here: [Contact support](#). Technical support does not include troubleshooting third-party services or add-ins. Learn about finding answers from other customers in the [Community](#).

Technical support case handling

21Vianet assigns a severity level to a case when it is opened, based on an assessment of the issue type and customer impact. Examples of issue types and severity levels are shown in the following table.

SEVERITY LEVEL	OPERATIONS AND SUPPORT DESCRIPTION	EXAMPLES
Sev A (Critical)	One or more services aren't accessible or are unusable. Production, operations, or deployment deadlines are severely affected, or there will be a severe impact on production or profitability. Multiple users or services are affected.	<ul style="list-style-type: none"> Widespread problems sending or receiving mail. SharePoint site down. All users can't send instant messages, join or schedule Skype for Business Meetings, or make Skype for Business calls.
Sev B (High)	The service is usable but in an impaired fashion. The situation has moderate business impact and can be dealt with during business hours. A single user, customer, or service is partially affected.	<ul style="list-style-type: none"> Send button in Outlook is garbled. Setting is impossible from EAC (Exchange admin center) but possible in Windows PowerShell.

SEVERITY LEVEL	OPERATIONS AND SUPPORT DESCRIPTION	EXAMPLES
Sev C (Non-critical)	The situation has minimal business impact. The issue is important but does not have a significant current service or productivity impact for the customer. A single user is experiencing partial disruption, but an acceptable workaround exists.	<ul style="list-style-type: none"> • How to set user password that never expires. • User can't delete contact information in Exchange Online.

Technical support initial response times

Initial response time is based on the severity levels described above. 21Vianet customer service team follow up with investigation and customer communication in reasonable rhythm according to severity levels. 21Vianet also expect customer to collaborate at reasonable level accordingly.

SECURITY LEVEL ¹	21VIANET CUSTOMER SUPPORT TEAM INITIAL RESPONSE	CUSTOMER RESPONSIBILITY
Sev A ² (Critical)	Initial Response: 1 hour or less; Follow up: continues effort until problem resolution.	Provide solid business impact statement (see the severity A description and examples above); Allocate resource to ensure continues collaboration with 21Vianet customer support agent for the joint investigation and necessary communication; Provide accurate contact information and ensure reliable communication throughout the service request lifecycle.
Sev B (High)	Initial Response: 1 business day or less.	Provide accurate contact information and ensure reliable communication throughout the service request lifecycle.
Sev C (Medium)	Initial Response: 3 business day or less.	Provide accurate contact information and ensure reliable communication throughout the service request lifecycle.

¹ If the customer cannot provide required resource or make response for collaboration with 21Vianet customer support agent investigation in reasonable time, 21Vianet support team may lower down the severity level of a service request.

² Severity A is only available to customers who had signed an advanced online service agreement with 21Vianet through a sales account manager. Severity A is available only for technical support. For billing and subscription management support, the highest severity level is B.

Technical support working hours

Severity A: 24*7 continuous service

Severity B/C: 9:00 ~24:00 (Beijing Time) a day, 365 days.

Contact support

NOTE

Assisted support options are for admins of Office 365 subscribed organizations only. If you use Office 365 but you're not an admin, you can still get support in the community forums, or by contacting your admin.

Open an online request

Save time by starting your service request online. In the Microsoft 365 admin center, choose **Support > New service request**.

Call support

Call support. If you encounter any problem with online request, phone support is available at (86) 400-089-0365.

Shared support responsibilities

21Vianet understands that receiving timely technical support from qualified professionals is a key aspect of cloud services. Equally important is the critical role that the customer's IT department plays in the support of its users.

Administrator roles and responsibilities

People with administrator roles are the only ones in the customer's organization authorized to access the Admin section of the Office 365 operated by 21Vianet portal and to communicate directly with 21Vianet about Office 365 service requests.

With Office 365 you can designate several types of administrators who serve different functions. This service description uses the generic title administrator to refer to all categories of administrators. For more information about the types of administrator roles, see [Assign admin roles in Microsoft 365 for business](#).

The administrator is:

- Responsible for service administration and account maintenance.
- The primary contact that sets up and supports each service user.
- Authorized to submit service requests to 21Vianet.

The administrator's role is to:

- Provide user account setup and configuration to allow users access to the services.
- Address client connectivity, client software, and mobility installation issues.
- Address service availability issues within the customer's organizational span of control.
- Use self-service support resources to resolve support issues.

