Contents

What is device enrollment in Intune?

9/23/2022 • 6 minutes to read • Edit Online

To use Microsoft Intune as your mobile device management (MDM) provider, you must enroll devices in Intune using a supported enrollment method. Enrollment sets up and secures the device so that it aligns with your organization's policies and is suitable for use at work or school. Intune deploys and enforces policies through a management profile, which is installed on the device during enrollment. Enrollment is enabled for all platforms by default.

Microsoft Intune supports Android, macOS, iOS, and Windows devices. Some enrollment methods require you, as the IT administrator, to initiate enrollment while other methods require your employees or students to initiate it. This article provides an overview of the types of devices and enrollment methods that Intune supports.

Supported device types

Microsoft Intune enables mobile device management for:

- Personal devices, including personally owned phones, tablets, and PCs.
- Corporate-owned devices, including phones, tablets, and PCs owned by your organization and distributed to employees and students for use at work or school.

Personal devices

Microsoft Intune supports bring-your-own-device, or *BYOD*, enrollment. This type of enrollment enables employees and students to use their personal devices for work or school things. As the admin, you're required to add device users in the Microsoft Endpoint Manager admin center, configure their enrollment experience, and set up Intune policies. Enrollment is initiated and completed by the device user in the Intune Company Portal app.

> **NOTE**
> Intune marks devices that are Azure AD-registered as personally-owned devices.

Corporate-owned devices

Microsoft Intune automatically marks certain devices as *corporate-owned*. This classification lets you manage and configure devices with more control and access. For more information about managing and configuring corporate-owned devices, see Identify devices as corporate-owned.

Compare enrollment options

Enrollment options vary by operating system (OS). When selecting a method, choose one that works with the devices and features you want to support.

In this section, we'll use data tables to compare the available methods. Each table, separated by OS, shows the following data:

- Method: The enrollment method used to enroll devices in Intune.
- Enrollment type (Android): The name of the Android enrollment type.
- Reset required: Tells you if devices are reset to factory default settings during enrollment. Options:
  - **Yes**: Existing data is wiped from devices during enrollment.
  - **No**: Existing data is retained on devices during enrollment.

- User affinity: Tells you whether devices are associated with users during enrollment. Options:
  - **Yes**: Each device is associated with an Intune-licensed user.
  - **No**: Devices aren't associated with a user during enrollment, which is a typical configuration for kiosk, point of sale (POS), or shared-utility devices.
  - **Optional**: Microsoft Intune makes this setting available for you to configure on your own.
- MDM profile removable: Tells you if users can remove the MDM profile from an enrolled device. Options:
  - **Yes**: Device users can unenroll devices.
  - **No**: Device users cannot unenroll devices.
  - **Configurable via policy** (Android Enterprise): There's a setting in Intune that lets you block factory resets on devices, which prevents users from unenrolling their devices, but it is not configured by default.

iOS/iPadOS enrollment methods

You can use the following methods to enroll iOS/iPadOS devices in Intune:

- Bring-your-own-device (BYOD)
- Device enrollment manager
- Apple Automated Device Enrollment
- Setup Assistant enrollment via USB
- Direct enrollment via USB

METHOD	RESET REQUIRED	USER AFFINITY	MDM PROFILE REMOVABLE
BYOD	No	Yes	Yes
Device enrollment manager	No	No	Yes
Automated Device Enrollment	Yes	Optional	Optional
Setup Assistant enrollment via USB	Yes	Optional	Yes
Direct enrollment via USB	No	No	Yes

For more information about the iOS/iPadOS enrollment methods supported in Intune, see Enroll iOS/iPadOS devices.

macOS enrollment methods

You can use the following methods to enroll macOS devices in Intune:

- Bring-your-own-device (BYOD)
- Device enrollment manager
- Apple Automated Device Enrollment

METHOD	RESET REQUIRED	USER AFFINITY	MDM PROFILE REMOVABLE
BYOD	No	Yes	Yes
Device enrollment manager	No	No	Yes

METHOD	RESET REQUIRED	USER AFFINITY	MDM PROFILE REMOVABLE
Apple Automated Device Enrollment	Yes	Optional	Optional

For more information about the macOS enrollment methods supported in Intune, see Set up enrollment for macOS devices.

Windows enrollment methods

You can use the following methods to enroll Windows devices in Intune:

- Bring-your-own-device (BYOD)
- Device enrollment manager
- Automatic enrollment via MDM
- Automatic enrollment via Group Policy
- Windows Autopilot
- Bulk enrollment
- Co-management with Microsoft Intune and Configuration Manager

METHOD	RESET REQUIRED	USER AFFINITY	MDM PROFILE REMOVABLE
BYOD	No	Yes	Yes
Device enrollment manager	No	No	Yes
Automatic enrollment via MDM	No	Yes	Yes
Automatic enrollment via Group Policy	No	Yes	Yes
Windows Autopilot	Yes	Yes	Yes
Bulk enrollment	No	No	Yes
Co-management	No	Yes	Yes

For more information about the Windows enrollment methods supported in Intune, see Enrollment methods for Windows devices .

Android enrollment methods

To select the appropriate enrollment method for Android devices, consider the enrollment type you'll use and the device's ownership status (personal versus corporate-owned). For more information about the Android enrollment methods supported in Intune, see Enroll Android devices.

Personal Android devices

You can set up user-initiated enrollment for people who want to use their personal devices at work or school. Employees and students initiate enrollment by signing into the Company Portal app with their work or school account.

Intune supports the following device management configurations on personal devices:

- Android Device Administrator (also referred to as *Android Device Admin*)
- Android Enterprise with work profile

In the table, this data is shown in the Enrollment type column.

ENROLLMENT TYPE	ENROLLMENT METHOD	RESET REQUIRED	USER AFFINITY	MDM PROFILE REMOVABLE
Android Device Admin	User-initiated via Company Portal	No	Yes	Yes
Android Enterprise, personal-owned with work profile	User-initiated via Company Portal	No	Yes	Yes

Corporate-owned Android devices

Intune supports the following device management configurations on corporate-owned devices:

- User associated and userless devices created from Android Open Source Project (AOSP)
- Android Device Administrator (also referred to as *Android Device Admin*)
- Android Device Admin with Zebra Mobility Extensions
- Android Enterprise dedicated/kiosk-style
- Android Enterprise fully managed
- Android Enterprise with work profile

In the table, this data is shown in the Enrollment type column. You can use the following methods to enroll corporate-owned Android devices in Intune:

- QR code
- Device enrollment manager (DEM) with Company Portal
- User initiated with Company Portal
- Near-field communication (NFC)
- Token entry
- Google zero-touch enrollment

ENROLLMENT TYPE	ENROLLMENT METHOD	RESET REQUIRED	USER AFFINITY	MDM PROFILE REMOVABLE
Android (AOSP) user-associated	QR code	Yes	Yes	Configurable via policy
Android (AOSP) userless	QR code	Yes	No	Configurable via policy
Android Device Admin	DEM-initiated via Company Portal	No	No	Yes
Android Device Admin	User-initiated via Company Portal with predeclared IMEI or serial number	No	Yes	Yes
Android Device Admin with Zebra Mobility Extensions	User or DEM-initiated via Company Portal	No	Yes if user-initiated; no if DEM-initiated	Yes
Android Enterprise dedicated	NFC, token, QR code, Google zero-touch	Yes	No	Configurable via policy

ENROLLMENT TYPE	ENROLLMENT METHOD	RESET REQUIRED	USER AFFINITY	MDM PROFILE REMOVABLE
Android Enterprise fully managed	NFC, token, QR code, Google zero-touch	Yes	Yes	Configurable via policy
Android Enterprise corporate-owned with work profile	NFC, token, QR code, Google zero-touch	Yes	Yes	Configurable via policy

Mobile device record cleanup

The MDM certificate renews automatically as long as enrolled devices are communicating with the Microsoft Intune service. The MDM certificate doesn't renew for devices that have been wiped, or that fail to sync with Microsoft Intune for an extended period of time. Microsoft Intune deletes idle devices from record 180 days after the MDM certificate expires.

Next steps

You can adjust the settings in Intune to restrict specific platforms from enrolling. For more information, see Create a device platform restriction.

Enrolled device management capabilities of Microsoft Intune

9/23/2022 • 4 minutes to read • Edit Online

Microsoft Intune lets you manage a range of devices by *enrolling* them into the service. You can enroll some device types yourself, or users can enroll using the *company portal* app. Enrolling lets them browse and install apps, make sure that their devices are compliant with company policies, and contact their IT support.

This article gives a full list of the capabilities that you get after devices are enrolled.

Management, inventory, app deployment, provisioning, and retirement are all handled through Intune in the Azure portal.

Users gain access to the company portal, which enables them to install apps, enroll and remove devices, and contact their IT department or helpdesk.

Device security and configuration

CAPABILITY	DETAILS	MORE INFORMATION
Configuration policies Custom policies	Lets you manage many settings and features on mobile devices in your organization. For example, you can require a password, limit the number of failed attempts, limit the amount of time before the screen locks, set password expiration, and prevent previously used passwords. You can also control the use of hardware and software features such as the device camera or the web browser. Use custom policies when configuration policies do not contain the settings that you require. For iOS/iPadOS devices, you can import settings that you exported from the Apple Configurator tool. For other devices, you can use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure settings and features on the device.	Manage settings and features on your devices with Microsoft Intune policies
Remote Wipe, Remote Lock, and Passcode Reset	Erases sensitive data when a device is lost or stolen. For example, you can remotely lock the device, restore it to factory settings, or wipe only corporate data. You can reset passcodes if users lose access to their device, lock missing or stolen devices, or even wipe data off of missing or stolen devices.	Help protect your devices with remote lock and passcode reset

CAPABILITY	DETAILS	MORE INFORMATION
Kiosk mode	Lets you lock down certain features of mobile devices such as screen captures and power switches. Also lets you restrict devices to run a single app that you specify.	iOS configuration policy settings in Microsoft Intune
Autopilot Reset	Sends a task to the device to start the reset process remotely, avoiding the need for IT staff or other administrators to visit each machine to start the process. When Autopilot reset is used on a device, the device's primary user will be removed. The next user who signs in after the reset will be set as the primary user.	Remote Windows Autopilot Reset

App management

CAPABILITY	DETAILS	MORE INFORMATION
App deployment and management	Provides a range of tools to help you manage mobile apps through their lifecycle, including app deployment from installation files and app stores, detailed monitoring of app status, and app removal.	Deploy apps in Microsoft Intune
Compliant and noncompliant apps	Lets you specify lists of compliant apps (that users are allowed to install) and noncompliant apps (that users aren't allowed to install).	iOS policy settings in Microsoft Intune
Mobile application management	Configures restrictions for apps by using mobile application management for all devices that are both managed with Intune and not managed with Intune. You can increase the security of your company data by restricting operations such as copy and paste, external backup of data, and the transfer of data between apps.	Configure and deploy mobile application management policies in the Microsoft Intune console
iOS mobile app configuration	Uses mobile app configuration policies to supply settings for iOS/iPadOS apps that might be required when the user runs the app. For example, an app might require the user to specify a port number or logon information. You can streamline app configuration and reduce the number of support calls.	Configure iOS/iPadOS apps with mobile app configuration policies in Microsoft Intune
iOS/iPadOS mobile app provisioning profiles	Helps you deploy provisioning profiles to iOS/iPadOS apps that are nearing expiration.	Use iOS/iPadOS mobile provisioning profile policies to prevent your apps from expiring

CAPABILITY	DETAILS	MORE INFORMATION
Managed browser	Configures managed browser policies to control the websites that device users can visit. In addition, you can also apply mobile application management policies to the managed browser.	Manage Internet access using managed browser policies with Microsoft Intune
Windows Hello for Business	Lets you integrate with Windows Hello for Business, which is an alternative sign-in method for Windows 10 that uses on-premises Active Directory or Azure Active Directory to replace passwords, smart cards, or virtual smart cards.	Control Windows Hello for Business settings on devices with Microsoft Intune
Volume purchased apps	Helps you manage apps that you purchased through a volume-purchase program by importing the license information from the app store, tracking how many of the licenses you have used, and preventing you from installing more copies of the app than you own.	Manage volume-purchased apps using Microsoft Intune

Company resource access

CAPABILITY	DETAILS	MORE INFORMATION
Certificate profiles	Creates and deploys trusted certificate profiles and Simple Certificate Enrollment Protocol (SCEP) certificates, which can be used to secure and authenticate Wi-Fi, VPN, and email profiles.	Secure resource access with certificate profiles in Microsoft Intune
Wi-Fi profiles	Deploys wireless network settings to your users. By deploying these settings, you minimize the user effort that's required to connect to the corporate network.	Wi-Fi connections in Microsoft Intune
Email profiles	Creates and deploys email settings to devices so that users can access corporate email on their personal devices without any required setup on their part.	Configure access to corporate email using email profiles with Microsoft Intune
VPN profiles	Deploys VPN settings to users and devices in your organization. By deploying these settings, you minimize the user effort that's required to connect to resources on the company network.	VPN connections in Microsoft Intune

CAPABILITY	DETAILS	MORE INFORMATION
Conditional Access policies	Manages access to Microsoft Exchange email and SharePoint Online from devices that are not managed by Intune.	Restrict access to email and SharePoint with Microsoft Intune

Next steps

See a list of devices that you can manage.

Enrollment options for devices managed by Intune

9/23/2022 • 2 minutes to read • Edit Online

As an Intune admin, you can configure device enrollment to help users and enable Intune capabilities. Intune includes the following enrollment options:

Terms and conditions

You can require that users accept your company's terms and conditions before they can use the Company Portal to enroll their devices and access resources like company apps and email. Configuration of terms and conditions is optional. Learn more about terms and conditions.

Enrollment restrictions

You can choose to restrict device enrollment by:

- Device platform
- Number of devices per user
- Block personal devices

Learn more about enrollment restrictions.

Enable Apple device enrollment

An MDM push certificate is required for iOS/iPadOS and macOS device enrollment. Learn more about MDM push certificates.

Corporate identifiers

You can list international mobile equipment identifier (IMEI) numbers and serial numbers to identify corporate-owned devices. Learn more about corporate identifiers.

Multi-factor authentication

You can require users to use an additional verification method, such as a phone, PIN or biometric data, when they enroll a device. Learn more about multi-factor authentication.

Device enrollment manager

You can make users device enrollment managers. DEM users can enroll large numbers of mobile devices with a single user account. The device enrollment manager (DEM) account can enroll up to 1,000 devices. Learn more about device enrollment managers.

Device categories

You can use device categories to automatically add devices to groups based on categories that you define. Organizing devices into groups makes it easier for you to manage those devices. Learn more about device categories.

Quickstart: Set up automatic enrollment for Windows 10/11 devices

9/23/2022 • 2 minutes to read • Edit Online

In this quickstart, you'll set up Microsoft Intune to automatically enroll devices when specific users sign in to Windows 10/11 devices.

If you don't have an Intune subscription, sign up for a free trial account.

Prerequisites

- Microsoft Intune subscription - sign up for a free trial account.
- To complete this quickstart, you must first create a user and create a group.

Sign in to Intune in the Microsoft Endpoint Manager

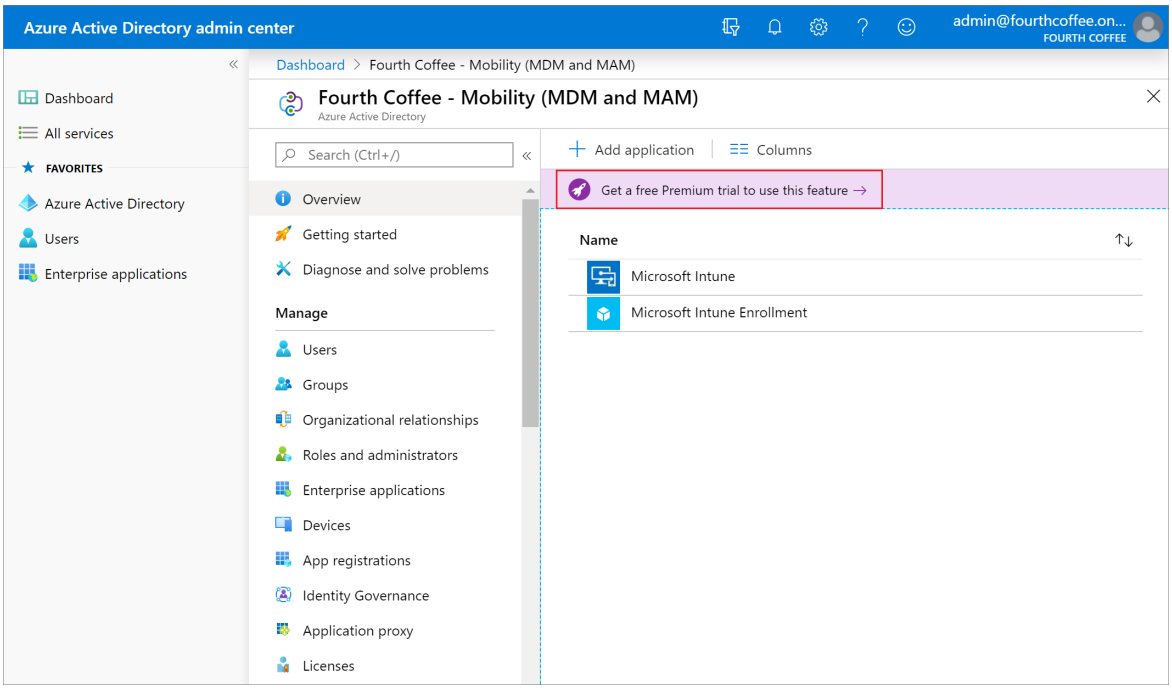
Sign in to the Microsoft Endpoint Manager admin center as a Global Administrator. If you have created an Intune Trial subscription, the account you created the subscription with is the Global administrator.

Set up Windows 10/11 automatic enrollment

For this example, you'll use MDM enrollment so that both corporate and bring-your-own-devices can be automatically enrolled. You will sign up for a free Azure Active Directory Premium subscription.

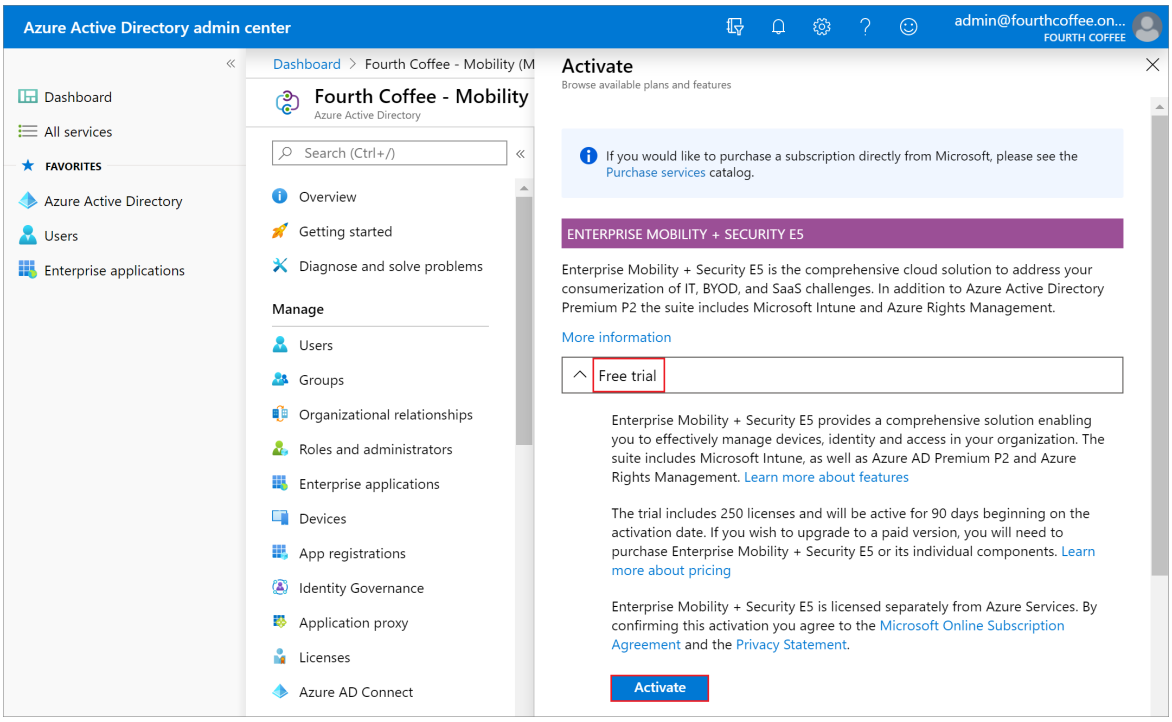
1. In the Microsoft Endpoint Manager admin center, choose **All services** > **M365 Azure Active Directory** > **Azure Active Directory** > **Mobility (MDM and MAM)**.

2. Select **Get a free Premium trial to use this feature**. Selecting this option will allow auto enrollment using the Azure Active Directory free Premium trial.



3. Choose the **Enterprise Mobility + Security E5** free trial option.

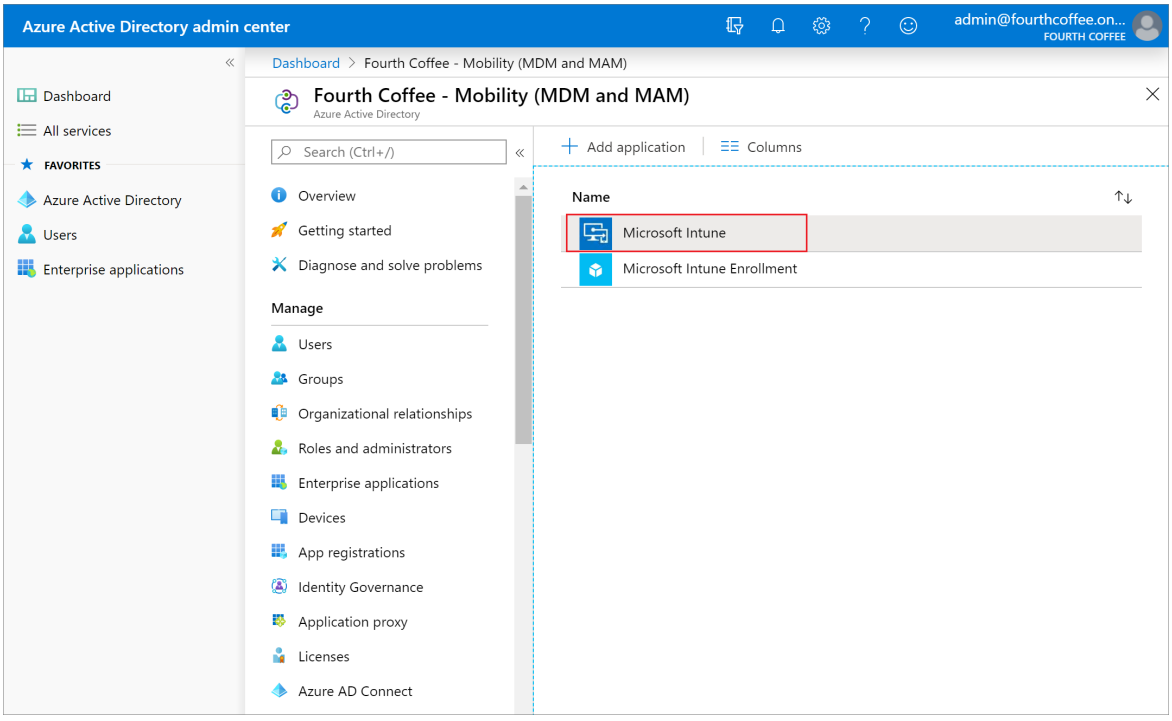
4. Click **Free trial** > **Activate** the free trial.



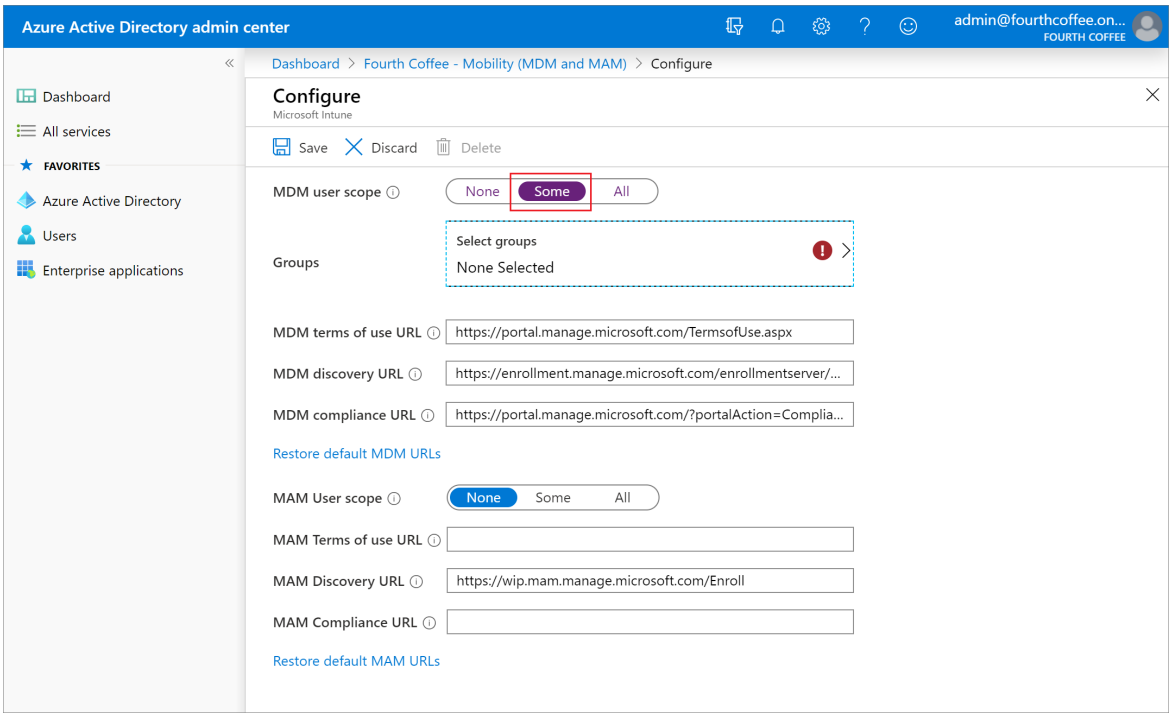
NOTE

It may take a minute to activate.

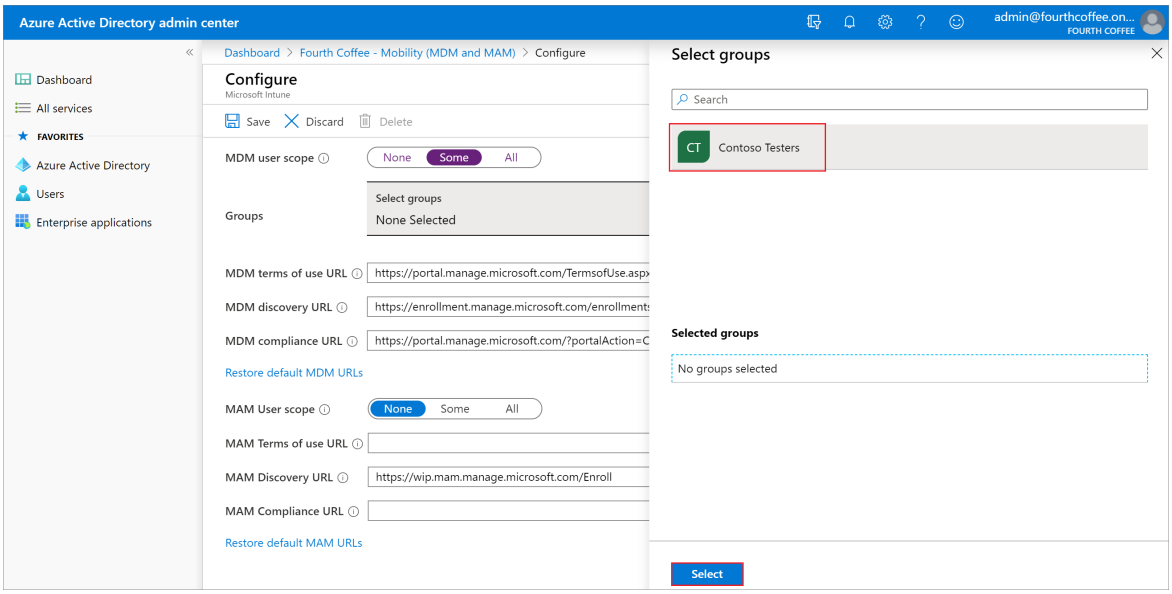
5. Select **Microsoft Intune** to configure Intune.



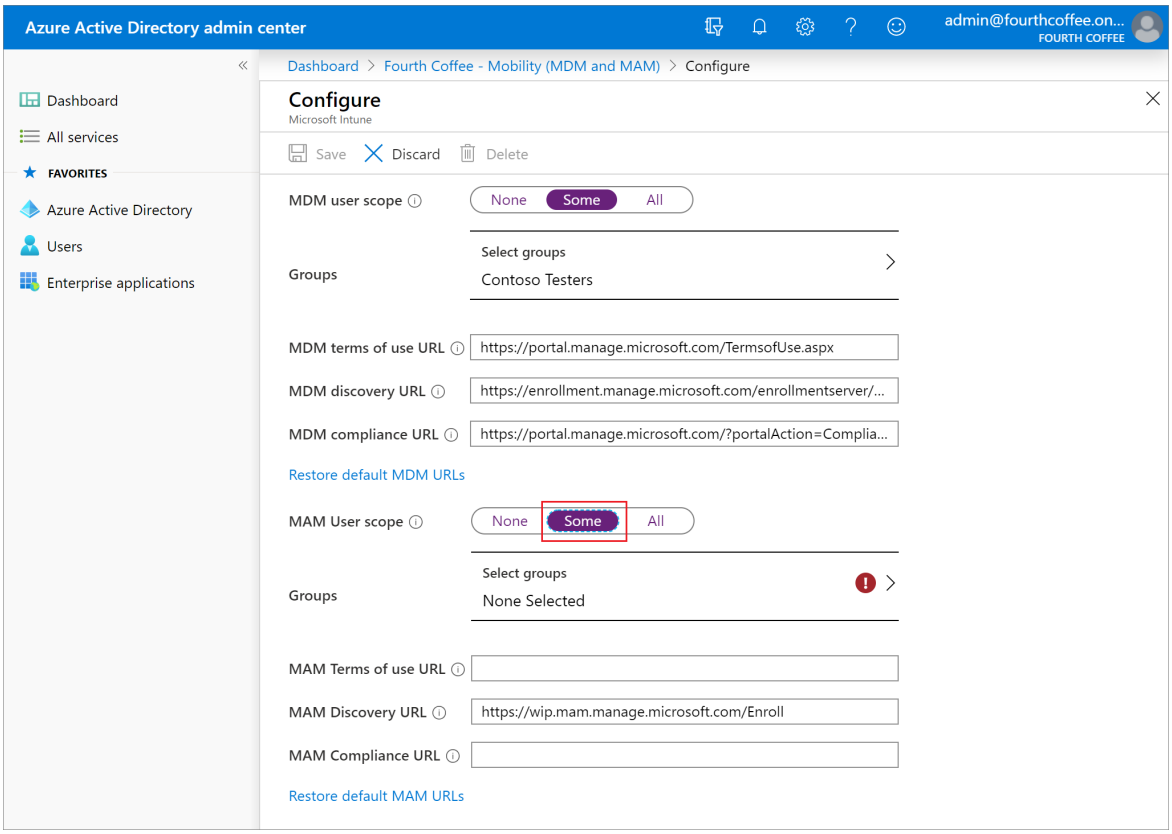
6. Select **Some** from the **MDM user scope** to use MDM auto-enrollment to manage enterprise data on your employees' Windows devices. MDM auto-enrollment will be configured for AAD joined devices and bring your own device scenarios.



7. Click **Select groups** > **Contoso Testers** > **Select** as the assigned group.



8. Select **Some** from the **MAM Users scope** to manage data on your workforce's devices.



9. Choose **Select groups** > **Contoso Testers** > **Select** as the assigned group.
10. Use the default values for the remaining configuration values.
11. Choose **Save**.

Clean up resources

To reconfigure Intune automatic enrollment, check out Set up enrollment for Windows devices.

Next steps

In this quickstart, you learned how to set up auto-enrollment for devices running Windows 10/11. For more information about device enrollment, see What is device enrollment?

To follow this series of Intune quickstarts, continue to the next quickstart.

Quickstart: Enroll your Windows 10/11 device

Quickstart: Enroll your Windows device

9/23/2022 • 2 minutes to read • Edit Online

Applies to

- Windows 10
- Windows 11

In this quickstart, you'll first take the role of an Intune user and enroll a device running Windows 10/11 into Microsoft Intune. Then you'll return to Intune and confirm that the device enrolled.

Enrolling your devices into Microsoft Intune allows you to access your organization's secure data, including email, files, and other resources, from your Windows device. This is true for both devices running Windows 10/11 devices (including desktop) and Windows 10 Mobile devices. Enrolling your devices helps secure this access for both you and your organization, and helps keep your work data separate from your personal data.

> **TIP**
> Find out what happens when you enroll your device in Intune and what that means for the information on your device.

If you don't have an Intune subscription, sign up for a free trial account.

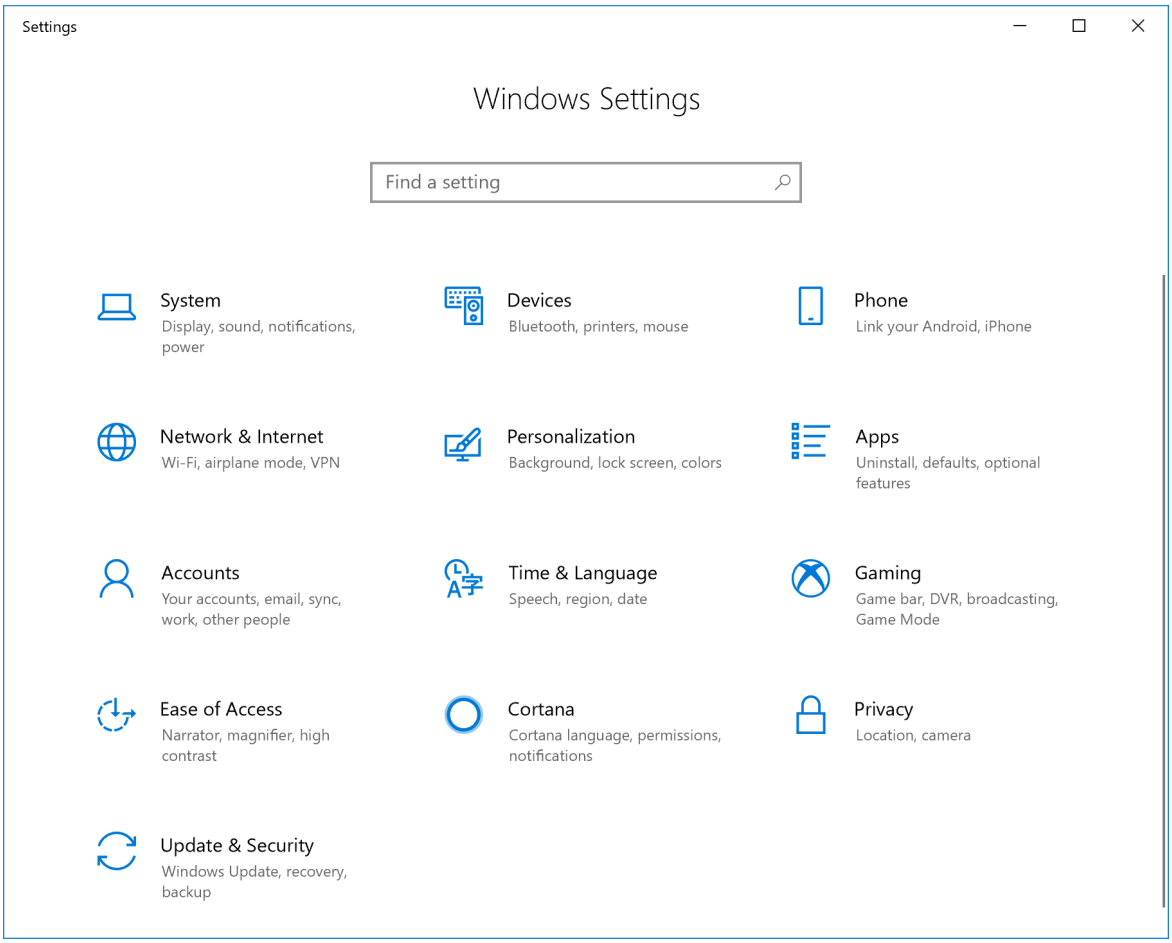
Prerequisites

- Microsoft Intune subscription - sign up for a free trial account
- To complete this quickstart, you must complete the steps to setup automatic enrollment in Intune.

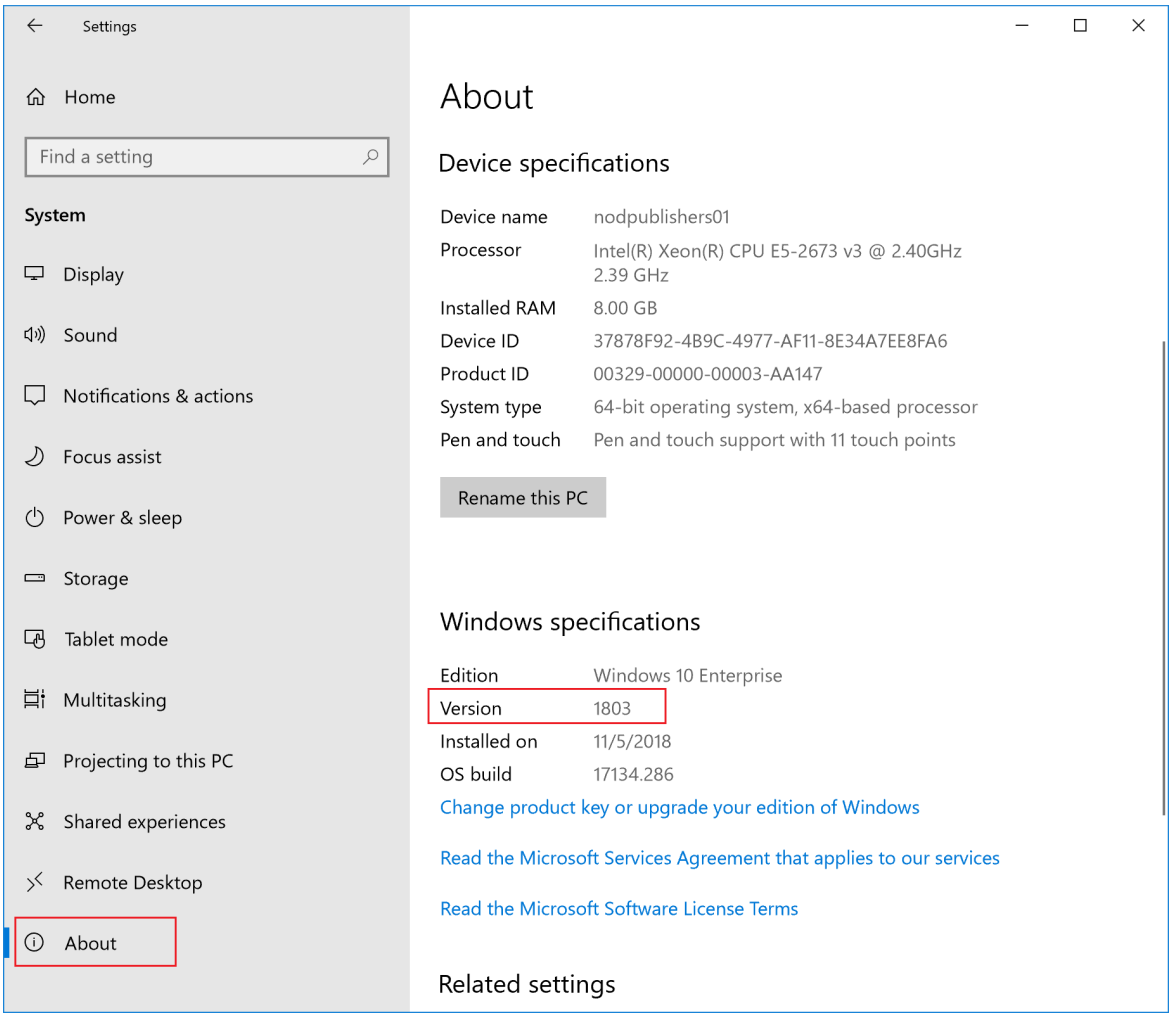
Confirm Windows version

Before enrolling your Windows device, you must confirm the version of Windows that you have installed.

1. Right-click the Windows **Start** icon and select **Settings** to display Windows Settings options.



2. Select **System** > **About**.



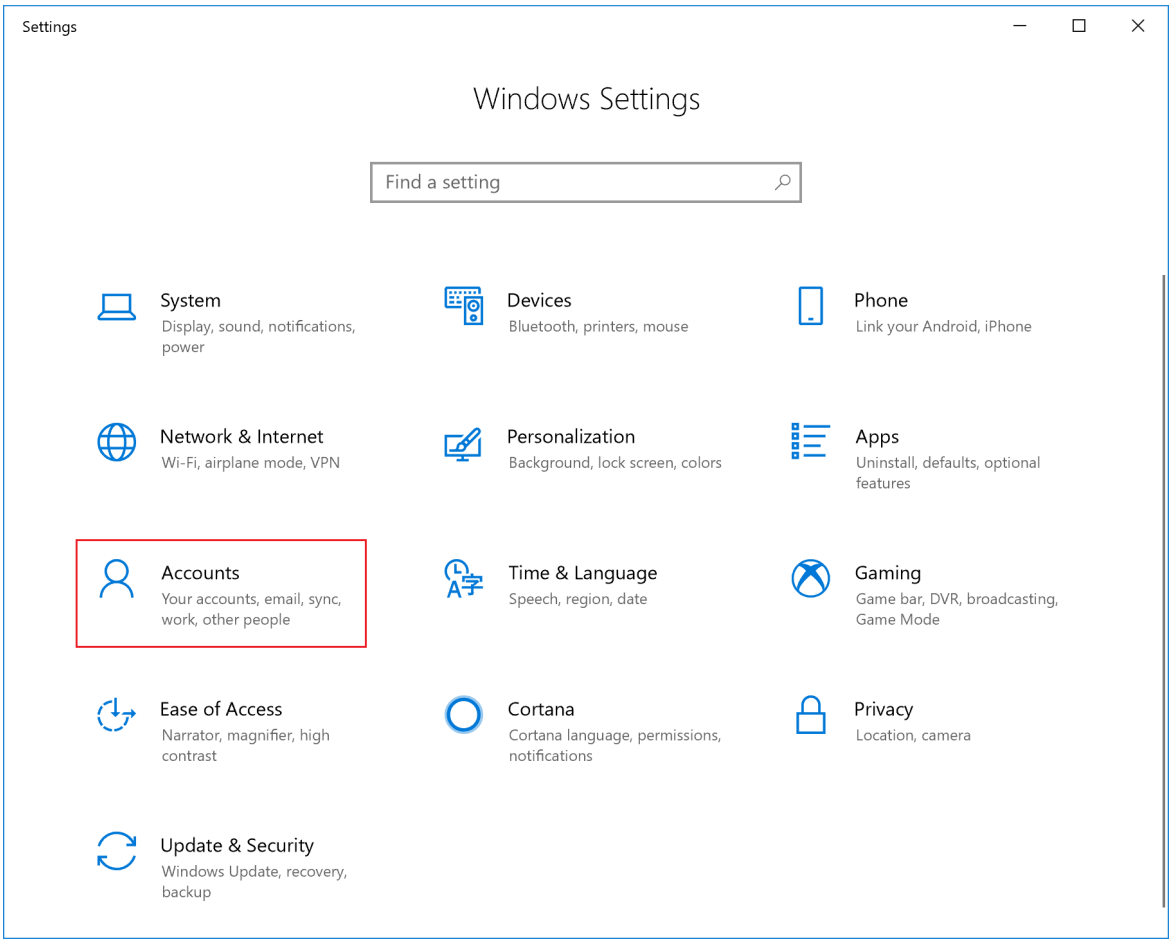
> **TIP**
>
> You can also type the phrase "About your PC" into the **search bar**, then select **About your PC**.

3. In the **Settings** window you will see a list of **Windows specifications** for your PC. Within this list, locate the **Version**.
4. Confirm that the Windows **Version** is Windows 10 (version 1607 or later) or Windows 11 (version 21H2 or later).

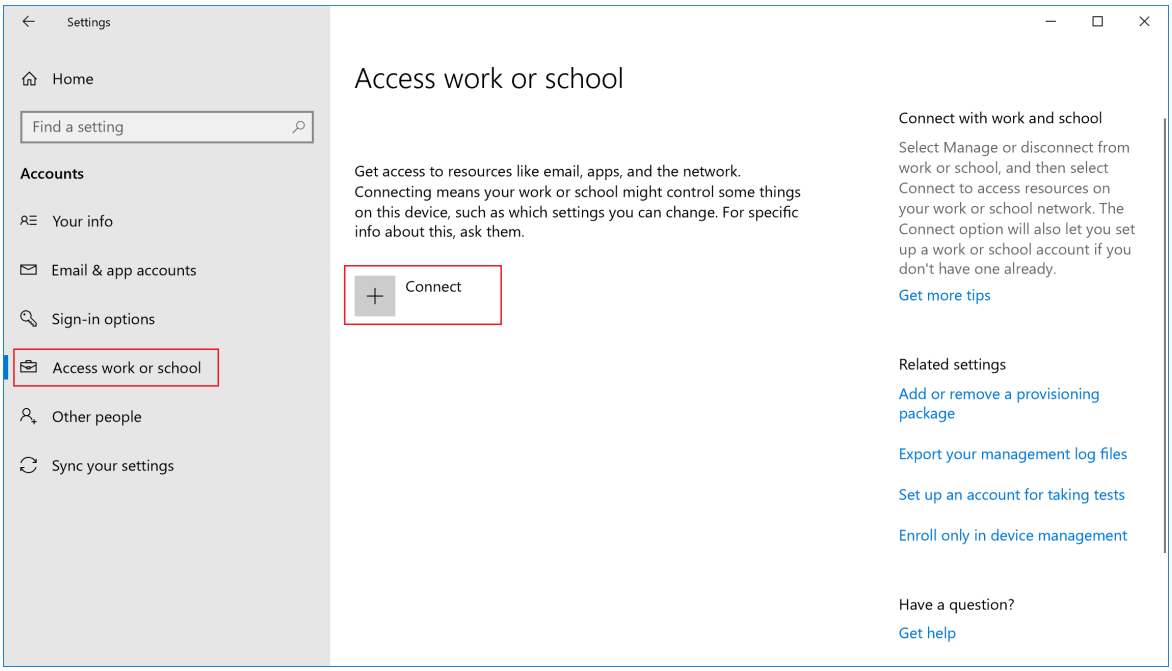
> **IMPORTANT**
>
> The steps presented in this quickstart are for Windows 10 (version 1607 or higher) or Windows 11 (version 21H2 or later). If your version is 1511 or earlier, see Enroll device running Windows 10, version 1511 and earlier.

Enroll Windows 10/11 desktop

1. Return to Windows Settings and select **Accounts**.

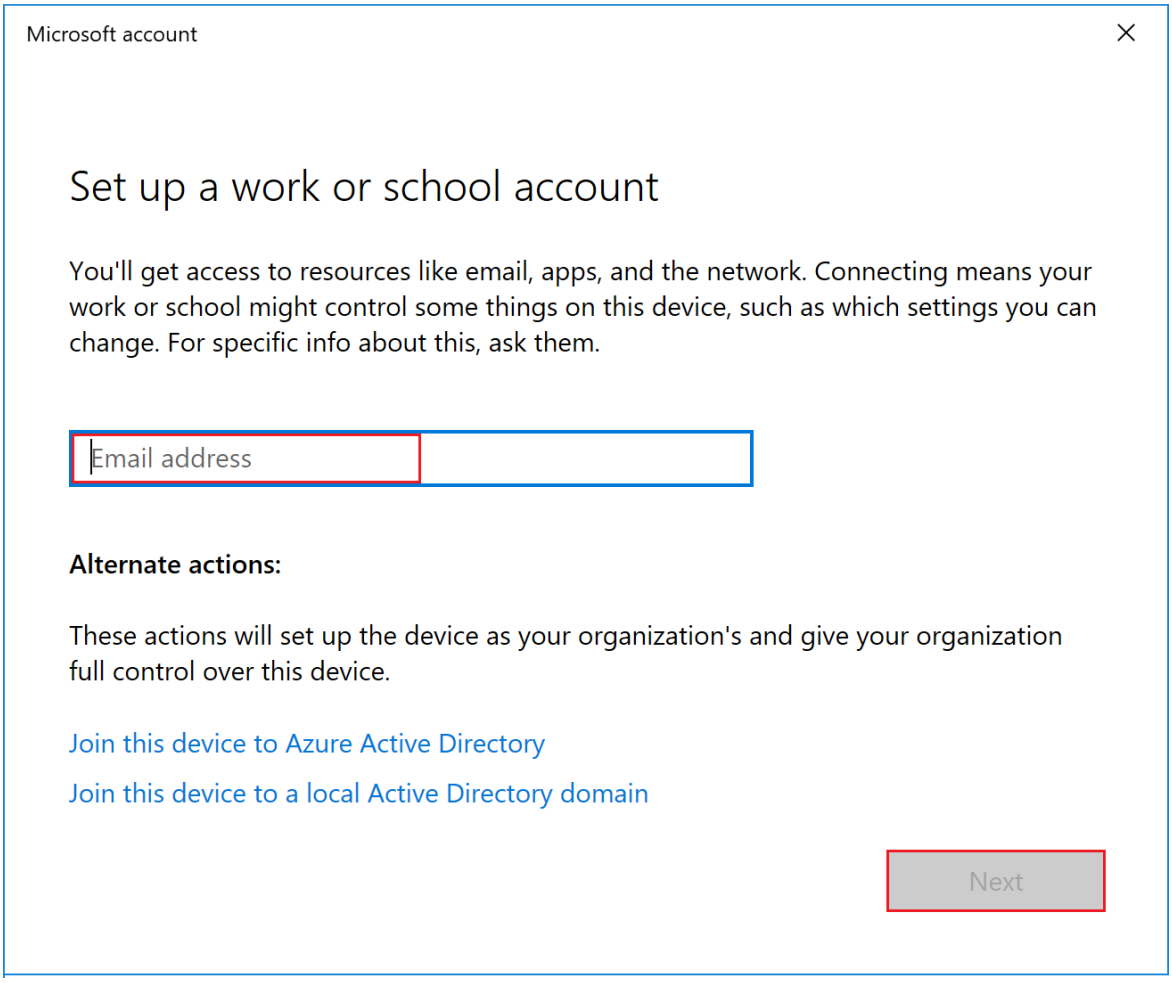


2. Select **Access work or school** > **Connect**.



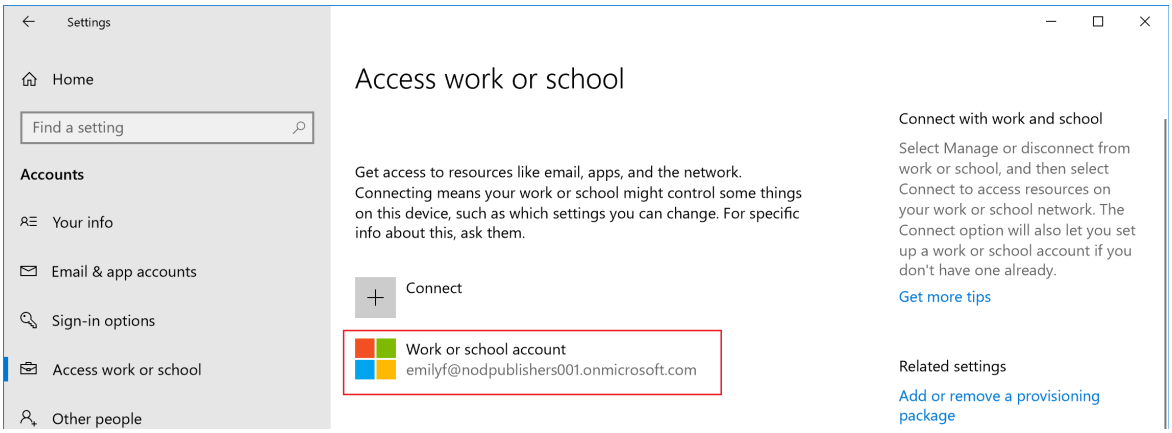
3. Sign in to Intune with your work or school account, and then select **Next**. If you followed the create a user and assign a license quickstart, you can sign in with the user account that you created.

