

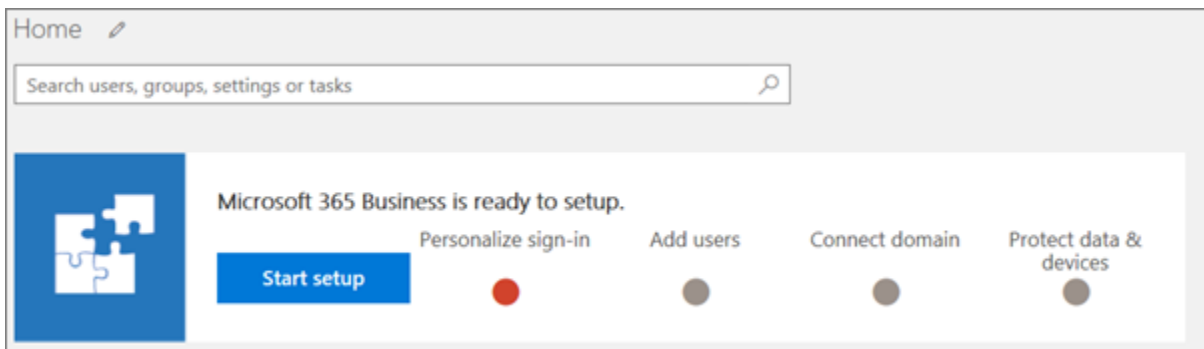
# Set up Microsoft 365

## Personalize sign-in

1. Sign in to [Microsoft 365](#) by using your global admin credentials. Choose the **Admin** tile to go to the admin center.
2. Choose **Start setup** (depending on your state you may see **Continue setup** instead) in the admin center to start the wizard.
3. Enter the domain name you want to use (like contoso.com).

Go ahead and enter your domain even if you have verified it while using Azure AD Connect, for example. The following two steps do not apply to you if you used Azure AD Connect to verify your domain.

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.



## Add users and assign licenses

1. You can add users here, or you can [add users later](#) in the admin center.

Any users you add get automatically assigned a Microsoft 365 Business license.

2. If your Microsoft 365 Business subscription has existing users (for example, if you used Azure AD Connect), you will get an option to assign licenses to them now. Go ahead and add licenses to them as well.
3. You will 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.
4. Skip migrating email messages and choose **Next** on **Migrate email messages** page.

If you are moving from another email provider and want to copy your data later, you can [Migrate email and contacts to Office 365](#).

## Connect your domain

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](#).
2. Email and other services will be set up for you

## Manage devices and work files

1. On the **Protect work files on your mobile devices** page set both **Protect work files when devices are lost or stolen** and **Manage how users access Office files on mobile devices** settings to **On**. You can also access each sub-setting by clicking the chevrons next to each setting.

All of your licensed users' work files are now protected on iOS and Android devices, as soon as they [install Office apps](#) (and authenticate with their Microsoft 365 Business credentials).

The screenshot shows the Microsoft 365 Business Admin center 'Setup' page. At the top, there's a navigation bar with 'Microsoft' and 'Admin center'. Below it, a progress bar shows four steps: Step 1 (Personalize sign-in), Step 2 (Add users), Step 3 (Connect domain), and Step 4 (Protect data & devices). Steps 1, 2, and 3 are marked with green checkmarks, while Step 4 is marked with a red dot. The main heading is 'Protect work files on mobile devices'. Below this, there's explanatory text: 'These settings let users safely access email and work files on their mobile devices, without you needing to manage the device or the user's personal information. If a device is lost or stolen, admins can remotely remove company data without affecting personal data.' Another line of text states: 'Office apps are protected by these settings and, by default, they are applied to Windows, iOS, and Android devices for all users. [Learn more about protecting work files on mobile devices](#)'. There are two toggle switches: 'Protect work files when devices are lost or stolen' and 'Manage how users access Office files on mobile devices', both of which are currently turned 'On'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted in red), and 'Exit and continue later'.

2. On the **Set Windows 10 device configuration** page, set **Secure Windows 10 Devices** setting to **On**.

You can also access each sub-setting by clicking the chevron next to it.

