Enroll an iPhone or iPad in Intune

Brandon Allen - 2026-11-08 - Frequently Asked Questions (FAQs)

About this procedure

Use this procedure to enroll an iPhone or iPad in Microsoft Intune. You must enroll your device to get access to company data, for example Outlook, Teams, and OneDrive.

This procedure applies to personal devices. The procedure takes approximately 10 minutes.

If your device is not enrolled, or is not compliant, you cannot get access to company data.

Before you start

Your device must agree with all of these requirements:

Requirement	How to examine or correct it
Enrolled in Intune Company Portal	Do the procedure in this article.
Microsoft Defender installed and set up	Defender installs automatically after enrollment. Do steps 8 to 11 to set it up.
Passes the Defender device risk check	Defender must show no active threats. If Defender shows a threat, do the instructions in Defender.
iOS 18.7.11 or later	Go to **Settings > General > About** and read **iOS Version**. To update, go to **Settings > General > Software Update**.
Not jailbroken	A jailbroken device cannot get access to company data. Restore the device to the standard Apple software.

NOTE: The minimum iOS version will increase when Apple releases security updates. Keep your device updated.

You must also have these items:

- Your company email address and password.
- Your multifactor authentication (MFA) method, for example Microsoft Authenticator.
- Your device passcode.
- An Apple Account that is signed in to the App Store.
- A Wi-Fi or mobile data connection.

Procedure

NOTE: The names of the buttons on your device can be slightly different from the names in this procedure.

Install Company Portal and enroll the device

If you read this article on a computer, scan this QR code with the camera on your iPhone or iPad. The QR code opens Company Portal in the App Store.



1. Open this link on your device, or scan the QR code with your device camera: Intune Company Portal on the App Store.

2. Tap **Get**. If the App Store asks, sign in with your Apple Account.

3. Open **Company Portal**.

    1. Tap **Sign In**.

    2. Enter your company email address and password.

    3. Do the MFA step.

4. On the **Set up access** screen, tap **Begin**.

    1. Read the privacy information.

    2. Tap **Continue**.

5. Download the management profile.

    1. Tap **Continue** or **Download profile**.

    2. When the device asks to download a configuration profile, tap **Allow**.

3. Tap **Close**.

6. Install the management profile.

    1. Open **Settings**.

    2. Tap **Profile Downloaded**. If you cannot see it, go to **Settings > General > VPN & Device Management** and tap the management profile.

    3. Tap **Install**.

    4. Enter your device passcode.

    5. Tap **Install** on each screen that follows.

    6. On the **Remote Management** screen, tap **Trust**.

    7. Tap **Done**.

CAUTION: Install the profile not more than 8 minutes after you download it. If you wait longer, the device deletes the profile. Then you must do step 5 again.

1. Go back to **Company Portal**. Wait while Company Portal examines the device settings. When Company Portal shows that setup is complete, tap **Done**.

Set up Microsoft Defender

1. Wait for a message that your company wants to install **Microsoft Defender**. Tap **Install**. If the App Store asks, sign in with your Apple Account.

NOTE: The message can take up to 15 minutes to show. If you do not see it, open **Company Portal**, tap **Apps**, tap **Microsoft Defender**, and tap **Install**.

1. Open **Microsoft Defender**. If Defender asks you to sign in, sign in with your company account.

2. Tap **Allow** for each permission that Defender asks for. If Defender asks to add VPN configurations, tap **Allow** and enter your device passcode.

NOTE: Defender uses the VPN only on your device to examine websites for threats. The VPN does not send your browsing activity to IT. The VPN does not connect your device to the company network.

1. Make sure that Defender shows that your device is protected.

CAUTION: Do not delete Company Portal, Microsoft Defender, or the management profile. Do not turn off the Defender VPN. If you do, your device is not compliant and you cannot get access to company data.

Make sure that the device is compliant

1. Open **Company Portal**.

2. Tap **Devices**.

3. Tap your device.

4. Make sure that the status shows that the device can get access to company resources.

5. If the status shows that the device is not compliant, tap **Check status** or **Check Settings**. Do the instructions that show.

6. Open Outlook or Teams and sign in with your company account.

NOTE: After enrollment, the compliance status can take up to 30 minutes to update.

Troubleshooting

Problem	Action
Profile Downloaded does not show in Settings.	The profile was deleted after 8 minutes. In Company Portal, do steps 5 and 6 again.
Company Portal shows that the device limit is reached.	Contact IT. IT must remove an old device from your account.
The device is managed by a different organization.	Contact IT. Do not remove a profile that a different organization installed.
Microsoft Defender did not install.	Open **Company Portal > Apps > Microsoft Defender** and tap **Install**. Wait 15 minutes.
Defender shows a threat.	Do the instructions in Defender. If the threat stays, contact IT.
The device is not compliant because of the iOS version.	Go to **Settings > General > Software Update** and install the update. Then do the steps in "Make sure that the device is compliant."
The device cannot update to iOS 18.7.11 or later.	The device cannot get access to company data. Contact IT for options.
You cannot get access to Outlook or Teams after enrollment.	Wait 30 minutes. Then open **Company Portal > Devices**, tap your device, and tap **Check status**.

Privacy on personal devices

Enrollment lets IT manage company apps and data. Enrollment does not give IT access to your personal information.

IT can see	IT cannot see
Device model and serial number	Personal email, text messages, and contacts
iOS version	Photos and files
Device name	Call history
Compliance status	Browsing history
Company apps that Intune manages	Location
	Personal apps

If you leave the company, or you remove your device from Intune, IT removes only company apps and data.