> **NOTE**
> If you setting up an ".onmicrosoft.com", the user account will have **.onmicrosoft.com** as part of the account address.



You'll see a message indicating that your company or school is registering your device.

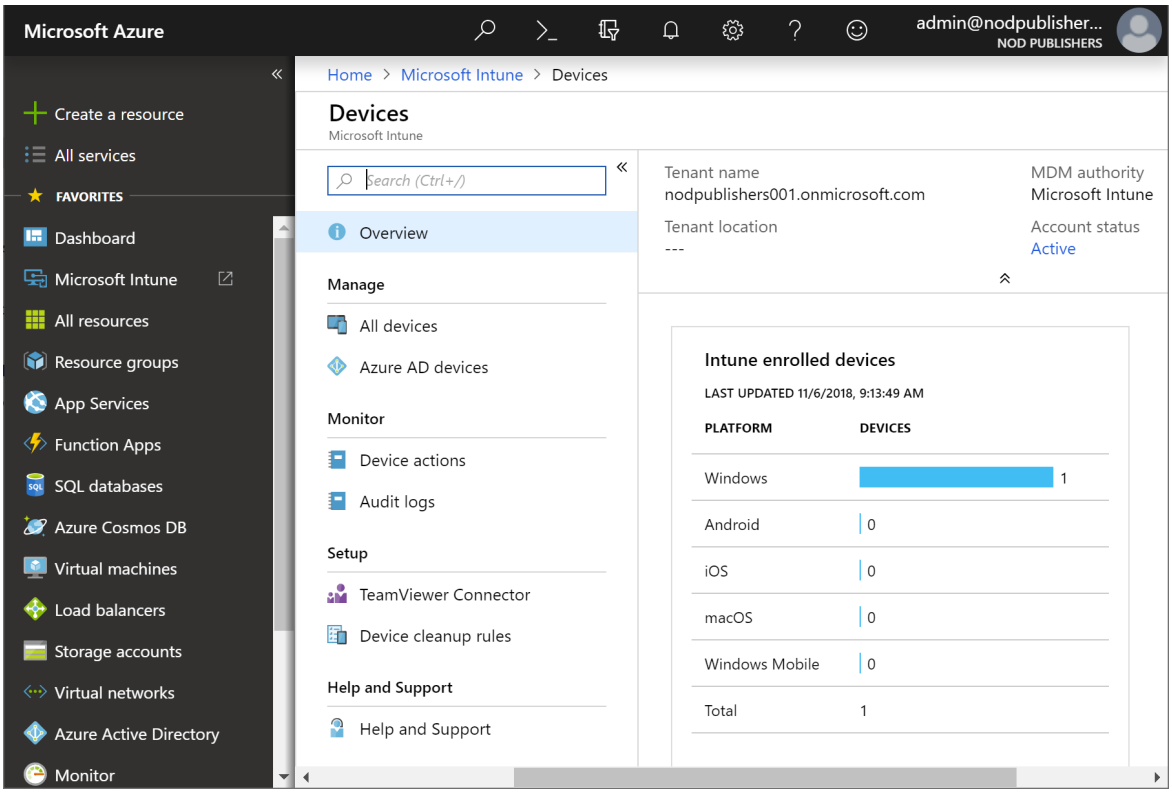
4. When you see the **You're all set!** screen, select **Done**. You're done.
5. You will now see the added account as part of the **Access work or school** settings on your Windows desktop.



If you followed the previous steps, but still can't access your work or school email account and files, follow the steps in Troubleshoot Windows 10/11 device access.

Confirm your device enrollment in Intune

1. Sign in to the Microsoft Endpoint Manager admin center as a Global Administrator.
2. Select **Devices** > **All devices** to view the enrolled devices in Intune.
3. Verify that you have an additional device enrolled within Intune.



Clean up resources

To unenroll your Windows device, see Remove your Windows device from management.

Next steps

In this quickstart, you learned how to enroll a Windows 10/11 device into Intune. You can learn about other

ways to enroll devices across all platforms. For more information about using devices with Intune, see Use managed devices to get work done.

To follow this series of Intune quickstarts, continue to the next quickstart.

Quickstart: Set a required password length for Android devices

Tutorial: Use Autopilot to enroll Windows devices in Intune

9/23/2022 • 3 minutes to read • Edit Online

Windows Autopilot simplifies enrolling devices. With Microsoft Intune and Autopilot, you can give new devices to your end users without the need to build, maintain, and apply custom operating system images.

In this tutorial, you'll learn how to:

- Add devices to Intune
- Create an Autopilot device group
- Create an Autopilot deployment profile
- Assign the Autopilot deployment profile to the device group
- Distribute Windows devices to users

If you don't have an Intune subscription, sign up for a free trial account.

For an overview of Autopilot benefits, scenarios, and prerequisites, see Overview of Windows Autopilot.

Prerequisites

- Set up Windows automatic enrollment
- Azure Active Directory Premium subscription

Add devices

The first step in setting up Windows Autopilot is to add the Windows devices to Intune. All you have to do is create a CSV file and import it into Intune.

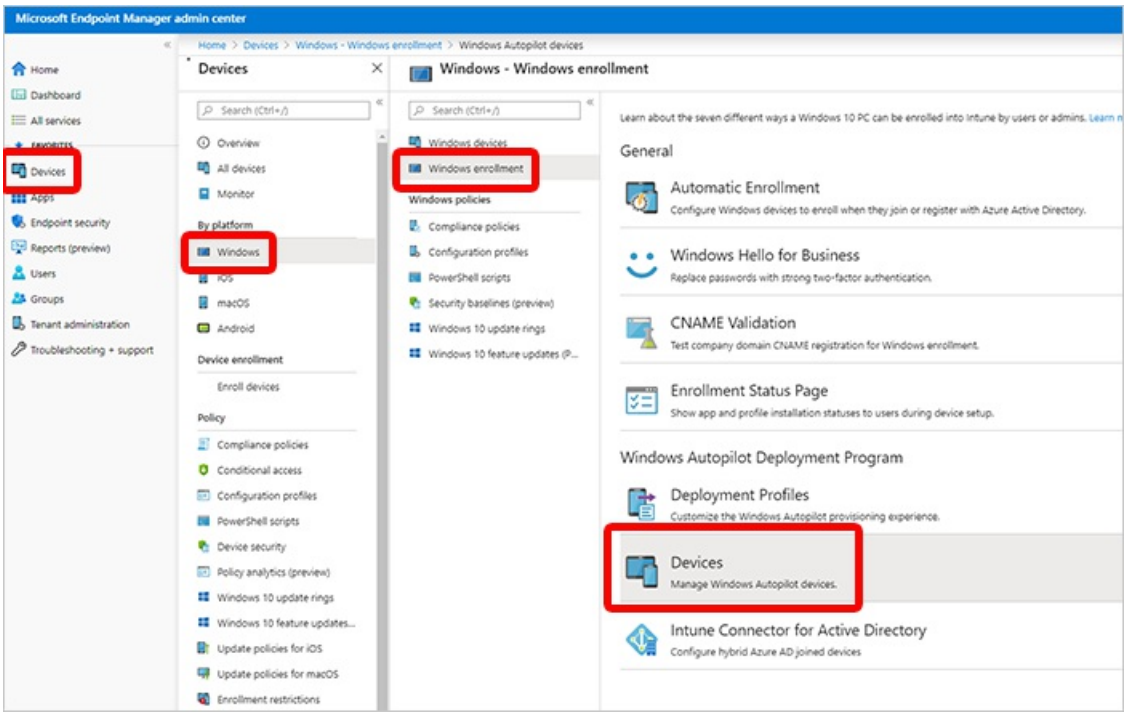
1. In any text editor, create a list of comma-separated values (CSV) that identify the Windows devices. Use the following format:

   serial-number, *windows-product-id*, *hardware-hash*, *optional-Group-Tag*

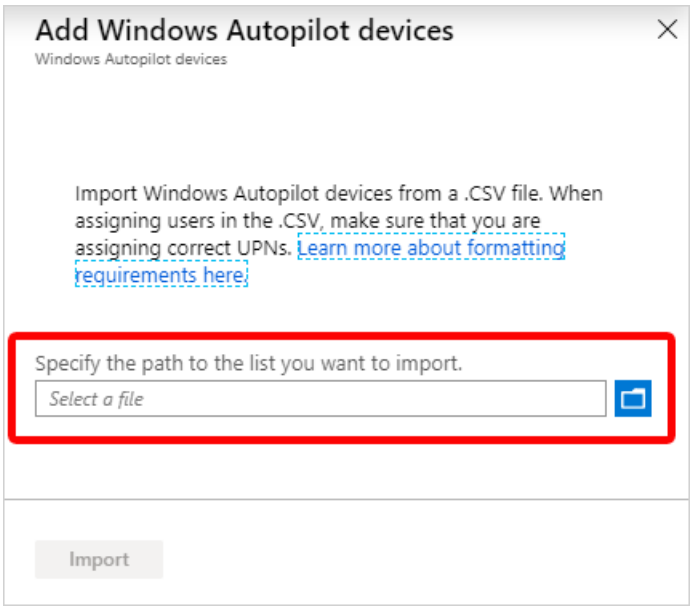
   The first three items are required, but the Group Tag (previously known "order ID") is optional.

2. Save the CSV file.

3. In the Microsoft Endpoint Manager admin center, choose **Devices** > **Windows** > **Windows Enrollment** > **Devices** (under **Windows Autopilot Deployment Program**) > **Import**.



4. Under **Add Windows Autopilot devices**, browse to the CSV file you saved.



5. Choose **Import** to start importing the device information. Importing can take several minutes.

6. After import is complete, choose **Devices** > **Windows** > **Windows enrollment** > **Devices** (under **Windows Autopilot Deployment Program** > **Sync**. A message displays that the synchronization is in progress. The process might take a few minutes to complete, depending on how many devices you're synchronizing.

7. Refresh the view to see the new devices.

Create an Autopilot device group

Next, you'll create a device group and put the Autopilot devices you just loaded into it.

1. In the Microsoft Endpoint Manager admin center, choose **Groups** > **New group**.
2. In the **Group** blade:
   a. For **Group type**, choose **Security**.
   b. For **Group name**, enter *Autopilot Group*. For **Group description**, enter *Test group for Autopilot*

devices.

c. For **Membership type**, choose either **Assigned**.

3. In the **Group** blade, choose **Members** and add the Autopilot devices to the group. Autopilot devices that aren't yet enrolled are devices where the name equals the serial number of the device.
4. Choose **Create**.

Create an Autopilot deployment profile

After creating a device group, you must create a deployment profile so that you can configure the Autopilot devices.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **Windows** > **Windows enrollment** > **Deployment Profiles** > **Create Profile**.
2. On the **Basics** page, for **Name**, enter *Autopilot Profile*. For **Description**, enter *Test profile for Autopilot devices*.
3. Set **Convert all targeted devices to Autopilot** to **Yes**. This setting makes sure that all devices in the list get registered with the Autopilot deployment service. Allow 48 hours for the registration to be processed.
4. Select **Next**.
5. On the **Out-of-box experience (OOBE)** page, for **Deployment mode**, choose **User-driven**. Devices with this profile are associated with the user enrolling the device. User credentials are required to enroll the device.
6. In the **Join to Azure AD as** box, choose **Azure AD joined**.
7. Configure the following options and leave others set to the default:
   - **End-user license agreement (EULA)**: **Hide**
   - **Privacy settings**: **Show**
   - **User account type**: **Standard**
8. Select **Next**.
9. On the **Assignments** page, choose **Selected groups** for **Assign to**.
10. Choose **Select groups to include**, choose **Autopilot Group**.
11. Select **Next**.
12. On the **Review + Create** page, choose **Create** to create the profile.

Hardware change detection

Microsoft Intune notifies you when it detects a hardware change on an Autopilot-registered device. When a hardware change occurs, Intune updates the device's profile status to one of the following states:

- **Attention required**: The device can't receive the Autopilot profile until you reset and re-register the device.
- **Fix pending**: Intune tries to register the new hardware. If successful, Intune updates the profile status at the next check-in.

To view all devices and their current states, go to **Devices** > **Windows Autopilot devices**.

Distribute devices to users

You can now distribute the Windows devices to your users. When they sign in for the first time, the Autopilot system will automatically enroll and configure the devices.

Clean up resources

If you don't want to use Autopilot devices anymore, you can delete them.

1. If the devices are enrolled in Intune, you must first delete them from the Azure Active Directory portal.
2. In the Microsoft Endpoint Manager admin center, choose **Devices** > **Windows** > **Windows enrollment** > **Devices** (under **Windows Autopilot Deployment Program**).
3. Choose the devices you want to delete, and then choose **Delete**.
4. Confirm the deletion by choosing **Yes**. It can take a few minutes to delete.

Next steps

You can find more information about other options available for Windows Autopilot.

In-depth Autopilot enrollment article

Tutorial: Use Apple's Corporate Device Enrollment features in Apple Business Manager (ABM) to enroll iOS/iPadOS devices in Intune

9/23/2022 • 7 minutes to read • Edit Online

The Device Enrollment features in Apple Business Manager simplifies enrolling devices. Intune also supports Apple's older Device Enrollment Program (DEP) portal, but we encourage you to start fresh with Apple Business Manager. With Microsoft Intune and Apple Corporate Device Enrollment, devices are automatically securely enrolled the first time the user turns on the device. You can therefore ship devices to many users without having to set up each device individually.

In this tutorial, you'll learn how to:

- Get an Apple Device Enrollment token
- Sync managed devices to Intune
- Create an Enrollment profile
- Assign the Enrollment profile to devices

If you don't have an Intune subscription, sign up for a free trial account.

Prerequisites

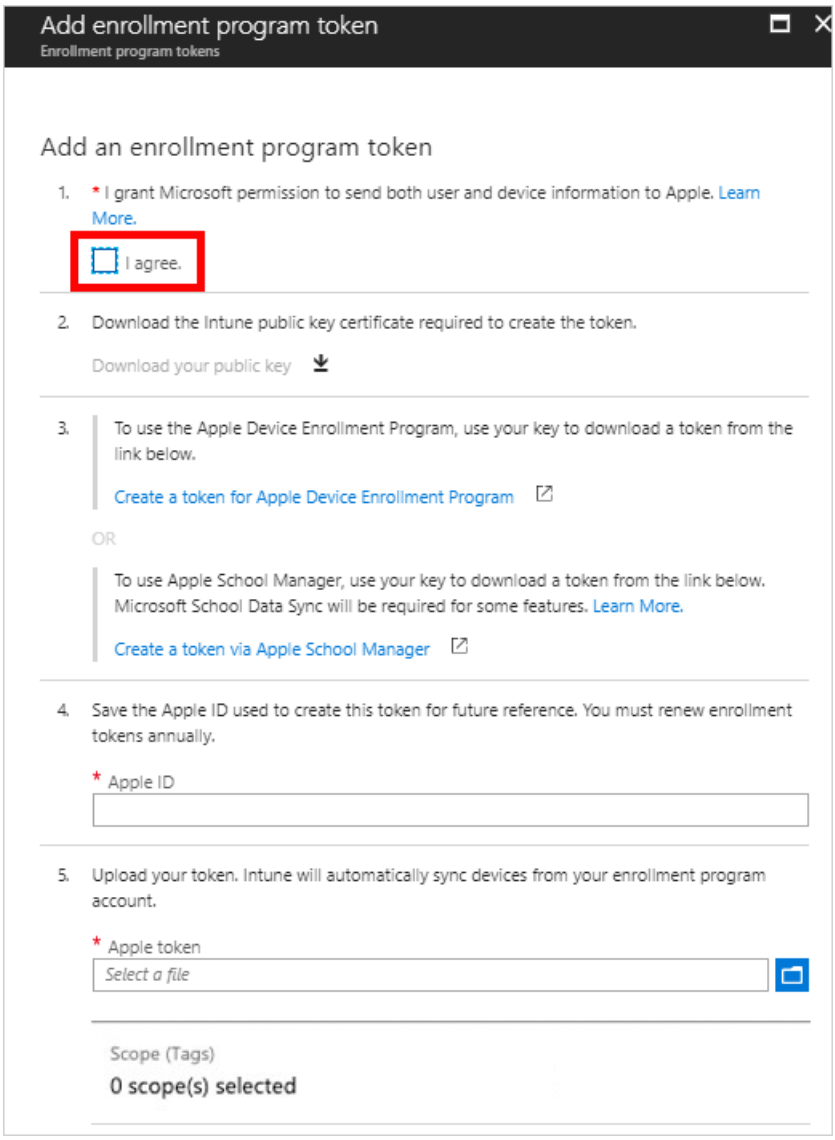
- Devices purchased in Apple Business Manager or Apple's Device Enrollment Program
- Set the mobile device management authority
- Get an Apple MDM Push certificate

Get an Apple Device Enrollment token

Before enrolling iOS/iPadOS devices with Apple's corporate enrollment features, you need an Apple Device Enrollment token (.pem) file. This token lets Intune sync information about Apple devices that your corporation owns. It also permits Intune to upload enrollment profiles to Apple and to assign devices to those profiles.

You use the Apple portal to create a Device Enrollment token. You also use the portals to assign devices to Intune for management.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment Program Tokens** > **Add**.
2. Grant permission to Microsoft to send user and device information to Apple by selecting **I agree**.

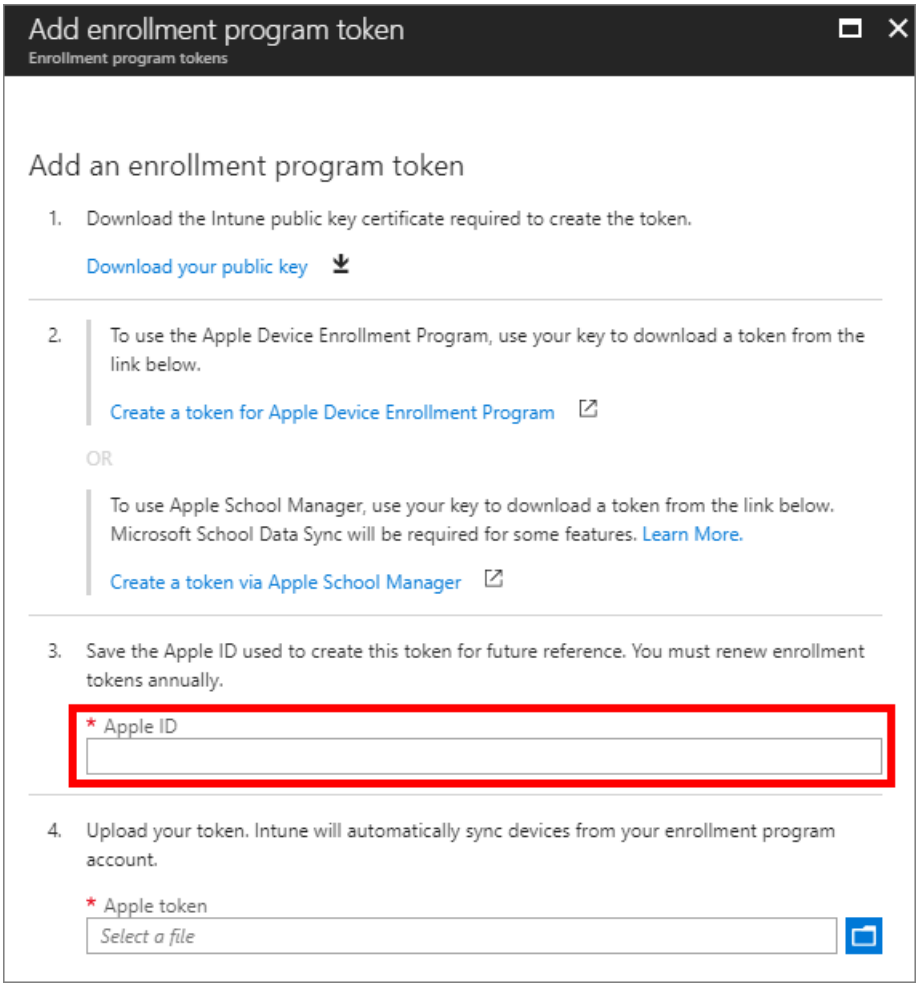


3. Choose **Download your public key** to download and save the encryption key (.pem) file locally. The .pem file is used to request a trust-relationship certificate from the Apple portal.
4. Choose **Create a token for Apple's Device Enrollment Program** to open Apple's Deployment Program portal, and sign in with your company Apple ID. You can use this Apple ID to renew your token.
5. In Apple's Deployment Programs portal, choose **Get Started** for **Device Enrollment Program**. Your process may be slightly different than the following steps in Apple Business Manager.
6. On the **Manage Servers** page, choose **Add MDM Server**.
7. For **MDM Server Name**, enter *TestMDMServer* and then choose **Next**. The server name is for your reference to identify the mobile device management (MDM) server. It isn't the name or URL of the Microsoft Intune server.
8. The **Add <ServerName>** dialog box opens, stating **Upload Your Public Key**. Select **Choose File...** to upload the .pem file, and then choose **Next**.
9. Go to **Deployment Programs** > **Device Enrollment Program** > **Manage Devices**.
10. Under **Choose Devices By**, choose **Serial Number**.
11. For **Choose Action**, choose **Assign to Server**, choose the <ServerName> specified for Microsoft Intune, and then choose **OK**. The Apple portal assigns the specified devices to the Intune server for management and then displays **Assignment Complete**.

    In the Apple portal, go to **Deployment Programs** > **Device Enrollment Program** > **View**

Assignment History to see a list of devices and their MDM server assignment.

12. For future reference, in Intune in the Azure portal, provide the Apple ID used to create this token.



13. In the **Apple token** box, browse to the certificate (.pem) file, choose **Open**, and then choose **Create**.

14. If you want to apply Scope Tags to limit which admins have access to this token, select scopes.

Create an Apple enrollment profile

Now that you've installed your token, you can create an enrollment profile for corporate-owned iOS/iPadOS devices. A device enrollment profile defines the settings applied to a group of devices during enrollment.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS enrollment** > **Enrollment Program Tokens**.

2. Select the token you just installed, choose **Profiles** > **Create profile** > **iOS/iPadOS**.

3. On the **Basics** page, enter *TestProfile* for **Name** and *Testing ADE for iOS/iPadOS devices* for **Description**. Users do not see these details.

4. Select **Next**.

5. On the **Management Settings** page, decide if you want your devices to enroll with or without **User Affinity**. User Affinity is designed for devices that will be used by particular users. If your users will want to use the Company Portal for services like installing apps, choose **Enroll with User Affinity**. If your users do not need the Company Portal or you want to provision the device for many users, choose **Enroll without User Affinity**.

6. If you chose to enroll with User Affinity, the **Select where users must authenticate** option appears. Decide if you want to Authenticate with Company Portal or Apple Setup Assistant.

- **Company Portal**: Select this option to use Multi-Factor Authentication, allow users to change passwords upon first sign in, or prompt users to reset their expired passwords during enrollment. If you want the Company Portal application to update automatically on end users' devices, separately deploy the Company Portal as a required app to these users through Apple's Volume Purchasing Program (VPP).
- **Setup Assistant**: Select this option to use Apple's provided basic HTTP authentication through Apple Setup Assistant

7. If you chose to enroll with User Affinity and Authenticate with Company Portal, the **Install Company Portal with VPP** option appears. If you install the Company Portal with a VPP token, your user won't have to enter an Apple ID and Password to download the Company Portal from the app store during enrollment. Choose **Use Token:** under **Install Company Portal with VPP** to select a VPP token that has free licenses of the Company Portal available. If you don't want to use VPP to deploy the Company Portal, choose **Don't use VPP**.

8. If you chose to enroll with User Affinity, Authenticate with Company Portal, and Install Company Portal with VPP, decide if you want to run the Company Portal in Single App Mode until Authentication. This setting allows you to ensure the user will not have access to other apps until they have finished the corporate enrollment. If you want to restrict the user to this flow until enrollment is completed, choose **Yes** under **Run Company Portal in Single App Mode until authentication**.

9. Under **Device Management Settings**, choose **Yes** under **Supervised** (if you chose **Enroll with User Affinity**, this is automatically set to **Yes**). Supervised devices give you the most management options for your corporate iOS/iPadOS devices.

10. Choose **Yes** under **Locked enrollment** to ensure your users cannot remove management of the corporate device.

11. Choose an option under **Sync with Computers** to determine if the iOS/iPadOS devices will be able to sync with computers.

12. By default, Apple names the device with the device type (i.e. iPad). If you want to provide a different name template, choose **Yes** under **Apply device name template**. Enter the name you want to apply to the devices, where the strings *{{SERIAL}}* and *{{DEVICETYPE}}* will substitute each device's serial number and device type. Otherwise, choose **No** under **Apply device name template**.

13. Choose **Next**.

14. On the **Setup Assistant** page, *Tutorial department* for **Department Name**. This string is what users see when they tap **About configuration** during device activation.

15. Under **Department Phone**, enter a phone number. This number appears when users tap the **Need help** button during activation.

16. You can **Show** or **Hide** a variety of screens during device activation. For the most seamless enrollment experience, set all screens to **Hide**.

17. Choose **Next** to go to the **Review + Create** page. Select **Create**.

Sync managed devices to Intune

After you set up an enrollment program token with the ABM, ASM, or ADE portal and assign devices there to the MDM server, you can wait for these devices to sync to the Intune service, or manually push a sync. Without a manual sync, devices may take up to 24 hours to show up in the Azure portal.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS enrollment** > **Enrollment Program Tokens** > choose a token in the list > **Devices** > **Sync**.

Assign an enrollment profile to iOS/iPadOS devices

You must assign an enrollment program profile to devices before they can enroll. These devices are synced to Intune from Apple, and must be assigned to the proper MDM server token in the ABM, ASM, or ADE portal.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS enrollment** > **Enrollment Program Tokens** > choose your token in the list.
2. Choose **Devices** > choose devices in the list > **Assign profile**.
3. Under **Assign profile**, choose a profile for the devices > **Assign**.

> **NOTE**
> Ensure that **Device Type Restrictions** under **Enrollment Restrictions** does not have the default **All Users** policy set to block the iOS/iPadOS platform. This setting will cause automated enrollment to fail and your device will show as Invalid Profile, regardless of user attestation. To permit enrollment only by company-managed devices, block only personally owned devices, which will permit corporate devices to enroll. Microsoft defines a corporate device as a device that's enrolled via a Device Enrollment Program or a device that's manually entered under **Corporate device identifiers**.

Distribute devices to users

You've set up management and syncing between Apple and Intune, and assigned a profile to let your ADE devices enroll. You can now distribute devices to users. Devices with user affinity require each user be assigned an Intune license.

Next steps

You can find more information about other options available for enrolling iOS/iPadOS devices.

In-depth iOS/iPadOS ADE enrollment article

Identify devices as corporate-owned

9/23/2022 • 5 minutes to read • Edit Online

As an Intune admin, you can identify devices as corporate-owned to refine management and identification. Intune can perform additional management tasks and collect additional information such as the full phone number and an inventory of apps from corporate-owned devices. You can also set device restrictions to block enrollment by devices that aren't corporate-owned.

At the time of enrollment, Intune automatically assigns corporate-owned status to devices that are:

- Enrolled with a device enrollment manager account (all platforms)
- Enrolled by using Google Zero Touch
- Enrolled by using Knox Mobile Enrollment
- Enrolled with the Apple Device Enrollment Program, Apple School Manager, or Apple Configurator (iOS/iPadOS only)
- Identified as corporate-owned before enrollment with an international mobile equipment identifier (IMEI) numbers (all platforms with IMEI numbers) or serial number (iOS/iPadOS and Android)
- Enrolled as Android Enterprise corporate-owned devices with work profile
- Enrolled as Android Enterprise fully managed devices
- Enrolled as Android Enterprise dedicated devices
- Joined to Azure Active Directory with work or school credentials. Devices that are Azure Active Directory registered will be marked as personal.
- Set as corporate in the device's properties list

After enrollment, you can change the ownership setting between **Personal** and **Corporate**.

Identify corporate-owned devices with IMEI or serial number

As an Intune admin, you can create and import a comma-separated value (.csv) file that lists 14-digit IMEI numbers or serial numbers. Intune uses these identifiers to specify device ownership as corporate during device enrollment. Each IMEI or serial number can have details specified in the list for administrative purposes.

This feature is supported for the following platforms:

PLATFORM	IMEI NUMBERS	SERIAL NUMBERS
Windows	Not supported	Not supported
iOS/iPadOS	Supported in some cases. See Important below.	Supported
macOS	Not supported	Supported
Android device administrator, before Android v10	Supported	Supported
Android device administrator, Android v10 and later	Not supported	Not supported

PLATFORM	IMEI NUMBERS	SERIAL NUMBERS
Android Enterprise personally-owned work profile, before Android 12	Supported	Supported
Android Enterprise personally-owned work profile, Android 12 and later	Not supported	Not supported
Android Enterprise corporate-owned work profile	Not supported	Not Supported
Android Enterprise fully managed	Not supported	Not Supported
Android Enterprise dedicated devices	Not supported	Not supported

Learn how to find an Apple device serial number.
Learn how to find your Android device serial number.

Add corporate identifiers by using a .csv file

To create the list, create a two-column, comma-separated value (.csv) list without a header. Add the 14-digit IMEI or serial numbers in the left column, and the details in the right column. Only one type of ID, IMEI or serial number, can be imported in a single .csv file. Details are limited to 128 characters and are for administrative use only. Details aren't displayed on the device. The current limit is 5,000 rows per .csv file.

Upload a .csv file that has serial numbers – Create a two-column, comma-separated value (.csv) list without a header, and limit the list to 5,000 devices or 5 MB per .csv file.

This .csv file when viewed in a text editor appears as:

```
01234567890123,device details
02234567890123,device details
```

IMPORTANT

Some Android and iOS/iPadOS devices have multiple IMEI numbers. Intune only reads one IMEI number per enrolled device. If you import an IMEI number but it is not the IMEI inventoried by Intune, the device is classified as a personal device instead of a corporate-owned device. If you import multiple IMEI numbers for a device, uninventoried numbers display **Unknown** for enrollment status.
Also note: Serial Numbers are the recommended form of identification for iOS/iPadOS devices. Android Serial numbers are not guaranteed to be unique or present. Check with your device supplier to understand if serial number is a reliable device ID. Serial numbers reported by the device to Intune might not match the displayed ID in the Android Settings/About menus on the device. Verify the type of serial number reported by the device manufacturer. Attempting to upload a file with serial numbers containing dots (.) will cause the upload to fail. Serial numbers with dots are not supported.

Upload a .csv list of corporate identifiers

1. Sign in to the Microsoft Endpoint Manager admin center, choose **Devices** > **Enroll devices** > **Corporate device identifiers** > **Add** > **Upload CSV file**.
2. In the **Add identifiers** blade, specify the identifier type: **IMEI** or **Serial**.
3. Click the folder icon and specify the path to the list you want to import. Navigate to the .csv file, and choose **Add**.

4. If the .csv file contains corporate identifiers that are already in Intune, but have different details, the **Review duplicate identifiers** popup appears. Select the identifiers that you want to overwrite into Intune and choose **Ok** to add the identifiers. For each identifier, only the first duplicate will be compared.

Manually enter corporate identifiers

1. Sign in to the Microsoft Endpoint Manager admin center, choose **Devices** > **Enroll devices** > **Corporate device identifiers** > **Add** > **Enter manually**.
2. In the **Add identifiers** blade, specify the identifier type: **IMEI** or **Serial**.
3. Enter the **Identifier** and **Details** for each identifier you want to add. When you're done entering identifiers, choose **Add**.
4. If you entered corporate identifiers that are already in Intune, but have different details, the **Review duplicate identifiers** popup appears. Select the identifiers that you want to overwrite into Intune and choose **Ok** to add the identifiers. For each identifier, only the first duplicate will be compared.

You can click **Refresh** to see new device identifiers.

Imported devices are not necessarily enrolled. Devices can have a state of either **Enrolled** or **Not contacted**. **Not contacted** means that the device has never communicated in with the Intune service.

Delete corporate identifiers

1. Sign in to the Microsoft Endpoint Manager admin center, choose **Devices** > **Enroll devices** > **Corporate device identifiers**.
2. Select the device identifiers you want to delete, and choose **Delete**.
3. Confirm the deletion.

Deleting a corporate identifier for an enrolled device does not change the device's ownership. To change a device's ownership, go **Devices**, select the device, choose **Properties**, and change **Device ownership**.

IMEI specifications

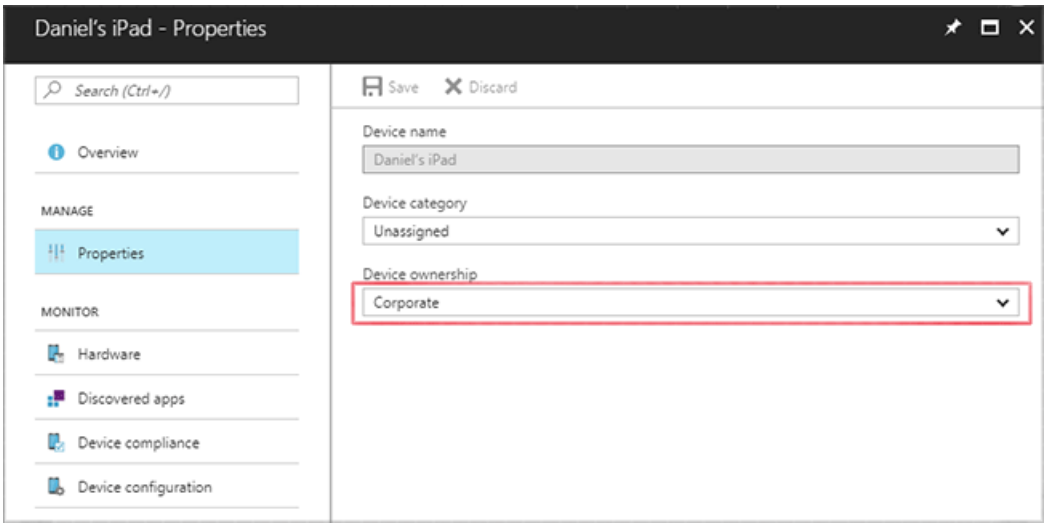
For detailed specifications about International Mobile Equipment Identifiers, see 3GGPP TS 23.003.

Change device ownership

Devices properties display **Ownership** for each device record in Intune. As an admin, you can specify devices as **Personal** or **Corporate**.

To change device ownership:

1. Sign in to the Microsoft Endpoint Manager admin center, choose **Devices** > **All devices** > choose the device.
2. Choose **Properties**.
3. Specify **Device ownership** as **Personal** or **Corporate**.



When a device's ownership type is changed from *Corporate* to *Personal*, Intune deletes all app information previously collected from that device within seven days. If applicable, Intune will also delete the phone number on record. Intune will still collect an inventory of apps installed by the IT admin on the device and will still collect a partial phone number for the device after it is marked as personal.

When an iOS/iPad or Android device's ownership type is changed from *Personal* to *Corporate*, a push notification is sent through the Company Portal app to inform the devices user of this change.

This setting can be found in the Microsoft Endpoint Manager by selecting **Tenant administration** > **Customization**. For more information, see Company Portal - Configuration.

Incomplete user enrollments report

9/23/2022 • 3 minutes to read • Edit Online

This report tells you where in the Company Portal enrollment process users are not completing the enrollment process.

To see the report, sign in to the Microsoft Endpoint Manager admin center. Then select **Devices** > **Monitor* > **Incomplete user enrollments**.

Using this information, you can update your onboarding documents to help users complete enrollment. For example, if many users are quitting at the Terms of Use, you might investigate that area and make it more intuitive for users.

What is an incomplete enrollment?

An incomplete enrollment is when a user does any of the following:

- Explicitly chooses an action to halt enrollment
- Closes the Company Portal during enrollment
- Spends more than 30 minutes between enrollment sections

If a user chooses to stop enrollment and restart multiple times, it shows up as multiple attempts and multiple incomplete enrollments. If a user waits for 30 minutes between different enrollment screens, it is considered multiple incomplete enrollments.

What does the report show?

The reports include data for iOS/iPadOS and Android devices.

The reports show data for the past two weeks, but you can filter the report to show any period up to 30 days in the past.

You can filter the date range, operating system, and enrollment section by choosing **Filter**.

Number and percentage tiles

At the top of the report, you can see the number and percentage of incomplete enrollments in relation to all enrollments.

- Initiated enrollments: The number of enrollments attempted.
- Incomplete enrollments: The number of attempted enrollments that didn't result in a fully enrolled and compliant device.
- Incomplete rate: The percentage of enrollment attempts that were abandoned (Abandoned enrollments / Initiated enrollments).

Line graph

The line graph shows the daily incomplete enrollments for each of the four core enrollment sections:

- Setup checklist
- Platform screens
- Terms of use
- Compliance/Activation

User abandonment actions

The following tables list the user actions that indicate enrollment is incomplete.

Setup checklist section

ACTION NAME	SCREEN OR FLOW	PLATFORM	ACTION
EnrollmentWrapUp	Prompt to open page in Company Portal	iOS/Android	**Cancel**
EnrollmentWrapUp	Enrolling device screen until finish of **Loading company resources**	iOS/Android	Took > 30 minutes
DeviceCategory	Device Category selection (if admin configured) until click **Done**	iOS/Android	Took > 30 minutes
PreEnrollmentWizard	Set up access screen when having started enrollment but returned to Set up access	iOS/Android	**Postpone**
PreEnrollmentWizard	Set up access screen until clicking **Next** on the **What's Next** screen	iOS/Android	Took > 30 minutes

Platform screens section

ACTION NAME	SCREEN OR FLOW	PLATFORM	ACTION
iOSProfileLaunch	Prompt to show a configuration profile	iOS/iPadOS	**Ignore**
iOSProfileLaunch	Installing profile screen	iOS/iPadOS	**Cancel**
iOSProfileLaunch	Prompt to trust the profile's source to enroll the device	iOS/iPadOS	**Cancel**
iOSProfileLaunch	Install profile screen until profile is installed	iOS/iPadOS	Took > 30 minutes
AndroidPermissions	Device administrator activation screen	Android	**Cancel**
AndroidPermissions	From prompt for approval to make and manage phone calls until device administrator **Activate**	Android	Took > 30 minutes
KnoxActivation	KLMS agent activation (Samsung only)	Android	**Cancel**
KnoxActivation	KLMS agent activation until **Confirm**	Android	Took > 30 minutes

Terms of use section

ACTION NAME	SCREEN OR FLOW	PLATFORM	ACTION
TermsofUse	Terms of use (if admin configured)	iOS/Android	**Decline All**
TermsofUse	Terms of use until **Accept all**	iOS/Android	Took > 30 minutes

Compliance/Activation section

ACTION NAME	SCREEN OR FLOW	PLATFORM	ACTION
Compliance	Device compliance (if admin configured) shows as non-green on access setup post enrollment	iOS/Android	**Postpone**
Compliance	Device compliance shows as non-green until updated to show green	iOS/Android	Took > 30 minutes
Activation	Enrollment activation (if admin configured) shows as non-green on access setup	iOS/Android	**Postpone**
Compliance	Device activation shows as non-green until updated to show green	iOS/Android	Took > 30 minutes

Next steps

After checking on your incomplete enrollment rates, you can review the enrollment options to see if you can make any changes to improve enrollment.

Terms and conditions for user access

9/23/2022 • 4 minutes to read • Edit Online

Use an Intune terms and conditions policy to present relevant disclaimers for legal or compliance requirements to device users. A terms and conditions policy requires targeted users to accept your terms in Company Portal before they can enroll devices or access protected resources.

This article describes how to get started with terms and conditions in Intune.

Create terms and conditions

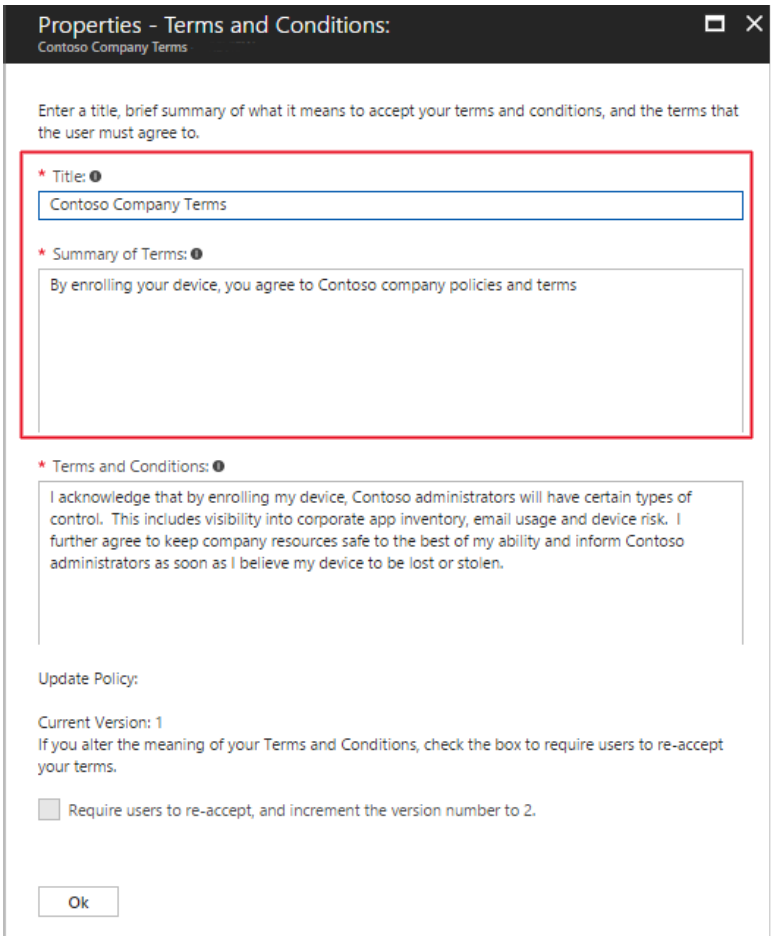
Complete these steps to create an Intune terms and conditions policy.

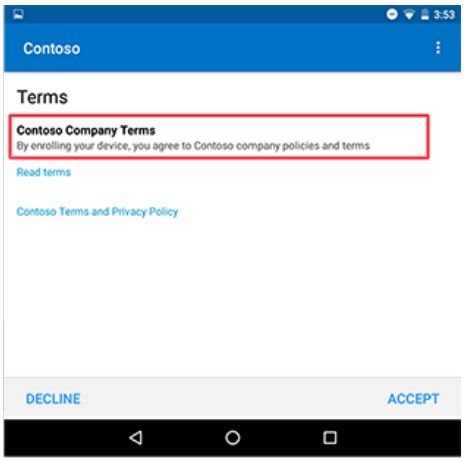
1. Sign in to the Microsoft Endpoint Manager admin center and select **Tenant administration** > **Terms and conditions**.
2. Select **Create**.
3. On the **Basics** page, enter the following information:
   - **Name**: Give your policy a name so that you can recognize it in Intune later. Device users don't see this name.
   - **Description**: Optionally, describe the purpose or intended use for this specific set of terms.
4. Select **Next**.
5. On the **Terms** page, enter the following information:
   - **Title**: The display name for your terms. Users see the title in the Company Portal app.
   - **Terms and conditions**: The terms and conditions that users see and must either accept or reject.
   - **Summary of Terms**: Enter a brief, high-level explanation of what the user is agreeing to. This text is visible to device users.

     Example message: *By enrolling your device, you're agreeing to the terms of use set out by Contoso. Read the terms carefully before proceeding.*
6. Select **Next**.
7. On the **Select scope tags**, select a scope tag from the list to add it to the terms and conditions, or select the default scope tag. Then select **Next**.
8. On the **Assignments** page, choose who you want to assign the terms to. Your options:
   - **Add all users**: Choose this option to assign these terms and conditions to all device users.
   - **Add groups**: Choose this option to assign these terms and conditions to users in select groups.
9. Select **Next**.
10. Review the summary of your new terms and conditions, and then select **Create**.

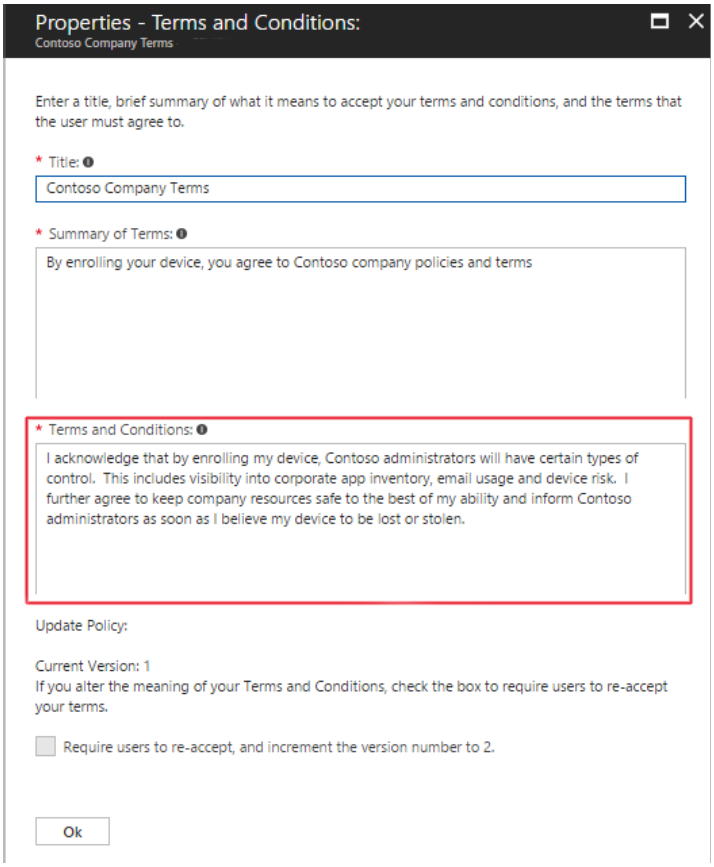
How it looks to users

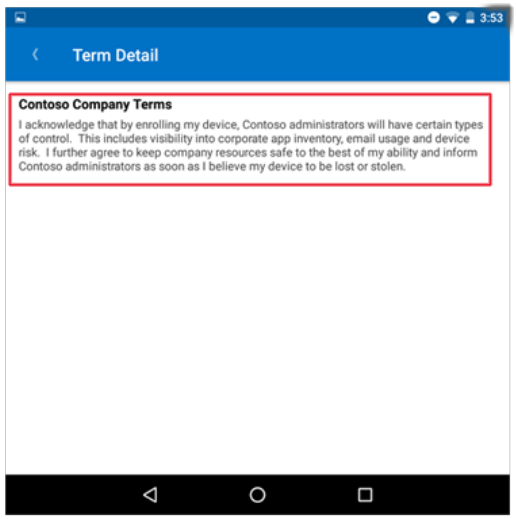
Targeted users can see the terms and conditions in the Intune Company Portal app. The following image shows what the title and summary of terms look like in the app. Intune formats the title with bold font to make it stand out, with the summary of terms positioned directly under it.





Device users tap **Read terms** to expand the terms and conditions to full-view. The following image shows what the terms and conditions look like when expanded.





Monitor acceptance of terms

An acceptance report provides the details of an individual's agreement to your terms and conditions. Intune

reports the following details:

- User name: The name of the user who accepted the terms.
- Accepted version: The version that was accepted.
- Accepted time: The date and time of acceptance.
- Accepted latest: Shows whether device user accepted the latest terms and conditions available.
- UPN: The user principal name assigned to the device user.

To view and export acceptance reports:

1. Go to **Tenant administration** > **Terms and conditions**.
2. Select your terms from the table.
3. Select **Acceptance Reporting** to view available reports.
4. Select **Export** to save the reports to your device.

> **NOTE**
> Report data is updated every 24 hours and can take up to 12 hours to finish generating. Because of this, data in the report can have up to a 36 hour latency.

Provide localized terms and conditions

You can create multiple policies using localized text, and then target each policy to the appropriate groups of users.

Update terms and conditions

Microsoft Intune provides a version control setting so that you can track versions and notify users of changes to your terms. As a best practice, every time you make a significant change to your terms and conditions, you should:

- Increase the version number in Intune.
- Require assigned users to review and reaccept the updated terms.

> **TIP**
> Do not change the version number for changes like typo and formatting fixes.

To edit terms and conditions:

1. Select **Tenant administration** > **Terms and conditions**.
2. From the table, choose the terms and conditions you want to edit.
3. Select **Properties** and then next to **Terms**, select **Edit.**
4. Adjust the existing content as needed.
5. If you edit the meaning of the terms at all, select the checkbox next to **Require users to re-accept, and increment the version number to *next version*.** In place of *next step*, you'll see the actual version number.
6. Select **Review + save**.
7. Review the summary for your terms and conditions, and then select **Save**.

Users only have to accept the updated terms and conditions once. This means that a user associated with multiple enrolled devices won't need to accept the terms and conditions on each device.

Use Azure AD Terms of use feature

You can use the Azure Active Directory terms of use feature to configure stricter compliance requirements. Capabilities include:

- Attach multiple localized versions to a single policy
- Render terms in PDF format for a richer experience that allows for branding, images, and hyperlinks
- Require users to expand the terms of use
- Require users to consent on every device
- Expire consents
- Require users to reaccept terms after a certain period of time
- Provide terms for non-enrollment scenarios

These terms are shown to users when they sign in to targeted apps and resources. If you configure both Azure AD terms of use and Intune terms and conditions, users will be required to accept both. For a comparison of both solutions, see Choosing the right Terms solution for your organization.

Understand Intune and Azure AD device limit restrictions

9/23/2022 • 3 minutes to read • Edit Online

Applies to

- Android
- iOS
- macOS
- Windows 10
- Windows 11

Device limit restrictions can be configured two ways:

- Intune enrollment
- Azure Active Directory (AD) joined or Azure AD registered

This article clarifies when these limits are applied based on your configuration.

Intune device limit restrictions

Intune device limit restrictions set the maximum number of devices that a user can control (maximum setting is 15). To set this **Device limit**, go to Microsoft Endpoint Manager admin center > **Devices** > **Enrollment restrictions**. For more information, see Create a device limit restriction.

Azure device limit restriction

Azure device limit restrictions set the maximum number of devices that either Azure AD joins or Azure AD registers. To set the **Maximum number of devices per user**, go to the Azure portal > **Azure Active Directory** > **Devices**. For more information, see Configure device settings

Settings applied based on user affinity

If you have both Intune and Azure device limit restrictions set, the following table shows you what is applied based on your user affinity setting.

DEVICE PLATFORM	USER AFFINITY	AZURE APPLIES	INTUNE APPLIES
Android Enterprise personally-owned work profile	Yes	Yes	Yes
Android Enterprise dedicated device	No	No	No
Android Enterprise fully managed	Yes	Yes	Yes

DEVICE PLATFORM	USER AFFINITY	AZURE APPLIES	INTUNE APPLIES
Android Enterprise corporate-owned work profile	Yes	Yes	Yes
Android device administrator	Yes	Yes	Yes
Android device administrator DEM	No		No
iOS/macOS BYOD	Yes	Yes	Yes
iOS/macOS Automated Device Enrollment (ADE)	Yes	Yes	Yes
Windows BYOD	Yes	Yes	Yes
Windows MD-only		Yes	Yes
Windows Azure AD joined	Yes	Yes	No
Windows Autopilot	Yes	Yes	No
Windows hybrid Azure AD joined	No	No	Yes
Windows co-management	No	Yes	No
Windows DEM	No	Yes	No
Windows bulk enrollment	No	Yes	No

Android and iOS devices

iOS or Android devices example 1

- The Azure **Maximum number of devices per user** setting is set to 3.
- The Intune **Device limit** setting is set to 5.