3. Set the **Install Office on Windows 10 Devices** setting to **Yes** if all of your users have Windows 10 computers, and either no existing Office installs, or click-to-run Office installs. If this is not the case, set this option to **No**. You can [automatically install Office](#) later from the admin center after you have prepared the user computers. For instructions, see [prepare for Office client installation](#).

The licensed users' work files on Windows 10 devices will be projected as soon as they [join their Windows 10 device](#) to a Microsoft 365 Business Azure AD domain or [install Windows 10 on a new computer](#) while simultaneously joining the Microsoft 365 Business Azure AD domain.

4. Click **Next** and you are done with setup.

Microsoft

Admin center

Setup  
Microsoft 365 Business

Step 1  
Personalize sign-in  
✓

Step 2  
Add users  
✓

Step 3  
Connect domain  
✓

Step 4  
Protect data & devices  
●

## Set Windows 10 device configuration

When a user connects a Windows 10 device to your organization, they'll automatically receive the settings you configure below. You can also make sure that users get the latest version of Office installed on their devices. We recommend that you start with the default settings and adjust your configuration later. [Learn more about configuring Windows 10](#)

Secure Windows 10 devices ⓘ

☒ On

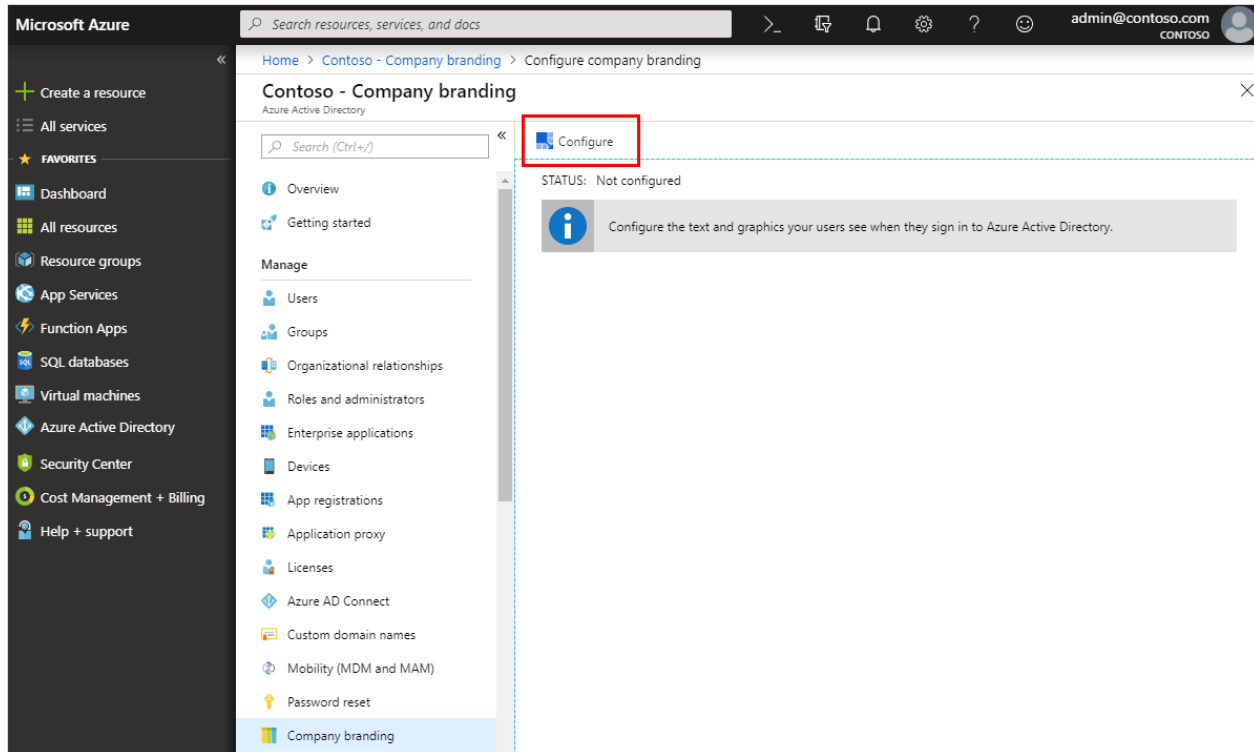
Install Office on Windows 10 devices ⓘ

☐ No

[Back](#) **Next** ⓘ [Exit and continue later](#)

## Customize your branding

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, and then select **Company branding**, and then select **Configure**.



