

# Manage Microsoft 365

## View policies and devices in Admin Center

### View device policies

1. Sign in to [Microsoft 365 Admin Center](#) with global admin credentials.
2. On the left nav, choose **Devices** > **Policies** > **Add**.

On this page you can create, edit, change target group, or delete a policy.

Home > Device policies

[+ Add](#)
[Edit](#)
[Change target group](#)
[Delete](#)

<input type="checkbox"/>	Name	Policy type	Groups applied to
<input type="checkbox"/>	Device policy for Windows 10	Windows 10 device configuration	All Users
<input type="checkbox"/>	Application policy for Android	Application management for Android	All Users
<input type="checkbox"/>	Application policy for iOS	Application management for iOS	All Users
<input type="checkbox"/>	Android Policy	Application management for Android	All Users

### View device actions

1. Sign in to [Microsoft 365 Admin Center](#) with global admin credentials.
2. In the admin center, on the **Device actions** card, choose **Device actions** to open the **Device actions** page.

On this page you can select one or more devices and either 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.

Home > Device actions

[Manage](#)

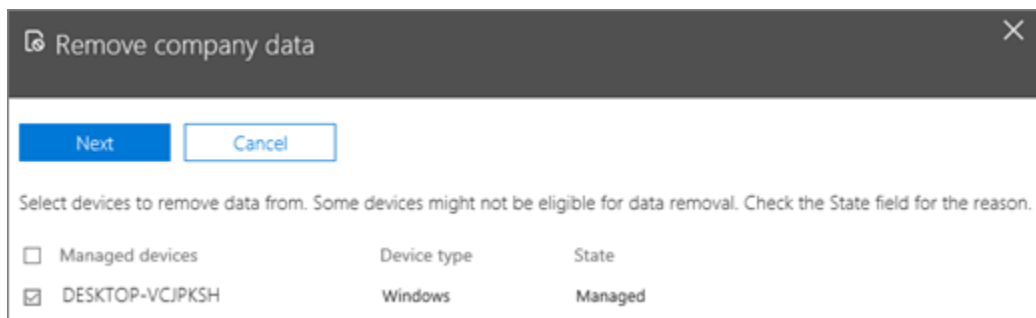
☐ Devices: 6

<input type="checkbox"/>	Device	User	Device type	OS version
<input type="checkbox"/>	DESKTOP-BC652GE	Alice@ contoso.com	Windows	10.0.15063.0
<input type="checkbox"/>	DESKTOP-GOD09I0	daniel@contoso.com	Windows	10.0.15063.0
<input type="checkbox"/>	DESKTOP-HRQ3DPM	Alice@ contoso.com	Windows	10.0.15063.0
<input type="checkbox"/>	DESKTOP-LRD5TKM	Alice@ contoso.com	Windows	10.0.15063.0
<input type="checkbox"/>	MAX's iPhone	Alice@ contoso.com	iOS	10.3.1
<input type="checkbox"/>	LGE LG-H871	Alice@ contoso.com	Android	7.0

## Remove company data

You can use Microsoft 365 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. Sign in to [Microsoft 365 Admin Center](#) with global admin credentials.
2. On the left nav, choose **Devices** > **Policies** > **Manage**.
3. On the **Manage** page, choose or search for a user whose data you want to remove, and choose the name.
4. On the next pane, select the device or devices from the **Managed devices** list to remove data from and choose **Next**.

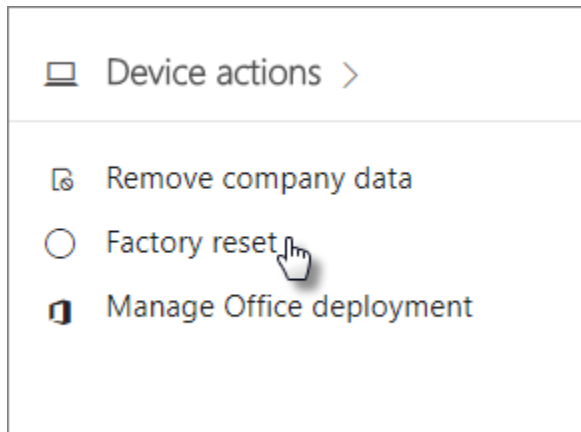


5. On the **Are you sure you want to remove company data on the devices** pane, choose **Remove** > **Close**.

## Reset Windows 10 devices to their factory settings

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 Business to factory reset Windows 10 devices you manage.

1. Sign in to the [Microsoft 365 Admin Center](#) with global admin credentials.
2. In the admin center, on the **Device actions** card, choose **Factory reset**.



3. On the **Factory reset** pane, check the checkbox next to the device you want to remove data from and then choose **Select**.
4. On the **Are you sure you want to factory reset the devices below** pane, choose **Confirm** > **Close**.

# Set device protection settings for Windows 10 PCs

## Secure Windows 10 devices

1. Sign in to [Microsoft 365 Admin Center](#) with global admin credentials.
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.

+

Add policy

Policy name \*

Enter a 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

- 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**.
- Finally, choose **Done** to save the policy, and assign it to devices.

## Set app protection settings for Android or iOS devices

### Create an app management policy

- Sign in to [Microsoft 365 Admin Center](#) with global admin credentials.
- In the admin center, choose **Devices** > **Policies** > **Add policy**.
- On the **Add policy** pane, enter a unique name for this policy.
- Under **Policy type**, choose **Application Management for Android**.
- 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. The **Manage how users access Office files on mobile devices** is **Off** by default, but it is recommended that you turn it **On** and accept the default values.

**+ 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 90 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 5

Require users to sign in again after Office apps have been idle for 30 minutes

Deny access to work files on [jailbroken or rooted devices](#) Off

Allow users to copy content from Office apps into personal apps Off

6. 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**.
7. Finally, choose **Done** to save the policy, and assign it to devices.

### Edit an app management policy

1. On the **Policies** card, choose **Edit policy**.
2. On the **Edit policy** pane, choose the policy you want to change
3. Choose **Edit** next to each setting to change the values in the policy. When you change a value, it is automatically saved into the policy
4. When you are finished, close the **Edit policy** pane.

### Delete an app management policy

1. On the **Policies** card, choose **Delete policy**.
2. On the **Delete policy** pane, choose the policies you want to delete > **Select**, then **Confirm** to delete the policy or policies you chose.