Outcome: The maximum number is per user. For example, if you enroll three Intune devices, the Azure registration for the fourth device will fail because of the settings to limit the number of registrations for the devices.

iOS or Android devices example 2

- The Azure **Maximum number of devices per user** setting is set to 20.
- The Intune **Device limit** setting is set to 2.

Outcome: You can successfully register and enroll two devices. Intune enrollment will be blocked for any additional devices. ADE without user affinity is restricted by Azure device registration limits although it's not associated with a user.

Windows devices

Intune device limit restrictions don't apply for the following Windows enrollment types:

- Co-managed enrollments
- Group policy object (GPO) enrollments
- Azure AD joined enrollments
- Bulk Azure AD joined enrollments
- Autopilot enrollments
- Device enrollment manager enrollments

You can't enforce device limit restrictions for these enrollment types because they're considered shared device scenarios. You can set hard limits for these enrollment types in Azure Active Directory.

For the device limit restriction in Azure, the **Maximum number of devices per user** setting applies to devices that are either Azure AD joined or Azure AD registered. This setting doesn't apply to hybrid Azure AD joined devices.

Windows 10/11 example 1

- The Azure **Maximum number of devices per user** setting is set to 5.
- The Intune **Device limit** setting is set to 3.
- The devices are hybrid Azure AD joined and enrolled automatically (GPO configured).

Outcome: Because the enrollment is pushed through GPO, the Azure device registration limit doesn't apply. The Intune device limit restriction also doesn't apply.

Windows 10/11 example 2

- The Azure **Maximum number of devices per user** setting is set to 5.
- The Intune **Device limit** setting is set to 2.
- The devices are local domain joined and enrolled by using **Settings** > **Access Work or School** > **Connect**.

Outcome: You can only enroll two devices before they're blocked. You can register up to five devices.

Next steps

- Create a device limit restriction in Azure.
- Learn more about registration and domain joined.

Add device enrollment managers

9/23/2022 • 2 minutes to read • Edit Online

A device enrollment manager (DEM) is a non-administrator user who can enroll devices in Intune. Device enrollment managers are useful to have when you need to enroll and prepare many devices for distribution. People signed in to a DEM account can enroll and manage up to 1,000 devices, while a standard non-admin account can only enroll 15.

A DEM account requires an Intune user or device license, and an associated Azure AD user. Global Administrators and Intune Service Administrators can add and manage device enrollment managers in the Microsoft Endpoint Manager admin center.

This article describes the limits and specifications of enrollment manager and how to manage permissions.

Supported enrollment methods

A device enrollment manager can use the following methods to enroll devices in Intune:

- Windows Autopilot
- Windows devices bulk enrollment
- DEM-initiated via Company Portal enrollment
- DEM-initiated via Azure AD-join

> **TIP**
> To compare DEM best practices and capabilities alongside other Windows enrollment methods, see Intune enrollment method capabilities for Windows devices.

Account permissions

These Azure AD roles can manage device enrollment managers:

- Global Administrator
- Intune Service Administrator role in Azure AD

People assigned these roles can add and delete device enrollment managers, and view all DEM users in the Microsoft Endpoint Manager admin center.

Add a device enrollment manager

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select **Devices** > **Enroll devices**.
3. Select **Device enrollment managers**.
4. Select **Add**.
5. In the **User name** field, enter the user principal name of the user you're adding.
6. Select **Add**. The new device enrollment manager is added to the list of DEM users.

To remove someone as a device enrollment manager, select their name in the list and then choose **Delete**.

Limitations

The device enrollment manager account can't be used with all features in Microsoft Intune and has some limitations when used with others. This section describes the limitations you could encounter while setting up devices from a DEM account.

Android Enterprise

You can enroll up to 10 personally owned devices with work profiles.

The following types of Android Enterprise devices can't be set up via DEM:

- Corporate-owned with a work profile
- Fully managed

Apple Automated Device Enrollment

DEM isn't compatible with Apple Automated Device Enrollment (ADE).

Apple volume purchased apps

DEM-enrolled devices can install VPP apps if they have Apple VPP device licenses. You can't use apps purchased through Apple VPP with Apple VPP user licenses, because of per-user Apple ID requirements for app management.

Azure AD

Applying an Azure AD device restriction to a DEM account will prevent you from reaching the 1,000 device limit that the DEM account can enroll.

Conditional access

Conditional access is only supported with DEM on devices running:

- Windows 10, version 1803 and later
- Windows 11

Device limit restrictions

DEM enrolls Windows 10/11 devices in shared device mode, so device limit restrictions won't work on them. Instead, you can configure a hard limit for these devices in the Azure AD admin center. For more information, see Manage device identities by using the Azure portal.

Intune Company Portal

Only the local device appears in the Company Portal app or Company Portal website. Device users can't wipe DEM-enrolled devices from Company Portal. You have to sign in to the Microsoft Endpoint Manager admin center to wipe these devices.

Number of accounts

There's a limit of 150 DEM accounts in Microsoft Intune.

Categorize devices into groups

9/23/2022 • 2 minutes to read • Edit Online

Device categories allow you to easily manage and group devices in Microsoft Intune. Create a category, such as *sales* or *accounting*, and Intune automatically add all devices that fall within that category to the corresponding device group in Intune.

To enable categories in your tenant, you must create a category in the Microsoft Endpoint Manager admin center and set up dynamic Azure Active Directory (Azure AD) security groups.

This article describes how to configure and edit device categories.

Configure device categories

You must be a Global Administrator or Intune Administrator to perform these steps.

Step 1: Create device category in Intune

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Choose **Devices** > **Device categories**.
3. Select **Create device category** to add a new category.
4. Enter the name of the new category, such as `HR` and an optional description.
5. Select **Next**.
6. Optionally, assign a scope tag, like `US-NC IT Team` or `JohnGlenn_ITDepartment`, to limit management of the category to specific IT groups. For more information about scope tags, see Use RBAC and scope tags for distributed IT.
7. Select **Next**.
8. Select **Create**. The new category is added to your **Device categories** list.

You'll use the device category name when you create Azure Active Directory (Azure AD) security groups in the next step.

Step 2: Create Azure AD security groups

To enable automatic grouping, you must create a dynamic group using attribute-based rules in Azure AD. For instructions, see Using attributes to create advanced rules in the Azure AD documentation. Create an advanced rule for your group using the **deviceCategory** attribute and the category name you created in Step 1 of this article.

For example, to create a rule that automatically groups devices belonging in the HR category, use the following rule syntax: `device.deviceCategory -eq "HR"`

View categories of all devices

Sign in to the Microsoft Endpoint Manager admin center and go to **Devices** > **All devices** for a list of all devices. The **Device category** column shows the category assigned to each device.

If the **Device category** column isn't visible in the table, select **Columns** and then choose **Category** > **Apply**.

When you delete a category, devices assigned to it appear as **Unassigned**.

Change the category of a device

If you edit a category, be sure to update any Azure AD security groups that reference the category in their rules.

1. Sign in to the Microsoft Endpoint Manager admin center.

2. Select **Devices** > **All devices**.
3. Select a device.
4. On the device details page, select **Properties**.
5. Change your selection in the **Device category** field.

Best practices

Device categories are supported on devices running Android, iOS/iPadOS, or Windows. People with Windows devices must use the Company Portal website to select their category. Regardless of platform, any device user can sign in to portal.manage.microsoft.com at anytime and go to **My devices** to select a category.

If an iOS/iPadOS or Android device is already enrolled before you configure categories, the user will receive a notification about the device on the Company Portal website. The notification informs them that they need to select a category the next time they're in the Company Portal app.

Get an Apple MDM push certificate

9/23/2022 • 3 minutes to read • Edit Online

Upload and renew your Apple MDM push certificates in Microsoft Intune. An Apple MDM Push certificate is required to manage iOS/iPadOS and macOS devices in Microsoft Intune, and enables devices to enroll via:

- The Intune Company Portal app.
- Apple bulk enrollment methods, such as the Device Enrollment Program, Apple School Manager, and Apple Configurator.

Certificates must be renewed annually.

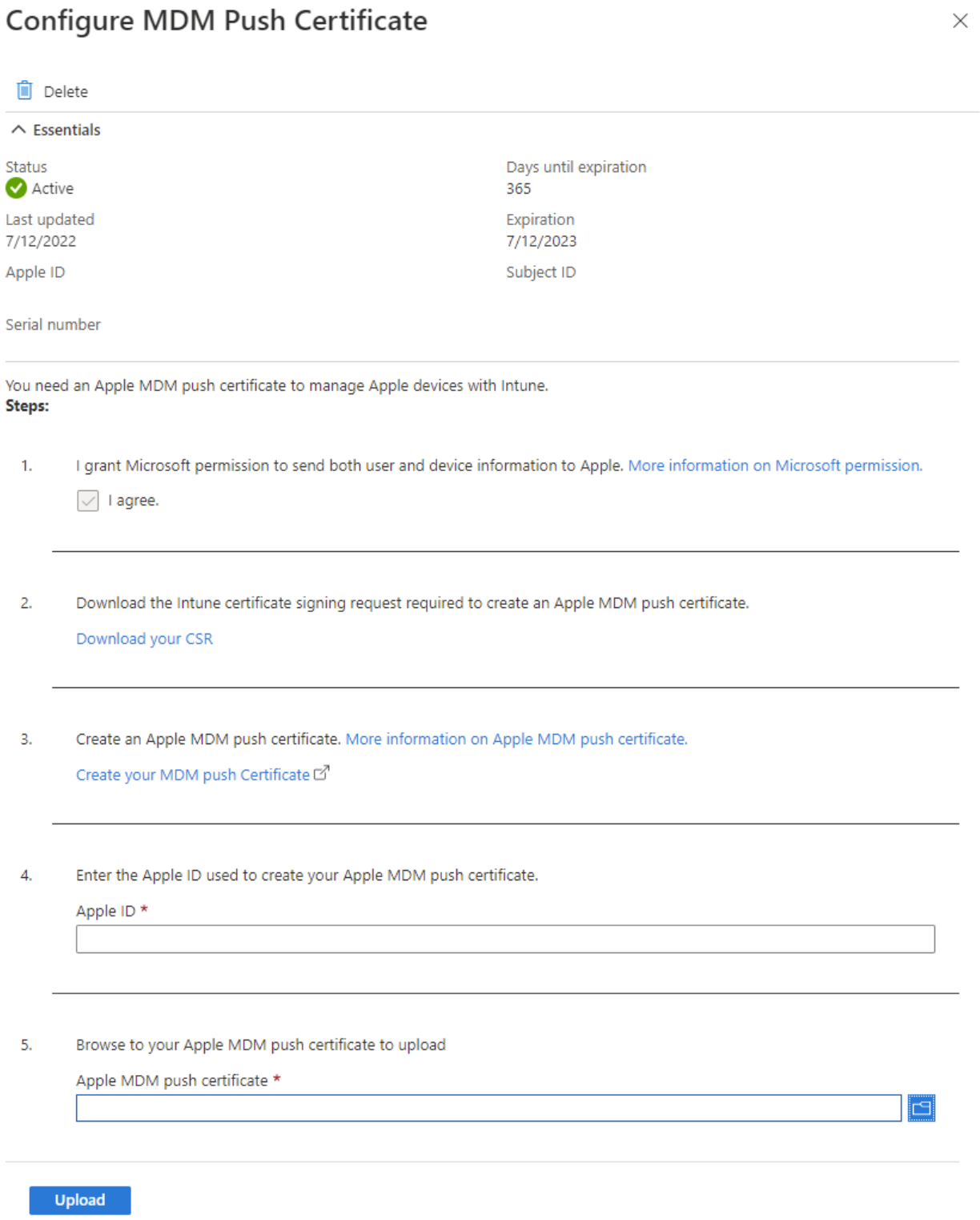
This article describes how to use Intune to create and renew an Apple MDM push certificate.

Steps to get your certificate

Sign in to the Microsoft Endpoint Manager admin center, choose **Devices** > **Enroll devices** > **Apple enrollment** > **Apple MDM Push Certificate**, and then follow these steps.

Step 1. Grant Microsoft permission to send user and device information to Apple

Select **I agree.** to give Microsoft permission to send data to Apple.



Step 2. Download the Intune certificate signing request required to create an Apple MDM push certificate

Select **Download your CSR** to download and save the request file locally. The file is used to request a trust relationship certificate from the Apple Push Certificates Portal.

Step 3. Create an Apple MDM push certificate

1. Select **Create your MDM push Certificate** to go to the Apple Push Certificates Portal.
2. Sign in with your organization's Apple ID.
3. Select **Create a Certificate**.
4. Read and agree to the terms and conditions. Then select **Accept**.
5. Select **Choose File** and then select the CSR file you downloaded in Intune.
6. Select **Upload**.
7. On the confirmation page, select **Download**. The certificate file (.pem) downloads to your device. Save this

file for later.

> **NOTE**
> The certificate is associated with the Apple ID used to create it. As a best practice, use a company email address as your Apple ID and make sure the mailbox is monitored by more than one person, such as by a distribution list. Avoid using a personal Apple ID.

Managed Apple ID

If you plan to federate your existing Azure AD accounts with Apple to use Managed Apple ID, contact Apple to have the existing APNS certificate migrated to your new Managed Apple ID. For more information, see the Apple Support user guide for Apple School Manager.

Step 4. Enter the Apple ID used to create your Apple MDM push certificate

Return to the admin center and enter your Apple ID as a reminder for when you need to renew the certificate.

Step 5. Browse to your Apple MDM push certificate to upload

1. Select the **Folder** icon.
2. Select the certificate file (.pem) you downloaded in the Apple portal.
3. Select **Upload** to finish configuring the MDM push certificate.

Renew Apple MDM push certificate

The Apple MDM push certificate is valid for 365 days. You must renew it annually to maintain iOS/iPadOS and macOS device management. Once the certificate expires, there is a 30-day grace period to renew it.

Renew the MDM push certificate with the same Apple ID you used to create it.

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select **Devices** > **Enroll devices** > **Apple enrollment** > **Apple MDM Push Certificate**.
3. Select **Download your CSR** to download and save the request file locally. The file is used to request a trust relationship certificate from the Apple Push Certificates Portal.
4. Select **Create your MDM push Certificate** to go to the Apple Push Certificates Portal.
5. Find the certificate you want to renew and select **Renew**.
6. Select **Choose File** and select the new CSR file you downloaded.
7. In the provided field, enter a unique note about the certificate so that you can easily identify it later.

   > **TIP**
   > Each certificate has a unique UID. To find it, look for the subject ID, which shows the GUID portion of the UID, in the certificate details. You can also find this information on the enrolled iOS/iPadOS device. Go to **Settings** > **General** > **Device Management** > **Management Profile** > **More Details** > **Management Profile**. The **Topic** value contains the unique GUID that you can match up to the certificate in the Apple Push Certificates portal.

8. Select **Upload**.
9. On the **Confirmation** screen, select **Download**.
10. Return to the admin center > **Configure MDM Push Certificate** page, and upload your certificate file.

Renewal is complete when your Apple MDM push certificate status appears active in both the admin center and Apple portal.

Next steps

For more information about enrollment options, see Choose how to enroll iOS/iPadOS devices.

Require multifactor authentication for Intune device enrollments

9/23/2022 • 2 minutes to read • Edit Online

Intune can use Azure Active Directory (Azure AD) Conditional Access policies to require multifactor authentication (MFA) for device enrollment to help you secure your corporate resources.

MFA works by requiring any two or more of the following verification methods:

- Something you know (typically a password or PIN).
- Something you have (a trusted device that isn't easily duplicated, like a phone).
- Something you are (biometrics, like a fingerprint).

MFA is supported for iOS/iPadOS, macOS, Android, and Windows 8.1 or later devices.

When you enable MFA, end users need a second device, and must supply two forms of credentials to enroll a device.

Configure Intune to require multifactor authentication at device enrollment

To require MFA when a device is enrolled, follow these steps:

> **IMPORTANT**
> You must have an Azure Active Directory Premium P1 or above assigned to your users to implement this policy.

> **IMPORTANT**
> Don't configure **Device based access rules** for Microsoft Intune enrollment.

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Browse to **Devices** > **Conditional Access**. The Conditional Access node accessed from *Intune* is the same node as accessed from *Azure AD*.
3. Choose **New policy**.
4. Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
5. Under **Assignments**, select **Users or workload identities**.
   a. Under **Include**, select **Select users or groups**, and check **Users and groups**. Then select the users and/or groups that will receive this policy
   b. Choose **Select**.
6. Under **Cloud apps or actions** > **Include**.
   a. Choose **Select apps** > **Microsoft Intune Enrollment**.
   b. Choose **Select**. By choosing Microsoft Intune Enrollment, Conditional Access MFA is applied only to

the enrollment of the device (one-time MFA prompt).

For Apple Automated Device Enrollments using **Setup assistant with modern authentication**, you have two options:

CLOUD APP	MFA PROMPT LOCATION	AUTOMATED DEVICE ENROLLMENT NOTES
Microsoft Intune	Setup Assistant, Company Portal app	With this option, MFA is required during enrollment and for each login to the Company Portal app/Company Portal website. Conditional Access MFA is applied only to the login of the Company Portal on the device.
Microsoft Intune Enrollment	Setup Assistant	With this option, MFA is applied only to the enrollment of the device (one-time MFA prompt). Conditional Access MFA is applied only to the login of the Company Portal on the device.

7. Under **Conditions** you don't need to configure any settings for MFA.
8. Under **Access controls** > **Grant**
   a. Select **Require multifactor authentication** and **Require device to be marked as compliant**.
   b. Ensure **Require all the selected controls** is selected under **For multiple controls**.
   c. Choose **Select**.
9. Under **Session**.
   a. Select **Sign-in frequency**.
   b. Ensure **Every time** is selected.
   c. Select **Select**.
10. In **New policy**, choose **Enable policy** > **On**, and then choose **Create**.

> **NOTE**
> A second device is required to complete the MFA challenge for corporate devices like the following:
>
> - Android Enterprise Fully Managed.
> - Android Enterprise Corporate Owned Work Profile.
> - iOS/iPadOS Automated Device Enrollment.
> - macOS Automated Device Enrollment.
>
> The second device is required because the primary device can't receive calls or text messages during the provisioning process.

Next steps

When end users enroll their device, they now must authenticate with a second form of identification, like a PIN, a phone, or biometrics.

Intune enrollment methods for Windows devices

9/23/2022 • 3 minutes to read • Edit Online

Applies to

- Windows 10
- Windows 11

To manage devices in Intune, devices must first be enrolled in the Intune service. Both personally owned and corporate-owned devices can be enrolled for Intune management.

There are two ways to get devices enrolled in Intune:

- Users can self-enroll their Windows PCs
- Admins can configure policies to force automatic enrollment without any user involvement

> **TIP**
> For guidance on which enrollment method is right for your organization, see Deployment guide: Enroll Windows devices in Microsoft Intune.

User self-enrollment in Intune

Users can self-enroll their Windows device by using any of these methods:

- Bring your own device (BYOD): Users enroll their personally owned devices by downloading and installing the **Company Portal App**. This process:
  - Registers the device with Azure Active Directory to gain access to corporate resource like email.
  - Enrolls the device in Intune as a personal owned device (BYOD).

  If an administrator has configured Auto enrollment (available with Azure AD premium subscriptions), the user only has to enter their credentials once. Otherwise, they'll have to enroll separately through MDM only enrollment and reenter their credentials.

- **MDM only enrollment** lets users enroll an existing Workgroup, Active Directory, or Azure Active directory joined PC into Intune. Users enroll from Settings on the existing Windows PC.

  This enrollment method isn't recommended because:

  - It doesn't register the device into Azure Active Directory (AD). Users might not get access to organization resources, such as email.
  - It prevents using some Azure AD features, such as Conditional Access.

- Azure Active Directory (Azure AD) Join - Joins the device with Azure Active Directory and enables users to sign in to Windows with their Azure AD credentials. If Auto Enrollment is enabled, the device is automatically enrolled in Intune. The benefit of auto enrollment is a single-step process for the user. Otherwise, they'll have to enroll separately through MDM only enrollment and reenter their credentials. Users enroll this way either during initial Windows OOBE or from Settings. The device is marked as a corporate owned device in Intune.

- Autopilot - Automates Azure AD Join and enrolls new corporate-owned devices into Intune. This method simplifies the out-of-box experience and removes the need to apply custom operating system images onto the devices. When admins use Intune to manage Autopilot devices, they can manage policies,

profiles, apps, and more after they're enrolled. There are four types of Autopilot deployment: Self Deploying Mode (for kiosks, digital signage, or a shared device), User Driven Mode (for traditional users), Windows Autopilot for pre-provisioned deployment enables partners or IT staff to pre-provision a PC running Windows 10 or Windows 11 so that it's fully configured and business-ready, and Autopilot for existing devices enables you to easily deploy the latest version of Windows to your existing devices.

Administrator-based enrollment in Intune

Administrators can set up the following methods of enrollment that require no user interaction:

- Hybrid Azure AD Join lets administrators configure Active Directory group policy to automatically enroll devices that are hybrid Azure AD joined.
- Configuration Manager Co-management lets administrators enroll their existing Configuration Manager managed devices into Intune to get the dual benefits of Intune and Configuration Manager.
- Device enrollment manager (DEM) is a special service account. DEM accounts have permissions that let authorized users enroll and manage multiple corporate-owned devices. These types of devices are good for point-of-sale or utility apps, for example, but not for users who need to access email or company resources. Be aware that there are some limitations with DEM accounts as documented here.
- Bulk enroll lets an authorized user join large numbers of new corporate-owned devices to Azure Active Directory and Intune. You create a provisioning package with the Windows Configuration Designer (WCD) app. Then, using USB media during initial Windows OOBE experience or from existing Windows PC, you install the provisioning package to automatically enroll the devices into Intune.
- Enrolling Windows IoT Core devices is accomplished by using the Windows IoT Core Dashboard to prepare the device, and then using Windows Configuration Designer to create a provisioning package. Then, using SD Card media during initial boot up, it installs the provisioning package to automatically enroll the devices into Intune.

Next steps

Learn the capabilities of the Windows enrollment methods

Intune enrollment method capabilities for Windows devices

9/23/2022 • 2 minutes to read • Edit Online

There are several methods to enroll your workforce's devices in Intune. Each method has different best practices and capabilities, as shown in the tables below.

Best practices by enrollment method

BEST PRACTICES	AZURE AD JOINED	AZURE AD JOINED WITH AUTOPILOT (USER DRIVEN MODE)	AZURE AD JOINED WITH AUTOPILOT (SELF DEPLOYING MODE)	BULK	DEM	BYOD	GPO	CO-MANAGEMENT
Commonly used in EDU	✗	✓	✗	✓	✓	✗	✗	✗
Devices can be used as shared devices	✗	✗	✓	✓	✓	✗	✗	✗
Personal devices must access company resources	✗	✗	✗	✗	✗	✓	✗	✗
Self-servicing of apps	✓	✓	✓	✗	✗	✓	✓	✓

Capabilities by enrollment method

CAPABILITIES	AZURE AD JOINED	AZURE AD JOINED WITH AUTOPILOT (USER DRIVEN MODE)	AZURE AD JOINED WITH AUTOPILOT (SELF DEPLOYING MODE)	BULK	DEM	BYOD	GPO	CO-MANAGEMENT
Conditional Access	✓	✓	✓	✓**	✓**	✓	✓	✓

CAPABILITIES	AZURE AD JOINED	AZURE AD JOINED WITH AUTOPILOT (USER DRIVEN MODE)	AZURE AD JOINED WITH AUTOPILOT (SELF DEPLOYING MODE)	BULK	DEM	BYOD	GPO	CO-MANAGEMENT
User gets associated with the device	✓	✓	✗	✗	✗	✓	✓	✓
Requires Azure AD Premium	✗	✓	✓	✓	✗	✗	✓	✓
Device can assess resources protected by CA	✓	✓	✓	✓	✗	✓	✓	✓
Users must not be admins on their devices	✗	✓	✓	✓	✗	✗	✗	✗
Ability to configure the device setup experience	✗	✓	✓	✗	✗	✗	✗	✗
Ability to enroll devices without user interaction	✗	✗	✓	✓	✓	✗	✓	✓
Ability to run PowerShell scripts	✓	✓	✓	✓	✓	✗	✓	✓*

CAPABILITIES	AZURE AD JOINED	AZURE AD JOINED WITH AUTOPILOT (USER DRIVEN MODE)	AZURE AD JOINED WITH AUTOPILOT (SELF DEPLOYING MODE)	BULK	DEM	BYOD	GPO	CO-MANAGEMENT
Supports automatic enrollment after AD domain join	✗	✗	✗	✗	✗	✗	✓	✓
Supports automatic enrollment after Hybrid Azure AD join	✗	✗	✗	✗	✗	✗	✓	✓
Supports automatic enrollment after Azure AD join	✓	✓	✓	✓	✓	✓	✗	✗

* Client apps workloads in Configuration Manager must be moved to Intune Pilot or Intune.

** Devices are blocked for Conditional Access with the exception of Windows 10 (version 1803 and later) and Windows 11.

Next steps

Set up enrollment for Windows

Set up enrollment for Windows devices

9/23/2022 • 7 minutes to read • Edit Online

Applies to

- Windows 10
- Windows 11

This article helps IT administrators simplify Windows enrollment for their users. Once you've set up Intune, users enroll Windows devices by signing in with their work or school account.

As an Intune admin, you can simplify enrollment in the following ways:

- Enable automatic enrollment (Azure AD Premium required).
- CNAME registration.
- Enable bulk enrollment (Azure AD Premium and Windows Configuration Designer required).

Two factors determine how you can simplify Windows device enrollment:

- **Do you use Azure Active Directory Premium?** Azure AD Premium is included with Enterprise Mobility + Security and other licensing plans.
- **What versions of Windows clients will users enroll?** Devices running Windows 11 or Windows 10 can automatically enroll by adding a work or school account. Devices running earlier versions must enroll using the Company Portal app.

	AZURE AD PREMIUM	OTHER AD
Windows 10/11	Automatic enrollment	User enrollment
Earlier Windows versions	User enrollment	User enrollment

Organizations that can use automatic enrollment can also configure bulk enroll devices by using the Windows Configuration Designer app.

Device enrollment prerequisites

Before an administrator can enroll devices to Intune for management, licenses should have already been assigned to the administrator's account. Read about assigning licenses for device enrollment.

You can also let unlicensed admins sign in to MEM. For more information, see Unlicensed admins.

Multi-user support

Intune supports multiple users on devices that both:

- Run Windows 11 or the Windows 10 Creator's update
- Are Azure Active Directory domain-joined

When standard users sign in with their Azure AD credentials, they receive apps and policies assigned to their user name. Only the device's Primary user can use the Company Portal for self-service scenarios like installing apps and device actions (like Remove or Reset). For shared Windows 10/11 devices that don't have a primary user assigned, the Company Portal can still be used to install Available apps.

Enable Windows automatic enrollment

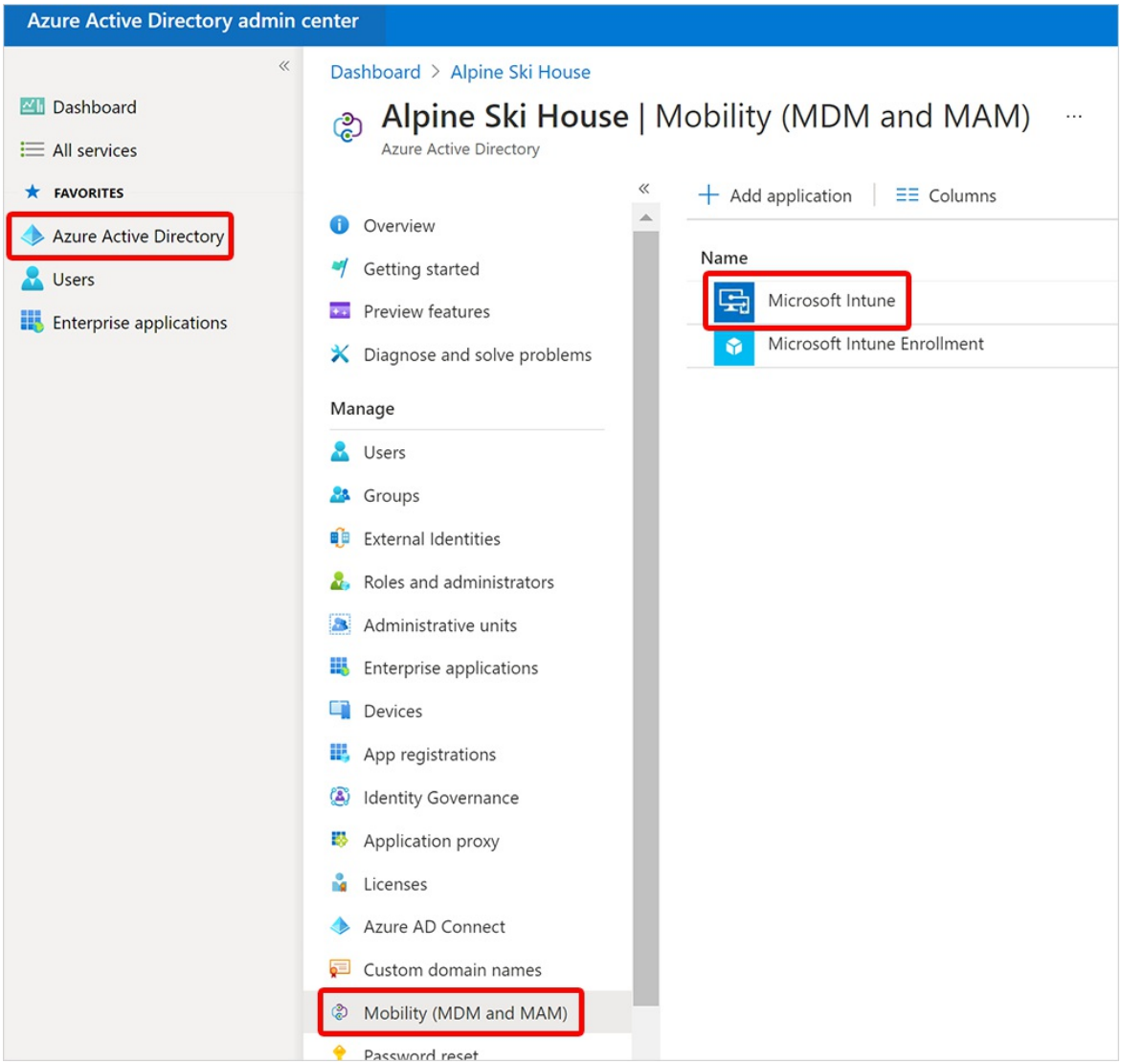
Automatic enrollment lets users enroll their Windows devices in Intune. To enroll, users add their work account to their personally owned devices or join corporate-owned devices to Azure Active Directory. In the background, the device registers and joins Azure Active Directory. Once registered, the device is managed with Intune.

Prerequisites

- Azure Active Directory Premium subscription (trial subscription)
- Microsoft Intune subscription
- Global Administrator permissions

Configure automatic MDM enrollment

1. Sign in to the Azure portal, and select **Azure Active Directory** > **Mobility (MDM and MAM)** > **Microsoft Intune**.



2. Configure **MDM User scope**. Specify which users' devices should be managed by Microsoft Intune. These Windows 10 devices can automatically enroll for management with Microsoft Intune.

   - **None** - MDM automatic enrollment disabled
   - **Some** - Select the **Groups** that can automatically enroll their Windows 10 devices
   - **All** - All users can automatically enroll their Windows 10 devices

IMPORTANT

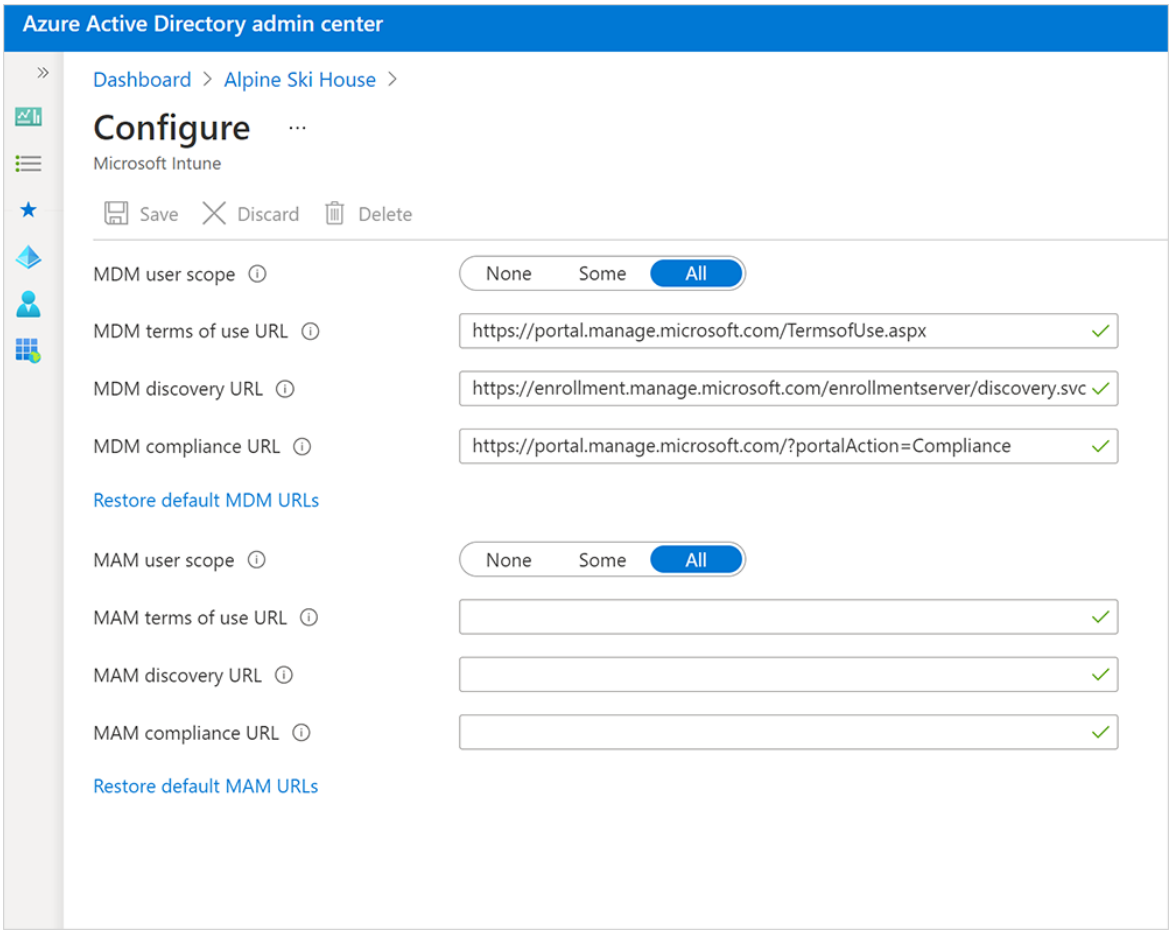
For Windows BYOD devices, the MAM user scope takes precedence if both the MAM user scope and the MDM user scope (automatic MDM enrollment) are enabled for all users (or the same groups of users). The device will not be MDM enrolled, and Windows Information Protection (WIP) Policies will be applied if you have configured them.

If your intent is to enable automatic enrollment for Windows BYOD devices to an MDM: configure the MDM user scope to **All** (or **Some**, and specify a group) and configure the MAM user scope to **None** (or **Some**, and specify a group – ensuring that users are not members of a group targeted by both MDM and MAM user scopes).

For corporate devices, the MDM user scope takes precedence if both MDM and MAM user scopes are enabled. The device will get automatically enrolled in the configured MDM.

NOTE

MDM user scope must be set to an Azure AD group that contains user objects.



3. Use the default values for the following URLs:

   - **MDM Terms of use URL**
   - **MDM Discovery URL**
   - **MDM Compliance URL**

4. Select **Save**.

By default, two-factor authentication is not enabled for the service. However, two-factor authentication is recommended when registering a device. To enable two-factor authentication, configure a two-factor authentication provider in Azure AD and configure your user accounts for multi-factor authentication. For more

information, see Getting started with the Azure Active Directory Multi-Factor Authentication Server.

Simplify Windows enrollment without Azure AD Premium

To simplify enrollment, create a domain name server (DNS) alias (CNAME record type) that redirects enrollment requests to Intune servers. Otherwise, users trying to connect to Intune must enter the Intune server name during enrollment.

Step 1: Create CNAME (optional)

Create CNAME DNS resource records for your company's domain. For example, if your company's website is contoso.com, you would create a CNAME in DNS that redirects EnterpriseEnrollment.contoso.com to enterpriseenrollment-s.manage.microsoft.com.

Although creating CNAME DNS entries is optional, CNAME records make enrollment easier for users. If no enrollment CNAME record is found, users are prompted to manually enter the MDM server name, enrollment.manage.microsoft.com.

TYPE	HOST NAME	POINTS TO	TTL
CNAME	EnterpriseEnrollment.company_domain.com	EnterpriseEnrollment-s.manage.microsoft.com	1 hour
CNAME	EnterpriseRegistration.company_domain.com	EnterpriseRegistration.windows.net	1 hour

If the company uses more than one UPN suffix, you need to create one CNAME for each domain name and point each one to EnterpriseEnrollment-s.manage.microsoft.com. For example, users at Contoso use the following formats as their email/UPN:

- name@contoso.com
- name@us.contoso.com
- name@eu.contoso.com

The Contoso DNS admin should create the following CNAMEs:

TYPE	HOST NAME	POINTS TO	TTL
CNAME	EnterpriseEnrollment.contoso.com	EnterpriseEnrollment-s.manage.microsoft.com	1 hour
CNAME	EnterpriseEnrollment.us.contoso.com	EnterpriseEnrollment-s.manage.microsoft.com	1 hour
CNAME	EnterpriseEnrollment.eu.contoso.com	EnterpriseEnrollment-s.manage.microsoft.com	1 hour

`EnterpriseEnrollment-s.manage.microsoft.com` – Supports a redirect to the Intune service with domain recognition from the email's domain name

Changes to DNS records might take up to 72 hours to propagate. You can't verify the DNS change in Intune until the DNS record propagates.

Step 2: Verify CNAME (optional)

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **Windows** > **Windows enrollment** > **CNAME Validation**.
2. In the **Domain** box, enter the company website and then choose **Test**.

Additional endpoints that aren't supported

EnterpriseEnrollment-s.manage.microsoft.com is the preferred FQDN for enrollment. There are two other endpoints that have been used previously and still work. However, they're no longer supported. EnterpriseEnrollment.manage.microsoft.com (without the -s) and manage.microsoft.com both work as the target for the auto-discovery server, but the user will have to touch OK on a confirmation message. If you point to EnterpriseEnrollment-s.manage.microsoft.com, the user won't have to do another confirmation step, so this is the recommended configuration

Alternate methods of redirection aren't supported

Using a method other than the CNAME configuration isn't supported. For example, using a proxy server to redirect enterpriseenrollment.contoso.com/EnrollmentServer/Discovery.svc to either enterpriseenrollment-s.manage.microsoft.com/EnrollmentServer/Discovery.svc or manage.microsoft.com/EnrollmentServer/Discovery.svc isn't supported.

Tell users how to enroll Windows devices

The Microsoft Intune user-help docs provide conceptual information, tutorials, and how-to guides for employees and students setting up their devices. You can point people directly to them or use these articles as guidance when developing and updating your org's own device management docs.

These articles describe how to enroll devices running Windows:

- Enroll Windows 10/11 device
- Enroll Windows 8.1 or Windows RT 8.1 device

For information about how enrollment affects the device and the information on it, see What information can my organization see when I enroll my device?

> **NOTE**
> End users must access the Company Portal website through Microsoft Edge to view Windows apps that you've assigned for specific versions of Windows. Other browsers, including Google Chrome, Mozilla Firefox, and Internet Explorer do not support this type of filtering.

> **IMPORTANT**
> If you do not have Auto-MDM enrollment enabled, but you have Windows 10/11 devices that have been joined to Azure AD, two records will be visible in the Intune console after enrollment. You can stop this by making sure that users with Azure AD joined devices go to **Accounts** > **Access work or school** and **Connect** using the same account.

Registration and Enrollment CNAMEs

Azure Active Directory has a different CNAME that it uses for device registration for iOS/iPadOS, Android, and Windows devices. Intune conditional access requires devices to be registered, also called "workplace joined". If you plan to use conditional access, you should also configure the EnterpriseRegistration CNAME for each company name you have.

TYPE	HOST NAME	POINTS TO	TTL
CNAME	EnterpriseRegistration.company_domain.com	EnterpriseRegistration.windows.net	1 hour

For more information about device registration, see Manage device identities using the Azure portal

Windows auto enrollment and device registration

This section applies to US government cloud customers on devices running Windows 10 or Windows 11.

Although creating CNAME DNS entries is optional, CNAME records make enrollment easier for users. If no enrollment CNAME record is found, users are prompted to manually enter the MDM server name, enrollment.manage.microsoft.us.

TYPE	HOST NAME	POINTS TO	TTL
CNAME	EnterpriseEnrollment.company_domain.com	EnterpriseEnrollment-s.manage.microsoft.us	1 hour
CNAME	EnterpriseRegistration.company_domain.com	EnterpriseRegistration.windows.net	1 hour

Next steps

- Considerations when managing Windows devices using Intune on Azure.

Bulk enrollment for Windows devices

9/23/2022 • 4 minutes to read • Edit Online

Applies to

- Windows 10
- Windows 11

As an administrator, you can join large numbers of new Windows devices to Azure Active Directory and Intune. To bulk enroll devices for your Azure AD tenant, you create a provisioning package with the Windows Configuration Designer (WCD) app. Applying the provisioning package to corporate-owned devices joins the devices to your Azure AD tenant and enrolls them for Intune management. Once the package is applied, it's ready for your Azure AD users to sign in.

> **NOTE**
>
> In the past, any standard user in the tenant could retrieve a bulk enrollment token and create a provisioning package. To increase security, users must now have a specific Azure AD role assignment to create a bulk enrollment token. You can assign roles in Intune for Education > **Tenant settings** or in the Microsoft Endpoint Manager admin center > **Tenant administration**. The roles are:
>
> - Global Administrator
> - Cloud Device Administrator
> - Intune Administrator
> - Password Administrator

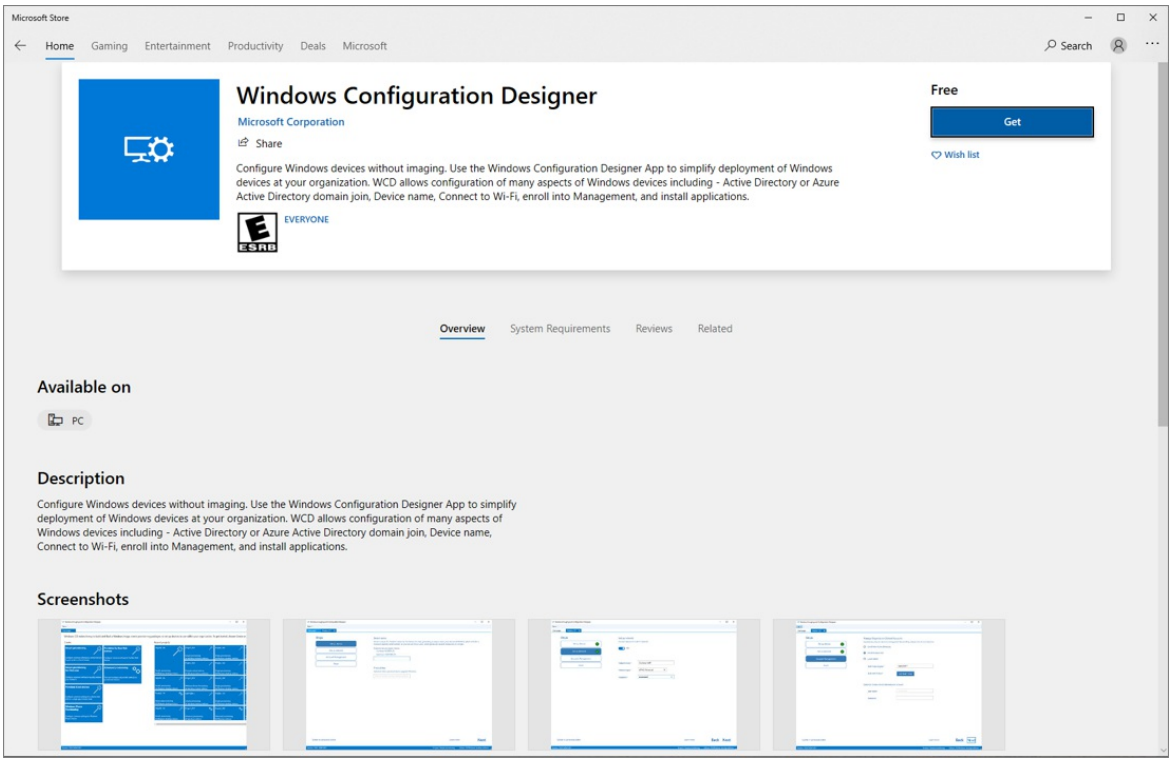
Azure AD users are standard users on these devices and receive assigned Intune policies and required apps. Windows devices that are enrolled into Intune using Windows bulk enrollment can use the Company Portal app to install available apps.

Prerequisites for Windows devices bulk enrollment

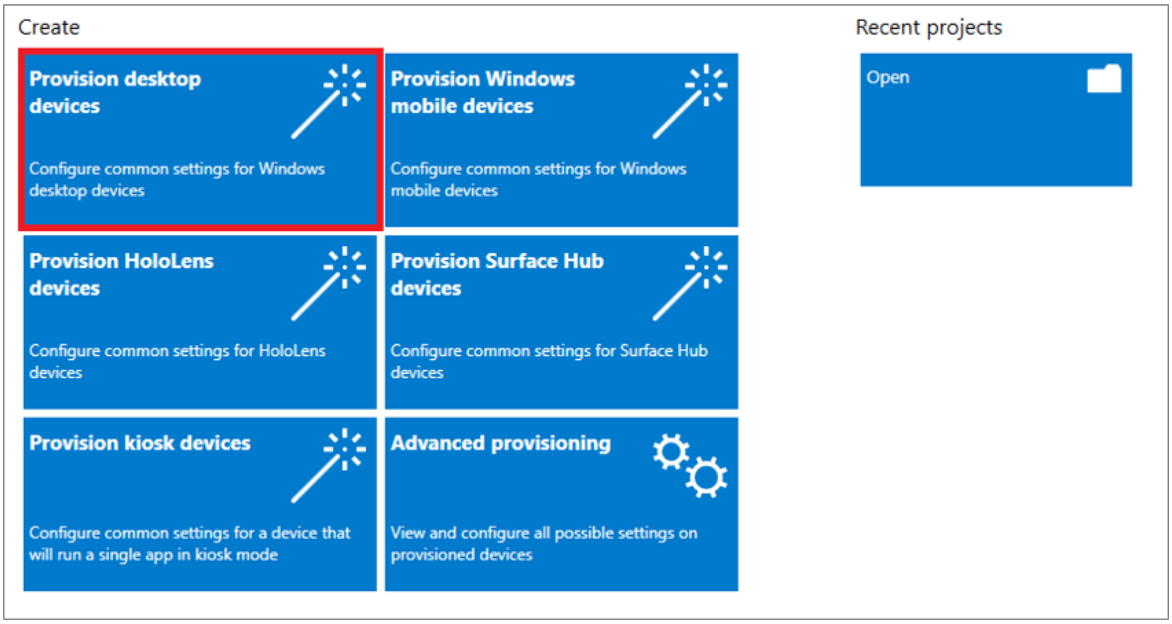
- Devices running Windows 11 or Windows 10 Creator update (build 1709) or later
- Windows automatic enrollment

Create a provisioning package

1. Download Windows Configuration Designer (WCD) from the Microsoft Store.

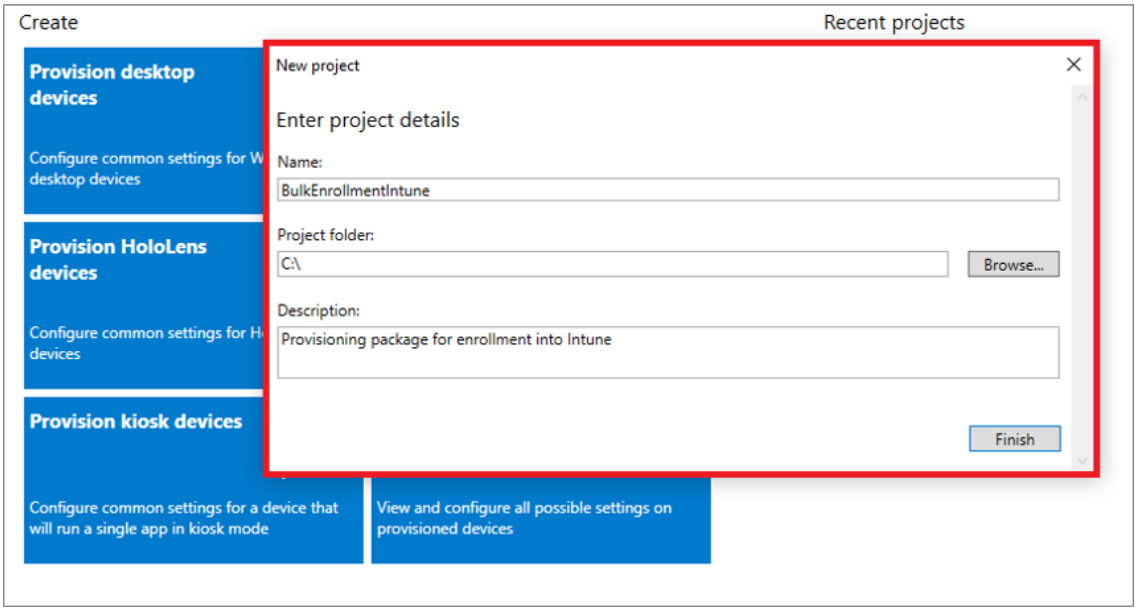


2. Open the **Windows Configuration Designer** app and select **Provision desktop devices**.

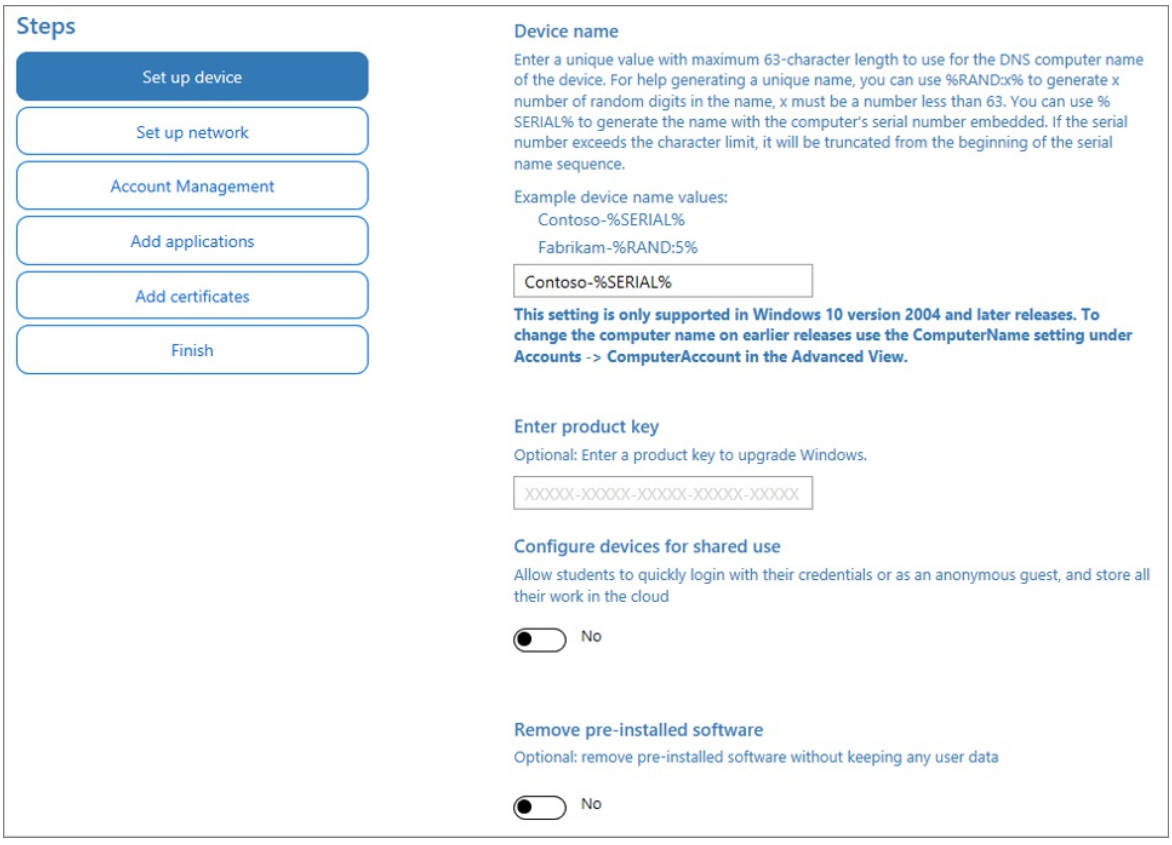


3. A **New project** window opens where you specify the following information:

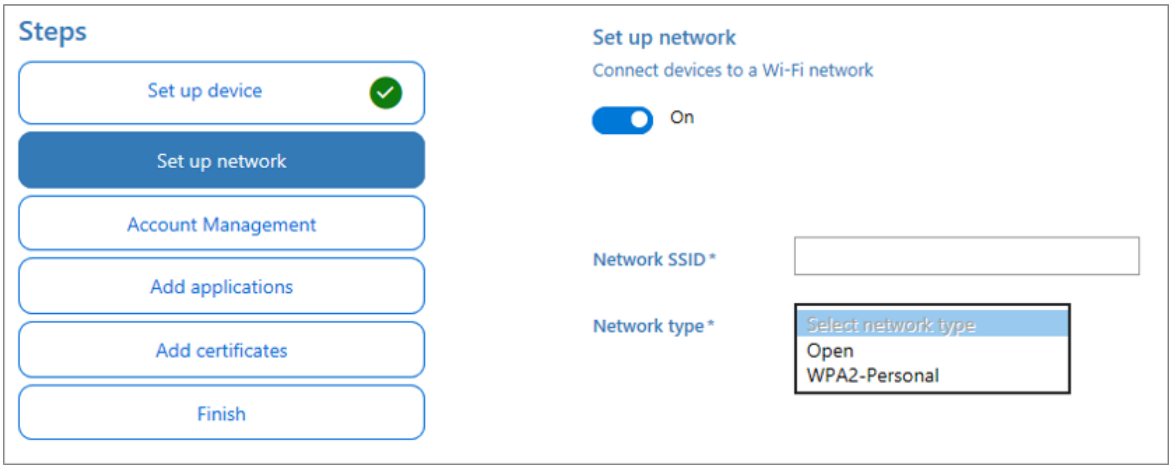
   - **Name** - A name for your project
   - **Project folder** - Save location for the project
   - **Description** - An optional description of the project



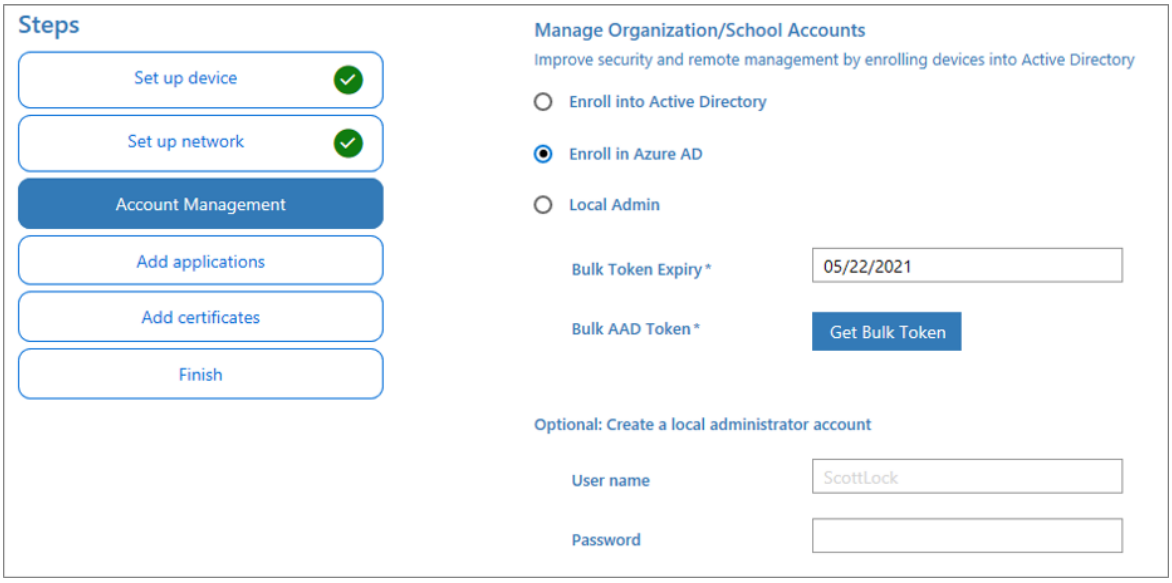
4. Enter a unique name for your devices. Names can include a serial number (%SERIAL%) or a random set of characters. Optionally, you can also enter a product key if you are upgrading the edition of Windows, configure the device for shared use, and remove pre-installed software.