3. On the **Configure company branding** page, provide any or all of the following information.
  - **General settings**

Home > Contoso - Company branding > Configure company branding

## Configure company branding

Contoso

Save Discard Delete

Language ⓘ Default

Sign-in page background image  
Image size: 1920x1080px  
File size: <300KB  
File type: PNG or JPG ⓘ

Remove  
Select a file

Banner logo  
Image size: 280x60px  
File size: 10KB  
File type: Transparent PNG or JPG ⓘ

Remove  
Select a file

Username hint ⓘ Forgot your username? ✓

Sign-in page text ⓘ If you need help, contact the Help Desk online at [www.contoso.com/helpdesk](http://www.contoso.com/helpdesk). ✓

- **Language.** The language is automatically set as your default and can't be changed.
- **Sign-in page background image.** Select a .png or .jpg image file to appear as the background for your sign-in pages.

The image can't be larger than 1920x1080 pixels in size and must have a file size of less than 300 KB.

- **Banner logo.** Select a .png or .jpg version of your logo to appear on the sign-in page after the user enters a username and on the **My Apps** portal page.

The image can't be taller than 36 pixels or wider than 245 pixels. We recommend using a transparent image since the background might not match your logo background. We also recommend not adding padding around the image or it might make your logo look small.



- **Username hint.** Type the hint text that appears to users if they forget their username. This text must be Unicode, without links or code, and can't exceed 64 characters. If guests sign in to your app, we suggest not adding this hint.
- **Sign-in page text.** Type the text that appears on the bottom of the sign-in page. You can use this text to communicate additional information, such as the phone number to your help desk or a legal statement. This text must be Unicode and not exceed 256 characters. We also suggest not including links or HTML tags.

- **Advanced settings**



**Advanced settings**

Sign-in page background color ⓘ  ✓

Square logo image  
Image size: 240x240x(resizable)  
Max file size: 10KB  
PNG (preferred) or JPG ⓘ

 Remove  

Square logo image, dark theme  
Image size: 240x240x(resizable)  
Max file size: 10KB  
PNG (preferred) or JPG ⓘ

 Remove  

Show option to remain signed in ⓘ ☒ Yes ☐ No

- **Sign-in page background color.** Specify the hexadecimal color (for example, white is #FFFFFF) that will appear in place of your background image in low-bandwidth connection situations. We recommend using the primary color of your banner logo or your organization color.
- **Square logo image.** Select a .png (preferred) or .jpg image of your organization's logo to appear to users during the setup process for new Windows 10 Enterprise devices. This image is only used for Windows authentication and appears only on tenants that are

using [Windows Autopilot](#) for deployment or for password entry pages in other Windows 10 experiences.

The image can't be larger than 240x240 pixels in size and must have a file size of less than 10 KB. We recommend using a transparent image since the background might not match your logo background. We also recommend not adding padding around the image or it might make your logo look small.

- **Square logo image, dark theme.** Same as the square logo image above. This logo image takes the place of the square logo image when used with a dark background, such as with Windows 10 Azure AD joined screens during the out-of-box experience (OOBE). If your logo looks good on white, dark blue, and black backgrounds, you don't need to add this image.
- **Show option to remain signed in.** You can choose to let your users remain signed in to Azure AD until explicitly signing out. If you choose **No**, this option is hidden, and users must sign in each time the browser is closed and reopened.