The administrator is expected to provide initial assistance for the customer's users. However, if the administrator is unable to resolve issues with the help of self-service support resources, he or she should [Contact support](#).

21Vianet support role

21Vianet's support role is to:

- Troubleshoot and provide technical guidance for customer issues and escalations.
- Gather and validate information related to specific service requests.
- Provide issue coordination and resolution management.
- Maintain communication with the administrators to help ensure that issues are addressed on an ongoing basis.

- Provide assistance with licensing, invoicing, and subscription inquiries.
- Provide assistance with purchasing and trial inquiries.
- Continually gather customer feedback on how to improve the service through surveys.

Feature availability

To view feature availability across Office 365 plans, see [Office 365 Service Description](#).

Follow us on WeChat

Scan this QR code to follow us on WeChat and get the latest updates for Office 365 operated by 21Vianet.



This article applies to customers of Office 365 Germany, which has domains ending onmicrosoft.de. For more information, see [Learn about Office 365 Germany](#).

As an admin for Office 365 Germany, you get free access to our knowledgeable support agents for help resolving technical issues, as well as for pre-sales, account, and billing support. You can also contact us on behalf of Office 365 Germany users in your organization.

NOTE

All of the support options below are for Microsoft Cloud Germany. For more information about how Microsoft uses the data that you provide when you contact Microsoft support, please see the [privacy statement](#).

Get assisted support

Assisted support options are for admins of Office 365 Germany subscribed organizations only. If you use Office 365 Germany at work or school, but you're not an admin, you can still get support in the community forums, or by contacting your admin or IT department.

- **Open an online request.** Save time by starting your service request online. In the admin center, choose **Support > New service request**. We'll help you find a solution or connect you to an expert who will contact you by email or phone.
- **Call support.** We're here to talk. Admins, have your account details ready when you call support.

REGION	PHONE NUMBER	HOURS
--------	--------------	-------

REGION	PHONE NUMBER	HOURS
Germany	0800 589 2330	<p>Billing Support:</p> <ul style="list-style-type: none"> • German: Mon-Fri 9-5 Berlin • English: Mon-Fri 9-5 Berlin <p>Technical Support:</p> <ul style="list-style-type: none"> • German: 24 hours a day, 7 days a week • English: 24 hours a day, 7 days a week <p>Alternative Phone Number: 069 380 789 305 (Local call charges apply)</p>
All other markets within the European Economic Area	+49 69 380 789 305	<p>Billing Support:</p> <ul style="list-style-type: none"> • German: Mon-Fri 9-5 Berlin(UTC+1) • English: Mon-Fri 9-5 Berlin (UTC +1) <p>Technical Support:</p> <ul style="list-style-type: none"> • German: 24 hours a day, 7 days a week • English: 24 hours a day, 7 days a week <p>Telephone support is available via international call to Germany. International call charges apply. Call charges can be avoided by submitting a support ticket through the admin center.</p>

Let our community help

You can also [search the Microsoft 365 for business community forums](#) to find known issues and trending topics, or to post a new question. The community forums are monitored by trained Microsoft support agents who can help resolve your issue.

Related content

[Find docs and training](#) (article)

[Employee quick setup](#) (article)

[Overview of Microsoft 365 Business Premium setup](#) (video)

Microsoft 365 docs navigation guide

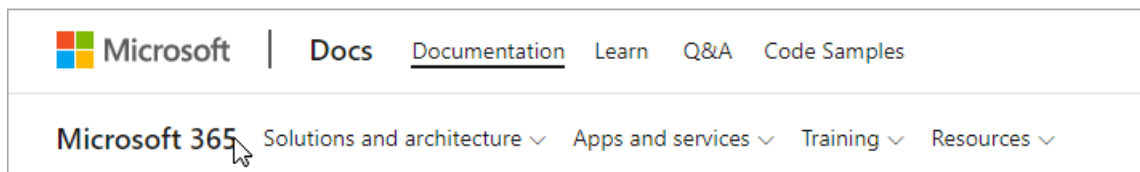
6/14/2021 • 2 minutes to read • [Edit Online](#)

This topic provides some tips and tricks for navigating the Microsoft 365 technical documentation space.

Hub page

The Microsoft 365 hub page can be found at <https://aka.ms/microsoft365docs> and is the entry point for finding relevant Microsoft 365 content.