5. Optionally, you can configure the Wi-Fi network devices connect to when they first start. If the network devices aren't configured, a wired network connection is required when the device is first started.

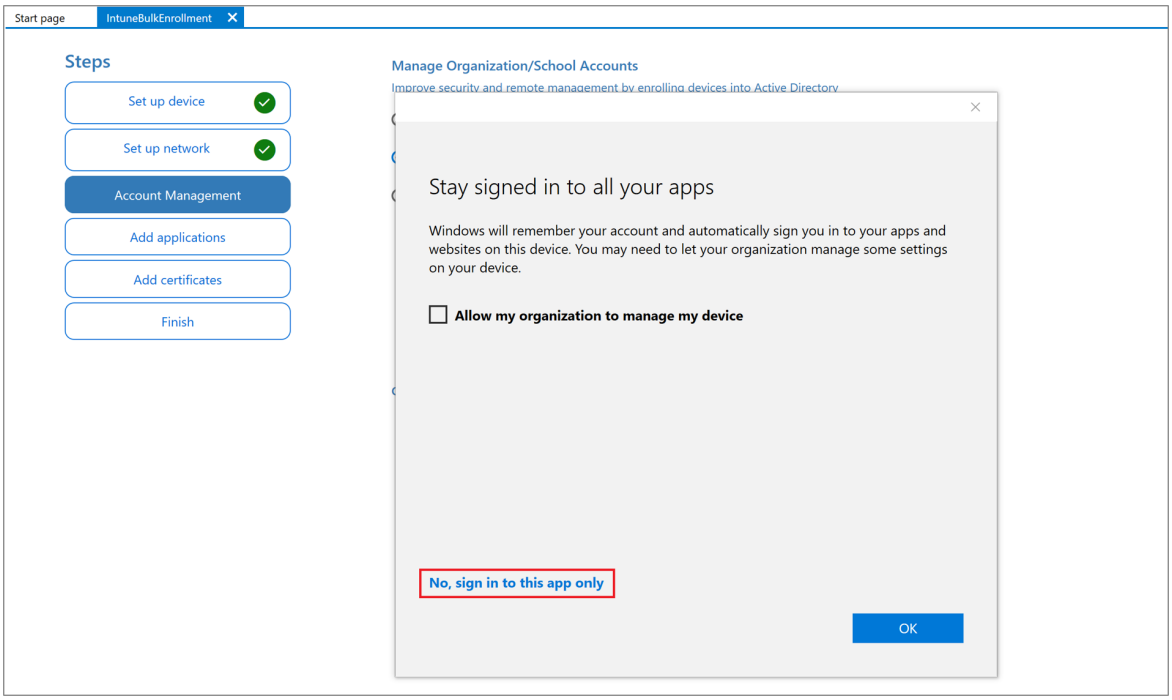


6. Select **Enroll in Azure AD**, enter a **Bulk Token Expiry** date, and then select **Get Bulk Token**. The token validity period is 180 days.

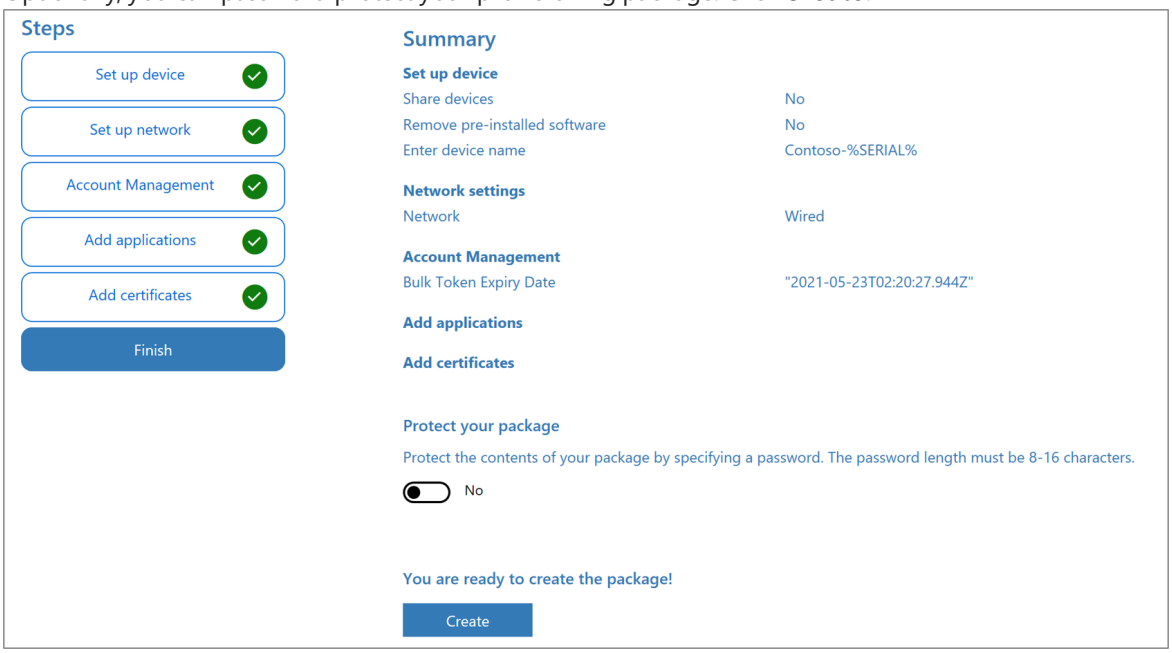


> **NOTE**
>
> Once a provisioning package is created, it can be revoked before its expiration by removing the associated package_{GUID} user account from Azure AD.

7. Provide your Azure AD credentials to get a bulk token.



8. In the **Stay signed in to all your apps** page, select **No, sign in to this app only**. If you keep the check box selected and press OK, the device you are using will become managed by your organization. If you do not intend for your device to be managed, make sure to select **No, sign in to this app only**.
9. Click **Next** when **Bulk Token** is fetched successfully.
10. Optionally, you can **Add applications** and **Add certificates**. These apps and certificates are provisioned on the device.
11. Optionally, you can password protect your provisioning package. Click **Create**.



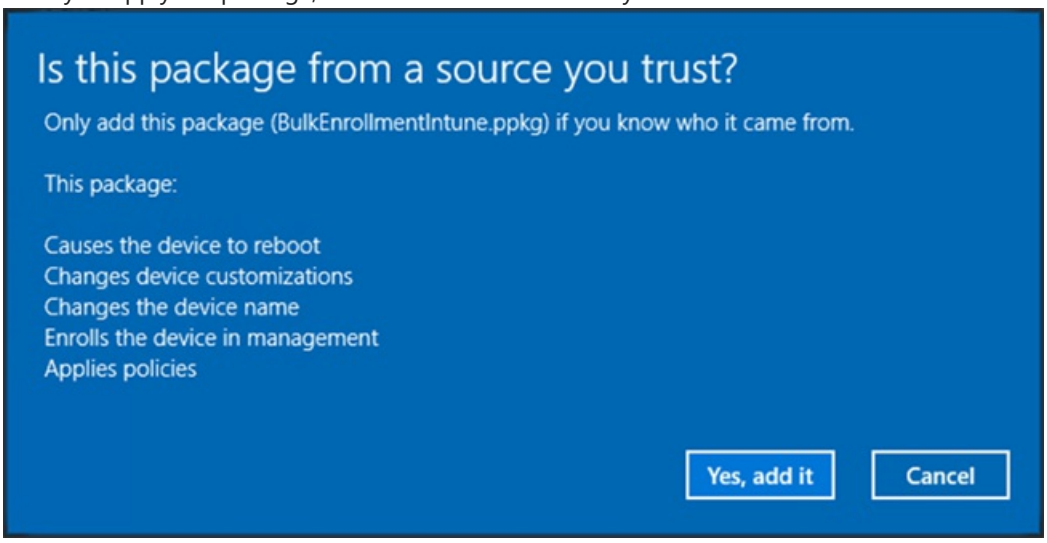
Provision devices

1. Access the provisioning package in the location specified in **Project folder** specified in the app.
2. Choose how you're going to apply the provisioning package to the device. A provisioning package can be applied to a device one of the following ways:
   - Place the provisioning package on a USB drive, insert the USB drive into the device you'd like to bulk enroll, and apply it during initial setup

- Place the provisioning package on a network folder, and apply it after initial setup

For step-by-step instruction on applying a provisioning package, see Apply a provisioning package.

3. After you apply the package, the device will automatically restart in one minute.



4. When the device restarts, it connects to the Azure Active Directory and enrolls in Microsoft Intune.

Troubleshooting Windows bulk enrollment

Provisioning issues

Provisioning is intended to be used on new Windows devices. Provisioning failures might require a wipe of the device or device recovery from a boot image. These examples describe some reasons for provisioning failures:

- A provisioning package that attempts to join an Active Directory domain or Azure Active Directory tenant that does not create a local account could make the device unreachable if the domain-join process fails due to lack of network connectivity.
- Scripts run by the provisioning package are run in system context. The scripts are able to make arbitrary changes to the device file system and configurations. A malicious or bad script could put the device in a state that can only be recovered by reimaging or wiping the device.

You can check for success/failure of the settings in your package in the **Provisioning-Diagnostics-Provider** Admin log in Event Viewer.

> **NOTE**
> Bulk enrollment is considered a userless enrollment method, and because of it, only the "Default" enrollment restriction in Intune would apply during enrollment. Make sure Windows platform is allowed in the default restriction, otherwise, the enrollment will fail. To check the capabilities alongside other Windows enrollment methods, see Intune enrollment method capabilities for Windows devices.

Bulk enrollment with Wi-Fi

When not using an open network, you must use device-level certificates to initiate connections. Bulk enrolled devices are unable to use to user-targeted certificates for network access.

Conditional access

Conditional access is available for devices enrolled via bulk enrollment running Windows 11 or Windows 10, version 1803 and later.

Set up the Enrollment Status Page

9/23/2022 • 13 minutes to read • Edit Online

Applies to

- Windows 10
- Windows 11

The enrollment status page (ESP) displays the provisioning status to people enrolling Windows devices and signing in for the first time. You can configure the ESP to block device use until all required policies and applications are installed. Device users can look at the ESP to track how far along their device is in the setup process.

The ESP can be deployed during the default out-of-box experience (OOBE) for Azure Active Directory (Azure AD) Join, and any Windows Autopilot provisioning scenario.

To deploy the ESP to devices, you have to create an ESP profile in Microsoft Intune. Within the profile, you can configure the ESP settings that control:

- Visibility of installation progress indicators
- Device access during provisioning
- Time limits
- Allowed troubleshooting operations

This article describes the information that the enrollment status page tracks and how to create an ESP profile.

Windows CSP

ESP uses the EnrollmentStatusTracking configuration service provider (CSP) and FirstSyncStatus CSP to track app installation.

Create new profile

1. Select **Windows** > **Windows enrollment** > **Enrollment Status Page**.
2. Select **Create**.
3. In **Basics**, enter the following properties:
   - **Name**: Name your profile so you can easily identify it later.
   - **Description**: Enter a description for the profile. This setting is optional, but recommended.
4. Select **Next**.
5. In **Settings**, configure the following settings:
   - **Show app and profile configuration progress**: Your options:
     - **No**: The enrollment status page doesn't appear during device setup. Select this option if you don't want to show the ESP to users.
     - **Yes**: The enrollment status page appears during device setup.
   - **Show an error when installation takes longer than specified number of minutes**: The default time-out is 60 minutes. Enter a higher value if you think more time is needed to install apps on your devices.

- **Show custom message when time limit or error occur**: Include a message that tells people what happened and who to contact for help. Your options:
  - **No**: The default message is shown to users when an error occurs. That message is: "Setup could not be completed. Please try again or contact your support person for help."
  - **Yes**: Your custom message is shown to users when an error occurs. Enter your message in the provided text box.
- **Turn on log collection and diagnostics page for end users**: The user's logs and diagnostics could aid with troubleshooting, so we recommend turning this on. Your options:
  - **No**: The collect logs button isn't shown to users when an installation error occurs. The Windows Autopilot diagnostics page isn't shown on devices running Windows 11.
  - **Yes**: The collect logs button is shown to users when an installation error occurs. The Windows Autopilot diagnostics page is shown on devices running Windows 11.
- **Only show page to devices provisioned by out-of-box experience (OOBE)**: Your options:
  - **No**: The enrollment status page is shown on all Intune-managed and co-managed devices that go through the out-of-box experience (OOBE), and to the first user that signs in to each device. So subsequent users who sign in don't see the ESP.
  - **Yes**: The enrollment status page is only shown on devices that go through the out-of-box experience (OOBE).

    > **TIP**
    > If you only want the ESP to appear on Autopilot devices during initial device setup, select the **No** option. Then create a new ESP profile, choose the **Yes** option, and target the profile to an Autopilot device group.

- **Block device use until all apps and profiles are installed**: Your options:
  - **No**: Users can leave the ESP before Intune is finished setting up the device.
  - **Yes**: Users can't leave the ESP until Intune is done setting up the device. This option unlocks additional settings for this scenario.
- **Allow users to reset device if installation error occurs**: Your options:
  - **No**: The ESP doesn't give users the option to reset theirs devices when an installation fails.
  - **Yes**: The ESP gives users the option to reset their devices when an installation fails.
- **Allow users to use device if installation error occurs**: Your options:
  - **No**: The ESP doesn't give users the option to bypass the ESP when an installation fails.
  - **Yes**: The ESP gives users the option to bypass the ESP and use their devices when an installation fails.
- **Block device use until these required apps are installed if they are assigned to the user/device**: Your options:
  - **All**: All assigned apps must be installed before users can use their devices.
  - **Selected**: Select-apps must be installed before users can use their devices. Choose this option to select from your managed apps.

6. Select **Next**.
7. In **Assignments**, select the groups that will receive your profile. Optionally, select **Edit filter** to restrict the assignment further.

> **NOTE**
> Due to OS restrictions, a limited selection of filters are available for ESP assignments. The picker only shows filters that have rules defined for `osVersion`, `operatingSystemSKU`, and `enrollmentProfileName` properties. Filters that contain other properties aren't available.

8. Select **Next**.
9. Optionally, in **Scope tags**, assign a tag to limit profile management to specific IT groups, such as `US-NC IT Team` or `JohnGlenn_ITDepartment`. Then select **Next**.

> **NOTE**
> Scope tags limit who can see and reprioritize ESP profiles in the admin center. A scoped user can tell the relative priority of their profile even if they can't see all of the other profiles in Intune. For more information about scope tags, see Use role-based access control and scope tags for distributed IT.

10. In **Review + create**, review your settings. After you select **Create**, your changes are saved, and the profile is assigned. Once deployed, the profile will be applied the next time the devices check in. You can access the profile from your profiles list.

Edit default profile

Intune applies the default profile to all users and all devices when no other ESP profiles are available to assign. You can configure the default profile to show or hide the ESP.

1. Sign in to the Microsoft Endpoint Manager admin center and select **Devices**.
2. Select **Windows** > **Windows enrollment** > **Enrollment Status Page**.
3. Select the **Default** profile in the table.
4. Select **Properties**.
5. Go to the **Settings** section and select **Edit**.
6. Configure **Show app and profile installation progress** to set the behavior of the default profile. Your options:
   - **No**: The ESP isn't visible to users during initial device setup and sign-in.
   - **Yes**: The ESP is visible to users during initial device setup and sign-in.

   If you select **Yes**, more settings become available for you to configure.
7. Select **Review + save**.
8. Review the summary of changes and then select **Save**.

Prioritize profiles

If you assign a user or device more than one ESP profile, the profile with the highest priority takes precedence over the other profiles. The profile set to 1 has the highest priority.

Intune applies profiles in the following order:

1. Intune applies the highest-priority profile assigned to the device.
2. If no profiles are targeted at the device, Intune applies the highest-priority profile assigned to the user. This only works in scenarios where there is a user. In white glove and self-deploying scenarios, only profiles

targeted at devices can be applied.
3. If no profiles are assigned to the device or user, Intune applies the default ESP profile.

To prioritize your profiles:

1. Hover over the profile in the list with your cursor until you see three vertical dots.
2. Drag the profile to the desired position in the list.

Block access to a device until a specific application is installed

Specify the apps that must be installed before the user can exit the ESP. You can choose up to 100 apps.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **Windows** > **Windows enrollment** > **Enrollment Status Page**.
2. Choose a profile > **Settings**.
3. Choose **Yes** for **Show app and profile installation progress**.
4. Choose **Yes** for **Block device use until all apps and profiles are installed**.
5. Choose **Selected** for **Block device use until these required apps are installed if they're assigned to the user/device**.
6. Choose **Select apps** > choose the apps > **Select** > **Save**.

The apps that are included in this list are used by Intune to filter the list that should be considered blocking. It doesn't specify what apps should be installed. For example, if you configure this list to include "App 1," "App 2," and "App 3" and "App 3" and "App 4" are targeted to the device or user, the ESP will track only "App 3." "App 4" will still be installed, but the ESP will not wait for it to complete.

ESP tracking

The enrollment status page tracks these phases of provisioning:

- Device preparation
- Device setup
- Account setup

This section describes the types of information, apps, and policies tracked during each phase.

Device preparation

During device preparation, the enrollment status page tracks these tasks for the device user:

- Secure your hardware
- Join your organization's network
- Register your device for mobile management

Secure your hardware

This task ensures that the device completes the Trusted Platform Module (TPM) key attestation and validates its identity with Azure AD. Azure AD sends a token to the device, which is used during Azure AD join.

This step is required for self-deploying mode and white glove deployment. It isn't needed for Windows Autopilot scenarios in user-driven mode.

Join your organization's network

The device uses the token received in the previous step to join Azure AD. This step is required in self-deploying mode and white glove deployment. Devices in user-driven mode have already completed this task by time they open the ESP.

Register your device for mobile management

The device enrolls in Microsoft Intune for mobile device management (MDM).

This step is required in self-deploying mode and white glove deployment. Devices in user-driven mode have already completed this step by time they open the ESP.

After enrollment, the device calculates the policies and apps required to track in the next phase. For Windows 10, version 1903 and later versions, the device also creates the tracking policy for the SideCar agent, and installs the Intune Management Extension that's used to install Win32 apps.

Device setup

The enrollment status page tracks these items during the device setup phase:

- Security policies
- Certificate profiles
- Network connection
- Apps

Security policies

ESP doesn't track security policies, such as device restrictions, but these policies are installed in the background. The ESP does track Microsoft Edge, Assigned Access, and Kiosk Browser policies.

> **TIP**
> When complete, the status for security policies appears on the ESP as **(1 of 1) completed**.

Certificates

The ESP tracks the installation of SCEP certificate profiles targeted at devices.

Network connections

The ESP tracks VPN and Wi-Fi profiles targeted at devices.

Apps

The ESP tracks the installation of apps deployed in a device context, and includes:

- Per machine line-of-business (LoB) MSI apps
- LoB store apps where installation context = device
- Offline store apps where installation context = device
- Win32 applications for Windows 10, version 1903 and later, and Windows 11.

> **NOTE**
> It's preferable to deploy the offline-licensed Microsoft Store for Business apps. Don't mix LOB and Win32 apps. Both LOB (MSI) and Win32 installers use TrustedInstaller, which doesn't allow simultaneous installations. If the OMA DM agent starts an MSI installation, the Intune Management Extension plugin starts a Win32 app installation by using the same TrustedInstaller. In this situation, Win32 app installation fails and returns an **Another installation is in progress, please try again later** error message. In this situation, ESP fails. Therefore, don't mix LOB and Win32 apps in any type of Autopilot enrollment.

Account setup

During the account setup phase, the ESP tracks apps and policies targeted at users, including:

- Security policies
- Certificates
- Network connections

- Apps

> **TIP**
> Before installation begins, the device creates a tracking policy and calculates all apps and policies that need to be tracked. While that's happening, the ESP shows subtasks in an **Identifying** state.

Security policies

ESP doesn't track security policies, such as device restrictions, but these policies are installed in the background. The ESP does track Microsoft Edge, Assigned Access, and Kiosk Browser policies.

Certificates

The ESP tracks the installation of SCEP certificate profiles assigned to users.

Network connections

The ESP tracks Wi-Fi profiles assigned to users.

Apps

During this phase, the ESP tracks the installation of apps assigned to the user. The ESP tracks Win32 apps for Windows 10, version 1903 and later.

It also tracks the following types of apps when they're assigned to all devices, all users, or a user group that includes the enrolling device user:

- Per user LoB MSI apps
- Per machine LoB MSI apps
- LoB store apps, online store apps, and offline store apps

Known issues

This section lists the known issues for the enrollment status page.

- When creating apps that will be deployed during ESP, any reboots that are packaged within the app may cause ESP to hang and fail the deployment. We recommend specifying the reboot behavior in Intune instead of triggering the reboot within the package.
- Disabling the ESP profile doesn't remove ESP policy from devices and users still get ESP when they log in to device for first time. The policy isn't removed when the ESP profile is disabled.
- A reboot during device setup forces the user to enter their credentials before the account setup phase. User credentials aren't preserved during reboot. Instruct the device users to enter their credentials to continue to the account setup phase.
- The ESP always times out on devices running Windows 10, version 1903 and earlier, and enrolled via the *Add work and school account* option. The ESP waits for Azure AD registration to complete. The issue is fixed on Windows 10 version 1903 and later.
- Hybrid Azure AD Autopilot deployment with ESP takes longer than the timeout duration entered in the ESP profile. On Hybrid Azure AD Autopilot deployments, the ESP takes 40 minutes longer than the value set in the ESP profile. For example, you set the timeout duration to 30 minutes in the profile. The ESP can take 30 minutes + 40 minutes. This delay gives the on-prem AD connector time to create the new device record to Azure AD.
- Windows logon page isn't pre-populated with the username in Autopilot User Driven Mode. If there's a reboot during the Device Setup phase of ESP:
  - the user credentials aren't preserved
  - the user must enter the credentials again before proceeding from Device Setup phase to the Account setup phase
- ESP is stuck for a long time or never completes the "Identifying" phase. Intune computes the ESP policies during the identifying phase. A device may never complete computing ESP policies if the current user doesn't

have an Intune licensed assigned.

- Configuring Microsoft Defender Application Control causes a prompt to reboot during Autopilot. Configuring Microsoft Defender Application (AppLocker CSP) requires a reboot. When this policy is configured, it may cause a device to reboot during Autopilot. Currently, there's no way to suppress or postpone the reboot.
- When the DeviceLock policy is enabled as part of an ESP profile, the OOBE or user desktop autologon could fail unexpectantly for two reasons.
  - If the device didn't reboot before exiting the ESP Device setup phase, the user may be prompted to enter their Azure AD credentials. This prompt occurs instead of a successful autologon where the user sees the Windows first login animation.
  - The autologon will fail if the device rebooted after the user entered their Azure AD credentials but before exiting the ESP Device setup phase. This failure occurs because the ESP Device setup phase never completed. The workaround is to reset the device.
- ESP doesn't apply to a Windows device that was enrolled with Group Policy (GPO).
- Scripts that run in user context ('Run this script using the logged on credentials' on the script properties is set to 'yes') may not execute during ESP. As a workaround, execute scripts in System context by changing this setting to 'no'.

Troubleshooting

For help with errors or messages related to the ESP, including how to disable an already-enabled ESP, see Troubleshoot the Windows Enrollment Status page.

Work with existing on-premises proxy servers

9/23/2022 • 2 minutes to read • Edit Online

This article explains how to configure the Intune Connector for Active Directory to work with outbound proxy servers. It's intended for customers with network environments that have existing proxies.

By default, the Intune Connector for Active Directory will attempt to automatically locate a proxy server on the network using Web Proxy Auto-Discovery (WPAD). If this has been configured on your network, other configuration may not be required. When changes are needed, the following sections describe how to override the default settings, using the standard .NET Framework capabilities for configuring proxy settings. More options are described in that documentation.

For more information about how connectors work, see Understand Azure AD Application Proxy connectors.

Completely bypass outbound proxies

You can configure the connector to bypass your on-premises proxy to ensure it uses direct connectivity to the Azure services. We recommend this approach, as long as your network policy allows for it, because it means that you have one less configuration to maintain.

To disable outbound proxy usage for the connector, edit the `:\Program Files\Microsoft Intune\ODJConnector\ODJConnectorUI\ODJConnectorUI.exe.config` file and set the default proxy to `"False"` as shown in the following code example:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <system.net>
        <defaultProxy>
            <defaultProxy enabled="False" />
        </defaultProxy>
    </system.net>
    <runtime>
        <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
            <dependentAssembly>
                <assemblyIdentity name="mscorlib" publicKeyToken="b77a5c561934e089" culture="neutral"/>
                <bindingRedirect oldVersion="0.0.0.0-2.0.0.0" newVersion="4.6.0.0" />
            </dependentAssembly>
        </assemblyBinding>
    </runtime>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6" />
    </startup>
    <appSettings>
        <add key="SignInURL" value="https://portal.manage.microsoft.com/Home/ClientLogon"/>
        <add key="LocationServiceEndpoint"
value="RestUserAuthLocationService/RestUserAuthLocationService/ServiceAddresses"/>
    </appSettings>
</configuration>
```

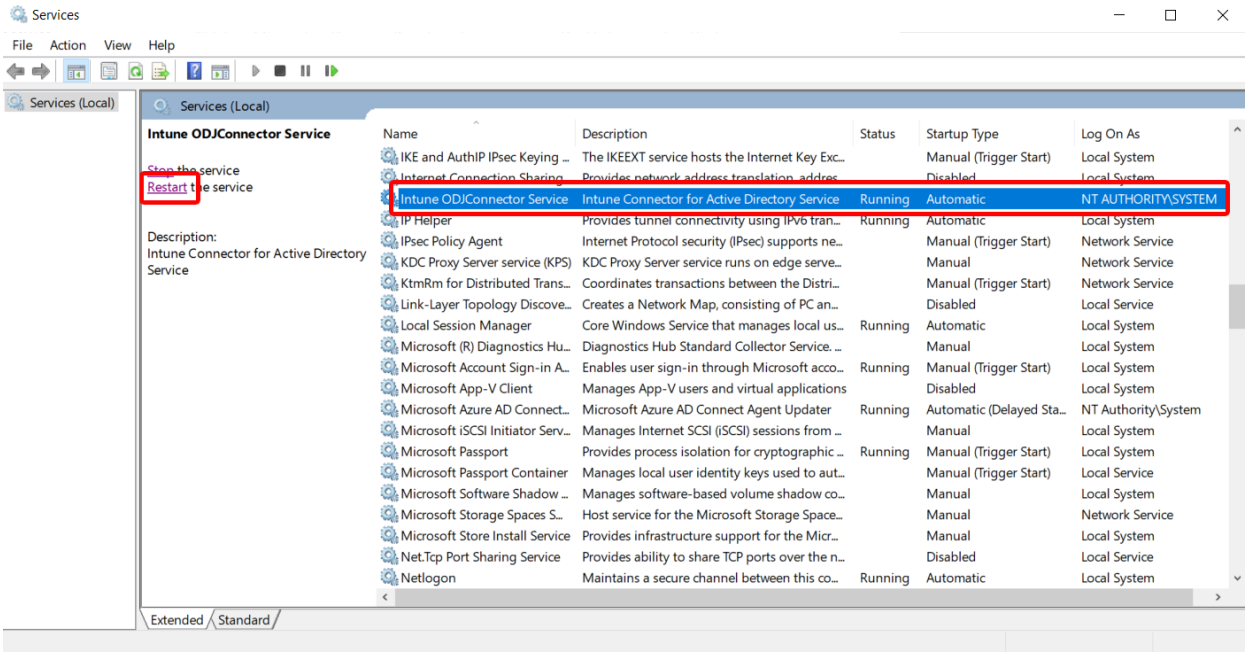
To ensure that the Connector Updater service also bypasses the proxy, make a similar change to C:\Program Files\Microsoft Intune\ODJConnector\ODJConnectorSvc\ODJConnectorSvc.exe.config.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <system.net>
        <defaultProxy>
            <defaultProxy enabled="False" />
        </defaultProxy>
    </system.net>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6" />
    </startup>
    <appSettings>
        <add key="BaseServiceAddress" value="https://manage.microsoft.com/" />
    </appSettings>
</configuration>
```

Be sure to make copies of the original files, in case you need to revert to the default .config files.

Once the configuration files have been modified, you'll need to restart the Intune Connector service.

1. Open **services.msc**.
2. Find and select the **Intune ODJConnector Service**.
3. Select **Restart**.



Specifying an alternative proxy server

If a different proxy server (for example, one that bypasses authentication) needs to be used with the Intune Connector for Active Directory, this can be specified in a similar manner. To use a different proxy, edit the `:\Program Files\Microsoft Intune\ODJConnector\ODJConnectorUI\ODJConnectorUI.exe.config` file and add the proxy address and proxy port in the section shown in this code sample:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <system.net>
        <defaultProxy>
            <proxy proxyaddress="<PROXY ADDRESS HERE>:<PORT HERE>" bypassonlocal="True"
usesystemdefault="True"/>
        </defaultProxy>
    </system.net>
    <runtime>
        <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
            <dependentAssembly>
                <assemblyIdentity name="mscorlib" publicKeyToken="b77a5c561934e089" culture="neutral"/>
                <bindingRedirect oldVersion="0.0.0.0-2.0.0.0" newVersion="4.6.0.0" />
            </dependentAssembly>
        </assemblyBinding>
    </runtime>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6" />
    </startup>
    <appSettings>
        <add key="SignInURL" value="https://portal.manage.microsoft.com/Home/ClientLogon"/>
        <add key="LocationServiceEndpoint"
value="RestUserAuthLocationService/RestUserAuthLocationService/ServiceAddresses"/>
    </appSettings>
</configuration>
```

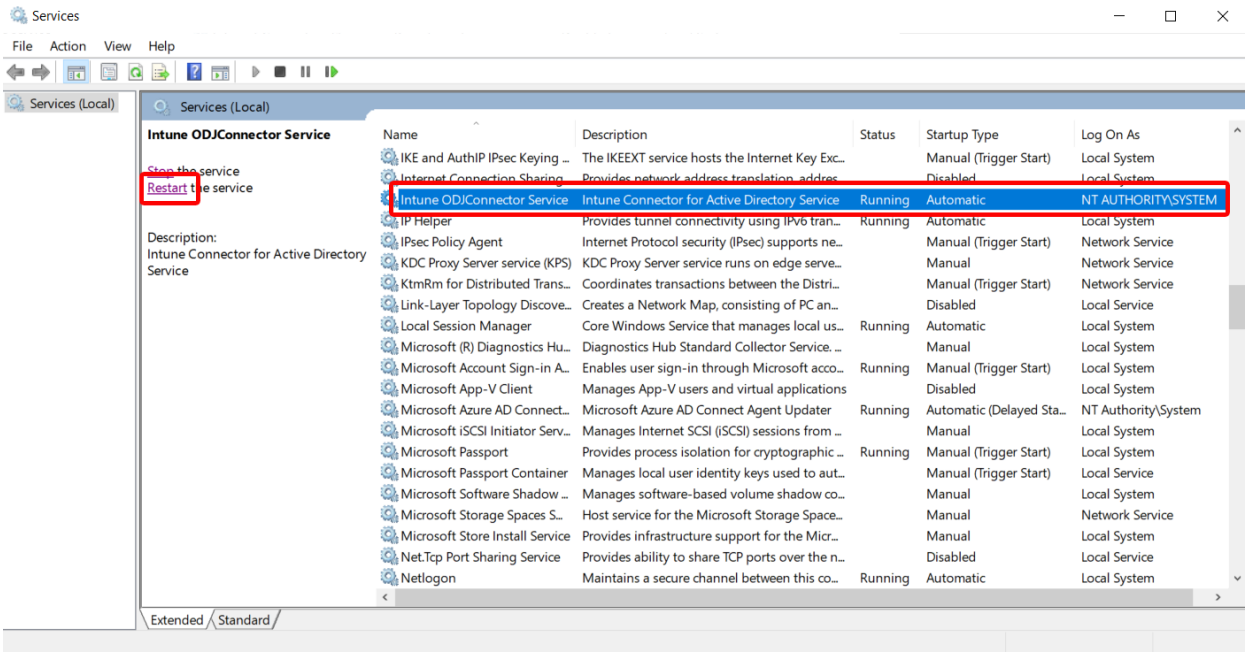
To ensure that the Connector Updater service also bypasses the proxy, make a similar change to C:\Program Files\Microsoft Intune\ODJConnector\ODJConnectorSvc\ODJConnectorSvc.exe.config.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <system.net>
        <defaultProxy>
            <proxy proxyaddress="<PROXY ADDRESS HERE>:<PORT HERE>" bypassonlocal="True"
usesystemdefault="True"/>
        </defaultProxy>
    </system.net>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6" />
    </startup>
    <appSettings>
        <add key="BaseServiceAddress" value="https://manage.microsoft.com/" />
    </appSettings>
</configuration>
```

Be sure to make copies of the original files, in case you need to revert to the default .config files.

Once the configuration files have been modified, you'll need to restart the Intune Connector service.

1. Open **services.msc**.
2. Find and select the **Intune ODJConnector Service**.
3. Select **Restart**.



Next steps

Manage your devices

Enroll Android devices

9/23/2022 • 2 minutes to read • Edit Online

As an Intune administrator, you can enroll Android devices in the following ways:

- Android Enterprise (offering a set of enrollment options that provide users with the most up-to-date and secure features):
  - **Android Enterprise personally owned with a work profile**: For personal devices granted permission to access corporate data. Admins can manage work accounts, apps, and data. Personal data on the device is kept separate from work data and admins don't control personal settings or data.
  - **Android Enterprise dedicated**: For corporate-owned, single use devices, such as digital signage, ticket printing, or inventory management. Admins lock down the usage of a device for a limited set of apps and web links. It also prevents users from adding other apps or taking other actions on the device.
  - **Android Enterprise fully managed**: For corporate-owned, single user devices used exclusively for work and not personal use. Admins can manage the entire device and enforce policy controls unavailable to personally owned/corporate-owned work profiles.
  - **Android Enterprise corporate-owned with a work profile**: For corporate-owned, single user devices intended for corporate and personal use.
- **Android device administrator**, including Samsung Knox Standard devices and Zebra devices. Device administrator should be used in areas where Android Enterprise or Google Mobile Services (GMS) is unavailable. Google has decreased support for device administrator (DA) management in areas where Android Enterprise is available, and encourages organizations to migrate to Android Enterprise device management. For a list of countries that support Android Enterprise, see Is Android Enterprise available in my country?
- Android (AOSP) offers a set of enrollment options for devices that aren't integrated with Google Mobile services.
  - Corporate-owned, user associated devices: For corporate-owned, single user devices intended exclusively for work and not personal use. Admins can manage the entire device.
  - Corporate-owned, userless devices: For corporate-owned, shared devices. Admins can manage the entire device.

> **TIP**
> For guidance on which enrollment method is right for your organization, see Deployment guide: Enroll Android devices in Microsoft Intune.

Prerequisites

To prepare to manage mobile devices, you must set the mobile device management (MDM) authority to **Microsoft Intune**. See Set the MDM authority for instructions. You set this item only once, when you're first setting up Intune for mobile device management.

For Android Enterprise, refer to the following support article from Google to ensure that Android Enterprise is available in your country or region: https://support.google.com/work/android/answer/6270910

For devices manufactured by Zebra Technologies, you may need to grant the Company Portal more permissions depending on the capabilities of the specific device. Mobility Extensions on Zebra devices has more details.

For Samsung Knox Standard devices, there are more prerequisites.

Next steps

- Set up Android Enterprise personally owned work profile enrollment
- Set up Android Enterprise dedicated device enrollment
- Set up Android Enterprise fully managed enrollment
- Set up Android device administrator enrollment
- Set up Android Enterprise corporate-owned work profile
- Set up Android (AOSP) corporate-owned user-associated enrollment
- Set up Android (AOSP) corporate-owned userless enrollment

Connect your Intune account to your Managed Google Play account

9/23/2022 • 3 minutes to read • Edit Online

To support the following Android enrollment types, you must connect your Intune tenant account to your Managed Google Play account:

- Android Enterprise personally-owned work profile
- Android Enterprise corporate-owned work profile
- Android Enterprise fully managed
- Android Enterprise dedicated devices

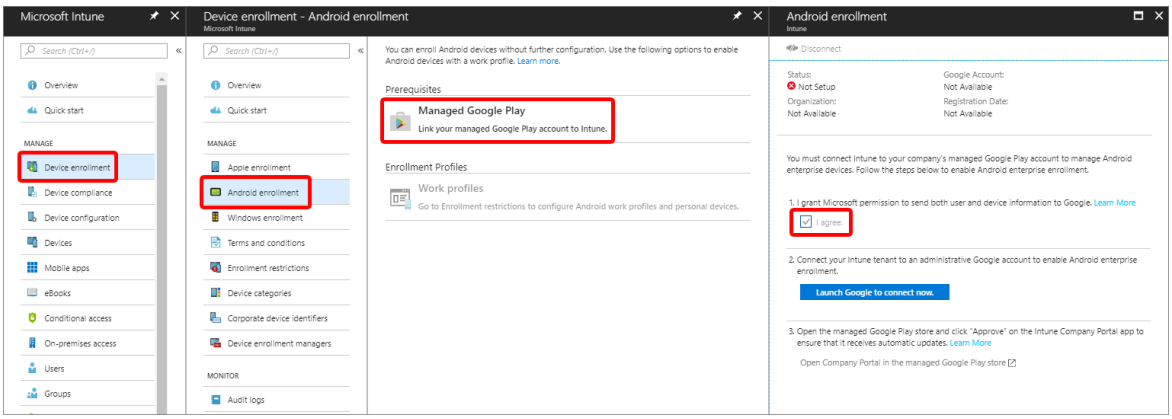
Refer to the following support article from Google to ensure that Android Enterprise is available in your country or region: https://support.google.com/work/android/answer/6270910

Intune makes it easier for you to configure and use Android Enterprise management. After connecting to Google Play, Intune automatically adds these four common Android Enterprise related apps to the Intune admin console:

- **Microsoft Intune** - Used for Android Enterprise fully managed, dedicated and corporate-owned work profile scenarios.
- **Microsoft Authenticator** - Helps you sign in to your accounts if you use two-factor verification, and is also used for Android Enterprise dedicated devices that enroll with Azure AD Shared device mode.
- **Intune Company Portal** - Used for Android Enterprise personally-owned work profile scenarios, as well as App Protection Policies (APP).
- **Managed Home Screen** - Used for multi-app kiosk mode on Android Enterprise dedicated devices. Learn more about Managed Home Screen.

> **NOTE**
> Due to interaction between Google and Microsoft domains, this step may require that you adjust your browser settings. Make sure that "portal.azure.com" and "play.google.com" are in the same security zone in your browser.

1. If you haven't already, set the mobile device management authority to **Microsoft Intune**.
2. Sign in to the Microsoft Endpoint Manager admin center, choose **Devices** > **Android** > **Android enrollment** > **Managed Google Play**. If you are using a custom Intune admin role, access to option this requires Organization Read and Update permissions.



3. Choose **I agree** to grant Microsoft permission to send user and device information to Google.
4. Choose **Launch Google to connect now** to open the Managed Google Play website. The website opens on a new tab in your browser.
5. On Google's sign-in page, enter the Google account that will be associated with all Android Enterprise management tasks for this tenant. This Google account is the one that your company's IT admins share to manage and publish apps in the Google Play console. You can use an existing Google account or create a new one. The account you choose must not be associated with a G-Suite domain.

> **IMPORTANT**
> Be sure to use or create an Enterprise account rather than a personal GMail account. Keep in mind that the account you use should be one that is easily shared or transferred in the case that the person setting up the Managed Google Play connection leaves the company or moves teams.

> **NOTE**
> If you are using the Microsoft Edge browser, click **Sign-In** in the upper right corner to sign-in to your Google account.

6. Provide your company's name for **Organization name**. For **Enterprise mobility management (EMM) provider**, **Microsoft Intune** should be displayed.
7. Agree to the Android agreement, and then choose **Confirm**. Your request will be processed.

> **NOTE**
> Choose a scope tag for your Managed Google Play apps. Under this section, you can select a scope tag that will apply to all newly-approved Managed Google Play apps. You must have the following permissions to interact with this section:
>
> - Android Sync - Read
> - Android Sync – UpdateOnBoarding
>
> Admins without these permissions will not be able to remove the scope tag selected on the pane. Tenant admins, or admins who are in charge of giving admin permissions to others, can update permissions in Microsoft Endpoint Manager admin center by selecting **Tenant Administration** > **Roles**.

> **IMPORTANT**
> Only link 1 Intune account to a managed Google Play account. Linking multiple accounts is unsupported and prevents basic functionality from working as expected.

Disconnect your Android Enterprise administrative account

You can turn off Android Enterprise enrollment and management by following these steps:

1. Retire all the following devices:
   - Android Enterprise personally-owned work profile devices
   - Android Enterprise corporate-owned work profile devices
   - Android Enterprise fully managed
   - Android Enterprise dedicated devices

2. As an Intune administrator, sign in to the Microsoft Endpoint Manager admin center.
3. Choose **Devices** > **Android** > **Android enrollment** > **Managed Google Play** > **Disconnect**.
4. Choose **Yes** to disconnect and unenroll all Android enterprise devices from Intune.

Next steps

After connecting to the Managed Google Play account, you can set up Android Enterprise:

- Personally-owned work profile devices.
- Corporate-owned work profile devices.
- Dedicated devices.
- Fully managed devices.

Set up enrollment of Android Enterprise personally-owned work profile devices

9/23/2022 • 2 minutes to read • Edit Online

Intune helps you deploy apps and settings to Android Enterprise personally-owned work profile devices to make sure work and personal information are separate. For specific details about Android Enterprise, see Android Enterprise requirements.

To set up Android Enterprise personally-owned work profile management, follow these steps:

1. Connect your Intune tenant account to your Android Enterprise account.
2. Specify Android Enterprise work profile enrollment settings. Android Enterprise personally-owned work profiles are supported on only certain Android devices. Any device that supports Android Enterprise personally-owned work profiles also supports Android device administrator management. Intune lets you specify how devices that support work profiles should be managed from within Enrollment Restrictions.
   - **Block**: All Android devices will be enrolled as Android device administrator devices, unless device administrator enrollment is also blocked. This behavior includes devices that support Android Enterprise personally-owned work profiles.
   - **Allow (set by default)**: All devices that support Android Enterprise personally-owned work profiles are enrolled as personally-owned work profile devices. Any Android device that doesn't support personally-owned work profiles is enrolled as an Android device administrator device, unless device administrator enrollment is blocked.

> **NOTE**
> The default set to **Allow** is true for new tenants as of July 2019. All previous tenants will experience no change to their Enrollment Restrictions, and will see whatever policies they have set in Enrollment Restrictions. For previous tenants that never had Enrollment Restrictions changes, **Block** will still be the default for personally-owned work profiles.

3. Tell your users how to enroll their devices. To enroll, users must be using the primary user account on their device. Enrolling with a secondary user account is not supported.

Devices previously enrolled with Android device administrator can be re-enrolled using personally-owned work profiles. You'll first need to unenroll the device administrator devices. Then you can re-enroll them with personally-owned work profiles.

> **NOTE**
> As an administrator, you can accomplish this remotely using the **Retire** function. This function can be found in the actions menu after selecting the device from the **All Devices** blade.

If you're enrolling personally-owned work profile devices by using a Device Enrollment Manager account, there's a limit of 10 devices that can be enrolled per account.

For more information, see Data Intune sends to Google.

Next steps

- Deploy Android Enterprise apps

- Add Android Enterprise configuration policies

See also

Configuring and troubleshooting Android Enterprise devices in Microsoft Intune

Set up Intune enrollment of Android Enterprise dedicated devices

9/23/2022 • 5 minutes to read • Edit Online

Android Enterprise supports corporate-owned, single-use, kiosk-style devices with its dedicated devices solution set. Such devices are used for a single purpose, such as digital signage, ticket printing, or inventory management, to name just a few. Admins can lock down the usage of a device to a single app, or a limited set of apps, inclusive of web apps. Users are prevented from adding other apps or taking actions on the device that unless explicitly approved by admins.

Devices that you manage in this way can be enrolled into Intune in two different ways:

1. As a standard Android Enterprise dedicated device. These devices are enrolled into Intune without a user account and are not associated with any end user. These devices are not intended for personal use applications or apps that have a strong requirement for user-specific account data such as Outlook or Gmail.

2. As a standard Android Enterprise dedicated device that is automatically set up with Microsoft's Authenticator application configured into Azure AD Shared device mode during enrollment. These devices are enrolled into Intune without a user account and are not associated with any end user. These devices are intended for use with applications that have integrated with Azure AD's Shared device mode to allow for single sign-in and single sign-out between users across participating applications.

Intune helps you deploy apps and settings to Android Enterprise dedicated devices. For specific details about Android Enterprise, see Android enterprise requirements.

Device requirements

Devices must meet these requirements to be managed by Endpoint Manager as an Android Enterprise dedicated device:

- Android OS version 8.0 and above.
- Devices must run a distribution of Android that has Google Mobile Services (GMS) connectivity. Devices must have GMS available and must be able to connect to GMS.

Set up Android Enterprise dedicated device management

To set up Android Enterprise dedicated device management, follow these steps:

1. To prepare to manage mobile devices, you must set the mobile device management (MDM) authority to **Microsoft Intune** for instructions. You set this item only once, when you're first setting up Intune for mobile device management.
2. Connect your Intune tenant account to your Managed Google Play account.
3. Create an enrollment profile.
4. Create a device group.
5. Enroll the dedicated devices.

Create an enrollment profile

> **NOTE**
> If a token has expired, the profile associated with it will not be displayed in **Device enrollment** > **Android enrollment** > **Corporate-owned dedicated devices**. To see all profiles associated with both active and inactive tokens, click on **Filter** and check the boxes for both "Active" and "Inactive" policy states.

You must create an enrollment profile so that you can enroll your dedicated devices. When the profile is created, it provides you with an enrollment token (random string) and a QR code. Depending on the Android OS and version of the device, you can use either the token or QR code to enroll the dedicated device.

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Devices** > **Android** > **Android enrollment** > **Corporate-owned dedicated devices**.
2. Choose **Create** and fill out the required fields.
   - **Name**: Type a name that you'll use when assigning the profile to the dynamic device group.
   - **Token type**: Choose the type of token you want to use to enroll dedicated devices.
     - **Corporate-owned dedicated device (default)**: This token enrolls devices as a standard Android Enterprise dedicated device. These devices require no user credentials at any point. This is the default token type that dedicated devices will enroll with unless updated by Admin at time of token creation.
     - **Corporate-owned dedicated device with Azure AD shared mode**: This token enrolls devices as a standard Android Enterprise dedicated device and, during enrollment, deploys Microsoft's Authenticator app configured into Azure AD Shared device mode. With this option, users can achieve single sign-in and single sign-out across apps on the device that are integrated with the Azure AD Microsoft Authentication Library and global sign-in/sign-out calls.
   - **Token expiration date**: The date when the token expires. Google enforces a maximum of 90 days.
3. Choose **Create** to save the profile.