4. After you've finished adding your branding, select **Save**.

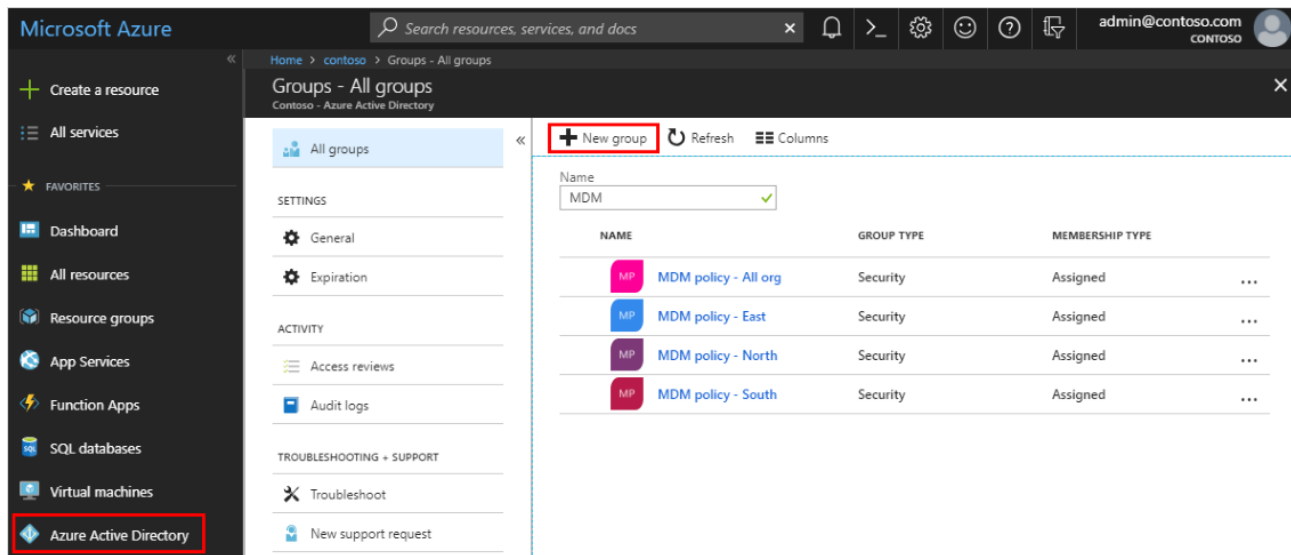


## Create a basic group and add members

You can create a basic group and add your members at the same time.

To create a basic group and add members

1. Sign in to the [Azure portal](#) using a Global administrator account for the directory.
2. Select **Azure Active Directory**, **Groups**, and then select **New group**.



3. In the **Group** page, fill out the required information.

Microsoft Azure

Home > contoso > Groups - All groups > Group

Group

\* Group type  
Security

\* Group name ⓘ  
MDM policy - West ✓

Group description ⓘ  
MDM users on West coast ✓

\* Membership type ⓘ  
Assigned

Members ⓘ  
0 members selected >

Create

- **Group type (required).** Select **Security**
- **Group name (required).** Add a name for the group, something that you'll remember and that makes sense.
- **Group description.** Add an optional description to your group.
- **Membership type (required).** Select **Dynamic device**

4. Select **Create**.

Your group is created and ready for you to add members.

5. Select the **Members** area from the **Group** page, and then begin searching for the members to add to your group from the **Select members** page.

The screenshot shows the 'Select members' dialog in Microsoft Intune. On the left, the group configuration is visible: Group type is 'Security', Group name is 'MDM policy - West', Group description is 'MDM users on West coast', and Membership type is 'Assigned'. A red box highlights the 'Members' section, which indicates '2 members selected'. At the bottom left is a 'Create' button. On the right, the 'Select member or invite an external user' search bar contains the name 'Alain' and has a green checkmark. Below this, a list of members is shown: 'Alain Charon' (alain@contoso.com) with a teal icon, 'Danielle McKay' (danielle@contoso.com) with a black icon, and 'Eggert Schafer' (eggert@contoso.com) with a pink icon. Each member has a 'Remove' button. A red box highlights the 'Select' button at the bottom right of the dialog.