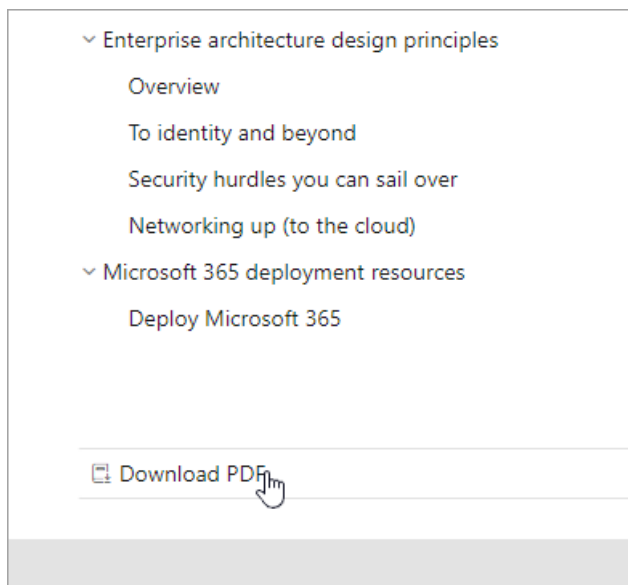
You can always navigate back to this page by selecting **Microsoft 365** from the header at the top of every page within the Microsoft 365 technical documentation set:



Offline documentation

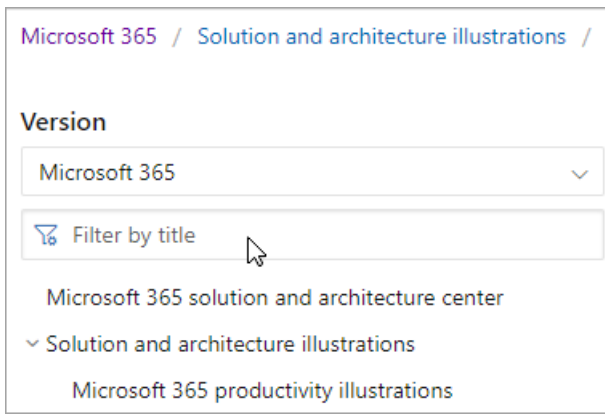
If you would like to view the Microsoft 365 documentation on an offline system, you can create a PDF wherever you are in the Microsoft 365 technical documentation.

If you'd like to create a PDF, select the **Download PDF** link found at the bottom of every table of contents.



TOC search

On docs.microsoft.com, you can search the content in the table of contents by using the filter search box at the top:



Version filter

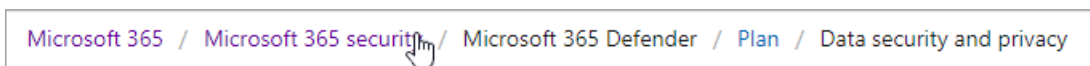
The Microsoft 365 technical documentation provides content for additional products, including Office 365 Germany and Office 365 operated by 21 Vianet (China). Features can vary between these versions, and as such, sometimes the content itself can vary.

You can use the version filter to ensure that you are seeing content for the appropriate version of Microsoft 365:



Breadcrumbs



Breadcrumbs can be found below the header and above the table of contents, and indicate where the current article is located in the table of contents. Not only does this help set the context to what type of content you're reading, but it also allows you to navigate back up the table of contents tree:



Article section navigation

The right-hand navigation pane allows you to quickly navigate to sections within an article, as well as identify your location within the article.

Is this page helpful?

 Yes  No

In this article

- Step 1: Set up multi-factor authentication and conditional access policies**
- Step 2: Configure Microsoft Defender for Identity
- Step 3: Turn on Microsoft 365 Defender
- Step 4: Configure Microsoft Defender for Office 365
- Step 5: Configure Microsoft Defender for Endpoint
- Step 6: Configure Microsoft Cloud App Security
- Step 7: Monitor status and take actions
- Step 8: Train users

Submit docs feedback

If you find something wrong within an article, you can submit feedback to the SQL Content team for that article by scrolling down to the bottom of the page and selecting **Content feedback**.

Feedback

Submit and view feedback for

"/>

Contribute to Microsoft 365 documentation

Did you know that you could edit the content on docs.microsoft.com yourself? If you do so, not only will our documentation improve, but you'll also be credited as a contributor to the page. To get started, see:

- [Microsoft Docs contributor guide](#)

Next steps

- Get started with the [Microsoft 365 technical documentation](#).