Create a device group

You can target apps and policies to either assigned or dynamic device groups. You can configure dynamic Azure AD device groups to automatically populate devices that are enrolled with a particular enrollment profile by following these steps:

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Groups** > **All groups** > **New group**.
2. In the **Group** blade, fill out the required fields as follows:
   - **Group type**: Security
   - **Group name**: Type an intuitive name (like Factory 1 devices)
   - **Membership type**: Dynamic device
3. Choose **Add dynamic query**.
4. In the **Dynamic membership rules** blade, fill out the fields as follows:
   - **Add dynamic membership rule**: Simple rule
   - **Add devices where**: enrollmentProfileName
   - In the middle box, choose **Equals**.
   - In the last field, enter the enrollment profile name that you created earlier. For more information about dynamic membership rules, see Dynamic membership rules for groups in Azure AD.
5. Choose **Add query** > **Create**.

Replace or remove tokens

- **Replace token**: You can generate a new token/QR code when one nears expiration by using Replace Token.
- **Revoke token**: You can immediately expire the token/QR code. From this point on, the token/QR code is no longer usable. You might use this option if you:
  - accidentally share the token/QR code with an unauthorized party

- complete all enrollments and no longer need the token/QR code

Replacing or revoking a token/QR code won't have any effect on devices that are already enrolled.

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Devices** > **Android** > **Android enrollment** > **Corporate-owned dedicated devices**.
2. Choose the profile that you want to work with.
3. Choose **Token**.
4. To replace the token, choose **Replace token**.
5. To revoke the token, choose **Revoke token**.

Enroll the dedicated devices

You can now enroll your dedicated devices.

> **NOTE**
> The **Microsoft Intune** app will be automatically installed during enrollment of a dedicated device. This app is required for enrollment and cannot be uninstalled. The **Microsoft Authenticator** app will be automatically installed during enrollment of a dedicated device when using the token type **Corporate-owned dedicated device with Azure AD shared mode**. This app is required for this enrollment method and cannot be uninstalled.

Managing apps on Android Enterprise dedicated devices

Only apps that have Assignment type set to Required can be installed on Android Enterprise dedicated devices. Apps are installed from the Managed Google Play store in the same manner as Android Enterprise personally-owned and corporate-owned work profile devices.

Apps are automatically updated on managed devices when the app developer publishes an update to Google Play.

To remove an app from Android Enterprise dedicated devices, you can do either of the following:

- Delete the Required app deployment.
- Create an uninstall deployment for the app.

Next steps

- Deploy Android apps
- Add Android configuration policies

Set up Intune enrollment of Android Enterprise fully managed devices

9/23/2022 • 2 minutes to read • Edit Online

Android Enterprise fully managed devices are corporate-owned devices associated with a single user and used exclusively for work and not personal use. Admins can manage the entire device and enforce policy controls unavailable to personally-owned/corporate-owned work profiles, such as:

- Allow app installation only from Managed Google Play.
- Block uninstallation of managed apps.
- Prevent users from factory resetting devices, and so on.

Intune helps you deploy apps and settings to Android Enterprise devices, including Android Enterprise fully managed devices. For specific details about Android Enterprise, see Android Enterprise requirements.

Technical requirements

You must have an Intune standalone tenant to manage Android Enterprise fully managed devices. Fully managed device management isn't available in the legacy Silverlight management console.

Devices must meet these requirements to be managed as an Android Enterprise fully managed device:

- Android OS version 8.0 and above.
- Devices must run a build of Android that has Google Mobile Services (GMS) connectivity. Devices must have GMS available and must be able to connect to GMS.

There is no restriction on device manufacturer/OEM if the above requirements are met.

Set up Android Enterprise fully managed device management

To set up Android Enterprise fully managed device management, follow these steps:

1. To prepare to manage mobile devices, you must set the mobile device management (MDM) authority to **Microsoft Intune**. You set this item only once, when you're first setting up Intune for mobile device management.
2. Connect your Intune tenant account to your Android Enterprise account.
3. Enable corporate-owned user devices
4. Enroll the fully managed devices.

Enable corporate owned user devices

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Devices** > **Android** > **Android enrollment** > **Corporate-owned, fully managed user devices**.
2. Under **Allow users to enroll corporate-owned user devices**, choose **Yes**.

NOTE

If you have an Azure AD Conditional Access policy defined that uses the *require a device to be marked as compliant* Grant control or a Block policy and applies to **All Cloud apps**, **Android**, and **Browsers**, you must exclude the **Microsoft Intune** cloud app from this policy. This is because the Android setup process uses a Chrome tab to authenticate your users during enrollment. For more information, see Azure AD Conditional Access documentation.

When this setting is set to **Yes**, it provides you with an enrollment token (a random string) and a QR code for your Intune tenant. This single enrollment token is valid for all your users and won't expire. Depending on the Android OS and version of the device, you can use either the token or QR code to enroll the device.

Enroll the fully managed devices

You can now enroll your fully managed devices (but not when using DEM accounts).

Next steps

- Add Android Enterprise fully managed device configuration policies
- Configure app configuration policies for Android Enterprise fully managed devices

Enroll your Android Enterprise dedicated, fully managed, or corporate-owned with work profile devices

9/23/2022 • 6 minutes to read • Edit Online

IMPORTANT

It's important that device users do not restart devices until enrollment is complete. If device users setting up fully managed devices or corporate-owned devices with a work profile restart their devices in the middle of enrollment, their devices may not be able to register with Microsoft Intune. Devices that restarted may appear to be enrolled but they won't be protected by your Intune policies.

After you've set up your Android Enterprise dedicated devices, fully managed devices, or corporate-owned work profile devices in Intune, you can enroll the devices. Intune enrollment for dedicated devices, fully managed devices, and corporate-owned with a work profile start with a factory reset. How you enroll your Android Enterprise devices depends on the operating system.

ENROLLMENT METHOD	MINIMUM ANDROID OS VERSION FOR DEDICATED AND FULLY MANAGED DEVICES
Near Field Communication	8.0
Token entry	8.0
QR code	8.0
Zero Touch	8.0 On participating manufacturers.
Knox Mobile Enrollment	8.0 On Samsung Knox 2.8 or higher devices only.

TIP

Corporate-owned work profile (COPE) device management is available on Android version 8.0 and newer.

NOTE

If you have an Azure AD Conditional Access policy defined that uses the *require a device to be marked as compliant* Grant control or a Block policy and applies to **All Cloud apps**, **Android**, and **Browsers**, you must exclude the **Microsoft Intune** cloud app from this policy. This is because the Android setup process uses a Chrome tab to authenticate your users during enrollment. For more information, see Azure AD Conditional Access documentation.

Enroll by using Near Field Communication (NFC)

Create a specially formatted NFC tag to provision NFC-supported devices running Android 8.0 or later. You can use your own app or any NFC tag-creation tool. For more information, see C-based Android Enterprise device enrollment with Microsoft Intune and Google's Android Management API documentation.

For corporate-owned work profile (COPE) devices, the NFC enrollment method is only supported on devices running Android versions 8.0 to 10.0. It's not supported with Android 11.0 or later.

Enroll by using a token

- For Android 8.0 and later devices, you can use the token value, such as `12345`, to enroll the device.
- You can leverage QR code scanning when using the **afw#setup** enrollment method to enroll devices running Android 8.0 and later.
- For corporate-owned work profile (COPE) devices, the **afw#setup** enrollment method is only supported on devices running Android versions 8.0 to 10.0. It's not supported with Android 11.0 or later. For more information, see the Google developer docs.

Steps

1. Turn on your wiped device.
2. On the **Welcome** screen, select your language.
3. Connect to your **Wi-fi**, and then choose **NEXT**.
4. Accept the Google Terms and conditions, and then choose **NEXT**.
5. On the Google sign-in screen, enter **afw#setup** instead of a Gmail account, and then choose **NEXT**.
6. Choose **INSTALL** for the **Android Device Policy** app.
7. Continue installation of this policy. Some devices may require additional terms acceptance.
8. On the **Enroll this device** screen, allow your device to scan the QR code. Or, choose to enter the token manually.
9. Follow the on-screen prompts to complete enrollment.

Enroll by using a QR code

Scan the QR code from the enrollment profile to enroll devices running Android 8.0 and later.

> **NOTE**
> Browser zoom can cause devices to not be able to scan QR code. Increasing the browser zoom resolves the issue.

1. After you wipe the device, tap the first screen you see repeatedly to launch the QR reader.
2. On devices running Android 8.0, you'll be prompted to install a QR reader. Devices running Android 9 and later are pre-installed with a QR reader.
3. Use the QR reader to scan the enrollment profile QR code and then follow the on-screen prompts to enroll.

Enroll by using Google Zero Touch

To use this method, zero-touch enrollment must be supported on devices and affiliated with a supplier that is part of the Android zero-touch enrollment service. For more information, such as prerequisites, where to purchase devices, and how to associate a Google Account with your corporate email, see Zero-touch enrollment for IT admins (opens Android Enterprise Help docs).

This section describes how to:

- Create a zero-touch configuration in the admin center
- Create a zero-touch configuration in the zero-touch enrollment portal

Create zero-touch configuration in admin center

The zero-touch iframe gives you access to the zero-touch enrollment portal and zero-touch configurations in the Microsoft Endpoint Manager admin center.

To enable the iframe, you must first add the *update app sync* permission and enable enrollment for corporate-owned, fully managed devices. Once you enable the iframe, you can:

- Link your zero-touch account to Intune
- Add support information
- Configure zero-touch enabled devices
- Customize provisioning extras

Complete the steps in this section to enable the iframe. To create configurations in the zero-touch enrollment portal instead, skip to Create configuration in zero-touch enrollment portal.

Step 1: Add required permission

Add the *update app sync* permission.

1. Sign in to the Microsoft Endpoint Manager admin center admin.
2. Select **Tenant administration** > **Roles**.
3. Select your role from the list.
4. Select **Properties**.
5. Go to **Permissions** and then select **Edit**.
6. Select **Android for Work**.
7. Next to **Update app sync**, select **Yes**.
8. Select **Review + save** to review your changes.
9. Select **Save**.

Step 2: Enable enrollment for corporate-owned devices

Verify that enrollment is enabled for corporate-owned, fully managed devices.

1. In the admin center, go to **Devices** > **Enroll devices**.
2. Select **Android enrollment**.
3. Under **Enrollment profiles**, choose **Corporate-owned, fully managed user devices**.
4. Verify that the setting for **Allow users to enroll corporate-owned user devices**, is set to **Yes**.

Step 3: Link zero-touch account to Intune

Link a zero-touch account with your Microsoft Intune account. Upon linking the account, Intune creates a default zero-touch configuration.

1. In the admin center, go to **Devices** > **Enroll devices**.
2. Select **Android enrollment**.
3. Under **Bulk enrollment methods**, choose **Zero-touch enrollment**.
4. The iframe opens. Select **Next** to begin setup.
5. Sign in with the Google account you provided to your reseller.
6. Select the zero-touch account you want to link, and then select **Link**.
7. A default configuration is created. A screen appears with basic information about the configuration. Intune will automatically apply the default configuration to any zero-touch enabled device that's without an existing configuration.

> **TIP**
> The token used for the default configuration is meant for a fully managed device. If you want to create a zero-touch configuration for a corporate-owned work profile device or a dedicated device, select **View devices in the zero-touch portal**. For next steps, see Create configuration in zero-touch enrollment portal in this article.

7. Select **Next** to continue.
8. Add support information to assist device users during setup.
9. Select **Save**.

Once your account is linked with Intune, the default configuration is applied to zero-touch enabled devices that do not already have a configuration. You can view existing zero-touch configurations, edit support information, unlink the account, and link other accounts in the admin center.

Create configuration in zero-touch enrollment portal

Add a zero-touch configuration in the zero-touch enrollment portal. You can use the portal by itself to manage configurations, or you can use it in combination with the zero-touch iframe. The portal supports configurations for fully managed and dedicated devices, and corporate-owned devices with a work profile.

1. Sign in to the zero-touch enrollment portal with your Google account.
2. Select the option to add a new configuration.
3. Fill out the information in the configuration panel.
4. Select **Microsoft Intune** as the EMM DPC app.
5. Copy the following JSON text into the DPC extras field. Replace `YourEnrollmentToken` with the enrollment token you created as part of your enrollment profile. Be sure to surround the enrollment token with double quotes.

```
{
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.google.android.apps.work.clouddpc/.receivers.CloudDeviceAdminReceiver",

    "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"I5YvS0O5hXY46mb01BlRjq4oJJGs2kuUcHvVkAPEXlg",

    "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?identifier=setup",

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
        "com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN": "YourEnrollmentToken"
```

6. Enter your organization's name and support information, which is shown on screen while users set up their devices.

For more information about how to assign a default configuration or apply a configuration in the zero-touch portal, see Zero-touch enrollment for IT admins (opens Android Enterprise Help docs).

Enroll by using Knox Mobile Enrollment

To use Samsung's Knox Mobile Enrollment, the device must be running Android OS version 8.0 or later and Samsung Knox 2.8 or higher. For more information, learn how to automatically enroll your devices with Knox Mobile Enrollment.

Next steps

- Deploy Android apps
- Add Android configuration policies

Android device administrator enrollment

9/23/2022 • 2 minutes to read • Edit Online

Android device administrator (sometimes referred to "legacy" Android management and released with Android 2.2) is a way to manage Android devices. However, improved management functionality is available with Android Enterprise. In an effort to move to modern, richer, and more secure device management, Google is decreasing device administrator support in new Android releases.

Therefore, to avoid such reduced functionality, we advise against enrolling new devices using the device administrator process described below.

For the same reasons, we also recommend that you migrate devices off of device administrator management if the devices are going to update to Android 10.

> **IMPORTANT**
>
> In areas where Android Enterprise is available(opens Google documentation), Google is encouraging people to move away from device administrator (DA) management by decreasing its management support in new Android releases.
>
> In areas where Android Enterprise is unavailable, or for devices incapable of integrating with Google Mobile Services, we still recommend using DA as your management solution in Microsoft Intune. For more information about using DA when Google Mobile Services are unavailable, see How to use Intune in environments without Google Mobile Services.
>
> DA is currently the recommended management solution for Microsoft Teams certified Android devices.

If you still decide to have users enroll their Android devices with device administrator management, continue to the next section.

For more information about Google's Android Enterprise features, see these articles:

- Google's guidance for migration from device administrator to Android Enterprise
- Google's documentation on the plan to deprecate the device administrator API

Set up device administrator enrollment

1. To prepare to manage mobile devices, you must set the mobile device management (MDM) authority to **Microsoft Intune**. See Set the MDM authority for instructions. You set this item only once, when you are first setting up Intune for mobile device management.
2. Sign in to the Microsoft Endpoint Manager admin center and choose > **Devices** > **Android** > **Android enrollment** > **Personal and corporate-owned devices with device administration privileges** > **Use device administrator to manage devices**.
3. Tell your users how to enroll their devices.

After a user has enrolled, you can begin managing their devices in Intune, including assigning compliance policies, managing apps, and more.

For information about other user tasks, see these articles:

- Resources about the end-user experience with Microsoft Intune
- Using your Android device with Intune

Block device administrator enrollment

To block Android device administrator devices, or to block only personally owned Android device administrator devices from enrollment, see Set device type restrictions.

Next steps

- Assign compliance policies
- Managing apps

Set up Intune enrollment for Android (AOSP) corporate-owned userless devices

9/23/2022 • 6 minutes to read • Edit Online

Set up enrollment in Microsoft Intune for corporate-owned, userless devices built on the Android Open Source Project (AOSP) platform. Intune offers an *Android (AOSP)* device management solution for corporate-owned Android devices that are:

- Not integrated with Google Mobile Services.
- Intended to be shared by more than one user.
- Used to accomplish a specific set of tasks at work.

This article describes how to set up Android (AOSP) device management and enroll RealWear devices for use at work.

Prerequisites

To enroll and manage AOSP devices, you must have:

- An active Microsoft Intune tenant.
- RealWear devices, updated to Firmware 11.2 or later.

You must also:

- Set Microsoft Intune as the mobile device management (MDM) authority in your tenant. You only need to do this once, when you first set up Intune for mobile device management.
- Assign valid licenses to all RealWear device users. For more information, see Microsoft Intune licensing.

Create an enrollment profile

Create an enrollment profile to enable enrollment on devices.

> **TIP**
> Intune also generates a token in plain text form, but that one can't be used to enroll devices.

1. Sign in to the Microsoft Endpoint Manager admin center and select **Devices** > **Android** > **Android enrollment** > **Corporate-owned, userless devices**.
2. Select **Create** and fill out the required fields.
   - **Name**: Type a name to use when assigning the profile to the dynamic device group.
   - **Description**: Add a profile description (optional).
   - **Token expiration date**: The date when the token expires. Intune enforces a maximum of 90 days.
   - **SSID**: Identifies the network that the device will connect to.

> **NOTE**
> Wi-Fi details are required because the RealWear device does not have a button or option that lets it automatically connect to other devices.

- **Hidden Network**: Choose whether this is a hidden network. By default, this setting is disabled.
- **Wi-Fi Type**: Select the type of authentication needed for this network.

  If you select **WEP Pre-Shared Key** or **WPA Pre-Shared Key**, also enter:

  - **Pre-shared key**: The pre-shared key that's used to authenticate with the network.

3. Select **Next** and optionally, select scope tags.
4. Select **Next**. Review the details of your profile and then select **Create** to save the profile.

Access enrollment token

After you create a profile, Intune generates a token that's needed for enrollment. To access the token:

1. Go to **Corporate-owned, userless devices**.
2. From the list, select your enrollment profile.
3. Select **Tokens**.

Another way to find the token is:

1. Go to **Corporate-owned, userless devices**.
2. Locate your profile in the list, and then select the **More** (...) menu that's next to it.
3. Select **View enrollment token**.

The token appears as a QR code. During device setup, when prompted to, scan the QR code to enroll the device in Intune.

> **IMPORTANT**
> - The QR code will contain any credentials provided in the profile in plain text to allow the device to successfully authenticate with the network. This is required as the user will not be able to join a network from the device.
> - Since you're managing the device via Intune, you should skip the RealWear first time setup. The Intune QR codes is the only thing you need to set up the device.

Replace token

Generate a new token to replace one that's nearing its expiration date. Replacing a token does not affect devices that are already enrolled.

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select **Devices** > **Android** > **Android enrollment** > **Corporate-owned, userless devices**.
3. Choose the profile that you want to work with.
4. Select **Token** > **Replace token**.
5. Enter the new token expiration date. Tokens must be replaced at least every 90 days.
6. Select **OK**.

Revoke token

Revoke a token to immediately expire it and make it unusable. For example, it's appropriate to revoke a token when:

- You accidentally share the token/QR code with an unauthorized party.

- You complete all enrollments and no longer need the token.

Revoking a token does not affect devices that are already enrolled.

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select **Devices** > **Android** > **Android enrollment** > **Corporate-owned, userless devices**.
3. Choose the profile that you want to work with.
4. Select **Token** > **Revoke token** > **Yes**.

Create a device group

You can create *assigned device groups* or *dynamic device groups* in Intune. For more information about both groups, see Add groups to organize users and devices.

Dynamic device groups are configured to automatically add and remove devices based on a set of rules and parameters. For example, you can group devices by enrollment profile name.

Complete the following steps to create a dynamic Azure AD device group for devices enrolled with an Android (AOSP) corporate-owned, userless enrollment profile.

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Groups** > **All groups** > **New group**.
2. In the **Group** blade, fill out the required fields as follows:
   - **Group type**: Security
   - **Group name**: Type an intuitive name (like Factory 1 devices)
   - **Membership type**: Dynamic device
3. Choose **Add dynamic query**.
4. In the **Dynamic membership rules** blade, fill out the fields as follows:
   - **Add dynamic membership rule**: Simple rule
   - **Add devices where**: enrollmentProfileName
   - In the middle box, choose **Equals**.
   - In the last field, enter the enrollment profile name that you created earlier.

   For more information about dynamic membership rules, see Dynamic membership rules for groups in Azure AD.
5. Choose **Add query** > **Create**.

Enroll devices

After you set up and assign the Android (AOSP) enrollment profiles, you can enroll devices via QR code.

1. Turn on your new or factory-reset device.
2. When the device prompts you to, scan the token's QR code.

> **TIP**
> To access the token in Intune, select **Devices** > **Android** > **Android enrollment** > **Corporate-owned, userless devices**. Select your enrollment profile, and then select **Tokens**.

3. Follow the on-screen prompts to finish enrolling and registering the device. During setup, Intune automatically installs and opens the apps that are needed for enrollment. Those apps include:

- Microsoft Authenticator app
- Microsoft Intune app
- Intune Company Portal app

After enrollment

App updates

The Microsoft Intune app automatically installs available app updates for itself, Authenticator, and Company Portal. When an update becomes available, the Intune app closes and installs the update. The app must be closed completely to install the update.

Manage devices remotely

The following remote actions are available for Android (AOSP) devices:

- Wipe
- Delete

You can take action on one device at a time. For more information about where to find remote actions in Intune, see Remove devices by using wipe, retire, or manually unenrolling the device.

> **NOTE**
> After you wipe an Android (AOSP) device, the device remains in a **Pending** state until it's fully restored to its factory default settings. Then Intune removes it from the device list. When you delete a device, the device is removed from the device list immediately, with no pending status, and the factory reset happens the next time the device checks in.

Troubleshooting

View version of Microsoft Intune and Microsoft Authenticator apps

To find out which version of the Microsoft Intune app or Microsoft Authenticator app is installed on a device:

1. Go to **Devices** and select the device name.
2. Select **Discovered apps**.
3. Find your app and then look in the **Application Version** column for the version number.

Troubleshooting + Support

Select **Troubleshooting + Support** from the Microsoft Endpoint Manager navigation menu to:

- See a list of Android (AOSP) devices enrolled by a user
- Enable troubleshooting of Android (AOSP) devices the same way you can troubleshoot other user devices.

Share app logs with Microsoft

If you experience problems with enrollment or the Microsoft Intune app, you can use the Intune app to upload and send app logs to Microsoft. After you submit the logs, you'll receive an incident ID to share with your Microsoft support person.

Known limitations

The following are known limitations when working with AOSP devices in Intune:

- You cannot enforce certain password types via device compliance and device restrictions profiles. Password types include:
  - Password required, no restriction

    - Alphabetic
    - Alphanumeric
    - Alphanumeric with symbols
    - Weak biometric
- Device compliance reporting is not available for Android (AOSP).
- Android (AOSP) management is not supported in these environments:
    - Intune for Government Community Cloud (GCC) High and Department of Defense (D0D)
    - Intune operated by 21Vianet

Next steps

- Create an Android (AOSP) device configuration policy to restrict settings on devices.
- Create an Android (AOSP) device compliance policy.
- For more information about how to get started with AOSP, see Android source requirements(opens Android source documentation).

Set up Intune enrollment for Android (AOSP) corporate-owned user-associated devices

9/23/2022 • 6 minutes to read • Edit Online

Set up enrollment in Intune for corporate-owned, user-associated devices built on the Android Open Source Project (AOSP) platform. Intune offers an *Android (AOSP)* device management solution for corporate-owned Android devices that are:

- Not integrated with Google Mobile Services.
- Intended to be used by a single user.
- Used exclusively for work.

This article describes how to set up Android (AOSP) device management and enroll RealWear devices for use at work.

Prerequisites

To enroll and manage AOSP devices, you must have:

- An active Microsoft Intune tenant.
- RealWear devices, updated to Firmware 11.2 or later.

You must also:

- Set Microsoft Intune as the mobile device management (MDM) authority in your tenant. You only need to do this once, when you first set up Intune for mobile device management.
- Assign valid licenses to all RealWear device users. For more information, see Microsoft Intune licensing.

Create an enrollment profile

Create an enrollment profile to enable enrollment on devices.

1. Sign in to the Microsoft Endpoint Manager admin center and select **Devices** > **Android** > **Android enrollment** > **Corporate-owned, user-associated devices**.
2. Select **Create** and fill out the required fields.
   - **Name**: Type a name to use when assigning the profile to the dynamic device group.
   - **Description**: Add a profile description (optional).
   - **Token expiration date**: The date when the token expires. Intune enforces a maximum of 90 days.
   - **SSID**: Identifies the network that the device will connect to.

     > **NOTE**
     > Wi-Fi details are required because the RealWear device doesn't have a button or option that lets it automatically connect to other devices.

   - **Hidden network**: Choose whether this is a hidden network. By default, this setting is disabled, which means the network can broadcast its SSID.

- **Wi-Fi type**: Select the type of authentication needed for this network.

  If you select **WEP Pre-shared key** or **WPA Pre-shared key**, also enter:

  - **Pre-shared key**: The pre-shared key that's used to authenticate with the network.

3. Select **Next** and optionally, select scope tags.
4. Select **Next**. Review the details of your profile and then select **Create** to save the profile.

Access enrollment token

After you create a profile, Intune generates a token that's needed for enrollment. The token appears as a QR code. During device setup, when prompted to, scan the QR code to enroll the device in Intune.

To view the token as a QR code:

1. Go to **Corporate-owned, user-associated devices**.
2. From the list, select your enrollment profile.
3. Select **Token**.

From the Token page, you can also export the enrollment profile JSON file.

> **IMPORTANT**
> - The QR code will contain any credentials provided in the profile in plain text to allow the device to successfully authenticate with the network. This is required as the user will not be able to join a network from the device.
> - Since you're managing the device via Intune, you should skip the RealWear first time setup. The Intune QR codes is the only thing you need to set up the device.

Replace a token

You can generate a new token to replace one that's nearing its expiration date. The replacement token doesn't affect devices that are already enrolled.

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select **Devices** > **Android** > **Android enrollment** > **Corporate-owned, user-associated devices**.
3. Choose the profile that you want to work with.
4. Select **Token** > **Replace token**.
5. Enter the new token expiration date. Tokens must be replaced at least every 90 days.
6. Select **OK**.

Revoke a token

Revoke a token to immediately expire it and make it unusable. For example, it's appropriate to revoke a token when:

- You accidentally share the token/QR code with an unauthorized party.
- You complete all enrollments and no longer need the token.

Revoking a token has no effect on devices that are already enrolled.

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select **Devices** > **Android** > **Android enrollment** > **Corporate-owned, user-associated devices**.
3. Choose the profile that you want to work with.
4. Select **Token** > **Revoke token** > **Yes**.

Create a device group

You can create *assigned device groups* or *dynamic device groups* in Intune. For more information about groups, see Add groups to organize users and devices.

Dynamic device groups are configured to automatically add and remove devices based on a set of rules and parameters. For example, you can group devices by enrollment profile name.

Complete the following steps to create a dynamic Azure AD device group for devices enrolled with an Android (AOSP) corporate-owned, user-associated enrollment profile.

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Groups** > **All groups** > **New group**.
2. In the **Group** blade, fill out the required fields as follows:
   - **Group type**: Security
   - **Group name**: Type an intuitive name (like Factory 1 devices)
   - **Membership type**: Dynamic device
3. Choose **Add dynamic query**.
4. In the **Dynamic membership rules** blade, fill out the fields as follows:
   - **Add dynamic membership rule**: Simple rule
   - **Add devices where**: enrollmentProfileName
   - In the middle box, choose **Equals**.
   - In the last field, enter the enrollment profile name that you created earlier.

   For more information about dynamic membership rules, see Dynamic membership rules for groups in Azure AD.
5. Choose **Add query** > **Create**.

Enroll devices

After you set up and assign the Android (AOSP) enrollment profiles, you can enroll devices via QR code.

1. Turn on your new or factory-reset device.
2. When the device prompts you to, scan the token's QR code.

> **TIP**
> To access the token in Intune, select **Devices** > **Android** > **Android enrollment** > **Corporate-owned, user-associated devices**. Select your enrollment profile, and then select **Token**.

3. Step through the on-screen prompts to finish enrolling and registering the device. The following apps are automatically installed during this time and used for enrollment:
   - Microsoft Intune app
   - Intune Company Portal app
   - Microsoft Authenticator app

After enrollment

Update apps

The Microsoft Intune app automatically updates itself. When an app update becomes available, the Intune app closes and installs the update. The app must remain closed to install the update. The app also installs updates for Microsoft Authenticator and the Company Portal app.

Manage devices remotely

The following remote actions are available for Android (AOSP) devices:

- Wipe
- Delete

You can take action on one device at a time. For more information about where to find remote actions in Intune, see Remove devices by using wipe, retire, or manually unenrolling the device.

> **NOTE**
> After you wipe an Android (AOSP) device, the device remains in a **Pending** state until it's fully restored to its factory default settings. Then Intune removes it from the device list. When you delete a device, the device is removed from the device list immediately, with no pending status, and the factory reset happens the next time the device checks in.

Troubleshooting

View app versions

Find out which version of the Intune app or Microsoft Authenticator app is installed on a device.

1. Go to **Devices** and select the device name.
2. Select **Discovered apps**.
3. Find your app and then look in the **Application Version** column for the version number.

Troubleshooting + Support

Select **Troubleshooting + Support** from the Microsoft Endpoint Manager navigation menu to:

- See a list of Android (AOSP) devices enrolled by a user
- Enable troubleshooting of Android (AOSP) devices the same way you can troubleshoot other user devices.

Share app logs with Microsoft

If you experience problems with enrollment or access to work resources, you can share diagnostic logs with Microsoft in the Intune app or Company Portal app. After you submit the logs, you'll receive an incident ID to share with your Microsoft support person.

Known limitations

The following are known limitations when working with AOSP devices in Intune:

- You cannot enforce certain password types via device compliance and device restrictions profiles. Password types include:
  - Password required, no restriction
  - Alphabetic
  - Alphanumeric
  - Alphanumeric with symbols
  - Weak biometric
- Device compliance reporting is not available for Android (AOSP).
- Android (AOSP) management is not supported in these environments:
  - Intune for Government Community Cloud (GCC) High and Department of Defense (DoD)
  - Intune operated by 21Vianet

Next steps

- Create an Android (AOSP) device configuration policy to restrict settings on devices.
- Create an Android (AOSP) device compliance policy.
- Create a policy that requires users to accept your terms and conditions before enrollment.
- For more information about how to get started with AOSP, see Android source requirements(opens Android source documentation).

Manage Android personally-owned/corporate-owned work profile devices with Intune

9/23/2022 • 6 minutes to read • Edit Online

Android Enterprise offers a set of enrollment options that provide users with the most up-to-date and secure features. Enrolling with an Android Enterprise personally-owned/corporate-owned work profile allows a set of features and services that separate personal apps and data from work apps and data. It also provides additional management capabilities and privacy when people use their personal Android devices for work.

Supported devices

Android Enterprise management capabilities rely upon features that are part of more recent Android operating systems. For devices that do not support Android Enterprise, conventional Android management remains available. For more information, see Android Enterprise requirements.

Onboarding

Before enrolling Android Enterprise work profile devices, you must complete some onboarding steps. These steps establish a connection between your Intune tenant and Managed Google Play. For more information, see Enable enrollment of Android Enterprise personally-owned work profile devices or Set up Intune enrollment of Android Enterprise corporate-owned devices with work profile.

Work profile management

When you manage an Android Enterprise personally-owned or corporate-owned work profile device with Intune, you don't manage the entire device. Management capabilities only affect the work profile that is created on the device during enrollment. Any apps deployed to the device with Intune get installed in the work profile. App icons in the work profile are differentiated from personal apps on the device. All Android apps and data outside the Android enterprise portion of the device remain personal and under the control of the end user. Users can install any app they choose to the personal side of the device. Administrators can manage and monitor apps and actions scoped to the work profile.

When configuring policies for device configuration or compliance, the broad range of settings enables you to tailor protection to your specific needs. To better understand how to implement specific security configuration scenarios, see the security configuration framework guidance for Android Enterprise device restriction policies.

The security configuration framework is organized into distinct configuration levels that provide guidance for personally owned and supervised devices, with each level building off the previous level. The available levels and settings in each level vary by enrollment mode:

- For Android Enterprise personally-owned work profile devices: Android personally-owned work profile security settings
- For Android Enterprise fully managed, dedicated, and corporate-owned work profile devices: Android fully managed-security settings

Alternatively, you can review the Device compliance settings for Android Enterprise in Intune and Android Enterprise device settings to allow or restrict features using Intune.

App publishing and distribution

Managed Google Play is an integral part of Android Enterprise app distribution and management. All apps deployed to Android Enterprise personally-owned and corporate-owned work profile devices in the work profile come from the Managed Google Play service. To manage and deploy apps in the Play Store, you sign in to the Google Play website with your company's administrator credentials for Google management. You can approve apps for Android Enterprise deployment to have them appear in devices' work profiles. These apps then sync to the Intune console where they can then be deployed and managed using Intune. Line of business (LOB) apps developed by your organization must be published to Managed Google Play using Google's Android app publishing console. Line-of-business apps must be configured in the Android app publishing console to restrict access to your organization.

Apps can be installed without user interaction and without requiring that the user allow **Installation from Unknown Sources**. To browse and install optional or available apps, the user can browse the Play for Work store on their device. For more information, see Assign apps to Android Enterprise work profile devices with Intune.

App configuration

Android Enterprise provides infrastructure for deploying app configuration values to apps that support them. By specifying configuration values for work apps, you ensure they are properly set when users launch the app for the first time. Support for app configuration requires that app developers create their Android apps specifically to support managed configuration values. If they do, then you can use Intune to specify and apply these configuration settings. For more information, see Add app configuration policies for managed Android devices.

Email configuration

Android Enterprise doesn't provide a default email app or native email profile object like those provided by iOS/iPadOS. Instead, email configurations can be set by applying app configuration settings to email apps that support them. Gmail and Nine Work are two Exchange ActiveSync (EAS) client apps in the Play Store that support configuration with Android Enterprise app configuration.

Intune provides configuration templates for Gmail and Nine Work apps when managed as work apps. Other email apps that support app configuration profiles can be configured with mobile app configuration policies.

If you are using Exchange ActiveSync Conditional Access for an Android Enterprise personally-owned or corporate-owned work profile device, consider using either the Gmail or Nine Work email app. The Microsoft Outlook for Android app, or any other email app that uses modern authentication via MSAL, is also supported. For more information, see How to configure email settings in Microsoft Intune.

> **NOTE**
>
> Azure Active Directory (Azure AD) Authentication Library (ADAL) will be deprecated, so we recommend updating apps that currently use it to MSAL. For more information, see Update your applications to use Microsoft Authentication Library (MSAL) and Microsoft Graph API.

App protection policies

App protection policies applied are fully supported in the personally-owned/corporate-owned work profile and in the personal profile. You can publish line-of-business apps in the Android app publishing console at https://play.google.com/apps/publish. This console includes an option to make apps private to your organization. For more information, see Add a device compliance policy for Android Enterprise work profile devices in Intune. For general information about app protection policies, see What are app protection policies?

VPN profiles

VPN support is similar to Android VPN profiles. The same VPN providers and basic configuration options are available for Android Enterprise management with two differences:

- **Work profile-scoped VPN** – VPN connections are limited to just the apps deployed to the personally-owned or corporate-owned work profile. Only Android Enterpise-managed apps can use the VPN connection. Personal apps on the device cannot use a managed VPN connection. For more information, see Android Enterprise VPN settings.
- **App-specific VPN** – App-specific VPN can be configured in Intune if the VPN provider supports:
  - configuration for app-specific VPN
  - the capability to configure per-app VPN via the Android Enterprise app configuration profile. For more information, see Use a Microsoft Intune custom profile to create a per-app VPN profile for Android devices.

Certificate profiles

The same certificate profile configuration options that are available to Android management are available on Android Enterprise personally-owned and corporate-owned work profile devices. Android Enterprise provides enhanced certificate management APIs. Enhanced certificate management provides the following functionality:

- Ensures that cert deployment is silent and seamless for the user.
- Ensures that deployed certs are removed when a device is retired from Intune and the work profile is removed.
- Provides improved messaging that informs users that the certificate was deployed and configured by their IT department via their management service.

For more information, see Configure a certificate profile for your devices in Microsoft Intune.

Wi-Fi profiles

Wi-Fi profiles managed by Android Enterprise are removed when the device is retired from Intune and the work profile is deleted. For more information, see How to configure Wi-Fi settings in Microsoft Intune.

Next steps

- Enroll Android devices
- Assign apps to Android Enterprise work profile devices with Intune

Set up Intune enrollment of Android Enterprise corporate-owned devices with work profile

9/23/2022 • 4 minutes to read • Edit Online

Android Enterprise corporate-owned devices with a work profile are single user devices intended for corporate and personal use.

End users can keep their work and personal data separate and are guaranteed that their personal data and applications will remain private. Admins can control some settings and features for the entire device, including:

- Setting requirements for the device password
- Controlling Bluetooth and data roaming
- Configuring factory reset protection

Intune helps you deploy apps and settings to Android Enterprise corporate-owned devices with work profile. For specific details about Android Enterprise, see Android enterprise requirements.

Device requirements

Devices must meet these requirements to be managed as Android Enterprise corporate-owned work profile devices:

- Android OS version 8.0 and above.
- Devices must run a distribution of Android that has Google Mobile Services (GMS) connectivity. Devices must have GMS available and must be able to connect to GMS.

Set up Android Enterprise corporate-owned work profile device management

To set up Android Enterprise corporate-owned work profile device management, follow these steps:

1. To prepare to manage mobile devices, you must set the mobile device management (MDM) authority to **Microsoft Intune** for instructions. You set this item only once, when you're first setting up Intune for mobile device management.
2. Connect your Intune tenant account to your Managed Google Play account.
3. Create an enrollment profile.
4. Create a device group.
5. Enroll the corporate-owned work profile devices.

Create an enrollment profile

NOTE

- Tokens for corporate-owned devices with a work profile will not expire automatically. If an admin decides to revoke a token , the profile associated with it will not be displayed in **Devices** > **Android** > **Android enrollment** > **Corporate-owned devices with work profile**. To see all profiles associated with both active and inactive tokens, click on **Filter** and check the boxes for both "Active" and "Inactive" policy states.
- For corporate-owned work profile (COPE) devices, the `afw#setup` enrollment method and the Near Field Communication (NFC) enrollment method are only supported on devices running Android 8-10. They are not available on Android 11. For further details, refer to the Google developer docs here.

You must create an enrollment profile so that users can enroll corporate-owned work profile devices. When the profile is created, it provides you with an enrollment token (random string) and a QR code. Depending on the Android OS and version of the device, you can use either the token or QR code to enroll the dedicated device.

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Devices** > **Android** > **Android enrollment** > **Corporate-owned devices with work profile**.
2. Choose **Create profile** and fill out the fields.
   - **Name**: Type a name that you'll use when assigning the profile to the dynamic device group.
   - **Description**: Add a profile description (optional).
3. Choose **Next**.
4. On the **Review + create** page, choose **Create** to create the policy.

Create a device group

You can target apps and policies to either assigned or dynamic device groups. You can configure dynamic Azure AD device groups to automatically populate devices that are enrolled with a particular enrollment profile by following these steps:

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Groups** > **All groups** > **New group**.
2. In the **Group** blade, fill out the required fields as follows:
   - **Group type**: Security
   - **Group name**: Type an intuitive name (like Factory 1 devices)
   - **Membership type**: Dynamic device
3. Choose **Add dynamic query**.
4. In the **Dynamic membership rules** blade, fill out the fields as follows:
   - **Add dynamic membership rule**: Simple rule
   - **Add devices where**: enrollmentProfileName
   - In the middle box, choose **Equals**.
   - In the last field, enter the enrollment profile name that you created earlier. For more information about dynamic membership rules, see Dynamic membership rules for groups in Azure AD.
5. Choose **Add query** > **Create**.

Revoke tokens

You can immediately expire the token/QR code. From this point on, the token/QR code is no longer usable. You might use this option if you:

- accidentally share the token/QR code with an unauthorized party
- complete all enrollments and no longer need the token/QR code

Revoking a token/QR code won't have any effect on devices that are already enrolled.

1. Sign in to the Microsoft Endpoint Manager admin center and choose **Devices** > **Android** > **Android enrollment** > **Corporate-owned devices with work profile**.

2. Choose the profile that you want to work with.
3. Choose **Token**.
4. To revoke the token, choose **Revoke token** > **Yes**.

Enroll the corporate-owned work profile devices

Users can now enroll their corporate-owned work profile devices.

> **NOTE**
> The **Microsoft Intune** app will be automatically installed during enrollment of a corporate-owned work profile device. This app is required for enrollment and cannot be uninstalled.

Managing apps on Android Enterprise corporate-owned work profile devices

Only apps that have Assignment type set to Required can be installed on Android Enterprise corporate-owned work profile devices. Apps are installed from the Managed Google Play store in the same manner as Android Enterprise personally-owned work profile devices.

Apps are automatically updated on managed devices when the app developer publishes an update to Google Play.

To remove an app from Android Enterprise corporate-owned work profile devices, you can do either of the following:

- Delete the Required app deployment.
- Create an uninstall deployment for the app.

Next steps

- Deploy Android apps
- Add Android configuration policies

Move Android devices from device administrator to personally-owned work profile management

9/23/2022 • 4 minutes to read • Edit Online

You can help users move their Android devices from device administrator to personally-owned work profile management by using the compliance setting to **Block devices managed with device administrator**. This setting lets you make devices non-compliant if they're managed with device administrator.

When users see that they're out of compliance for this reason, they can tap **Resolve**. They'll be taken to a checklist that will guide them through:

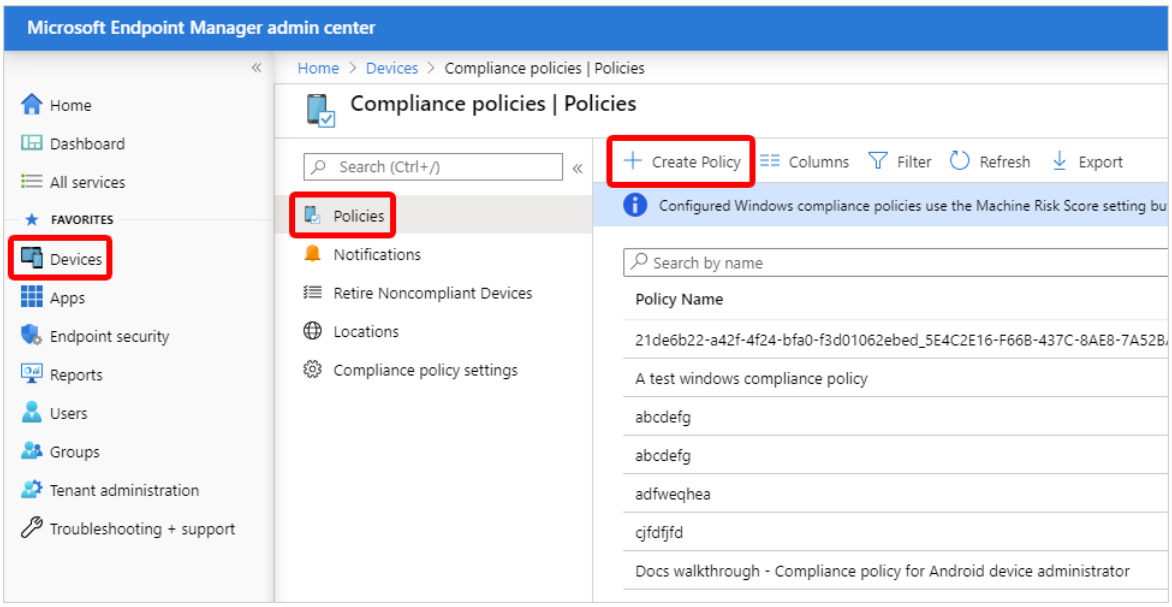
1. Unenrolling from device administrator management
2. Enrolling into personally-owned work profile management
3. Resolving any compliance issues.

Prerequisites

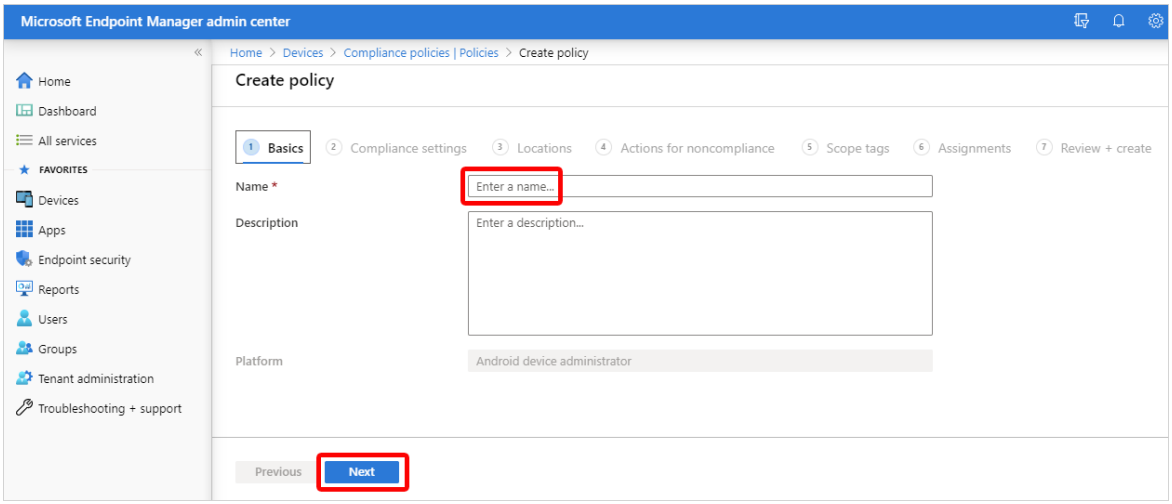
- Users must have Android device administrator enrolled devices with Android Company Portal version 5.0.4720.0 or later.
- Set up Android personally-owned work profile management by connecting your Intune tenant account to your Android Enterprise account.
- Set Android Enterprise personally-owned work profile enrollment for the group of users who are moving to personally-owned work profile.
- Consider increasing your user device limits. When unenrolling devices from device administrator management, device records might not be immediately removed. To provide cushion during this period, you might need to increase device limit capacity. This increase is so that the users can enroll into personally-owned work profile management.
  - Configure Azure Active Directory device settings for Maximum number of devices per user.
  - Adjust the Intune device limit restrictions by setting the device limit.

Create device compliance policy

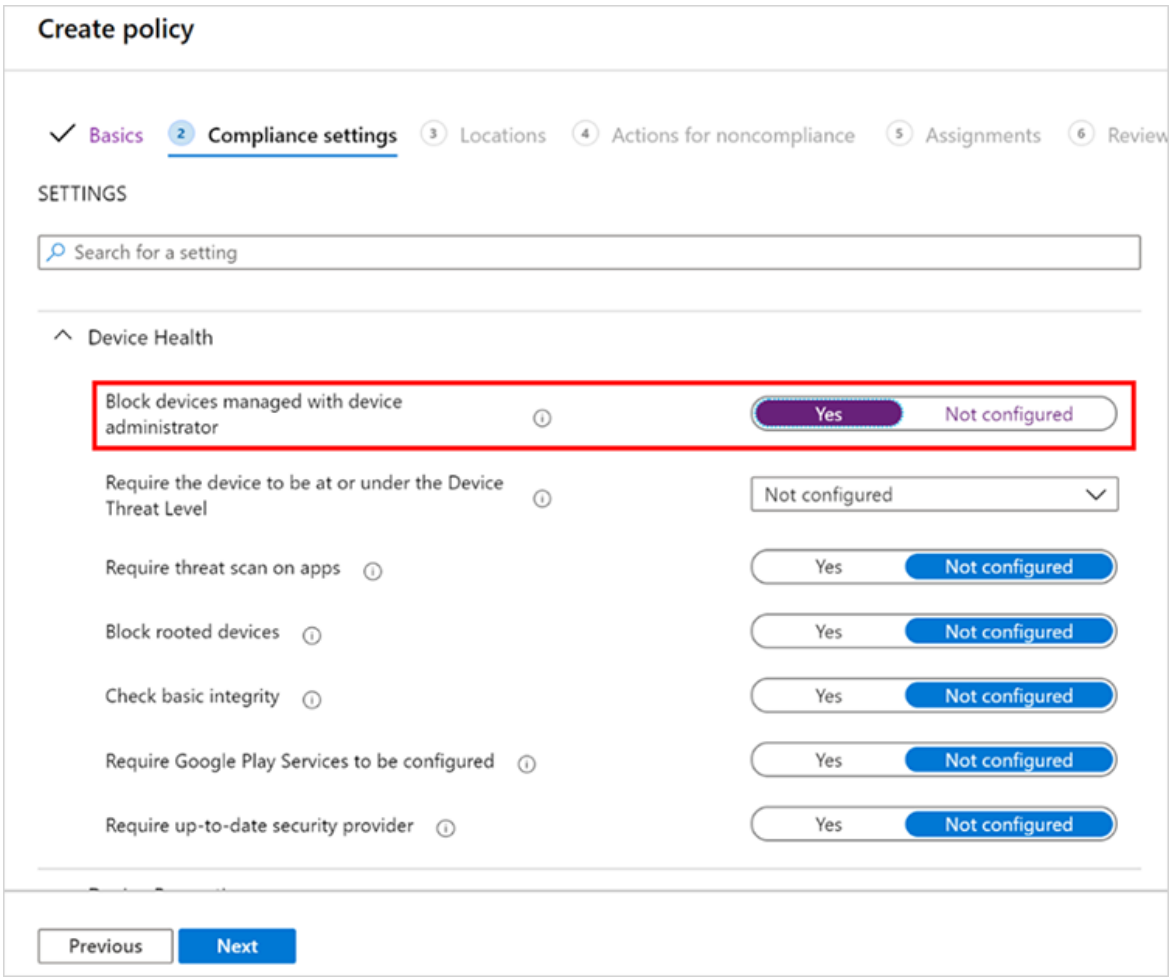
1. In the Microsoft Endpoint Manager admin center, select **Devices** > **Compliance policies** > **Policies** > **Create Policy**.



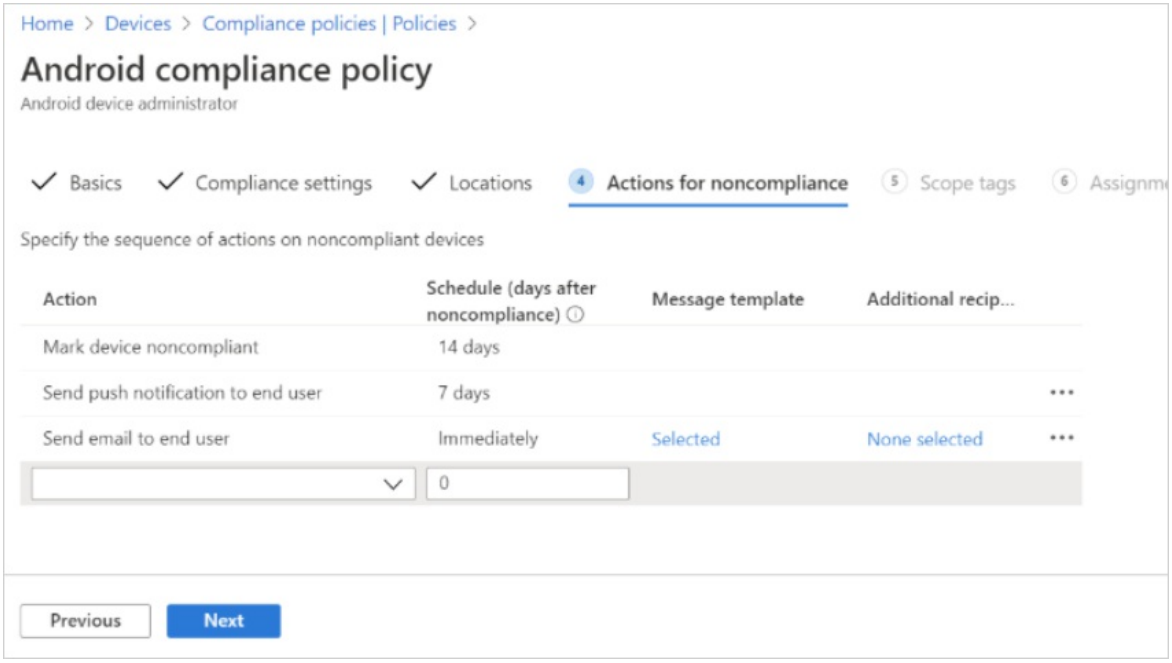
2. On the **Create a policy** page, set **Platform** to **Android device administrator** > **Create**.
3. On the **Basics** page, type in the **Name** and **Description** > **Next**.