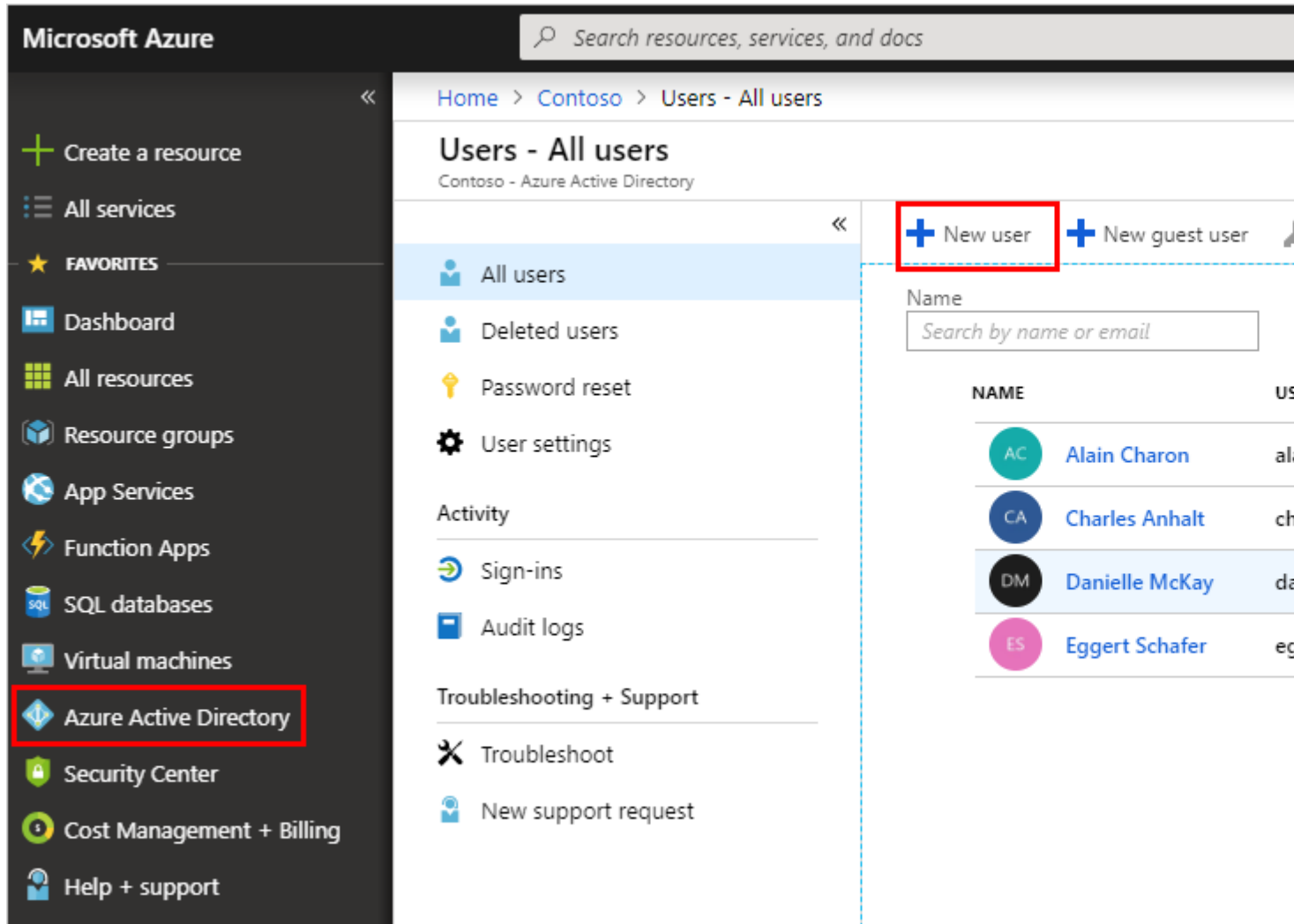
6. When you're done adding members, choose **Select**.

The **Group Overview** page updates to show the number of members who are now added to the group.

The screenshot shows the 'MDM policy - West' Group Overview page. The left sidebar contains navigation options: Overview (selected), Properties, Members, Owners, Group memberships, Applications, Licenses, Azure resources, Access reviews, and Audit logs. The main content area displays the group's details: 'MDM policy - West' with a green icon labeled 'MP'. Below this, a table shows the group's configuration: Membership type is 'Assigned', Type is 'Security', Source is 'Cloud', and Group membership is 'Cloud'. A red box highlights the 'Members' section, which shows '50 User(s)'. Below this, a summary of group statistics is displayed: 0 Group(s), 50 Device(s), and 0 Other(s). At the bottom, the 'Group memberships' and 'Owners' sections are shown, with 0 group memberships and 2 owners respectively.

## Add a new user

1. Sign in to the [Azure portal](#) as a Global administrator or user administrator for the directory.
2. Select **Azure Active Directory**, select **Users**, and then select **New user**.