4. On the **Compliance settings** page, in the **Device Health** section, set **Block devices managed with device administrator** to **Yes** > **Next**.



5. On the **Actions for noncompliance** tab, you can configure the available actions for noncompliance to customize the end-user experience for this flow.



Some actions to consider include:

- **Mark device noncompliant**: By default, this action is set to zero (0) days, marking devices as noncompliant immediately. You can increase the number of days to give users a grace period. During this grace period they can see the flow to move to personally-owned work profile management without yet being marked noncompliant. For example, you can set this action to 14 days to give users the time to move from device administrator to work profile management without the risk of losing access to resources.

- **Send push notification to end user**: Configure this action to send push notifications to the device administrator devices. When a user selects the notification, it will launch the Android Company Portal to the **Update device settings** page where they can start the flow to move to personally-owned work profile management.
- **Send email to end user**: Use this action to notify users about the move from device administrator to personally-owned work profile management. In the email, you can include the following URL. When this URL is selected, it launches the Android Company Portal to the Update device settings page. From this page, they can start the flow to move to work profile management.
  - `https://portal.manage.microsoft.com/UpdateSettings.aspx`.
  - For US government, you can use this link instead: `https://portal.manage.microsoft.us/UpdateSettings.aspx`.

  > **NOTE**
  > - Of course, you can use user-friendly hyper-text for the links in your communication with users. However, don't use URL-shorteners because the links may not work if changed that way.
  > - If the Android Company Portal is open and in the background, when a user taps the link they might go to the last page they had open instead.
  > - Users must tap the link on an Android device. If they instead paste it into a browser, it will not launch the Android Company Portal.

Choose **Next**.

6. On the **Scope tags** page, select any scope tags you want to include.
7. On the **Assignments** page, assign the policy to a group that has devices enrolled with device administrator management > **Next**.
8. On the **Review + create** page, confirm all your settings, and then select **Create**.

Troubleshooting

The end user flow to move to new device management setup guides users through unenrolling from device administrator management. It also helps users get set up with personally-owned work profile management. Users must have Android device administrator enrolled devices with Android Company Portal version 5.0.4720.0 or later.

User sees an error after tapping Resolve

If users see an error after tapping the **Resolve** button, it's likely because of one of these reasons:

- Personally-owned work profile enrollment isn't set up correctly. Either an Android Enterprise account isn't connected or enrollment restrictions are set to block personally-owned work profile enrollment.
- The device is running Android 4.4 or earlier, which doesn't support personally-owned work profile enrollment.
- The device manufacturer doesn't support personally-owned work profile enrollment on the device model.

Resolve button doesn't appear on the user's device

The **Resolve** button won't appear on the user's device if the user enrolls into device administrator management after they've been targeted with the device compliance policy explained above.

To get the **Resolve** button to appear, the user must postpone setup and restart the process from the notification.

To avoid this condition, use enrollment restrictions to block enrollment into device administrator management.

User sees an error after tapping URL to Update device settings page

Users might see an error page in the browser when they tap the URL to the **Update device settings page** of the Android Company Portal. This error can be caused by one of the following conditions:

- The device isn't an Android.
- The Android device doesn't have the Company Portal app.
- The Android Company Portal version is earlier than 5.0.4720.0.
- The Android device uses Android 6 or earlier.

Next steps

See the end user flow

Manage Android work profile devices with Intune

Automatically enroll Android devices by using Samsung's Knox Mobile Enrollment

9/23/2022 • 6 minutes to read • Edit Online

This topic helps you set up Intune for enrolling supported Android devices using Samsung Knox Mobile Enrollment (KME). Using Intune with Samsung KME, you can enroll large numbers of company-owned Android devices when end users turn on their devices for the first time and connect to a WiFi or cellular network. Also, devices can be enrolled using Bluetooth or NFC when using the Knox Deployment App.

To enable Intune enrollment using Samsung KME, you use both the Intune and Samsung Knox portals in this order:

1. In the Knox portal:
   a. Create an MDM profile
   b. Add devices
   c. Assign an MDM profile to the devices
2. In the Knox portal, configure end user sign in.
3. Distribute the devices.

A list of device identifiers (serial numbers and IMEIs) is automatically added to the Knox Portal when purchasing devices from authorized resellers participating in the Knox Deployment Program.

Prerequisites

To enroll into Intune using KME, you must first register your company on the Samsung Knox portal by following these steps:

1. Make sure KME is available in your country/region: KME is available in over 55 countries/regions. Ensure that your country/region of deployment is supported.
2. Supported devices: KME is available on all Samsung devices with a minimum of Knox 2.4 for Android enrollment and a minimum of Knox 2.8 for Android enterprise enrollment.
3. Network requirements: Make sure that the necessary firewall and network access rules are permitted on your network.
4. Register for a Samsung account: A Samsung account is needed to register and enable KME and manage all Knox Enterprise entitlements in a single place.
5. Registration Review: After your profile is completed and submitted, Samsung reviews your application and either approves it immediately or puts it in a pending review status for further follow-up. After your account is approved, you can continue to further steps.

Create MDM profile

When your company is successfully registered, you can create your MDM profile for Microsoft Intune in the Knox portal using the information below. You can create MDM profiles for both Android and Android enterprise in the Knox portal.

- To create an Android MDM profile, select **Device Admin** as the profile type in the Knox Portal.
- To create an Android Enterprise MDM profile, select **Device Owner** as the profile type in the Knox Portal.

For Android device administrator

MDM PROFILE FIELDS	REQUIRED?	VALUES
Profile Name	Yes	Enter a profile name of your choice.
Description	No	Enter text describing the Profile.
MDM Information	Yes	Choose **Server URI not required for my MDM**.
MDM Agent APK	Yes	https://aka.ms/intune_kme
Custom JSON	No	Leave this blank.
Skip Setup wizard	No	Choose this option to skip standard device setup prompts for the end user.
Allow End User to Cancel Enrollment	No	Choose this option to allow users to cancel KME.
Privacy Policy, EULAs and Terms of Service	No	Leave this blank.
Support contact details	Yes	Choose Edit to update your contact details
Associate a Knox license with this profile	No	Leave this option unselected. Enrolling to Intune using KME doesn't require a Knox license.

For Android Enterprise

For step-by-step guidance, see the Samsung's Create Profile instructions.

MDM PROFILE FIELDS	REQUIRED?	VALUES
Profile Name	Yes	Enter a profile name of your choice.
Description	No	Enter text describing the Profile.
Pick your MDM	Yes	Choose Microsoft Intune.
MDM Agent APK	Yes	https://aka.ms/intune_kme_deviceowner
MDM Server URI	No	Leave this blank.
Custom JSON Data	Yes*	{"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN": "Enter Intune enrollment token string"}. Learn how to create an enrollment token for dedicated devices and fully managed devices.
Dual DAR	No	Leave this blank.

MDM PROFILE FIELDS	REQUIRED?	VALUES
QR code for enrollment	No	You can add a QR code to speed enrollment.
System applications	Yes	Choose the **Leave all system apps enabled** option to ensure all apps are enabled and available to the profile. If this option isn't selected, only a limited set of system apps displays in the device's apps tray. Apps such as the Email app remain hidden.
Privacy Policy, EULAs and Terms of Service	No	Leave this blank.
Company Name	Yes	This name will display during device enrollment.

* This field is not required to complete profile creation in the Knox portal. However, Intune does require this field to be filled in so that the profile can successfully enroll the device in Intune.

Add devices

To assign MDM Profiles to devices, supported Samsung Knox devices must be added to the Knox Portal using one of the following methods:

- **Using Samsung-Approved Reseller(s):** Use this method if you're purchasing devices from one of the Samsung-approved resellers. Resellers can auto-upload devices for you when approved. Visit the Samsung Knox Enrollment User Guide to learn how to add resellers.
- **Using the Knox Deployment App (KDA):** Use this method if you have existing devices that need to be enrolled using KME. You can either use Bluetooth or NFC to add devices to the Knox Portal using this method. Visit the Samsung Knox Enrollment User Guide to learn about using the KDA.

Assign an MDM profile to devices

You must assign an MDM profile to added devices in the Knox Portal before they can be enrolled. Visit the Samsung Knox Enrollment User Guide to learn about device configuration.

Configure how end users sign in

For devices enrolled in Intune using KME for Android, you can configure how an end user signs in as follows:

- **Without user name association:** In the Knox Portal under **Device details**, leave the **User ID** and **Password** fields blank for the added devices. This option requires the end user to enter both user name and password when enrolling to Intune.
- **With user name association:** In the Knox Portal under **Device details**, provide a **User ID** (such as a user name for the assigned user or a Device Enrollment Manager account) for the added devices. This option prepopulates the user name and requires the end user to enter a password when enrolling to Intune.

> **NOTE**
> User association only applies to Android device administrator enrollment. When user association is defined, only the associated user can enroll the device using KME. This is true even after a factory reset of the device. When no user association is defined in the Knox portal, any user with a valid Intune license can enroll the device using KME. For Android Enterprise fully managed devices, even if user association is defined, it will not be passed to the device or tie the device to the user.

Distribute devices

After creating and assigning an MDM profile, associating a user name, and identifying the devices as corporate-owned in Intune, you can distribute devices to users.

Still need help? Check out the complete KME User Guide.

Frequently asked questions

- **Device Owner support:** Intune supports enrolling Dedicated and Fully Managed devices by using the KME portal. Other Android enterprise device owner modes will be supported as they become available in Intune.
- **Work profile support:** KME is a corporate device enrollment method and devices enrolled in Android personally-owned work profile ensure work and personal data are separate on personal devices. Device enrollment to personally-owned work profile using KME is not a supported scenario in Intune.
- **Factory reset to enroll to Android enterprise:** If repurposing devices that have already been set up, devices need to be factory reset when enrolling to Android Enterprise.
- **Updates using Google Play account:** Google Play account isn't necessary for enrolling the device to Microsoft Intune. But, for Android device administrator enrollments, future updates to the Intune Company Portal app may require a Google Play account on the device. Google Play account isn't required when enrolling to Google Device Owner.
- **"Password" field is ignored:** If the **password** field is populated in **Device details** in the Knox Portal, it's ignored by the Intune Company Portal app during Android enrollment. The end user must enter a password on the device to complete device enrollment.

Getting support

Learn more about how to get support for Samsung KME.

Android Enterprise security configuration framework

9/23/2022 • 2 minutes to read • Edit Online

The Android Enterprise security configuration framework is a series of recommendations for device compliance and configuration policy settings. These recommendations help you tailor your organization's mobile device security protection to your specific needs.

Security conscious organizations look at ways to ensure corporate data on mobile devices are protected. One method used to protect that data is through device enrollment. Device enrollment helps organizations:

- deploy compliance policies (like PIN strength, jailbreak/root validation, and so on).
- deploy configuration policies (like WIFI, certificates, VPN).
- manage the app lifecycle.

To help you set up a complete security scenario, Microsoft introduced a new taxonomy for security configurations in Windows 10. Intune is using a similar taxonomy for this security configuration framework. They include recommended device compliance and device restriction settings for basic, enhanced, and high security. This taxonomy is explained in the following articles:

1. Android Enterprise framework deployment methodology: A recommended methodology for deploying the security configuration framework.
2. Android device enrollment restrictions: Pre-enrollment device restrictions for Android Enterprise devices.
3. Set app configuration policies for Android Enterprise devices: Configure apps on the devices to disallow personal accounts.
4. Android Enterprise personally-owned/corporate-owned work profile security settings: Specific configuration settings for basic and high security on personally-owned/corporate-owned work profile devices.
5. Android Enterprise fully managed security settings: Specific configuration settings for basic, enhanced, and high security on fully managed devices.

Android Enterprise enrollment modes

Google Android Enterprise includes two enrollment modes. The Android Enterprise security configuration framework provides recommendations for both modes.

- Fully managed devices (device owner): For corporate-owned that are associated with a single user. Such devices are exclusively for work and not personal use.
- Personally-owned work profile and Corporate-owned work profile (profile owner): Typically, for personally owned devices where IT wants a clear boundary between work and personal data. Policies controlled by IT make sure that work data can't be transferred into the personal profile.

Next steps

Android Enterprise framework deployment methodology

Android Enterprise framework deployment methodology

9/23/2022 • 2 minutes to read • Edit Online

Before deploying the framework, Microsoft recommends using a ring methodology for testing validation. Defining deployment rings is generally a one-time event (or at least infrequent). However, IT should revisit these groups to ensure that the sequencing is still correct.

Deployment ring approach

Microsoft recommends the following deployment ring approach for the framework:

DEPLOYMENT RING	TENANT	ASSESSMENT TEAMS	OUTPUT	TIMELINE
Quality Assurance	Pre-production tenant	Mobile capability owners, Security, Risk Assessment, Privacy, UX	Functional scenario validation, draft documentation	0-30 days
Preview	Production tenant	Mobile capability owners, UX	End-user scenario validation, user facing documentation	7-14 days, post Quality Assurance
Production	Production tenant	Mobile capability owners, IT help desk	N/A	7 days to several weeks, post Preview

All policy setting changes should be first applied in a pre-production environment to understand the policy setting implications. After testing is complete, move the changes into production and apply them to a subset of production users, the IT department, and other applicable groups. Finally, the complete the rollout to the rest of the mobile user community. Roll out to production may take longer depending on the changes' scale of impact. If there's no user impact, the change should roll out quickly. If there is user impact, rollout may need to go slower because of the need to communicate changes to the user population.

When testing changes to Android Enterprise devices, be aware of the delivery timing. The status of compliance policies for devices can be monitored. For more information, see Monitor Intune device compliance policies and Monitor device profiles in Microsoft Intune.

Next steps

Android Enterprise device enrollment restrictions

Android Enterprise device enrollment restrictions for personally owned work profile devices

9/23/2022 • 2 minutes to read • Edit Online

Before enrolling Android Enterprise personally owned work profile devices for the Android Enterprise security configuration framework, organizations must configure the appropriate restrictions. These restrictions ensure that users can only enroll

- approved devices.
- a specified number of devices.
- devices with specified platforms.
- devices with specified operating systems.
- devices from specified manufacturers.

For more information on device enrollment restrictions, see Set enrollment restrictions.

Personally owned work profile basic (level 1) security restrictions

For Android Enterprise personally owned work profile basic security (Level 1), the following device restrictions must be implemented:

TYPE	PLATFORM	VERSION	ALLOWS PERSONAL DEVICES
Android Enterprise	Allow	Android 8.0 and later. Microsoft recommends configuring the minimum Android major version to match the supported Android versions for Microsoft apps. OEMs and devices adhering to Android Enterprise recommended requirements must support the current shipping release + one letter upgrade. Currently, Android recommends Android 9.0 and later for knowledge workers. For more information, see Android Enterprise Recommended requirements.	Yes
Android device administrator	Block	All versions	Yes

Personally owned work profile high (level 3) security restrictions

For Android Enterprise personally owned work profile high security (Level 3), the following device restrictions should be implemented:

TYPE	PLATFORM	VERSION	ALLOWS PERSONAL DEVICES
Android Enterprise	Allow	Android 9.0 and later	Yes
Android device administrator	Block	All versions	Yes

Fully managed security restrictions

Ensure the organization supports Android Enterprise fully managed device enrollment by reviewing Enroll the fully managed devices.

Conditional access policies

Organizations can use Azure AD Conditional Access policies to ensure that users can only access work or school content on enrolled Android devices. To do this, you will need a conditional access policy that targets all potential users. Details on creating this policy can be found in Require managed devices for cloud app access with Conditional Access.

Follow the steps in Scenario: Require device enrollment for iOS and Android devices, which ensures that only enrolled mobile devices that are compliant can connect to Microsoft 365 endpoints.

Next steps

Set app configuration policies

Android Enterprise security configuration framework app configuration policies

9/23/2022 • 2 minutes to read • Edit Online

As part of the Android Enterprise security configuration framework, you must properly set app configuration policies for Android Enterprise devices.

Android Enterprise personally-owned/corporate-owned work profile devices are designed to isolate work and personal data from one another. Android Enterprise fully managed devices are designed work or school data only. So, Microsoft apps deployed on these devices must be configured to disallow personal accounts.

Disallow personal accounts for Microsoft apps on Android Enterprise devices

1. Add the apps to Managed Google Play. For more information, see Add Managed Google Play apps to Android Enterprise devices with Intune.
2. Create a policy for each Managed Google Play app as described in Add app configuration policies for managed Android Enterprise devices.
3. Create the following single key in each policy:

KEY	VALUES
com.microsoft.intune.mam.AllowedAccountUPNs	One or more; delimited UPNs. Only account(s) allowed are the managed user account(s) defined by this key. For Intune enrolled devices, the {{userprincipalname}} token may be used to represent the enrolled user account.

Next steps

Apply Android Enterprise personally-owned/corporate-owned work profile security settings or Android Enterprise fully managed security settings.

Android Enterprise personally-owned work profile security configurations

9/23/2022 • 10 minutes to read • Edit Online

As part of the Android Enterprise security configuration framework, apply the following settings for Android Enterprise work profile mobile users. For more information on each policy setting, see Android Enterprise settings to mark devices as compliant or not compliant using Intune and Android Enterprise device settings to allow or restrict features using Intune.

When choosing your settings, be sure to review and categorize usage scenarios. Then, configure users following the guidance for the chosen security level. You can adjust the suggested settings based on the needs of your organization. Make sure to have your security team evaluate the threat environment, risk appetite, and impact to usability.

For personally-owned work profile devices, there are two recommended security configuration frameworks:

- Personally-owned work profile enhanced security (level 2)
- Personally-owned work profile high security (level 3)

> **NOTE**
> Because of the settings available for personally-owned work profile devices, there is no basic security (level 1) offering. The available settings don't justify a difference between level 1 and level 2.

Administrators can incorporate the below configuration levels within their ring deployment methodology for testing and production use by importing the sample Android Enterprise Security Configuration Framework JSON templates with Intune's PowerShell scripts.

Personally-owned work profile enhanced security

Level 2 is the recommended minimum security configuration for personal devices where users access work or school data. This configuration can apply to most mobile users. Some of the controls may impact user experience.

Device compliance

To simplify the table below, only configured settings are listed. Undocumented device compliance settings are not configured.

SECTION	SETTING	VALUE	NOTES
Device Health	Rooted devices	Block	
Device Health	Google Play Services is configured	Require	
Device Health	Up-to-date security provider	Require	

SECTION	SETTING	VALUE	NOTES
Device Health	SafetyNet device attestation	Check basic integrity & certified devices	This setting configures Google's SafetyNet Attestation on end-user devices. Basic integrity validates the integrity of the device. Rooted devices, emulators, virtual devices, and devices with signs of tampering fail basic integrity. Basic integrity and certified devices validates the compatibility of the device with Google's services. Only unmodified devices that have been certified by Google can pass this check.

SECTION	SETTING	VALUE	NOTES
Device Health	Required SafetyNet evaluation type	Hardware-backed key	Hardware backed attestation enhances the existing SafetyNet attestation service check by leveraging a new evaluation type called Hardware Backed, providing a more robust root detection in response to newer types of rooting tools and methods that cannot always be reliably detected by a software only solution. As its name implies, hardware backed attestation leverages a hardware-based component which shipped with devices installed with Android 8.1 and later. Devices that were upgraded from an older version of Android to Android 8.1 are unlikely to have the hardware-based components necessary for hardware backed attestation. While this setting should be widely supported starting with devices that shipped with Android 8.1, Microsoft strongly recommends testing devices individually before enabling this policy setting broadly.
Device Properties	Minimum OS version	Format: Major.Minor Example: 9.0	Microsoft recommends configuring the minimum Android major version to match the supported Android versions for Microsoft apps. OEMs and devices adhering to Android Enterprise recommended requirements must support the current shipping release + one letter upgrade. Currently, Android recommends Android 9.0 and later for knowledge workers. For Android's latest recommendations, see Android Enterprise Recommended requirements.

SECTION	SETTING	VALUE	NOTES
System Security	Require a password to unlock mobile devices	Require	
System Security	Required password type	Numeric Complex	Organizations may need to update this setting to match their password policy.
System Security	Minimum password length	6	Organizations may need to update this setting to match their password policy.
System Security	Maximum minutes of inactivity before password is required	5	Organizations may need to update this setting to match their password policy.
System Security	Encryption of data storage on device	Require	
System Security	Block apps from unknown sources	Block	
System Security	Company Portal app runtime integrity	Require	
System Security	Block USB debugging on device	Block	While this setting blocks debugging using a USB device, it also disables the ability to gather logs which may be useful in troubleshooting purposes.
System Security	Minimum security patch level	Not configured	Android devices can receive monthly security patches, but the release is dependent on OEMs and/or carriers. Organizations should ensure that deployed Android devices do receive security updates before implementing this setting. For the latest patch releases, see Android Security Bulletins.
Actions for noncompliance	Mark device noncompliant	Immediately	By default, the policy is configured to mark the device as noncompliant. Additional actions are available. For more information, see Configure actions for noncompliant devices in Intune.

Device restrictions

To simplify the table below, only configured settings are listed. Undocumented device restrictions are not configured.

SECTION	SETTING	VALUE	NOTES
Work profile settings	Copy and paste between work and personal profiles	Block	
Work profile settings	Data sharing between work and personal profiles	Apps in work profile can handle sharing request from personal profile	
Work profile settings	Work profile notifications while device locked	Not configured	Blocking this setting ensures sensitive data is not exposed in work profile notifications, which may impact usability.
Work profile settings	Default app permissions	Device Default	Admins need to review and adjust the permissions granted by apps they are deploying.
Work profile settings	Add and remove accounts	Block	
Work profile settings	Contact sharing via Bluetooth	Enable	By default, access to work contacts is not available on other devices, like automobiles via Bluetooth integration. Enabling this setting improves hands free user experiences. However, the Bluetooth device may cache the contacts upon first connection. Organizations should consider balancing the usability scenarios with data protection concerns when implementing this setting.
Work profile settings	Screen capture	Block	
Work profile settings	Search work contacts from personal profile	Not configured	Blocking users from accessing work contacts from the personal profile may impact certain usability scenarios like text messaging and dialer experiences within the personal profile. Organizations should consider balancing the usability scenarios with data protection concerns when implementing this setting.
Work profile settings	Allow widgets from work profile apps	Enable	

SECTION	SETTING	VALUE	NOTES
Work profile settings	Require Work Profile Password	Require	
Work profile settings	Minimum password length	6	Organizations may need to update this setting to match their password policy.
Work profile settings	Maximum minutes of inactivity until work profile locks	5	Organizations may need to update this setting to match their password policy.
Work profile settings	Number of sign-in failures before wiping the work profile	10	Organizations may need to update this setting to match their password policy.
Work profile settings	Password expiration (days)	Not configured	Organizations may need to update this setting to match their password policy.
Work profile settings	Required password type	Numeric complex	
Work profile settings	Prevent reuse of previous passwords	Not configured	Organizations may need to update this setting to match their password policy.
Device password	Minimum password length	6	Organizations may need to update this setting to match their password policy.
Device password	Maximum minutes of inactivity until screen locks	5	Organizations may need to update this setting to match their password policy.
Device password	Number of sign-in failures before wiping device	10	This setting triggers a work profile wipe, and not a wipe of the device.
Device password	Password expiration (days)	Not configured	Organizations may need to update this setting to match their password policy.
Device password	Required password type	Numeric complex	
Device password	Prevent reuse of previous passwords	Not configured	Organizations may need to update this setting to match their password policy.

SECTION	SETTING	VALUE	NOTES
System Security	Threat scan on apps	Require	This setting ensures that Google's Verify Apps scan is turned on for end user devices. If configured, the end user will be blocked from access until they turn on Google's app scanning on their Android device.
System Security	Prevent app installations from unknown sources in the personal profile	Block	

> **NOTE**
> When a personally-owned work profile is enabled, "One Lock" is configured by default to combine device and work profile passcodes. One Lock may be disabled to separate work profile and device passcodes if necessary, under work profile settings.

Personally-owned work profile high security

Level 3 is the recommended configuration for devices used by users or groups who are uniquely high risk. For example, users who handle highly sensitive data where unauthorized disclosure causes considerable material loss. An organization likely to be targeted by well-funded and sophisticated adversaries merit the additional constraints described below. This configuration expands upon the configuration in Level 2 by:

- implementing mobile threat defense or Microsoft Defender for Endpoint.
- restricting personally-owned work profile data scenarios.
- enacting stronger password policies.

The policy settings enforced in level 3 include all the policy settings recommended for level 1. However, the settings listed below include only those that have been added or changed. These settings may have a slightly higher impact to users or applications. They enforce a level of security more appropriate for risks facing users with access to sensitive information on mobile devices.

Device compliance

SECTION	SETTING	VALUE	NOTES
Microsoft Defender for Endpoint	Require the device to be at or under the machine risk score	Clear	This setting requires Microsoft Defender for Endpoint. For more information, see Enforce compliance for Microsoft Defender for Endpoint with Conditional Access in Intune. Customers should consider implementing Microsoft Defender for Endpoint or a mobile threat defense solution. It is not necessary to deploy both.

SECTION	SETTING	VALUE	NOTES
Device Health	Require the device to be at or under the Device Threat Level	Secured	This setting requires a mobile threat defense product. For more information, see Mobile Threat Defense for enrolled devices. Customers should consider implementing Microsoft Defender for Endpoint or a mobile threat defense solution. It is not necessary to deploy both.
Device Properties	Minimum OS version	Format: Major.Minor Example: 11.0	Microsoft recommends configuring the minimum Android major version to match the supported Android versions for Microsoft apps. OEMs and devices adhering to Android Enterprise recommended requirements must support the current shipping release + one letter upgrade. Currently, Android recommends Android 9.0 and later for knowledge workers. See Android Enterprise Recommended requirements for Android's latest recommendations
System Security	Number of days until password expires	365	Organizations may need to update this setting to match their password policy.
System Security	Number of previous passwords to prevent use	5	Organizations may need to update this setting to match their password policy.

Device restrictions

SECTION	SETTING	VALUE	NOTES
Work profile settings	Work profile notifications while device locked	Block	Blocking this setting ensures sensitive data is not exposed in work profile notifications, which may impact usability.

SECTION	SETTING	VALUE	NOTES
Work profile settings	Contact sharing via Bluetooth	Not configured	By default, access to work contacts is not available on other devices, like automobiles via Bluetooth integration. Enabling this setting improves hands free user experiences. However, the Bluetooth device may cache the contacts upon first connection. Organizations should consider balancing the usability scenarios with data protection concerns when implementing this setting.
Work profile settings	Search work contacts from personal profile	Block	Blocking users from accessing work contacts from the personal profile may impact certain usability scenarios like text messaging and dialer experiences within the personal profile. Organizations should consider balancing the usability scenarios with data protection concerns when implementing this setting.
Work profile settings	Allow widgets from work profile apps	Not configured	
Work profile settings	Number of sign-in failures before wiping the work profile	5	Organizations may need to update this setting to match their password policy.
Work profile settings	Password expiration (days)	365	Organizations may need to update this setting to match their password policy.
Work profile settings	Prevent reuse of previous passwords	5	Organizations may need to update this setting to match their password policy.
Work profile settings	Smart Lock and other trust agents	Block	
Device password	Number of sign-in failures before wiping device	5	This setting triggers a work profile wipe and not a wipe of the device.

SECTION	SETTING	VALUE	NOTES
Device password	Password expiration (days)	365	Organizations may need to update this setting to match their password policy.
Device password	Prevent reuse of previous passwords	5	Organizations may need to update this setting to match their password policy.

Next steps

Administrators can incorporate the above configuration levels within their ring deployment methodology for testing and production use by importing the sample Android Enterprise Security Configuration Framework JSON templates with Intune's PowerShell scripts.

Android Enterprise fully managed security configurations

9/23/2022 • 8 minutes to read • Edit Online

As part of the Android Enterprise security configuration framework, apply the following settings for Android Enterprise fully managed mobile users. For more information on each policy setting, see Android Enterprise device owner settings to mark devices as compliant or not compliant using Intune and Android Enterprise device settings to allow or restrict features using Intune.

When choosing your settings, be sure to review and categorize usage scenarios. Then, configure users following the guidance for the chosen security level. You can adjust the suggested settings based on the needs of your organization. Make sure to have your security team evaluate the threat environment, risk appetite, and impact to usability.

For corporate owned fully-managed devices, there are three recommended security configuration frameworks:

- Fully managed basic security (level 1)
- Fully managed enhanced security (level 2)
- Fully managed high security (level 3)

Administrators can incorporate the below configuration levels within their ring deployment methodology for testing and production use by importing the sample Android Enterprise Security Configuration Framework JSON templates with Intune's PowerShell scripts.

Fully managed basic security

Level 1 is the recommended minimum security configuration for mobile devices owned by the organization.

The policies in level 1 enforce a reasonable data access level while minimizing the impact to users. This is done by enforcing password policies, a minimum operating system version, SafetyNet Device attestation, and disabling certain device functions (like USB file transfers).

Device compliance

To simplify the table below, only configured settings are listed. Undocumented device compliance settings are not configured.

SECTION	SETTING	VALUE	NOTES

SECTION	SETTING	VALUE	NOTES
Device Health	SafetyNet device attestation	Check basic integrity & certified devices	This setting configures Google's SafetyNet Attestation on end-user devices. Basic integrity validates the integrity of the device. Rooted devices, emulators, virtual devices, and devices with signs of tampering fail basic integrity. Basic integrity and certified devices validates the compatibility of the device with Google's services. Only unmodified devices that have been certified by Google can pass this check.
Device Properties	Minimum OS version	Format: Major.Minor Example: 9.0	Microsoft recommends configuring the minimum Android major version to match the supported Android versions for Microsoft apps. OEMs and devices adhering to Android Enterprise recommended requirements must support the current shipping release + one letter upgrade. Currently, Android recommends Android 9.0 and later for knowledge workers. For Android's latest recommendations, see Android Enterprise Recommended requirements.
Device Properties	Minimum security patch level	Not configured	Android devices can receive monthly security patches, but the release is dependent on OEMs and/or carriers. Organizations should ensure that deployed Android devices do receive security updates before implementing this setting. For the latest patch releases, see Android Security Bulletins.
System Security	Require a password to unlock mobile devices	Require	
System Security	Required password type	Numeric Complex	Organizations may need to update this setting to match their password policy.

SECTION	SETTING	VALUE	NOTES
System Security	Minimum password length	6	Organizations may need to update this setting to match their password policy.
System Security	Maximum minutes of inactivity before password is required	5	Organizations may need to update this setting to match their password policy.
System Security	Encryption of data storage on device	Require	
System Security	Intune app runtime integrity	Require	
Actions for noncompliance	Mark device noncompliant	Immediately	By default, the policy is configured to mark the device as noncompliant. Additional actions are available. For more information, see Configure actions for noncompliant devices in Intune.

Device restrictions

To simplify the table below, only configured settings are listed. Undocumented device restrictions are not configured.

SECTION	SETTING	VALUE	NOTES
General	Default permission policy	Device Default	
General	Factory reset	Block	
General	USB file transfer	Block	
General	External media	Block	
General	Data sharing between work and personal profiles	Device Default	
System security	Threat scan on apps	Require	
Device experience	Enrollment profile type	Fully managed	

SECTION	SETTING	VALUE	NOTES
Device experience	Make Microsoft Launcher the default launcher	Not configured	Organizations may choose to implement Microsoft Launcher to ensure a consistent home screen experience on Fully managed devices. For more information, see How to Setup Microsoft Launcher on Android Enterprise Fully Managed Devices with Intune
Device password	Required password type	Numeric Complex	
Device password	Minimum password length	6	
Device password	Number of sign-in failures before wiping device	10	
Power settings	Time to lock screen	5	
Users and Accounts	User can configure credentials	Block	
Applications	Allow access to all apps in Google Play store	Not configured	By default, users cannot install personal apps from the Google Play Store on fully managed devices. If organizations would like to allow fully managed devices to be utilized for personal use, consider changing this setting.
Applications	App auto-updates	Wi-Fi only	Organizations should adjust this setting as necessary as data plan charges may occur if app updates occur over the cellular network.
Work profile password	Required password type	Numeric Complex	Organizations may need to update this setting to match their password policy.
Work profile password	Minimum password length	6	Organizations may need to update this setting to match their password policy.
Work profile password	Number of sign-in failures before wiping device	10	Organizations may need to update this setting to match their password policy.

Fully managed enhanced security

Level 2 is the recommended configuration for company owned devices where users access more sensitive information. These devices are a natural target in enterprises today. These settings don't assume a large staff of highly skilled security personnel. Therefore, they should be accessible to most enterprise organizations. This configuration expands upon the configuration in Level 1 by enacting stronger password policies, and disabling user/account capabilities.

The level 2 settings include all the policy settings recommended for level 1. However, the settings listed below include only those settings that have been added or changed. These settings may have a slightly higher impact to users or to applications. They enforce a level of security more appropriate for risks facing users with access to sensitive information on mobile devices.

Device compliance

SECTION	SETTING	VALUE	NOTES
System Security	Number of days until password expires	365	Organizations may need to update this setting to match their password policy.
System Security	Number of passwords required before user can reuse a password	5	Organizations may need to update this setting to match their password policy.

Device restrictions

SECTION	SETTING	VALUE	NOTES
General	Factory reset protection emails	Google account email addresses	
General	List of email addresses (Google account email addresses option only)	example@gmail.com	Manually update this policy to specify the Google email addresses of device administrators that can unlock the devices after they are wiped.
Device password	Number of days until password expires	365	Organizations may need to update this setting to match their password policy.
Device password	Number of passwords required before user can reuse a password	5	Organizations may need to update this setting to match their password policy.
Device password	Number of sign-in failures before wiping device	5	
Users and Accounts	Add new users	Block	
Users and Accounts	User removal	Block	
Users and Accounts	Personal Google Accounts	Block	

SECTION	SETTING	VALUE	NOTES
Work profile password	Number of passwords required before user can reuse a password	5	Organizations may need to update this setting to match their password policy.

Fully managed high security

Level 3 is the recommended configuration for both:

- organizations with large and sophisticated security organizations.
- specific users and groups who will be uniquely targeted by adversaries. Such organizations are typically targeted by well-funded and sophisticated adversaries. Therefore, they merit the additional constraints and controls listed below.

This configuration expands upon Level 2 by:

- ensuring that the device is compliant by enforcing the most secure Microsoft Defender for Endpoint or mobile threat defense level.
- increasing the minimum operating system version.
- enforcing additional device restrictions (like disabling unredacted notifications on lock screen).
- requiring apps to always be up-to-date.

The policy settings enforced in level 3 include all the policy settings recommended for level 2. The settings listed below include only those that have been added or changed. These settings may have significant impact to users or applications. They enforce a level of security more appropriate for risks facing targeted organizations.

Device compliance

SECTION	SETTING	VALUE	NOTES
Microsoft Defender for Endpoint	Require the device to be at or under the machine risk score	Clear	This setting requires Microsoft Defender for Endpoint. For more information, see Enforce compliance for Microsoft Defender for Endpoint with Conditional Access in Intune. Customers should consider implementing Microsoft Defender for Endpoint or a mobile threat defense solution. It is not necessary to deploy both.

SECTION	SETTING	VALUE	NOTES
Device Health	Require the device to be at or under the Device Threat Level	Secured	This setting requires a mobile threat defense product. For more information, see Mobile Threat Defense for enrolled devices. Customers should consider implementing Microsoft Defender for Endpoint or a mobile threat defense solution. It is not necessary to deploy both.
Device Properties	Minimum OS version	Format: Major.Minor Example: 11.0	Microsoft recommends configuring the minimum Android major version to match the supported Android versions for Microsoft apps. OEMs and devices adhering to Android Enterprise recommended requirements must support the current shipping release + one letter upgrade. Currently, Android recommends Android 9.0 and later for knowledge workers. See Android Enterprise Recommended requirements for Android's latest recommendations

Device restrictions

SECTION	SETTING	VALUE	NOTES
General	Date and Time changes	Block	
General	Tethering and access to hotspots	Block	
General	Beam data using NFC	Block	
General	Search work contacts and display work contact caller-id in personal profile	Block	
Device password	Disabled lock screen features	Trust Agents, Unredacted Notifications	
Applications	App auto-updates	Always	Organizations should adjust this setting as necessary as data plan charges may occur if app updates occur over the cellular network.

SECTION	SETTING	VALUE	NOTES
Work profile password	Number of sign-in failures before wiping device	5	Organizations may need to update this setting to match their password policy.

Next steps

Administrators can incorporate the above configuration levels within their ring deployment methodology for testing and production use by importing the sample Android Enterprise Security Configuration Framework JSON templates with Intune's PowerShell scripts.

Enroll iOS/iPadOS devices in Intune

9/23/2022 • 4 minutes to read • Edit Online

Intune enables mobile device management (MDM) of iPads and iPhones to give users secure access to company email, data, and apps.

As an Intune admin, you can set up enrollment for iOS/iPadOS and iPadOS devices to access company resources. You can let users enroll personally-owned devices, known as "bring your own device" (BYOD) enrollment. You can also set up enrollment of company-owned devices.

Prerequisites for iOS/iPadOS enrollment

Before you can enable iOS/iPadOS devices, complete the following steps:

- Make sure your devices are supported.
- Set up Intune - These steps set up your Intune infrastructure. In particular, device enrollment requires that you set your MDM authority.
- Get an Apple MDM Push certificate - Apple requires a certificate to enable management of iOS/iPadOS and macOS devices.

User-owned iOS/iPadOS and iPadOS devices (BYOD)

You can let users enroll their personal devices for Intune management, know as "bring your own device" or BYOD. There are three options for enrolling users:

- App Protection Policies give you the lightest BYOD experience, providing management at an app level only. However, if you want to also secure the device with a 6-digit complex PIN, you can use these policies along with User Enrollment.
- Device Enrollment is what you may think of as typical BYOD enrollment. It provides admins with a wide range of management options.
- User Enrollment is a more streamlined enrollment process that provides admins with a subset of device management options. This feature is currently in preview.

After you've completed the prerequisites and assigned user licenses, users can download the Intune Company Portal app from the App Store, and follow enrollment instructions in the app. You can customize the Company Portal privacy statement on iOS/iPadOS devices as explained in How to customize the Intune Company Portal apps, Company Portal website, and Intune app.

Company-owned iOS/iPadOS devices

For organizations that buy devices for their users, Intune supports the following iOS/iPadOS company-owned device enrollment methods:

- Apple's Automated Device Enrollment (ADE)
- Apple School Manager
- Apple Configurator Setup Assistant enrollment
- Apple Configurator direct enrollment

You can also enroll company-owned iOS/iPadOS devices with a device enrollment manager account.

Automated Device Enrollment

Organizations can purchase iOS/iPadOS devices through Apple's Automated Device Enrollment (ADE). ADE lets you deploy an enrollment profile "over the air" to bring devices into management. For more information, see Automatically enroll iOS/iPadOS devices with Apple's Automated Device Enrollment.

User enrollment

User Enrollment gives admins a subset of management options compared to other enrollment methods. For more information, see User Enrollment supported actions, passwords, and other options and Set up iOS/iPadOS and iPadOS User Enrollment.

Apple School Manager

Apple School Manager is a device purchase and enrollment program for schools. Like ADE, you can deploy a profile to enroll devices in management. Learn more about Apple School Manager.

Apple Configurator

You can enroll iOS/iPadOS devices with Apple Configurator running on a Mac computer. To prepare devices, you USB-connect them and install an enrollment profile. You can enroll devices with Apple Configurator in two ways:

- Setup Assistant enrollment - Wipes the device, prepares it to run Setup Assistant, and installs the company's policies for the device's new user.
- Direct enrollment - Doesn't wipe the device and enrolls the device with a predefined policy. This method is for devices with no user affinity.

Learn more about Apple Configurator enrollment.

Use the Company Portal on ADE-enrolled or Apple Configurator-enrolled devices

Devices configured with user affinity can install and run the Company Portal app to download apps and manage devices. After users receive their devices, they must complete a number of additional steps to complete the Setup Assistant and install the Company Portal app.

User affinity is required to support the following:

- App Protection Policy (APP) apps
- Conditional Access to email and company data
- Company Portal app

How users enroll corporate-owned iOS/iPadOS devices with user affinity

1. When users turn on their device, they are prompted to complete the Setup Assistant.
2. After completing setup, users are prompted for an Apple ID. They must provide an Apple ID to allow the device to install Company Portal.
3. The iOS/iPadOS device automatically installs the Company Portal app from the App Store.
4. Users should launch the Company Portal app and sign in using the credentials (like the unique personal name or UPN) that are associated with their subscription in Intune.
5. After logging in, enrollment is complete. Users can now use this device with the full set of capabilities.

About corporate-owned managed devices with no user affinity

The Company Portal app is designed for users who have corporate credentials, and require access to personalized corporate resources (like email). On devices configured with no user affinity, the Company Portal

app isn't needed. Devices that are enrolled with no user affinity aren't intended to have a dedicated user sign in. Kiosk, point of sale (POS), or shared-utility devices are typical use cases for devices that are enrolled with no user affinity.

In some situations, you might want to associate a primary user on devices enrolled without user affinity. To do this, add the Company Portal app using an app configuration policy. For more information, see Configure the Company Portal app to support iOS and iPadOS devices enrolled with Automated Device Enrollment.

If user affinity is required, be sure that the device's enrollment profile has **User Affinity** selected before enrolling the device. To change the affinity status on a device, you must retire the device and reenroll it.

See also

Troubleshooting iOS/iPadOS device enrollment problems in Microsoft Intune

Automatically enroll iOS/iPadOS devices by using Apple's Automated Device Enrollment

9/23/2022 • 30 minutes to read • Edit Online

You can set up Intune to enroll iOS/iPadOS devices purchased through Apple's Automated Device Enrollment (ADE). Automated Device Enrollment lets you enroll large numbers of devices without ever touching them. Devices like iPhones, iPads, and MacBooks can be shipped directly to users. When a user turns on the device, Setup Assistant, which includes the typical out-of-box-experience for Apple products, runs with preconfigured settings and the device enrolls into management.

To enable ADE, you use the Intune portal and either the Apple Business Manager (ABM) portal or the Apple School Manager (ASM) portal. In either Apple portal, you need a list of serial numbers or a purchase order so you can assign devices to Intune for management. You create ADE enrollment profiles in Intune. These profiles contain settings that are applied to devices during enrollment. ADE can't be used with a Device Enrollment Manager account.

> **NOTE**
> ADE sets device configurations that can't necessarily be removed by end users. Therefore, before ADE is used, the device must be wiped to return it to an out-of-box (new) state. For more information, see Deployment guide: Enroll iOS and iPadOS devices.

If you experience sync problems during the enrollment process, you can look for solutions at Troubleshoot iOS/iPadOS device enrollment problems.

Deploy Company Portal app

> **IMPORTANT**
> We don't recommend using the App Store version of the Company Portal app because it isn't compatible with automated device enrollment and doesn't provide the automatic updates and availability like deployment does.

Deploying the Intune Company Portal app through Intune is the best way to provide the app to users and the only way to:

- Ensure all ADE devices, including already-enrolled ones, receive the app.
- Enable automatic app updates for Company Portal on ADE devices.

Deploy the app as a required, VPP app with device licensing. For information about how to sync, assign, and manage a VPP app, see assign a volume-purchased app.

To enable automatic app updates for Company Portal, go to your app token settings in the admin center and change **Automatic app updates** to **Yes**. See Upload an Apple VPP or Apple Business Manager location token for the steps to access your token settings. If you don't enable automatic updates, the device user will need to manually check for them on their own.

Device staging is used to transition a device without user affinity, to a device with user affinity. To stage a device, set up VPP deployment as described earlier in this section. Then configure and deploy an app configuration policy. Make sure the policy only targets those ADE devices without user affinity.

IMPORTANT

During initial enrollment, Intune automatically pushes the app configuration policy settings for devices enrolled with Setup Assistant with modern authentication, configured in Configure the Company Portal app to support iOS and iPadOS devices enrolled with Automated Device Enrollment, when the enrollment profile setting **Install Company Portal** is set to yes. This configuration should not be deployed manually to users because it will cause a conflict with the configuration sent during the initial enrollment. If both are deployed, Intune will incorrectly prompt device users to sign in to Company Portal and download a management profile they've already installed.

What is supervised mode?

Apple introduced supervised mode in iOS/iPadOS 5. An iOS/iPadOS device in supervised mode provides more management control, like blocking of screen captures and blocking of the installation of apps from App Store. So it's especially useful for corporate-owned devices. Intune supports configuring devices for supervised mode as part of ADE.

Support for unsupervised ADE devices was deprecated in iOS/iPadOS 11. In iOS/iPadOS 11 and later, ADE-configured devices should always be supervised. The ADE *is_supervised* flag will be ignored in iOS/iPadOS 13.0 and later. All iOS/iPadOS devices with version 13.0 and later are automatically supervised when enrolled with Automated Device Enrollment.

Prerequisites

- Devices purchased in Apple's ADE
- Mobile device management (MDM) authority
- An Apple MDM push certificate

Supported volume

- Maximum enrollment profiles per token: 1,000.
- Maximum Automated Device Enrollment devices per profile: Same as the maximum number of devices per token (200,000 devices per token).
- Maximum Automated Device Enrollment tokens per Intune account: 2,000.
- Maximum Automated Device Enrollment devices per token: We recommend that you don't exceed 200,000 devices per token. Otherwise you might have sync problems. If you have more than 200,000 devices, split the devices into multiple ADE tokens.
    - About 3,000 devices per minute sync from ABM/ASM over to Intune. We recommend that you wait to manually sync again from the admin console until enough time has passed for all of the devices to sync over (total number of devices/3,000 devices per minute).

Get an Apple Automated Device Enrollment token

Before you can enroll iOS/iPadOS devices with ADE, you need an ADE token (.p7m) file from Apple. This token lets Intune sync information about ADE devices that your corporation owns. It also allows Intune to upload enrollment profiles to Apple and to assign devices to those profiles.

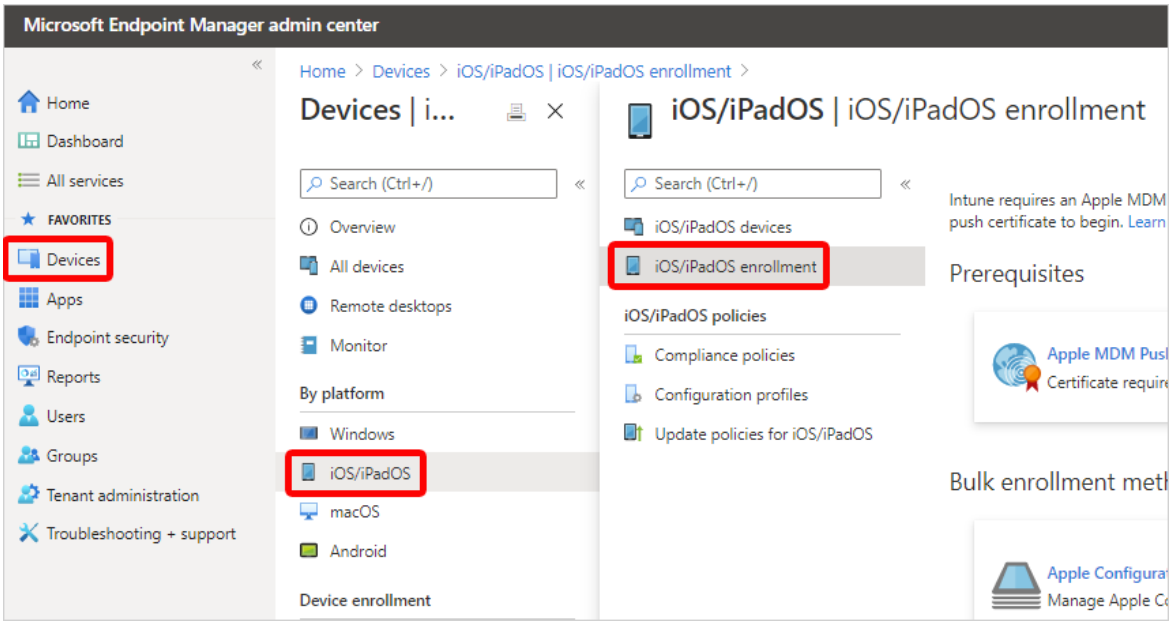
You use the Apple Business Manager (ABM) or Apple School Manager (ASM) portal to create a token. You also use the ABM or ASM portal to assign devices to Intune for management.

NOTE

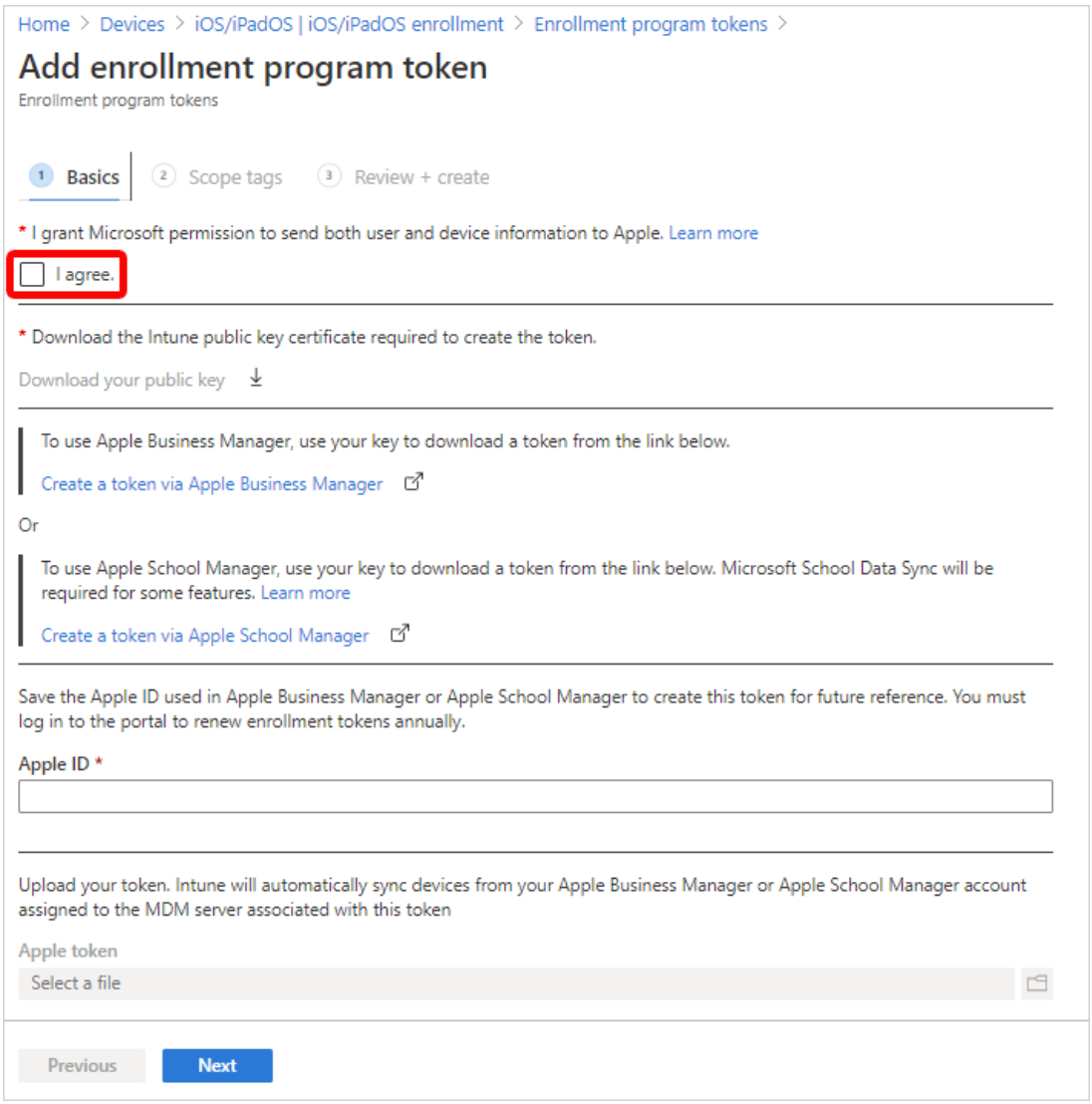
You can use either the ABM portal or the ASM portal to enable ADE. The rest of this article refers to the ABM portal, but the steps are the same for both portals.