3. On the **User** page, fill out the required information.

Home > Contoso > Users - All users > User

## User

Contoso

\* Name ⓘ  
Mary Parker ✓

\* User name ⓘ  
mary@contoso.com ✓

---

Profile ⓘ  
Not configured >

---

Properties ⓘ  
Default >

---

Groups ⓘ  
0 groups selected >

---

Directory role  
User >

---

Password  
.....  
☐ Show Password

Create

- **Name (required).** The first and last name of the new user. For example, Mary Parker.
- **User name (required).** The user name of the new user. For example, mary@contoso.com.

The domain part of the user name must use either the initial default domain name, `<yourdomainname>.onmicrosoft.com`, or a custom domain name, such as `contoso.com`.

- **Profile.** Optionally, you can add more information about the user. You can also add user information at a later time.
- **Groups.** Optionally, you can add the user to one or more existing groups. You can also add the user to groups at a later time.

- **Directory role.** Optionally, you can add the user to a directory role. You can assign the user to be a global administrator, or to one or more of the other administrator roles in Azure AD.
4. Copy the auto-generated password provided in the **Password** box. You'll need to give this password to the user for the initial sign-in process.
  5. Select **Create**.

The user is created and added to your Azure AD tenant.

## Assign a license to the user

After you've created a user, you must use the [Microsoft 365 Admin Center](#) to assign an Intune license to that user. Without assigning a license, they can't enroll their device into Intune.

1. Sign in to the [Microsoft 365 Admin Center](#) with the same credentials you used to sign in to Intune.
2. Choose **Users > Active Users** > choose the user you just created.
3. Next to **Product licenses** select **Edit**.
4. Under **Location**, choose a location for the user.
5. Click **On** next to the Intune license (or another license that you have that includes Intune). The displayed [product name](#)\*\* is used as the service plan in the Azure management

### Note

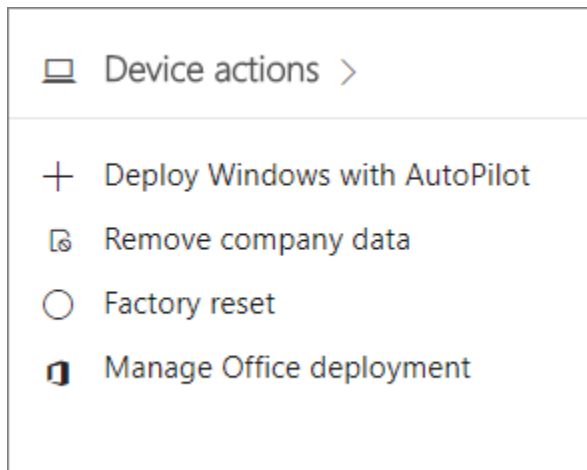
This setting uses one of your licenses for this user. If you are using a trial environment, you would later reassign this license to a real user in a live environment.

6. Choose **Save > Close**.

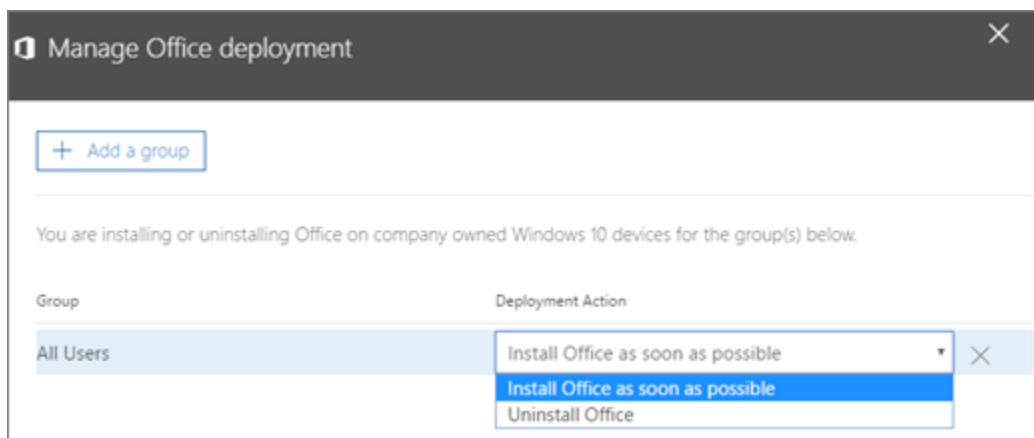
The new active Intune user will now show that they are using an **Intune** license.

## Automatically install or uninstall Office on Windows 10 devices

1. Sign in to the [admin center](#) with global admin credentials.
2. On the **Devices** card, choose **Manage Office Deployment**. If you do not see the **Device actions** card, in the admin center **Homepage**, click **Add** (+) to add it to your admin home.



3. On the **Manage Office deployment** pane that opens, choose **Add a group**, then select the groups you want use.
4. After you have added the group or groups you want to use, from the **Deployment Action** drop-down, select either **Install Office as soon as possible** or **Uninstall Office**.

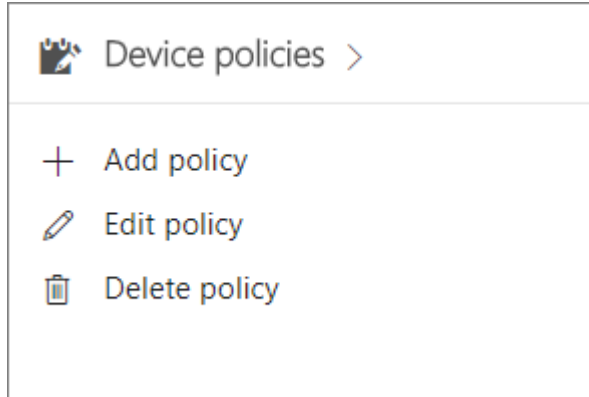


5. Choose **Next** > review the settings and then choose **Confirm**.

A 32-bit Office will be automatically installed, or uninstalled in the devices owned by users specified by the group or groups you used.

## Set device protection settings for Windows 10 PCs

1. Sign in to [Microsoft 365 Admin Center](#) with global admin credentials.
2. in the admin center, on the **Device policies** card, choose **Add policy**.



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.

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](#)

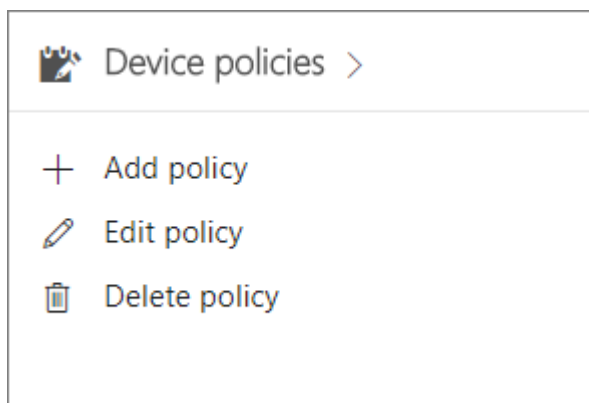
All Users

AddCancel

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.

## Set application protection settings for Windows 10 devices

1. Sign in to [Microsoft 365 Business](#) with global admin credentials. Choose the **Admin** tile to go to the admin center.
2. On the **Device policies** card of the admin portal, choose **Add policy**.



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 **Manage how users access Office files on devices** > configure the settings how you would like. The **Manage how users access Office devices on mobile devices** is **Off** by default, but it is recommended that you turn it **On** and accept the default values. See [Available settings](#) for more information.

You can always use the **Reset default settings** link to return to the default setting.

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 will be protected. If you need to enter more than one item for either field, use a semicolon (;) between the items.

^ Protect additional network and cloud locations On

Domains you own \*

contoso.com;contosoco.com

SharePoint Online locations

contoso.sharepoint.com

Files in these apps will be protected:

<input checked="" type="checkbox"/> Excel	<input checked="" type="checkbox"/> OneDrive	<input checked="" type="checkbox"/> OneNote	<input checked="" type="checkbox"/> Outlook
<input checked="" type="checkbox"/> PowerPoint	<input checked="" type="checkbox"/> Word	<input checked="" type="checkbox"/> Skype for Business	<input checked="" type="checkbox"/> Office Desktop
<input checked="" type="checkbox"/> Microsoft Edge	<input checked="" type="checkbox"/> Internet Explorer		

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.