Step 1: Download the Intune public key certificate

1. In Microsoft Endpoint Manager admin center, select **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment**:



2. Select **Enrollment Program Tokens** > **Add**.
3. On the **Basics** tab:
   a. Select **I agree** to give permission to Microsoft to send user and device information to Apple:



b. Select **Download the Intune public key certificate required to create the token**. This step downloads and saves the encryption key (.pem) file locally. The .pem file is used to request a trust-relationship certificate from the Apple Business Manager portal.

   You'll upload this .pem file in Apple Business Manager in Step 2: Go to the Apple Business Manager portal (in this article).

c. Keep this web browser tab and page open. If you close the tab:

   - The certificate you downloaded is invalidated.
   - You have to repeat steps.
   - On the **Review + create** tab, the **Create** button isn't available, and you can't complete this procedure.

Step 2: Go to the Apple Business Manager portal

Use the Apple Business Manager portal to create and renew your ADE token (MDM server). This token is added to Intune and communicates between Intune and Apple.

> **NOTE**
> The following steps describe what you need to do in Apple Business Manager. For the specific steps, refer to Apple's documentation. Apple Business Manager User Guide (on Apple's website) might be helpful.

Download the Apple token

1. In Apple Business Manager, sign in with your company's Apple ID.

2. In this portal, complete the following steps.

   - In settings, all tokens are shown. Add an MDM server, and upload the public key certificate (.pem file) that you downloaded from Intune in Step 1: Download the Intune public key certificate (in this article).

     Use the server name to identify the mobile device management (MDM) server. It isn't the name or URL of the Microsoft Intune service.

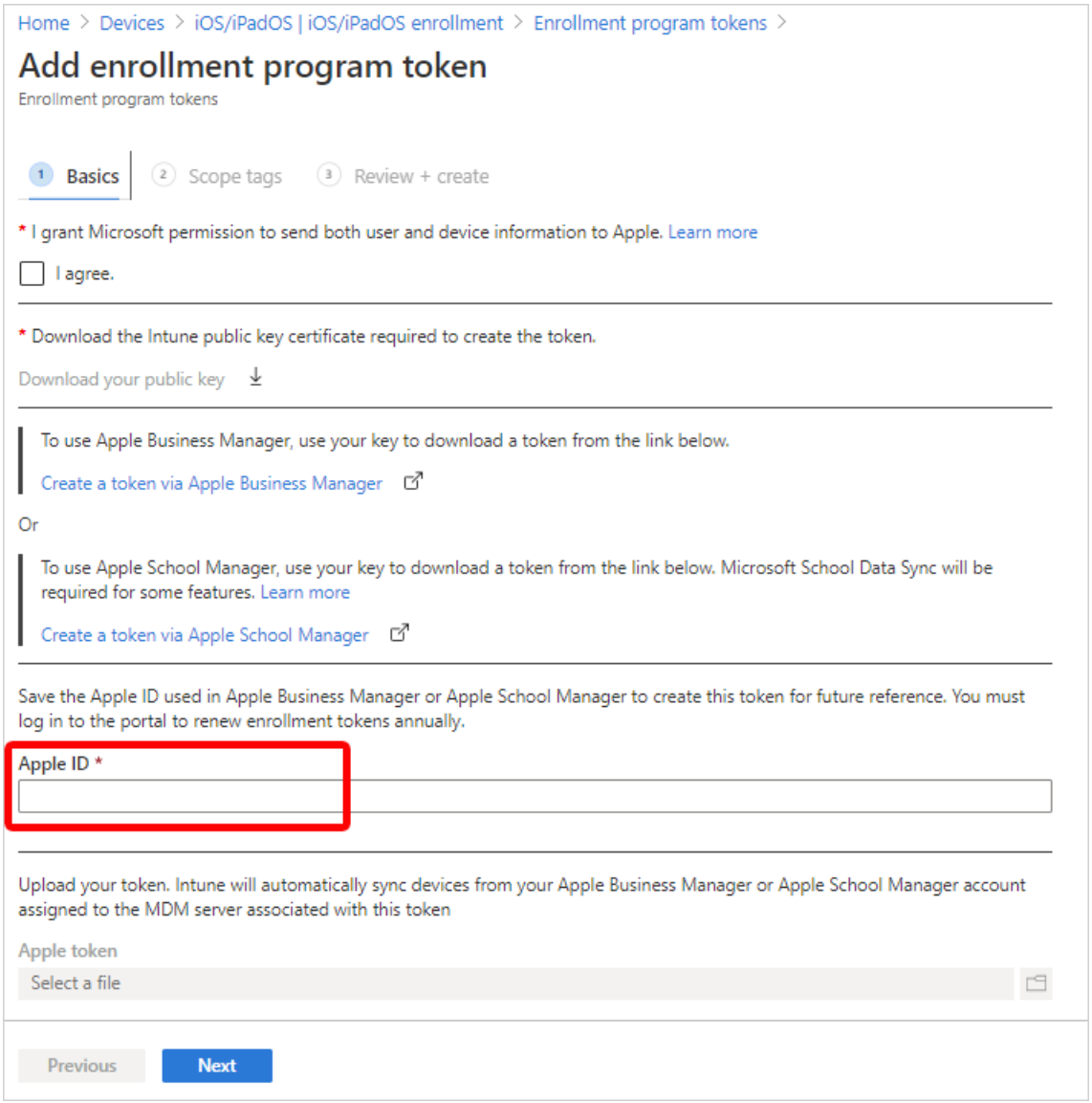
   - After you save the MDM server, select it, and then download the token (.p7m file). You'll upload this .p7m token in Intune in Step 4: Upload your token and finish (in this article).

Assign devices to the Apple token (MDM server)

1. In Apple Business Manager > **Devices**, select the devices you want to assign to this token. You can sort by various device properties, like serial number. You can also select multiple devices simultaneously.
2. Edit device management, and select the MDM server you just added. This step assigns devices to the token.

Step 3: Save the Apple ID

1. In your web browser, go back to the **Add enrollment program token** page in Intune. You should have kept this page open, as noted in Step 1: Download the Intune public key certificate (in this article).
2. In **Apple ID**, enter your ID. This step saves the ID. The ID can be used in the future.



Step 4: Upload your token and finish

1. In **Apple token**, browse to the .p7m certificate file, and then select **Open**.

You downloaded this .p7m token in Step 2: Go to the Apple Business Manager portal.

2. Select **Next**.
3. (Optional.) If you want to apply scope tags to this ADE token, click **Select scope tags**, and then select existing scope tags. Scope tags applied to a token are inherited by profiles and ADE enrolled devices added to the token. The devices that are being referred to are the devices that have synced over from ABM/ASM, and are enrolled through Automated Device Enrollment and show up within the specific token.

   For more information on scope tags, see Use role-based access control (RBAC) and scope tags for distributed IT.

   Select **Next**.
4. On the **Review + create** tab, select **Create**.

With the push certificate, Intune can enroll and manage iOS/iPadOS devices by pushing policies to enrolled mobile devices. Intune automatically synchronizes with Apple to access your enrollment program account.

Create an Apple enrollment profile

Now that you've installed your token, you can create an enrollment profile for ADE devices. A device enrollment profile defines the settings applied to a group of devices during enrollment. There's a limit of 1,000 enrollment profiles per ADE token.

> **NOTE**
> Devices will be blocked if there aren't enough Company Portal licenses for a VPP token or if the token is expired. Intune alerts you when a token is about to expire or licenses are running low.

1. In Microsoft Endpoint Manager admin center, select **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment program tokens**.
2. Select a token, and then select **Profiles**.
3. Select **Create profile** > **iOS/iPadOS**.
4. For **Basics**, give the profile a **Name** and **Description** for administrative purposes. Users don't see these details.
5. Select **Next**.

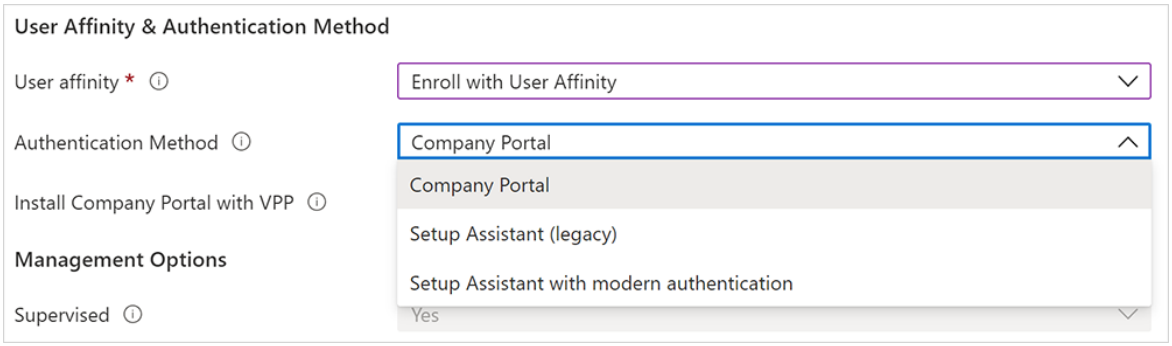
> **IMPORTANT**
> If you make changes to existing enrollment profile settings, the new changes will not take effect on assigned devices until devices are reset back to factory settings and reactivated. Reactivation occurs when the Remote Management Payload is received on ADE devices. Renaming the device name template is the only change you can make that doesn't require a factory reset.

6. In the **User Affinity** list, select an option that determines whether devices with this profile must enroll with or without an assigned user.

   - **Enroll with User Affinity**. Select this option for devices that belong to users who want to use Company Portal for services like installing apps.
   - **Enroll without User Affinity**. Select this option for devices that aren't affiliated with a single user. Use this option for devices that don't access local user data. This option is typically used for kiosk, point of sale (POS), or shared-utility devices.

In some situations, you might want to associate a primary user on devices enrolled without user affinity. To do this task, you can send the `IntuneUDAUserlessDevice` key to the Company Portal app in an app configuration policy for managed devices. The first user that signs in to the Company Portal app is established as the primary user. If the first user signs out and a second user signs in, the first user remains the primary user of the device. For more information, see Configure the Company Portal app to support iOS and iPadOS ADE devices.

7. If you selected **Enroll with User Affinity** for the **User Affinity** field, you now have the option to choose the authentication method to use when authenticating users. For **Authentication method**, select one of the following options:



- **Company Portal**: Authenticate with the Company Portal app if you want to:
  - Use multifactor authentication.
  - Prompt users to change their passwords when they first sign in.
  - Prompt users to reset their expired passwords during enrollment.

  These features aren't supported when you authenticate by using Apple Setup Assistant.

- **Setup Assistant (legacy)**: Use the legacy Setup Assistant if you want users to experience the typical, out-of-box-experience for Apple products. This installs standard preconfigured settings when the device enrolls with Intune management. If you're using Active Directory Federation Services and you're using Setup Assistant to authenticate, a WS-Trust 1.3 Username/Mixed endpoint is required. Learn more.

- **Setup Assistant with modern authentication**: Devices running iOS/iPadOS 13.0 and later can use this method. Older iOS/iPadOS devices in this profile will fall back to using the **Setup Assistant (legacy)** process.

  > **NOTE**
  > MFA won't work for Setup Assistant with modern authentication if you're using a 3rd party MFA provider to present the MFA screen during enrollment. Only the Azure AD MFA screen works during enrollment. For the latest support updates about custom controls for MFA, see Upcoming changes to Custom Controls.

  This method provides the same security as Company Portal authentication but avoids the issue of leaving end users with a device they can't use until the Company Portal installs.

  The Company Portal will be installed without user interaction (the user won't see the **Install Company Portal** option) in both of the following situations:

  - If you use the **Install Company Portal with VPP** option below (recommended).
  - If the end user sets up their Apple ID account during Setup Assistant.

  In both of these situations, the Company Portal will be a required app on the device. Also, when the end user gets to the home screen, the correct app configuration policy will automatically be

applied to the device.

Don't send a separate app configuration policy to the Company Portal for iOS/iPadOS devices after enrolling with Setup Assistant with modern authentication. Doing so will result in an error.

If you don't use the VPP option, the user must supply an Apple ID to install the Company Portal (either during Setup Assistant or when Intune tries to install the Company Portal).

If a conditional access policy that requires multi-factor authentication (MFA) applies at enrollment or during Company Portal sign in, then MFA is required. However, MFA is optional based on the AAD settings in the targeted Conditional Access policy.

After completing all the Setup Assistant screens, the end user lands on the home page (at which point their user affinity is established). However, until the user signs in to the Company Portal using their Azure AD credentials and taps "Begin" at the "Setup *Company* access" screen, the device:

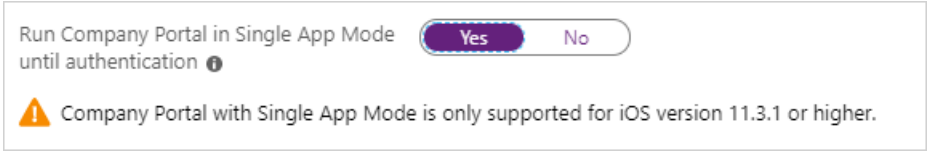
- Won't be fully registered with Azure AD.
- Won't show up in the user's device list in the Azure AD portal.
- Won't have access to resources protected by conditional access.
- Won't be evaluated for device compliance.
- Will be redirected to the Company Portal from other apps if the user tries to open any managed applications that are protected by conditional access.

8. If you selected **Setup Assistant (legacy)** for the authentication method but you also want to use Conditional Access or deploy company apps on the devices, you need to install Company Portal on the devices and sign in to complete the Azure AD registration. To do so, select **Yes** for **Install Company Portal**. If you want users to receive Company Portal without having to authenticate in to the App Store, in **Install Company Portal with VPP**, select a VPP token. Make sure the token doesn't expire and that you have enough device licenses for the Company Portal app to deploy correctly.

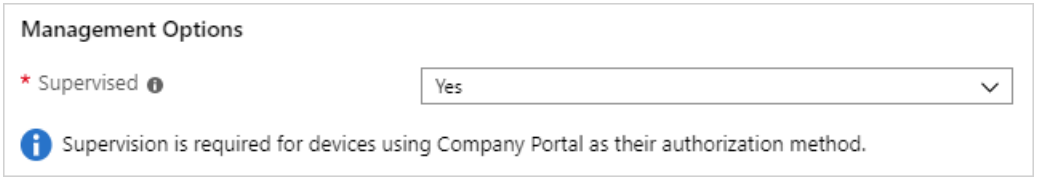
9. If you select a token for **Install Company Portal with VPP**, you can lock the device in Single App Mode (specifically, the Company Portal app) right after the Setup Assistant completes. Select **Yes** for **Run Company Portal in Single App Mode until authentication** to set this option. To use the device, the user must first authenticate by signing in with Company Portal.

   > **NOTE**
   > Multifactor authentication isn't supported on a single device locked in Single App Mode. This limitation exists because the device can't switch to a different app to complete the second factor of authentication. If you want multifactor authentication on a Single App Mode device, the second factor must be on a different device.

   This feature is supported only for iOS/iPadOS 11.3.1 and later.

10. If you want devices using this profile to be supervised, select **Yes** in the **Supervised** list:

Supervised devices give you more management options and disabled Activation Lock by default. Microsoft recommends that you use ADE as the mechanism for enabling supervised mode, especially if you're deploying large numbers of iOS/iPadOS devices. Apple Shared iPad for Business devices must be supervised.

Users are notified that their devices are supervised in two ways:

- The lock screen says: **This iPhone is managed by *company name***.
- The **Settings** > **General** > **About** screen says: **This iPhone is supervised. *Company name* can monitor your Internet traffic and locate this device.**

> **NOTE**
>
> If a device is enrolled without supervision, you need to use Apple Configurator if you want to set it to supervised. To reset the device in this way, you need to connect it to a Mac with a USB cable. For more information, see Apple Configurator Help.

11. In the **Locked enrollment** list, select **Yes** or **No**. Locked enrollment disables iOS/iPadOS settings that allow the management profile to be removed from the **Settings** menu. After device enrollment, you can't change this setting without wiping the device. To use this option, the device must have the **Supervised** management option set to **Yes**.

    > **NOTE**
    >
    > If a device is enrolled with locked enrollment, the user won't be able to use **Remove Device** or **Factory Reset** in the Company Portal app. The options will be unavailable to the user. Also, the user won't be able to remove the device on the Company Portal website.
    >
    > If a BYOD device is converted to an Apple ADE device and enrolled with a profile that has locked enrollment enabled, the user will be allowed to use **Remove Device** and **Factory Reset** for 30 days. After 30 days, the options will be disabled or unavailable. For more information, see Prepare devices manually.

12. If you selected **Enroll without User Affinity** and **Supervised** in the previous steps, you need to decide whether to configure the devices to be Apple Shared iPad for Business devices. Select **Yes** for **Shared iPad** to enable multiple users to sign in to a single device. Users will authenticate by using their Managed Apple IDs and federated authentication accounts or by using a temporary session (like the Guest account). This option requires iOS/iPadOS 13.4 or later. With Shared iPad, all Setup Assistant panes after activation are automatically skipped.

    > **NOTE**
    >
    > - A device wipe will be required if an iOS/iPadOS enrollment profile with Shared iPad enabled is sent to an unsupported device. Unsupported devices include any iPhone models, and iPads running iPadOS/iOS 13.3 and earlier. Supported devices include iPads running iPadOS 13.3 and later.
    > - To set up Apple Shared iPad for Business, configure these settings:
    >   - In the **User Affinity** list, select **Enroll without User Affinity**.
    >   - In the **Supervised** list, select **Yes**.
    >   - In the **Shared iPad** list, select **Yes**.

    If you're setting up Apple Shared iPad for Business devices, also configure:

    - **Maximum cached users**: Enter the number of users that you expect to use the shared iPad. You can cache up to 24 users on a 32-GB or 64-GB device. If you choose a low number, it might take a while for your users' data to appear on their devices after they sign in. If you choose a high

number, your users could run out of disk space.

- **Maximum seconds after screen lock before password is required**: Enter the number of seconds from 0 to 14,400. If the screen lock exceeds this amount of time, a device password will be required to unlock the device. Available for devices in Shared iPad mode running iPadOS 13.0 and later.
- **Maximum seconds of inactivity until user session logs out**: The minimum allowed value for this setting is 30. If there isn't any activity after the defined period, the user session ends and signs the user out. If you leave the entry blank or set it to zero (0), the session will not end due to inactivity. Available for devices in Shared iPad mode running iPadOS 14.5 and later.
- **Require Shared iPad temporary session only**: Configures the device so that users only see the guest version of the sign-in experience and must sign in as guests. They can't sign in with a Managed Apple ID. Available for devices in Shared iPad mode running iPadOS 14.5 and later.

  When set to **Yes**, this setting cancels out the following shared iPad settings, because they are not applicable in temporary sessions:

  - Maximum cached users
  - Maximum seconds after screen lock before password is required
  - Maximum seconds of inactivity until user session logs out
- **Maximum seconds of inactivity until temporary session logs out**: The minimum allowed value for this setting is 30. If there isn't any activity after the defined period, the temporary session ends and signs the user out. If you leave the entry blank or set it to zero (0), the session will not end due to inactivity. Available for devices in Shared iPad mode running iPadOS 14.5 and later.

  This setting is available when **Require Shared iPad temporary session only** is set to **Yes**.

> **NOTE**
>
> - If temporary sessions are enabled, all of the user's data is deleted when they sign out of the session. This means that all targeted policies and apps will come down to the user when they sign-in, and they'll be erased when the user sign outs.
> - To alter a Shared iPads configuration to not have temporary sessions, the device will need to be fully reset and a new enrollment profile with the updated configurations will need to be sent down to the iPad.

13. In the **Sync with computers** list, select an option for the devices that use this profile. If you select **Allow Apple Configurator by certificate**, you need to choose a certificate under **Apple Configurator Certificates**.

> **NOTE**
>
> If you set **Sync with computers** to **Deny all**, the port will be limited on iOS and iPadOS devices. The port will be limited to only charging. It will be blocked from using iTunes or Apple Configurator 2.
>
> If you set **Sync with computers** to **Allow Apple Configurator by certificate**, make sure you have a local copy of the certificate that you can use later. You won't be able to make changes to the uploaded copy, and it's important to retain an copy of this certificate. If you want to connect to the iOS/iPadOS device from a macOS device or PC, the same certificate must be installed on the device making the connection to the iOS/iPadOS device.

14. If you selected **Allow Apple Configurator by certificate** in the previous step, choose an Apple Configurator certificate to import.
15. You can specify a naming format for devices that's automatically applied when they're enrolled and upon

each successive check-in. To create a naming template, select **Yes** under **Apply device name template**. Then, in the **Device Name Template** box, enter the template to use for the names that use this profile. You can specify a template format that includes the device type and serial number. This feature supports iPhone, iPad, and iPod Touch. The device name template entry cannot exceed the length of 63 characters, including the variables.

16. You can activate a cellular data plan. This setting applies to devices running iOS/iPadOS 13.0 and later. Configuring this option will send a command to activate cellular data plans for your eSim-enabled cellular devices. Your carrier must provision activations for your devices before you can activate data plans using this command. To activate cellular data plan, click **Yes** and then enter your carrier's activation server URL.
17. Select **Next**.
18. On the **Setup Assistant** tab, configure the following profile settings:

DEPARTMENT SETTING	DESCRIPTION
Department	Appears when users tap **About Configuration** during activation.
Department Phone	Appears when users tap the **Need Help** button during activation.

You can choose to hide Setup Assistant screens on the device during user setup.

- If you select **Hide**, the screen won't be displayed during setup. After setting up the device, the user can still go to the **Settings** menu to set up the feature.
- If you select **Show**, the screen will be displayed during setup, but only if there are steps to complete after the restore or after the software update. Users can sometimes skip the screen without taking action. They can then later go to the device's **Settings** menu to set up the feature.
- With Shared iPad, all Setup Assistant panes after activation are automatically skipped regardless of the configuration.

SETUP ASSISTANT FEATURES	WHAT HAPPENS WHEN VISIBLE
Passcode	Prompt the user for a passcode. Always require a passcode for unsecured devices unless access is controlled in some other way. (For example, a kiosk mode configuration that restricts the device to one app.) For iOS/iPadOS 7.0 and later.
Location Services	Prompt the user for their location. For macOS 10.11 and later, and iOS/iPadOS 7.0 and later.
Restore	Display the Apps & Data screen. This screen gives users the option to restore or transfer data from iCloud Backup when they set up the device. For macOS 10.9 and later, and iOS/iPadOS 7.0 and later.
Apple ID	Give the user the options to sign in with their Apple ID and use iCloud. For macOS 10.9 and later, and iOS/iPadOS 7.0 and later.
Terms and conditions	Require the user to accept Apple's terms and conditions. For macOS 10.9 and later, and iOS/iPadOS 7.0 and later.

SETUP ASSISTANT FEATURES	WHAT HAPPENS WHEN VISIBLE
Touch ID and Face ID	Give the user the option to set up fingerprint or facial identification on their device. For macOS 10.12.4 and later, and iOS/iPadOS 8.1 and later. On iOS/iPadOS 14.5 and later, the Passcode and Touch ID Setup Assistant screens during device setup aren't working. If you use version 14.5+, then don't configure the Passcode or Touch ID Setup Assistant screens. If you require a passcode on devices, then use a device configuration policy or a compliance policy. After the user enrolls and they receive the policy, they're prompted for a passcode.
Apple Pay	Give the user the option to set up Apple Pay on the device. For macOS 10.12.4 and later, and iOS/iPadOS 7.0 and later.
Zoom	Give the user to the option to zoom the display when they set up the device. For iOS/iPadOS 8.3 and later.
Siri	Give the user the option to set up Siri. For macOS 10.12 and later, and iOS/iPadOS 7.0 and later.
Diagnostics Data	Display the Diagnostics screen. This screen gives the user the option to send diagnostic data to Apple. For macOS 10.9 and later, and iOS/iPadOS 7.0 and later.
Display Tone	Give the user the option to turn on Display Tone. For macOS 10.13.6 and later, and iOS/iPadOS 9.3.2 and later.
Privacy	Display the Privacy screen. For macOS 10.13.4 and later, and iOS/iPadOS 11.3 and later.
Android Migration	Give the user the option to migrate data from an Android device. For iOS/iPadOS 9.0 and later.
iMessage & FaceTime	Give the user the option to set up iMessage and FaceTime. For iOS/iPadOS 9.0 and later.
Onboarding	Display onboarding informational screens for user education, like Cover Sheet and Multitasking and Control Center. For iOS/iPadOS 11.0 and later.
Screen Time	Display the Screen Time screen. For macOS 10.15 and later, and iOS/iPadOS 12.0 and later.
SIM Setup	Give the user the option to add a cellular plan. For iOS/iPadOS 12.0 and later.
Software Update	Display the mandatory software update screen. For iOS/iPadOS 12.0 and later.
Watch Migration	Give the user the option to migrate data from a watch device. For iOS/iPadOS 11.0 and later.
Appearance	Display the Appearance screen. For macOS 10.14 and later, and iOS/iPadOS 13.0 and later.

SETUP ASSISTANT FEATURES	WHAT HAPPENS WHEN VISIBLE
Device to Device Migration	Give the user the option to migrate data from an old device to this device. This feature isn't available for ADE devices running iOS 13 and later, so this screen won't appear on those devices.
Restore Completed	Shows users the Restore Completed screen after a backup and restore is performed during Setup Assistant.
Software Update Completed	Shows the user all software updates that happen during Setup Assistant.
Get Started	Shows users the Get Started welcome screen.

19. Select **Next**.
20. To save the profile, select **Create**.

> **NOTE**
>
> If you need to re-enroll your Automated Device Enrollment device, you need to first wipe the device from the Intune admin console. To re-enroll:
>
> 1. Wipe the device from the Intune console.
>   - Alternatively, retire the device from the Intune console and factory reset the device using the Settings app, Apple Configurator 2, or iTunes.
> 2. Activate the device again and run through Setup Assistant to receive the *Remote Management Profile*.

Dynamic groups in Azure Active Directory

You can use the enrollment **Name** field to create a dynamic group in Azure Active Directory (Azure AD). For more information, see Azure Active Directory dynamic groups.

You can use the profile name to define the enrollmentProfileName parameter to assign devices with this enrollment profile.

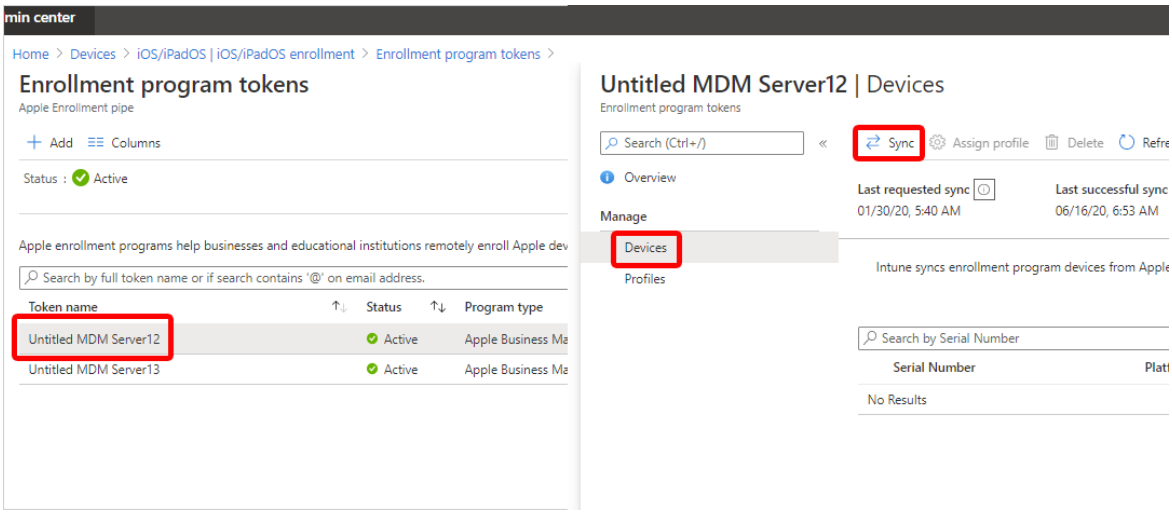
For the fastest policy delivery on ADE devices that have user affinity, make sure the enrolling user is a member, before device setup, of an Azure AD user group.

If you assign dynamic groups to enrollment profiles, there might be a delay in delivering applications and policies to devices after the enrollment.

Sync managed devices

Now that Intune has permission to manage your devices, you can synchronize Intune with Apple to see your managed devices in Intune in the Azure portal.

1. In Microsoft Endpoint Manager admin center, select **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment Program Tokens**.
2. Select a token in the list, and then select **Devices** > **Sync**:



To follow Apple's terms for acceptable enrollment program traffic, Intune imposes the following restrictions:

- A full sync can run no more than once every seven days. During a full sync, Intune fetches the complete updated list of serial numbers assigned to the Apple MDM server connected to Intune.

  > **IMPORTANT**
  > If a device is deleted from Intune, but remains assigned to the ADE enrollment token in the ASM/ABM portal, it will reappear in Intune on the next full sync. If you don't want the device to reappear in Intune, unassign it from the Apple MDM server in the ABM/ASM portal.

- If a device is released from ABM/ASM, it can take up to 45 days for it to be automatically deleted from the devices page in Intune. You can manually delete released devices from Intune one by one if needed. Released devices will be accurately reported as being Removed from ABM/ASM in Intune until they are automatically deleted within 30-45 days.
- A delta sync is run automatically every 12 hours. You can also trigger a delta sync by selecting the **Sync** button (no more than once every 15 minutes). All sync requests are given 15 minutes to finish. The **Sync** button is disabled until a sync is completed. This sync will refresh existing device status and import new devices assigned to the Apple MDM server. If a delta sync fails for any reason, the next sync will be a full sync to hopefully resolve any issues.

Assign an enrollment profile to devices

Before devices can be enrolled, you need to assign an enrollment program profile to them.

> **NOTE**
> You can also assign serial numbers to profiles in the **Apple Serial Numbers** pane.

1. In Microsoft Endpoint Manager admin center, select **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment Program Tokens**. Select a token in the list.
2. Select **Devices**. Select devices in the list, and then select **Assign profile**.
3. Under **Assign profile**, choose a profile for the devices, and then select **Assign**.

Assign a default profile

You can pick a default profile to be applied to all devices that enroll with a specific token.

1. In Microsoft Endpoint Manager admin center, select **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment Program Tokens**. Select a token in the list.

2. Select **Set Default Profile**, select a profile in the list, and then select **Save**. The profile will be applied to all devices that enroll with the token.

> **NOTE**
> Ensure that **Device Type Restrictions** under **Enrollment Restrictions** does not have the default **All Users** policy set to block the iOS/iPadOS platform. This setting will cause automated enrollment to fail and your device will show as Invalid Profile, regardless of user attestation. To permit enrollment only by company-managed devices, block only personally owned devices, which will permit corporate devices to enroll. Microsoft defines a corporate device as a device that's enrolled via a Device Enrollment Program or a device that's manually entered under **Corporate device identifiers**.

Distribute devices

You enabled management and syncing between Apple and Intune and assigned a profile so your ADE devices can be enrolled. You're now ready to distribute devices to users. Some things to know:

- Devices enrolled with user affinity require that each user be assigned an Intune license.
- Devices enrolled without user affinity typically don't have any associated users. These devices need to have an Intune device license. If devices enrolled without user affinity will be used by an Intune-licensed user, a device license isn't needed.

  To summarize, if a device has a user, the user needs to have an assigned Intune license. If the device doesn't have an Intune-licensed user, the device needs to have an Intune device license.

  For more information on Intune licensing, see Microsoft Intune licensing and the Intune planning guide.
- A device that's been activated needs to be wiped before it can enroll properly using ADE in Intune. After it's been wiped but before activating it again, you can apply the enrollment profile. See Set up an existing iPhone, iPad, or iPod touch
- If you're enrolling with ADE and user affinity, the following error can happen during setup:

  ```
  The SCEP server returned an invalid response.
  ```

  You can resolve this error by trying to download the management again within 15 minutes. If it's been more than 15 minutes, to resolve this error you'll need to factory reset the device. This error occurs because of a 15-minute time limit on SCEP certificates, which is enforced for security.

For information on the end-user experience, see Enroll your iOS/iPadOS device in Intune by using ADE.

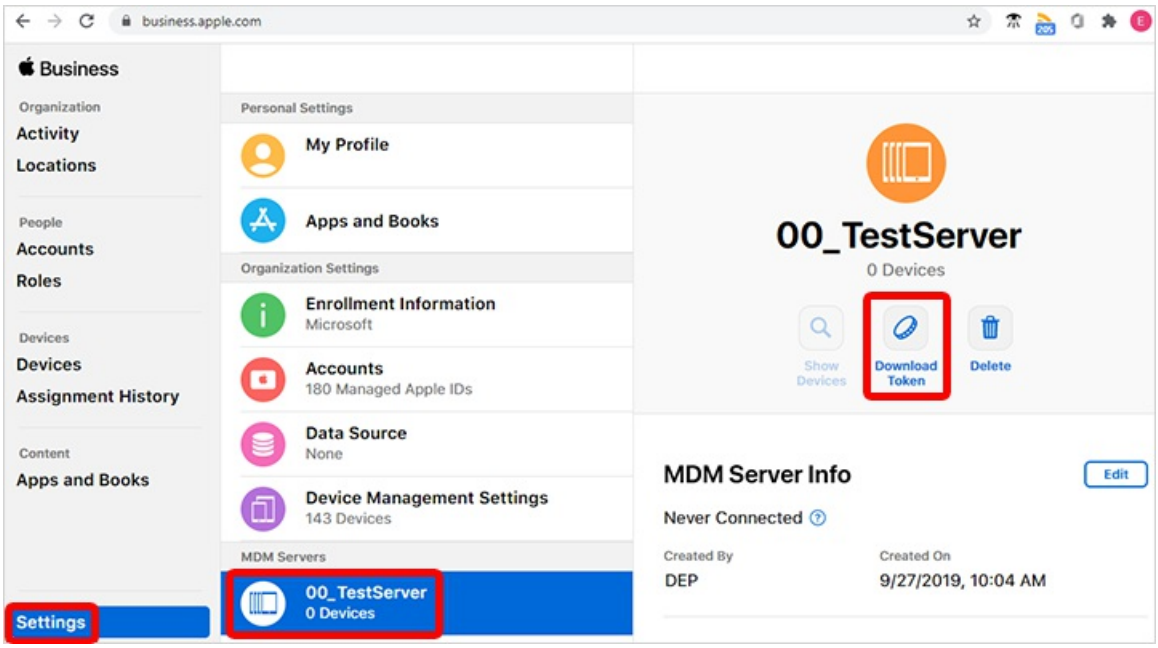
Renew an Automated Device Enrollment token

You'll sometimes need to renew your tokens:

- Renew your ADE token yearly. The Endpoint Manager admin center shows the expiration date.
- If the Apple ID password changes for the user who set up the token in Apple Business Manager, renew your enrollment program token in Intune and Apple Business Manager.
- If the user who set up the token in Apple Business Manager leaves the organization, renew your enrollment program token in Intune and Apple Business Manager.

Renew your tokens

1. Go to business.apple.com and sign in with an account that has an Administrator or Device Enrollment Manager role.
2. Select **Settings**. Under **MDM Servers**, select the MDM server associated with the token file that you want to renew. Select **Download Token**:

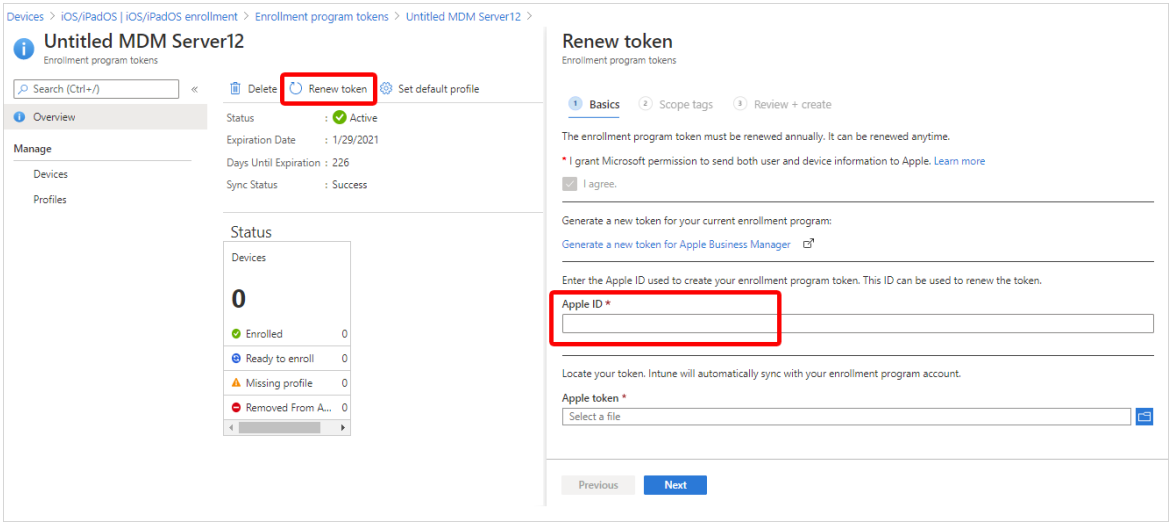


3. Select **Download Server Token**.

> **NOTE**
>
> As it says in the prompt, don't select **Download Server Token** if you don't intend to renew the token. Doing so will invalidate the token being used by Intune (or any other MDM solution). If you already downloaded the token, be sure to continue with the next steps until the token is renewed.

4. After you download the token, go to Microsoft Endpoint Manager admin center. Select **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment program tokens**. Select the token.

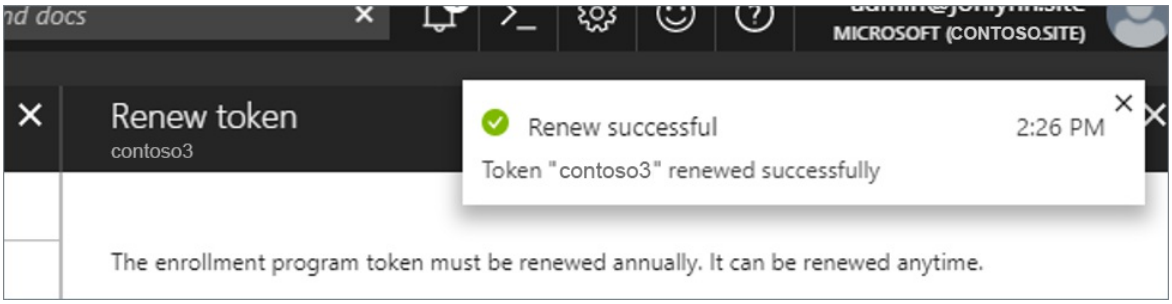
5. Select **Renew token**. Enter the **Apple ID** used to create the original token (if it's not automatically populated):



6. Upload the newly downloaded token.

7. Select **Next** to go to the **Scope tags** page. Assign scope tags if you want to.

8. Select **Renew token**. You'll see a confirmation that the token is renewed:



Delete an Automated Device Enrollment token from Intune

You can delete an enrollment profile token from Intune as long as:

- No devices are assigned to the token.
- No devices are assigned to the default profile.
- There are no enrollment profiles under that token.

To delete an enrollment profile token:

1. In Microsoft Endpoint Manager admin center, select **Devices** > **iOS/macOS** > **iOS/macOS enrollment** > **Enrollment Program Tokens**. Select the token, and then select **Devices**.
2. Delete all the devices assigned to the token.
3. Go to **Devices** > **iOS/macOS** > **iOS/macOS enrollment** > **Enrollment Program Tokens**. Select the token, and then select **Profiles**.
4. If there's a default profile or any other enrollment profile, they must all be deleted.
5. Go to **Devices** > **iOS/macOS** > **iOS/macOS enrollment** > **Enrollment Program Tokens**. Select the token, and then select **Delete**.

Next steps

Backup and restore scenarios for iOS/iPadOS

iOS/iPadOS enrollment overview

What are shared iOS and iPadOS devices?

9/23/2022 • 2 minutes to read • Edit Online

Shared devices are organization-owned multi-user devices. These devices can be special-purpose or multi-purpose as needed in each environment. Shared devices enable front-line workers in healthcare, hospitality, retail, manufacturing, and other industries to access critical applications and tools essential to their role in the organization. In education, shared devices are used as learning aids or test-taking devices in classrooms.

Shared device solutions on iOS and iPadOS

Microsoft Endpoint Manager supports two types of shared device solutions for iOS and iPadOS:

- Shared iPads
- Shared Device Mode

Important considerations when choosing a shared device solution for iOS and iPadOS

The following table captures the key differences between the two available shared devices solutions on iOS/iPadOS. Review this to select the most appropriate iOS/iPadOS shared device strategy for your organization.

CONSIDERATION	SHARED IPAD	SHARED DEVICE MODE
Supported device types	iPad	iPhone, iPod touch, iPad
Minimum device requirements	iPadOS 13.4 or later with at least 32 GB of storage.	iOS 13 or later, iPadOS 13 or later
AAD federation with Apple Business or School Manager	Required. This enables users to sign in using their AAD username and password.	Not required
Managed Apple ID	AAD federation automatically creates Managed Apple ID when user signs in on Shared iPad for the first time. If AAD federation is not set up, Managed Apple IDs can be created manually in Apple Business or School Manager and shared with users for signing in.	Not required
Device provisioning	Shared iPad can be enabled on iPads enrolled using Automated Device Enrollment without user affinity.	Shared Device Mode can be configured on devices enrolling using Automated Device Enrollment without user affinity. For more information, see Use Intune to enable shared device mode & SSO extension.

CONSIDERATION	SHARED IPAD	SHARED DEVICE MODE
Temporary session without signing in	Temporary sessions that do not require a Managed Apple ID or password are allowed by default. Temporary sessions can be allowed or blocked by Intune policy. For more information, see Shared iPad.	Not applicable
Supported app types	Device-licensed purchased or custom apps (VPP), line-of-business apps, web apps.	Apps that have been modified to support Shared Device Mode including MSAL integration. For more information, see Modify your iOS application to support shared device mode.
Policy and app assignment	Device-assigned required apps and policies are supported. The same apps and policies apply to any user signing in on a Shared iPad. Some device configuration policies can be user-assigned. For more information, see Configure settings for Shared iPads.	Device-assigned required apps and policies are supported.
Unsupported scenarios	Conditional Access (see note below) App Protection Policies Intune Company Portal app Available apps	Conditional Access (see note below) App Protection Policies Intune Company Portal app Available apps Apps that don't support Shared Device Mode User-assigned policies and apps

IMPORTANT

The following Conditional Access configurations are not supported:

- Granting Conditional Access conditions for a device that require an approved client app, require an app protection policy, require per-device terms of use, or must be marked as compliant.
- Conditional Access conditions that use filters for devices.

Recommended iOS/iPadOS shared device strategy

Shared iPad is the recommended shared device solution for Microsoft 365 on iPadOS. If you are planning your organization's shared device strategy, it is highly recommended that you choose iPadOS devices that meet the minimum requirements for Shared iPad (see section above). If your organization's shared device strategy requires cellphone capabilities or includes iOS devices, Shared Device Mode is the recommended shared device solution on iOS. Review the differences between Shared iPad and Shared Device Mode to ensure that the recommendations above will fit your organization's needs.

Next steps

- Set up iOS/iPadOS device enrollment with Apple Configurator

Shared iPad devices

9/23/2022 • 11 minutes to read • Edit Online

Provisioning a device as a Shared iPad sets it up for use by multiple users. iPads running on iPadOS 13.4 and later can be provisioned as a Shared iPad when enrolled using Automated Device Enrollment without user affinity.

A Shared iPad consists of a pre-defined number of user partitions. User partitions ensure that each user's apps, data, and preferences are stored separately on Shared iPad and can be backed up to iCloud (if allowed by admin) for seamless transition across multiple Shared iPads.

By federating your organization's AAD instance in Apple Business or School Manager, a user can sign in on a Shared iPad using their AAD username and password. This automatically creates a Managed Apple ID for the user that matches their AAD username when they sign in on a Shared iPad for the first time. In addition, at first sign-in on a Shared iPad, the user sets up an alphanumeric passcode for their user partition and the apps assigned to the device are installed to the user partition. The next time the user accesses a Shared iPad, they only need to provide their Managed Apple ID (same as their AAD username) and the alphanumeric passcode.

Configure Shared iPad

Follow these steps to set up Shared iPads in your environment:

1. Federate your AAD instance with Apple Business Manager or Apple School Manager. For more information, see Intro to federated authentication with Apple Business Manager.
2. Create an enrollment profile by navigating to Microsoft Endpoint Manager admin center and selecting **Devices** > **iOS/iPadOS** > **iOS/iPadOS Enrollment** > **Enrollment program tokens* > *select a token* > **Profiles** > **Create profile** > **iOS/iPadOS**.
3. Enable **Shared iPad** in the enrollment profile under **Management settings**. Set **User affinity** to **Enroll without user affinity** and **Supervised** to **Yes** and then **Shared iPad** to **Yes**. Important note - A device wipe will be required if an iOS/iPadOS enrollment profile with Shared iPad enabled is sent to an unsupported device. Unsupported devices include any iPhone models, and iPads running iPadOS/iOS 13.3 and earlier. Supported devices include iPads running iPadOS 13.3 and later. Shared iPads must be supervised.
4. Complete configuring the enrollment profile as desired and then select **Save**.
5. Assign devices synced from Apple Business Manager by selecting the new enrollment profile, then select **Assign devices** > **Add devices**.
6. Create a dynamic device group containing devices by using the new enrollment profile for Shared iPad by navigating to **Groups** > **New group**. Set **Membership type** to **dynamic device** and select **Add dynamic query** and set **enrollmentProfileName** to the *name of desired enrollment profile*.
7. Assign required apps and configuration profiles for Shared iPads to the dynamic device group.
8. For new devices, power on and follow the prompts to set up the device as a Shared iPad. For existing devices, factory reset the device and follow the prompts to set it up as a Shared iPad.

Configure settings for Shared iPads

> **NOTE**
> *This feature is in public preview.*

You can configure settings in device configuration profiles for a Shared iPad both in device and user context.

However, the settings on a Shared iPad follow the applicability rules in the table below. In general, a device applicable setting applies to any active user on a Shared iPad device, while a user applicable setting applies when the user is active on any Shared iPad device.

NOTE

- Your Azure AD instance must be federated in Apple Business Manager for user group policy assignment to succeed.
- All device configuration profile settings are device applicable for Shared iPad temporary sessions.
- User-assigned policies apply to a Shared iPad when the user signs in using their federated Azure AD credentials. See Apple's documentation on federating an Azure AD instance with Apple Business Manager.
- Device-assigned policies apply to a Shared iPad when you initiate a device-sync from MEM admin console or when Intune notifies the device to check in with the Intune service. Learn more about frequency of device check-in with the Intune service.

PROFILE TYPE	SETTING NAME	APPLICABILITY ON DEVICE GROUP ASSIGNMENT	APPLICABILITY ON USER GROUP ASSIGNMENT
Device features	Home screen layout	Device	User
Device features	App notifications	Device	User
Device features	Single sign on app extension	Device	User
Device features	AirPrint settings	Device	Not applicable
Device features	Lock screen message	Device	Not applicable
Device features	Web content filter	Device	Not applicable
Device restrictions	Block Shared iPad temporary sessions	Device	Not applicable
Device restrictions	Defer software updates	Device	Not applicable
Device restrictions	Force automatic date and time	Device	Not applicable
Device restrictions	Require joining Wi-Fi networks only using configuration profiles	Device	Not applicable
Device restrictions	Block auto lock	Device	Not applicable
Device restrictions	Allow users to boot devices into recovery mode with unpaired devices	Device	Not applicable
Device restrictions	Block Siri for dictation	Device	Not applicable
Device restrictions	All other settings in device restrictions	Device	User
Email	All settings	Device	User

PROFILE TYPE	SETTING NAME	APPLICABILITY ON DEVICE GROUP ASSIGNMENT	APPLICABILITY ON USER GROUP ASSIGNMENT
VPN, Wi-Fi, Certificate	All settings	Device	Not applicable

Configure temporary sessions on Shared iPads

In iPadOS 13.4 or later, users can initiate a temporary session without the need for a username or password by tapping Guest at the login screen. All their data — including browsing history — is deleted when the user signs out. Temporary sessions allow users to sign in as Guest, and users are not required to enter a Managed Apple ID or password. This can be configured using iOS Device Restrictions in Endpoint Manager. For more information, see Shared iPad - Automated device enrollment (supervised) as mentioned in this document. Temporary sessions are allowed by default on Shared iPads.

Add Apps on Shared iPads

You can deploy volume-purchased (VPP) apps or custom apps or line-of-business apps or web apps to Shared iPads.

1. To deploy a VPP or custom app to Endpoint Manager, add the apps in Apple Business Manager or Apple School Manager and synchronize the VPP token. Assign a VPP or custom app as device-licensed to Azure AD device groups in Intune. For more information, see Synchronize a VPP token.
2. To add a line-of-business app in Endpoint Manager and assign it to Azure AD device group. For more information, see Add an iOS/iPadOS line-of-business app to Microsoft Intune.
3. To add a web app in Endpoint Manager and assign it to Azure AD groups. For more information, see Add a web app to Intune.
4. For assigning apps to Shared iPads, you should use Azure AD device groups. You can use home screen layout settings in device configuration profile assigned to Azure AD user groups to show or hide different sets of apps to different users on a Shared iPad.

App installations on Shared iPads follow the applicability rules in the table below.

APP TYPE	APPLICABILITY ON DEVICE GROUP ASSIGNMENT	APPLICABILITY ON USER GROUP ASSIGNMENT
Line-of-business app	Device	Not applicable
Device-licensed volume-purchased or custom app (VPP)	Device	Not applicable
User-licensed volume-purchased or custom app (VPP)	Not applicable	Not applicable
Web app	Device	User
App Store app	Not applicable	Not applicable

Recommended policy and app assignment for Shared iPads

You should review the scenarios and recommendations in the table below when planning Shared iPad deployment and configuration in your environment.

SCENARIO	ADMIN CONFIGURATION	SHARED IPAD EXPERIENCE	EXAMPLE
All users on a Shared iPad are in the same role. All users on a Shared iPad are using temporary sessions.	Assign all apps and profiles to Azure AD device group containing Shared iPads.	All apps and profiles apply to any active user on the Shared iPad or to Shared iPad temporary sessions.	You assign a Wi-Fi profile, device restrictions, VPP apps and home screen layout to an Azure AD device group containing a Shared iPad. These profiles apply to any user signing in on the Shared iPad.
Users on a Shared iPad are in different roles.	• Assign all apps and profiles common to all roles to an Azure AD device group containing Shared iPads. • Assign profiles that vary by role and are user applicable to user groups. Ensure that the profile does not conflict with any setting assigned to the device group above.	When a user signs in on a Shared iPad, the combination of device-targeted profiles and user-targeted profiles creates a customized experience for the active user. Only apps and profiles assigned to the device apply to Shared iPad temporary sessions.	You assign a common Wi-Fi profile and all VPP apps to a device group containing a Shared iPad. Then you assign varying home screen layouts to different roles using Azure AD user groups. This customizes the Shared iPad experience for users in each role.
Apply different device restrictions to different users on a Shared iPad.	• Assign device restrictions that should apply to all users of the Shared iPad to an Azure device group containing the Shared iPads. • Assign user-applicable device restrictions that vary by user to Azure AD user groups. Ensure that the device restrictions do not conflict with any device restrictions assigned to the device group.	When a user signs in on a Shared iPad, the combination of device targeted restrictions and user-targeted restrictions creates a customized experience for the active user. Only device restrictions assigned to device groups apply to Shared iPad temporary sessions.	You want to prevent all Shared iPad users from using AirDrop. But you only want managers to be able to turn off Wi-Fi on Shared iPads. You assign a device configuration profile that blocks AirDrop to a device group containing a Shared iPad. Then you assign a device configuration profile that requires Wi-Fi to be always on to a user group containing non-manager employees.

SCENARIO	ADMIN CONFIGURATION	SHARED IPAD EXPERIENCE	EXAMPLE
Show/hide different apps to different users on a Shared iPad.	• Assign all apps to the Azure AD device group containing Shared iPads. • Create home screen layouts to show/hide the apps and assign the home screen layouts to Azure AD user groups.	When a user signs in on a Shared iPad, the user-assigned home screen layout applies to show/hide the apps as configured in Microsoft Endpoint Manager. All apps assigned to the device show in Shared iPad temporary sessions.	You assign Microsoft Outlook, Teams and Safari to a device group containing a Shared iPad. Then you assign a home screen layout that only shows Teams to a user group containing users who only require Teams when using Shared iPad. You assign another home screen layout that shows Outlook, Teams and Safari to a user group containing managers who need access to all 3 apps when using Shared iPad.
Hide unnecessary system apps on a Shared iPad.	Create a home screen layout containing the desired system apps and managed apps. Assign the home screen layout to the Azure AD device group containing Shared iPads.	The same home screen layout will apply to any user signing in on the Shared iPad and to Shared iPad temporary sessions.	You create a home screen layout that excludes unnecessary system apps like Settings, App Store, Clock and assign the layout to a device group containing a Shared iPad.

NOTE

- It is recommended that a setting is configured only once for Shared iPads.
- Configuring multiple values of a setting for a Shared iPad is not recommended. If multiple values of a setting are configured, the setting that applies cannot be pre-determined.
  - Intune may detect the conflict and the first setting assigned to the device would apply.
  - If a setting that is both device applicable and user applicable is assigned to an Azure AD device group and an Azure AD user group, the applied value of the setting is chosen by iPadOS.

Known limitations

The following are known limitations when working with shared iPads:

- **Disabled settings and system apps:** Shared iPads provide users access to a limited number of settings and system apps. For more information on what settings and apps are disabled on Shared iPads. For more information, see Shared iPad and Managed Apple IDs.
- **App Store installations are disabled:** The App Store is available by default on Shared iPad. But app installation is disabled for App Store apps when a device is set up as a Shared iPad. It is recommended that you disable App Store using configuration profiles in Intune.
- **Company Portal and available apps are not supported:** Intune Company Portal app and the Intune Company Portal website are not supported on Shared iPad. Apps must be assigned as *required* to device groups containing the Shared iPad to install. Available apps are not supported on Shared iPad.
- **Passcode complexity cannot be managed on Shared iPad:** The passcode complexity for Shared iPad is a complex 8 character alphanumeric and cannot be changed in Apple Business Manager. The passcode complexity and length settings available in device configuration profile do not apply to Shared iPads. The MDM administrator can set the grace period – a number of minutes during which the user can unlock the iPad without a passcode.

- **Unsupported scenarios:** Some Intune scenarios are not supported on Shared iPads, namely, app-based and device-based Conditional Access, app protection policies and compliance policies.
- **Wallpaper is not supported:** Setting a wallpaper image is currently not supported on Shared iPad. For more information on wallpaper, see iOS/iPadOS Device Features.
- Email profile shows error: if you assign an email profile to Shared iPads, it reports error. Email profiles on Shared iPad are currently not supported.
- User-assigned policies applying to Shared iPads do not show in reports: apps and profiles assigned to Azure AD user groups do not reflect status in "device status" and "user status" under Monitoring section of the apps or profiles when they apply on Shared iPads.
- Azure AD federation requirement is not enforced: if the Managed Apple ID matches the Azure AD UPN and the Azure AD user is assigned a user applicable device configuration profile, the profile will apply to the user when they sign in using their Managed Apple ID on a Shared iPad. The Azure AD federation requirement is currently not enforced.

Next steps

- Set up iOS/iPadOS device enrollment with Apple Configurator

Backup and restore scenarios for iOS/iPadOS

9/23/2022 • 6 minutes to read • Edit Online

You might have to back up and restore an Intune Automated Device Enrollment (ADE) managed iOS/iPadOS device during the setup assistant process. For example, when:

- A device is factory reset and is then restored from a previous backup.
- A user receives a new device and wants to migrate the data from the old device.

To back up and restore an iOS/iPadOS device, you must follow the Apple instructions:

- To back up your device, see How to back up your iPhone, iPad, and iPod touch.
- To restore your device, see Restore your iPhone, iPad, or iPod touch from a backup.
- To transfer data to a new device, see the following Apple support article:
  - Use iCloud to transfer data from your previous iOS device to your new iPhone, iPad, or iPod touch

For more information about restoring Apple devices from backup, see Get started using Apple Business Manager or Apple School Manager with Mobile Device Management.

> **NOTE**
> Device-to-Device migration as offered on the Quick Start screen after resetting an iOS device isn't supported with Apple Business Manager (ABM). For details refer to the following Apple support document. Since this screen appears on the device before a wi-fi connection has been established and before the ABM profile has been downloaded, this quick start screen cannot be hidden via ABM.

Back up Microsoft Authenticator

If you're using the Microsoft Authenticator app, it's also important to back up your credentials and accounts. For more information, visit Back up and recover account credentials in the Authenticator app.

Restoring a backup to an iOS/iPadOS device

When a user restores their content from an iCloud or iTunes backup, there are many considerations to bear in mind:

- Restoring a backup is only possible during Apple Setup Assistant. This backup is a 'one-time' opportunity. Linking the Apple ID in settings post-setup isn't the same as a restore. While it links files and documents, it doesn't typically restore any user data and preferences (think 'look and feel' such as wallpaper, widgets, installed applications, user preferences, and so on). Only a limited set of data may be restored such as iCloud Photo Library and messages for example.
- The restore process workflow is different, depending on whether you restore the backup to the same device, or a different device.
  - When restoring to a different device than the one on which the backup was performed, after the backup is successfully restored, setup assistant will continue with the enrollment process (from the 'remote management' screen onwards). The result is that you are enrolled in the MDM vendor and also maintain your content that has been restored from your iCloud account.
  - When restoring to the same device on which the backup was performed, after the backup is successfully restored, setup assistant doesn't resume. You're left on the device's home screen. The result is that you don't go through any 'remote management' and subsequent enrollment steps. You

retain the management state (and management profile) that you had at the time the backup was done. This result is typically a good thing, unless this process is being performed as part of a migration to a different EMM vendor (see below).
    - In addition, specific to Intune, there are two different methods to reset a device and they will affect the post-restore behavior regarding enrollment state:
        - If you performed a local reset of the device, then the device will remain enrolled post-restore and shouldn't require any intervention. This is typically the desired behavior.
        - If you performed a remote wipe by using the MEM/Intune web portal, this will first unenroll the device before the wipe. As a result, post-restore, the device will need to be re-enrolled using the Company Portal app before it will be functional.
- Also consider the amount of time that has elapsed since the backup was taken, and what impact a restore (which essentially sets the device back to that prior time), might have. For example, has the corresponding device record in Intune been deleted? (either by accident or an intentional retirement/clean-up). What about the Azure AD record? What about the management certificate? These certificates are valid for a year for iOS/iPadOS. Is the management certificate being restored still valid? Was the management certificate renewed after the backup was done? These scenarios might be less common, but they are worth being aware of – especially if the backup being restored isn't recent.
- To avoid issues, ensure that users do not perform a backup whilst the device is enrolled – you want users to perform any backup/restore activities without impacting the management profile and related certificates. If the management profile was locked on the device by the prior EMM, the end user won't have an option to remove the management profile on the device. To facilitate this type of migration, one option would be to retire the device from the prior EMM before the user does a backup of the iOS/iPadOS device. Alternatively, if you cannot ensure that the device was unenrolled when the backup was taken, consider hiding the 'restore' setup assistant screen in your iOS/iPadOS enrollment profile in the Microsoft Endpoint Manager console.

Migrating to MEM/Intune from another EMM vendor

Specific to backup/restore

- In most cases, your MDM enrollment state (at the time of backup) isn't of any special significance. However, in a migration scenario where you are moving from one MDM vendor to another, it is important to be aware of.
    - When restoring a backup, taken while enrolled in MDM vendor A and restoring it on the same device but attempting to enroll in Intune, this will result in failure. The restore will be successful (no errors) as explained above, however since the management profile from MDM vendor A has been restored, the device isn't under management by Intune. Attempting to manually enroll the device using the Company Portal app will result in an error when trying to install the new Intune management profile "The new MDM payload doesn't match the old payload". To remediate this error, you would need to remove the existing management profile belonging to MDM vendor A and then re-enroll into Intune using Company Portal. Migrating from one Intune tenant to another Intune tenant would exhibit the same behavior.
    - To correctly and fully re-enroll an ADE device, a factory reset is required, and the device cannot be restored from its own backup (otherwise the ADE configuration and profiles in the backup will be applied).

Migrating without wiping the device

There is an additional migration scenario to consider, which should not be impacted by any of the above.

- If a migration is performed from one MDM vendor to another without a device wipe (such as by using a tool such as EBF Onboarder for example), there should be no negative impact to the device, as it is never restored. Instead, the device is 'off-boarded/unenrolled' from one MDM vendor and has the management profile removed, and then enrolls manually into Intune using the Company Portal app. The users iCloud account isn't removed and no backup is restored as setup assistance isn't involved in this scenario.

- There are other considerations in a scenario where the device is migrated without performing a device wipe:
  - If the device was supervised under the current EMM vendor, the supervised state will be maintained
  - The new management profile (MEM/Intune) cannot be 'locked' – meaning the user is able to remove the management profile in Settings.
  - These devices will enroll into MEM/Intune as 'personal' devices, rather than 'corporate' devices. This condition will have an impact on the app inventory gathered from the device, the displayed phone number, etc., as described here.
    - If you want to designate these migrated devices as corporate devices, following either of these steps:
      - Add Corporate device identifiers as described here. Provided you can obtain a list of serial numbers from your current EMM vendor and this list is imported prior to enrolling the devices in Intune, this is the simplest option and avoids scripting.
      - Use a script to modify the OwnershipType from Personal to Corporate. A sample script, which uses an exported list (.csv) of device serial numbers (taken from your current EMM vendor) as input, is located here.

> **NOTE**
> If you use enrollment restrictions to prevent (block) personally owned devices from enrolling, you will need to add the devices using corporate device identifiers, prior to enrollment.

Next steps

Learn more about Automated Device Enrollment.

Set up iOS/iPadOS and iPadOS User Enrollment (preview)

9/23/2022 • 3 minutes to read • Edit Online

You can set up Intune to enroll iOS/iPadOS and iPadOS devices using Apple's User Enrollment process. User Enrollment gives admins a streamlined subset of management options compared to other enrollment methods.

For more information about the options available with User Enrollment, see User Enrollment supported actions, passwords, and other options.

> **NOTE**
> Support for Apple's User Enrollment in Intune is currently in preview.

Prerequisites

- Mobile Device Management (MDM) Authority
- Apple MDM Push certificate
- Managed Apple ID
- iOS 13 or later
- Federated Authentication with Apple Business Manager

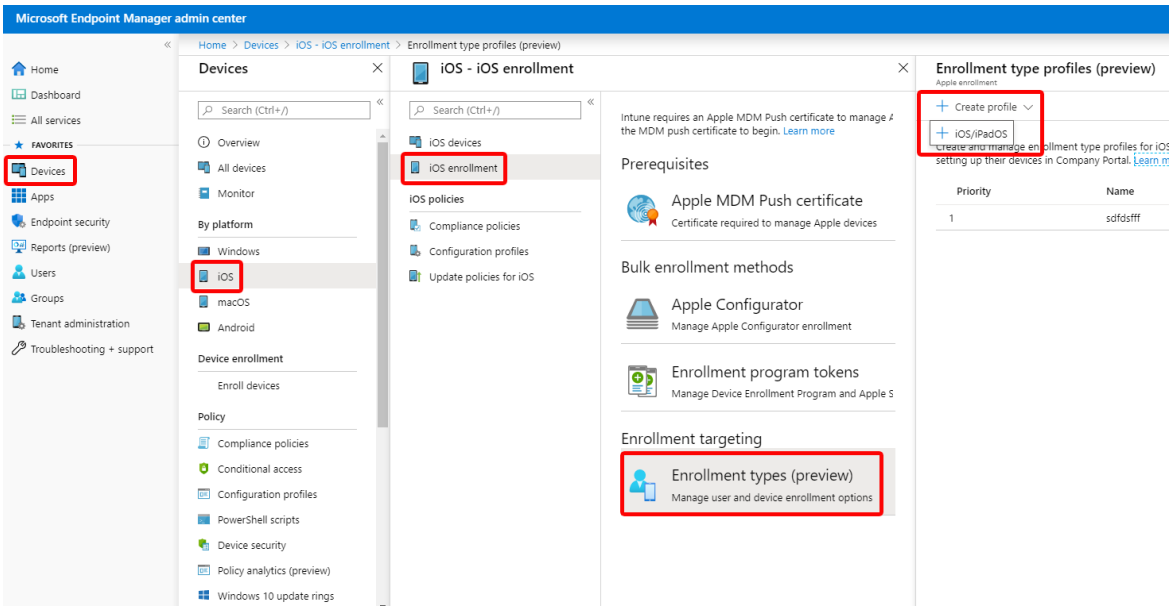
> **NOTE**
> Apple released iPadOS in September 2019, which introduced a change that can affect Microsoft Azure Active Directory (Azure AD) and Intune customers who use Conditional Access policies in their organization. For more information about how this affects your policies and what actions to take, see Evaluate and update Conditional Access policies after new iPadOS release.

Create a User Enrollment profile in Intune

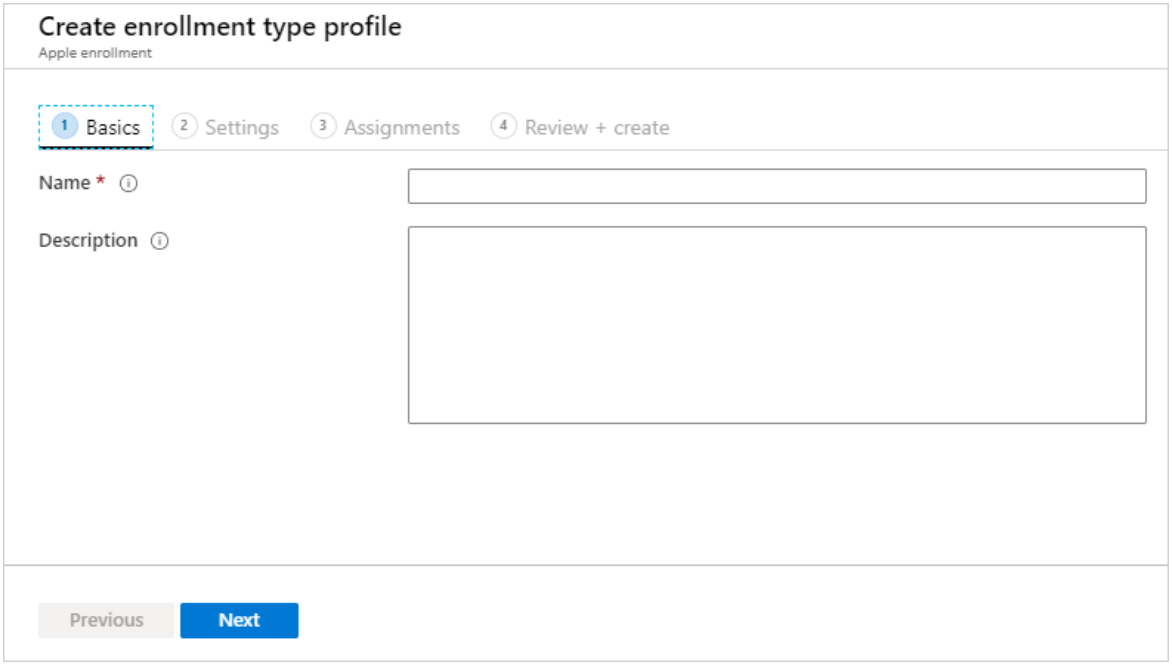
> **NOTE**
> An iOS User Enrollment profile overrides an enrollment restriction policy.

An enrollment profile defines the settings applied to a group of devices during enrollment.

1. Federate your Azure AD instance with Apple Business Manager or Apple School Manager. For more information, see Intro to federated authentication with Apple Business Manager.
2. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS enrollment** > **Enrollment types (preview)** > **Create profile** > **iOS/iPadOS**. This profile is where you'll indicate what enrollment experience your iOS/iPadOS and iPadOS end users will have on devices not enrolled through a corporate Apple method. If you'd like to make changes, you can edit this profile after you've created it.

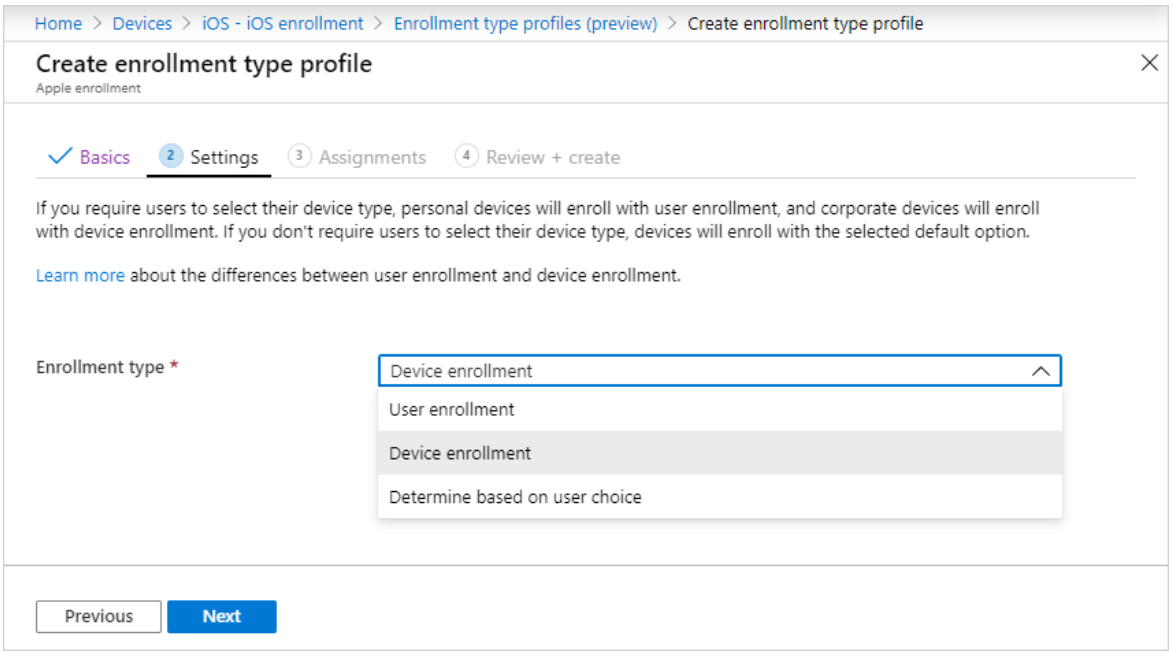


3. On the **Basics** page, enter a **Name** and **Description** for the profile for administrative purposes. Users don't see these details. You can use this **Name** field to create a dynamic group in Azure Active Directory. Use the profile name to define the enrollmentProfileName parameter to assign devices with this enrollment profile. Learn more about Azure Active Directory dynamic groups.



4. Select **Next**.

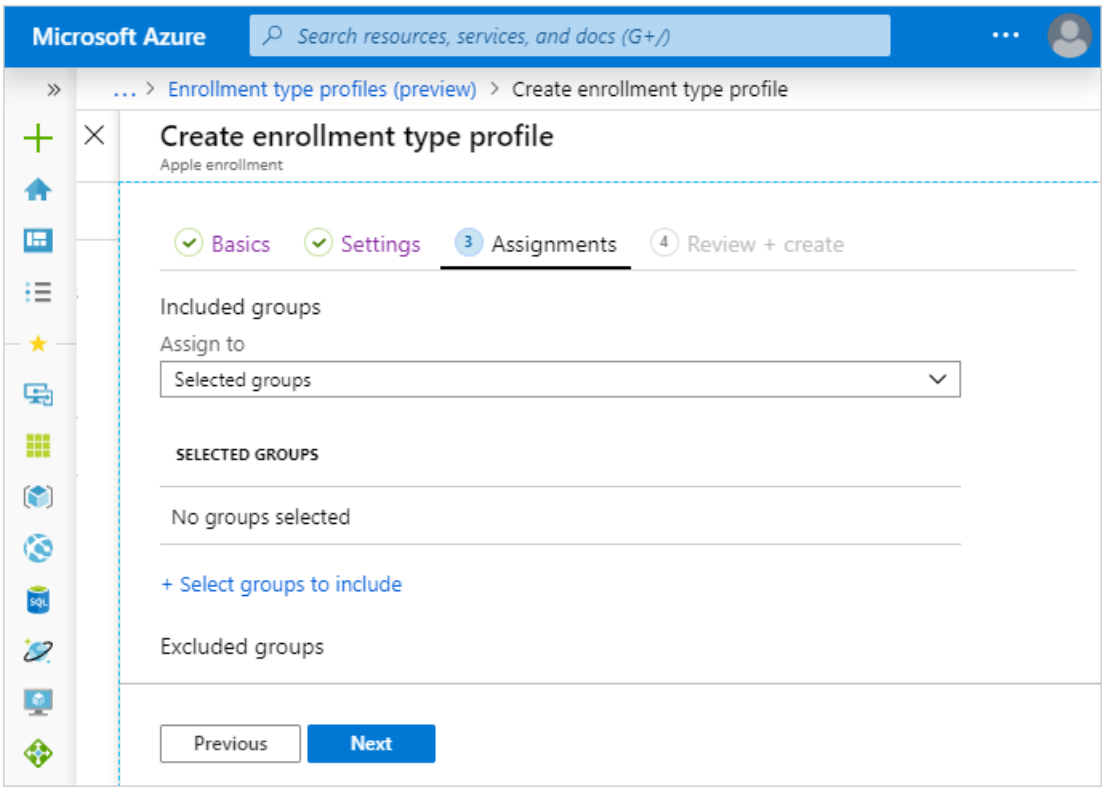
5. On the **Settings** page, select one of the following options for **Enrollment type**:



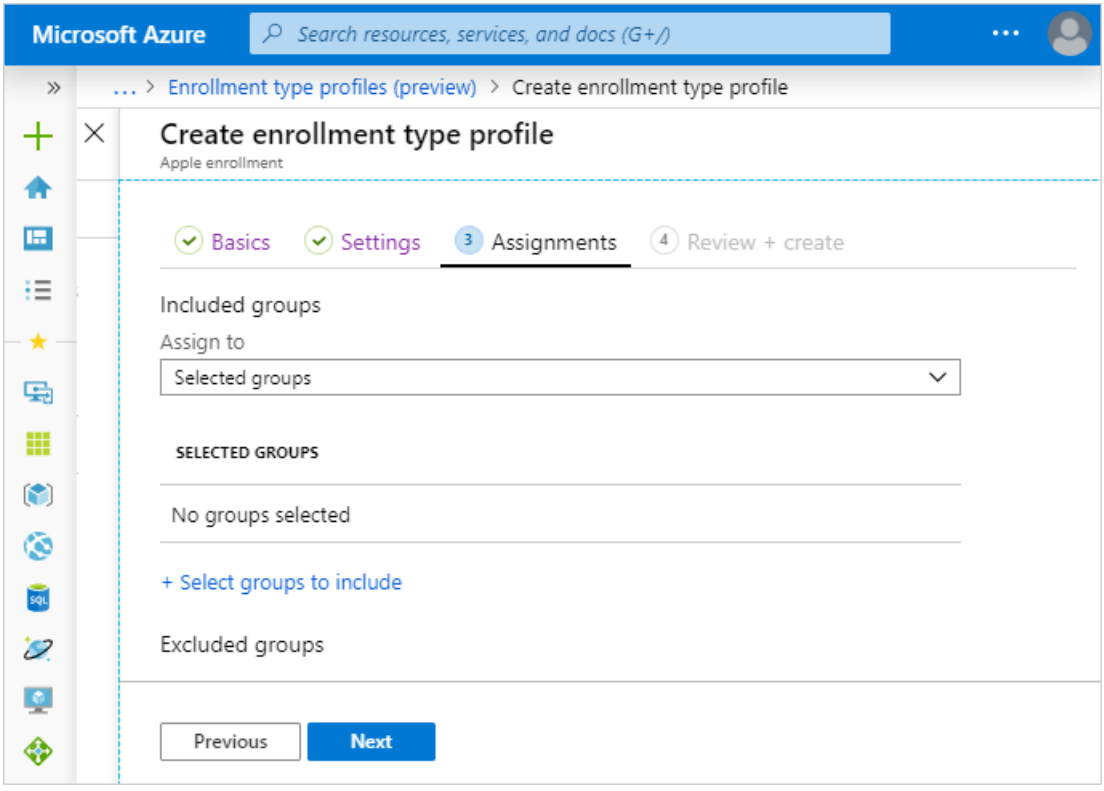
- **Device enrollment**: All the users in this profile will use Device Enrollment.
- **User enrollment**: All the users in this profile will use User Enrollment.
- **Determine based on user choice**: All users in this group will be given the choice of which enrollment type to use. When users enroll their devices, they'll see an option to choose between **I own this device** and **(Company) owns this device**. If they choose the latter, the device will be enrolled by using Device Enrollment. If the user chooses **I own this device**, they'll get another option to secure the entire device or only secure work-related apps and data. The end user's selection of whether they own the device determines which enrollment type is implemented on their device. This user choice is also reflected in the Device Ownership attribute in Intune. To learn more about the user experience, see Set up iOS/iPadOS device access to your company resources.

6. Select **Next**.

7. On the **Assignments** page, choose the user groups containing the users to which you want this profile assigned. You can choose to assign the profile to all users or specific groups. All users in the selected groups will use the enrollment type chosen above. Device groups aren't supported for User Enrollment scenarios because the feature is based on user identities, rather than devices. You can choose to assign the profile to all users or specific groups.



8. Select **Next**.
9. On the **Review and Create** page, review your choices, and then select **Create** to assign the profile to the users.



Profile priority

After you've created more than one enrollment type profile, you can change the priority order in which they're applied.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS enrollment** > **Enrollment types (preview)**.

2. Drag and drop the profiles in the list in the order you want them applied.

In case of conflicts between profiles for any user, the higher priority profile is applied for the user.

Intune actions and options supported with Apple User Enrollment

9/23/2022 • 3 minutes to read • Edit Online

User Enrollment supports a subset of device management options. If a pre-existing configuration profile is applied to a User Enrollment device, only settings supported by User Enrollment will be applied to that device.

> **NOTE**
> Support for Apple's User Enrollment in Intune is currently in preview for iOS and iPadOS.

Password settings

On User Enrollment devices, if you configure any password setting, then the **Simple passwords** settings is automatically set to **Block**, and a 6 digit PIN is enforced.

For example, you configure the **Password expiration** setting, and push this policy to user-enrolled devices. On the devices, the following happens:

- The **Password expiration** setting is ignored.
- Simple passwords, such as `111111` or `123456`, aren't allowed.
- A 6 digit pin is enforced.

Administrator remote device actions and options

Admins can perform the following actions and options on User Enrollment devices:

- Retire
- Delete
- Remote Lock
- Sync

All other actions aren't supported.

End-user actions

On User Enrollment devices, end users can perform these actions on their devices from the Company Portal application and website:

- Rename. This action applies only to the user-facing name within the Company Portal. It won't fully rename the device outside of that context.
- Remove
- Remote Lock
- Check Status

App deployment options

Following app types can be deployed on User Enrollment devices:

- User-licensed Volume Purchasing Plan (VPP) apps including custom apps
- Line-of-business (LOB) apps
- Web apps

Other supported options

The following options are supported in Intune for devices enrolled by using Apple User enrollment:

- Per-App VPN. This support excludes Safari Domains as User Enrollment doesn't support configuring Safari settings.
- WiFi
- Corporate app removal upon unenrollment
- Jailbreak Detection

The following restrictions are supported:

- View corporate documents in unmanaged apps
- Viewing non-corporate documents in corporate apps
- Allow unmanaged apps to read from managed contacts accounts
- AirDrop as an unmanaged destination
- Required encrypted backup
- Managed apps sync to cloud
- Control Center access while device locked
- Notification Center access while device locked
- Today view while device locked
- Block screenshots
- Block Enterprise Book backup
- Block Enterprise Book metadata sync
- Require encrypted backup
- Require watch wrist detection
- Block Siri
- Block Siri while device is locked
- Require Safari fraud warnings
- Block diagnostics submission to Apple

Options not supported

The following options aren't supported on devices enrolled with User Enrollment. If you need these options, check out Device Enrollment for personally-owned devices or Automated Device Enrollment for corporate devices.

- Collect app inventory for apps outside of the managed APFS volume.
- Collect inventory of certificates and provisioning profiles outside of the managed APFS volume.
- Collect UDID and other persistent device identifiers, such as phone number, serial number, and IMEI
- User Enrollment supports a unique enrollment ID for each device enrolled, but this ID doesn't persist after unenrollment.
- The following Intune features aren't supported because of this limitation:
- SCEP User profiles with Subject Name Format of Serial Number.
- Device-level VPN.
- Device-licensed VPP app deployment.

- Install App Store apps as managed apps.
- MDM control of applications outside of the managed APFS volume.
- Application Protection Policies will still apply to these apps. However, you won't be able to take over management or deploy a managed version of these apps unless the user deletes them from their device.
- Actions, configurations, settings, and commands requiring supervision.

Known issues in preview

- VPP license revocation: A notification that the license has been revoked does not appear. The current behavior is that the revocation is successful, but the end user is not notified.
- VPP application reporting: In the report located at Client Apps > Apps > [App Name] > Device Install Status, VPP applications deployed to User Enrolled devices are reporting as "failed", even when the application successfully deploys to the device.
- VPP License Assignment: If the VPP license is already associated with the AppleID, or the user has another device enrolled with Device Enrollment, the license will associate to the AppleID successfully. However, if the only iOS device the user has enrolled is User Enrolled, the VPP license assignment will fail and install will fail with **Can't Find VPP License For App** (0x87D13B95). Re-enrolling the device with Device Enrollment to allow the assignment then re-enrolling again as User Enrollment resolves the assignment.
- Application reporting: For app types unsupported with User Enrollment, reports may provide irrelevant error messages.
- Company Portal app experience: Users see all applications targeted to them, regardless of whether those application types are supported for User Enrolled devices.
- Company Portal app experience: Users see the same text indicating what organizations can see for User and Device Enrollment if the admin has customized the text indicating what organizations can't see.

Next steps

Set up iOS/iPadOS and iPadOS User Enrollment

Set up iOS/iPadOS device enrollment with Apple School Manager

9/23/2022 • 9 minutes to read • Edit Online

You can set up Intune to enroll iOS/iPadOS devices purchased through the Apple School Manager program. Using Intune with Apple School Manager, you can enroll large numbers of iOS/iPadOS devices without ever touching them. When a student or teacher turns on the device, Setup Assistant runs with preconfigured settings and the device enrolls into management.

To enable Apple School Manager enrollment, you use both the Intune and Apple School Manager portals. A list of serial numbers or a purchase order number is required so you can assign devices to Intune for management. You create Automated Device Enrollment (ADE) enrollment profiles containing settings that applied to devices during enrollment.

Apple School Manager enrollment can't be used with Apple's Automated Device Enrollment or the device enrollment manager.

Prerequisites

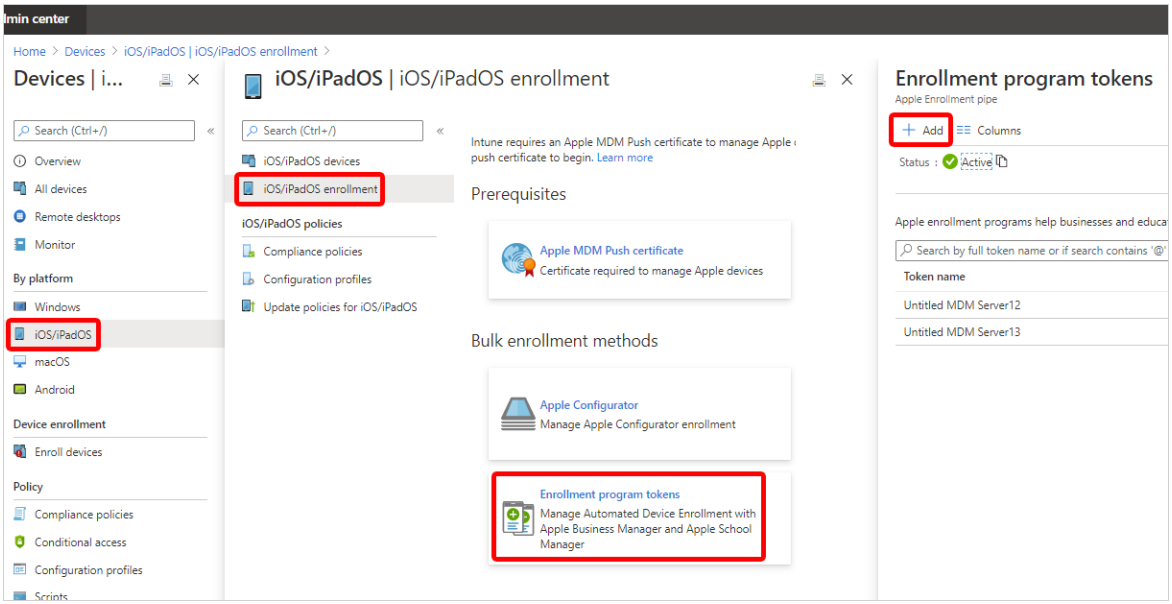
- Apple Mobile Device Management (MDM) Push certificate
- MDM Authority
- If using ADFS, user affinity requires WS-Trust 1.3 Username/Mixed endpoint. Learn more.
- Devices purchased from the Apple School Management program

Get an Apple token and assign devices

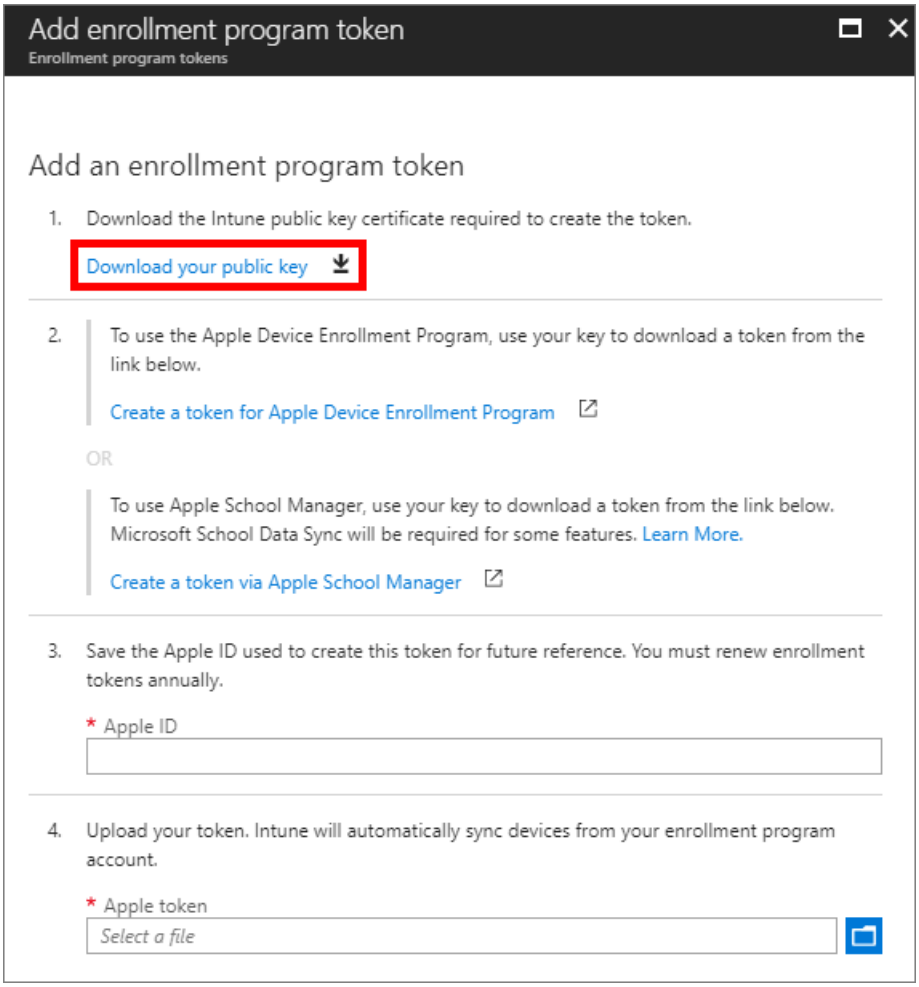
Before you can enroll corporate-owned iOS/iPadOS devices with Apple School Manager, you need a token (.p7m) file from Apple. This token lets Intune sync information about Apple School Manager-participating devices. It also permits Intune to perform enrollment profile uploads to Apple and to assign devices to those profiles. While you are in the Apple portal, you can also assign device serial numbers to manage.

Step 1. Download the Intune public key certificate required to create an Apple token

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment Program Tokens** > **Add**.

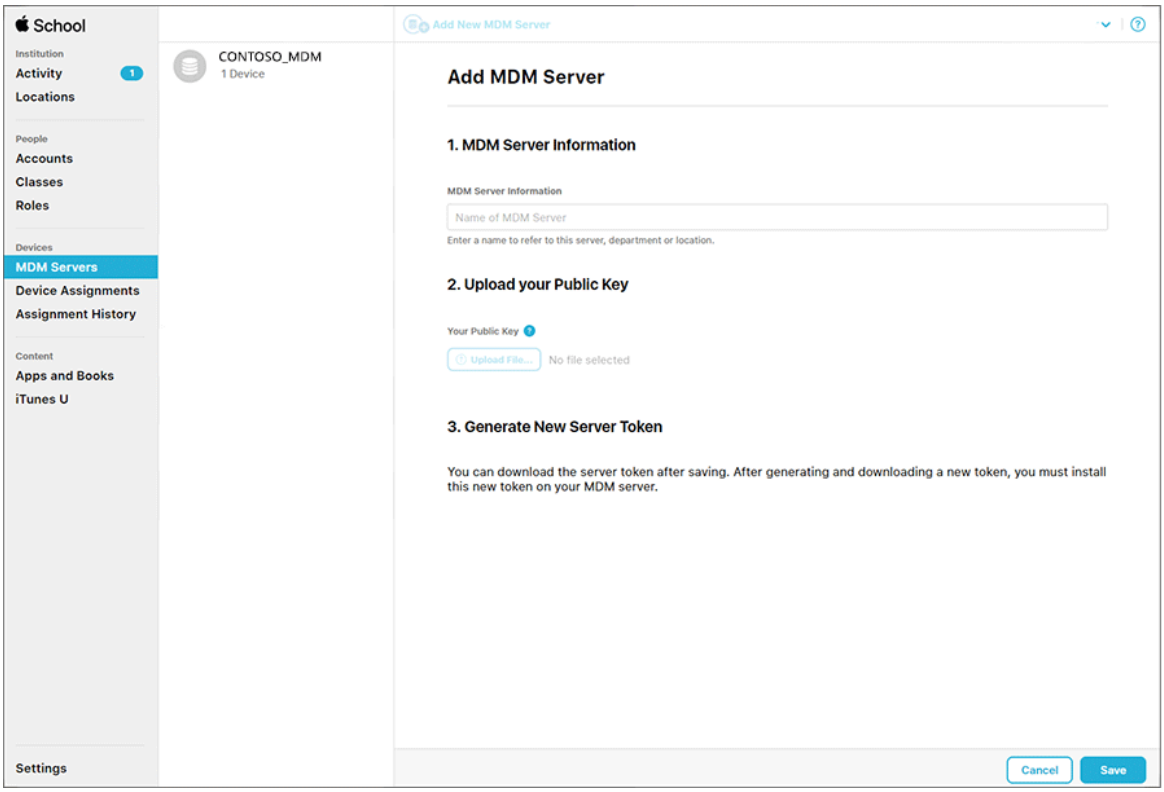


2. In the **Enrollment program token** blade, choose **Download your public key** to download and save the encryption key (.pem) file locally. The .pem file is used to request a trust-relationship certificate from the Apple School Manager portal.

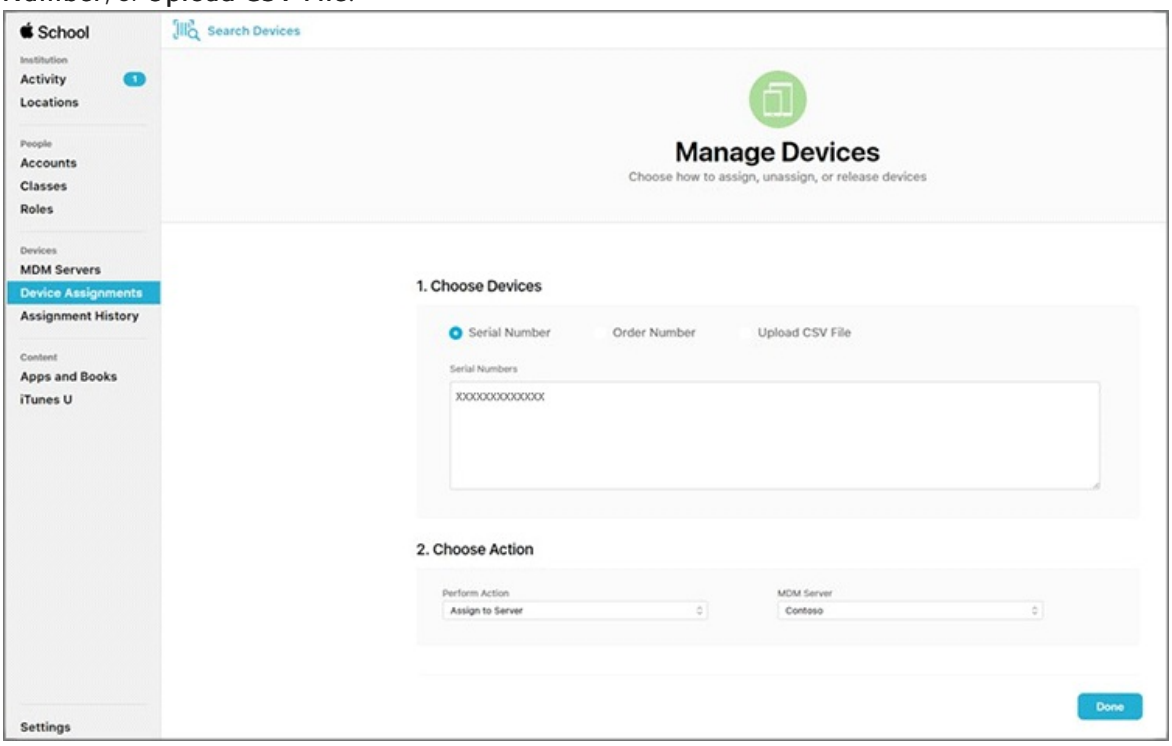


Step 2. Download a token and assign devices

1. Choose **Create a token via Apple School Manager**, and sign in to Apple School with your company Apple ID. You can use this Apple ID to renew your Apple School Manager token.
2. In the Apple School Manager portal, go to **MDM Servers**, and then choose **Add MDM Server** (upper right).
3. Enter the **MDM Server Name**. The server name is for your reference to identify the mobile device management (MDM) server. It isn't the name or URL of the Microsoft Intune server.



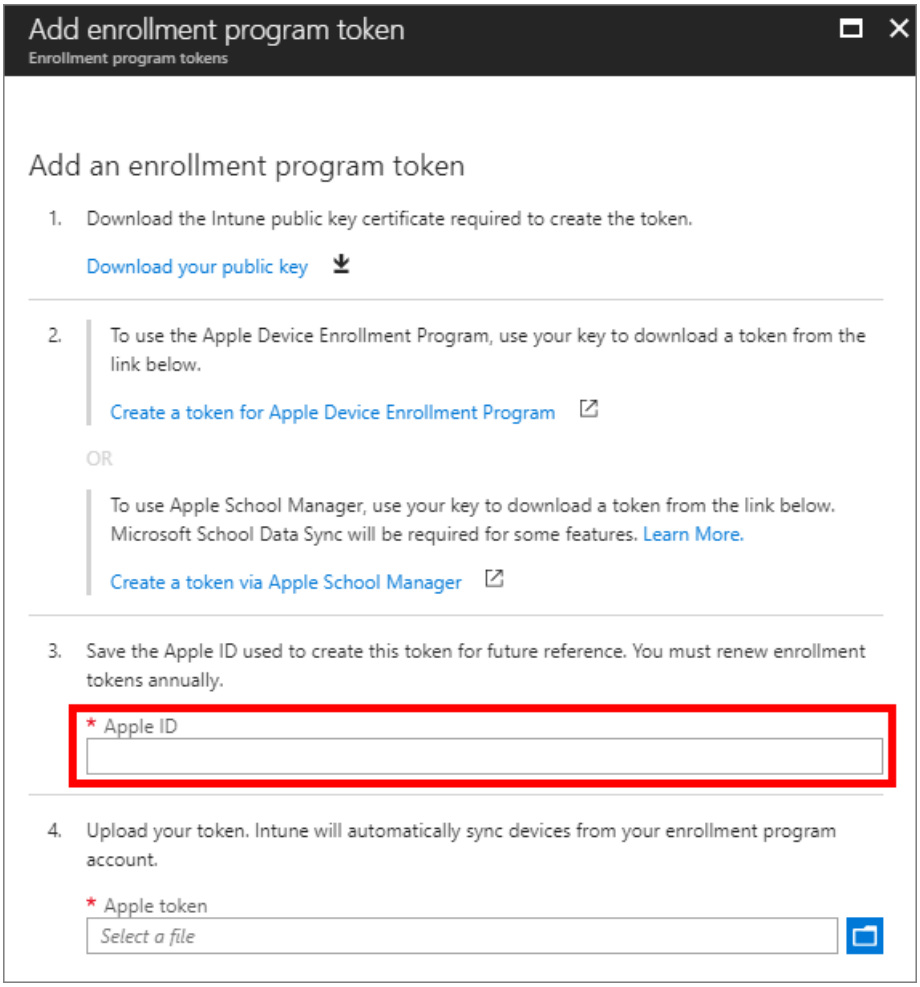
4. Choose **Upload File...** in the Apple portal, browse to the .pem file, and choose **Save MDM Server** (lower right).
5. Choose **Get Token** and then download the server token (.p7m) file to your computer.
6. Go to **Device Assignments**, and **Choose Device** by manual entry of **Serial Numbers**, **Order Number**, or **Upload CSV File**.



7. Choose the action **Assign to Server**, and choose the **MDM Server** you created.
8. Specify how to **Choose Devices**, then provide device information and details.
9. Choose **Assign to Server** and choose the <ServerName> specified for Microsoft Intune, and then choose **OK**.

Step 3. Save the Apple ID used to create this token

In the Microsoft Endpoint Manager admin center, provide the Apple ID for future reference.



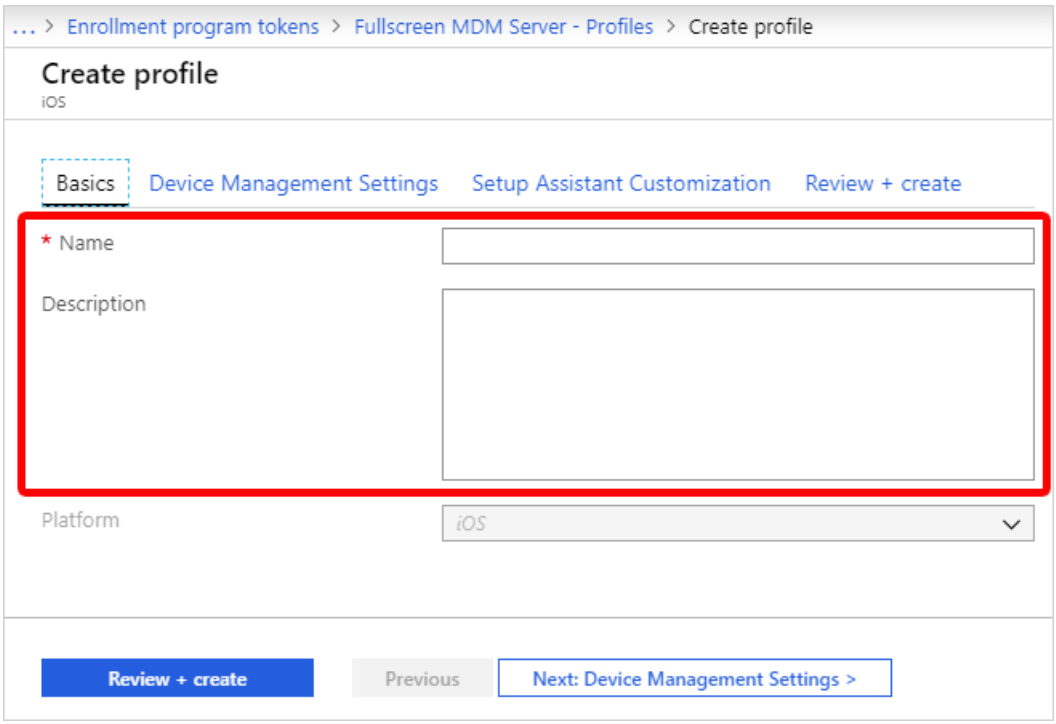
Step 4. Upload your token

In the **Apple token** box, browse to the certificate (.pem) file, choose **Open**, and then choose **Create**. With the push certificate, Intune can enroll and manage iOS/iPadOS devices by pushing policy to enrolled mobile devices. Intune automatically synchronizes your Apple School Manager devices from Apple.

Create an Apple enrollment profile

Now that you've installed your token, you can create an enrollment profile for Apple School devices. A device enrollment profile defines the settings applied to a group of devices during enrollment.

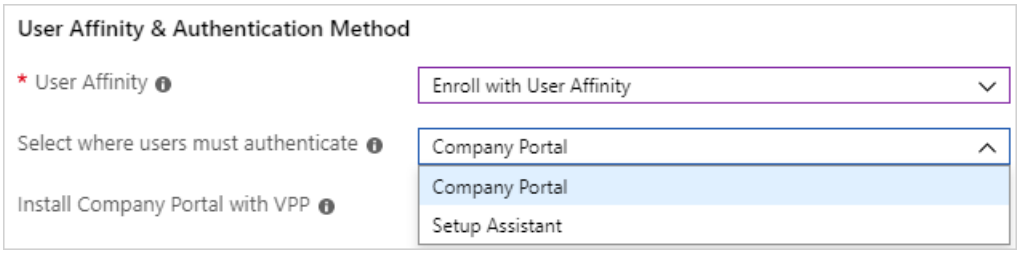
1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment program tokens**.
2. Select a token, choose **Profiles**, and then choose **Create profile**.
3. Under **Create Profile**, enter a **Name** and **Description** for the profile for administrative purposes. Users don't see these details. You can use this **Name** field to create a dynamic group in Azure Active Directory. Use the profile name to define the enrollmentProfileName parameter to assign devices with this enrollment profile. Learn more about Azure Active Directory dynamic groups.



4. For **User Affinity**, choose whether devices with this profile must enroll with or without an assigned user.

   - **Enroll with User Affinity** - Choose this option for devices that belong to users and that want to use the company portal for services like installing apps. This option also lets users authenticate their devices by using the company portal. If using ADFS, user affinity requires WS-Trust 1.3 Username/Mixed endpoint. Learn more. Apple School Manager's Shared iPad mode requires user enroll without user affinity.
   - **Enroll without User Affinity** - Choose this option for devices unaffiliated with a single user, such as a shared device. Use this option for devices that perform tasks without accessing local user data. Apps like the Company Portal app don't work.

5. If you chose **Enroll with User Affinity**, you can let users authenticate with Company Portal instead of the Apple Setup Assistant.



> **NOTE**
>
> If you want do any of the following, set **Authenticate with Company Portal instead of Apple Setup Assistant** to **Yes**.
>
> - use multifactor authentication
> - prompt users who need to change their password when they first sign in
> - prompt users to reset their expired passwords during enrollment
>
> These aren't supported when authenticating with Apple Setup Assistant.

6. Choose **Device Management Settings** and choose if you want devices using this profile to be supervised. **Supervised** devices give you more management options and disabled Activation Lock by default. Microsoft recommends using ADE as the mechanism for enabling Intune's supervised mode,

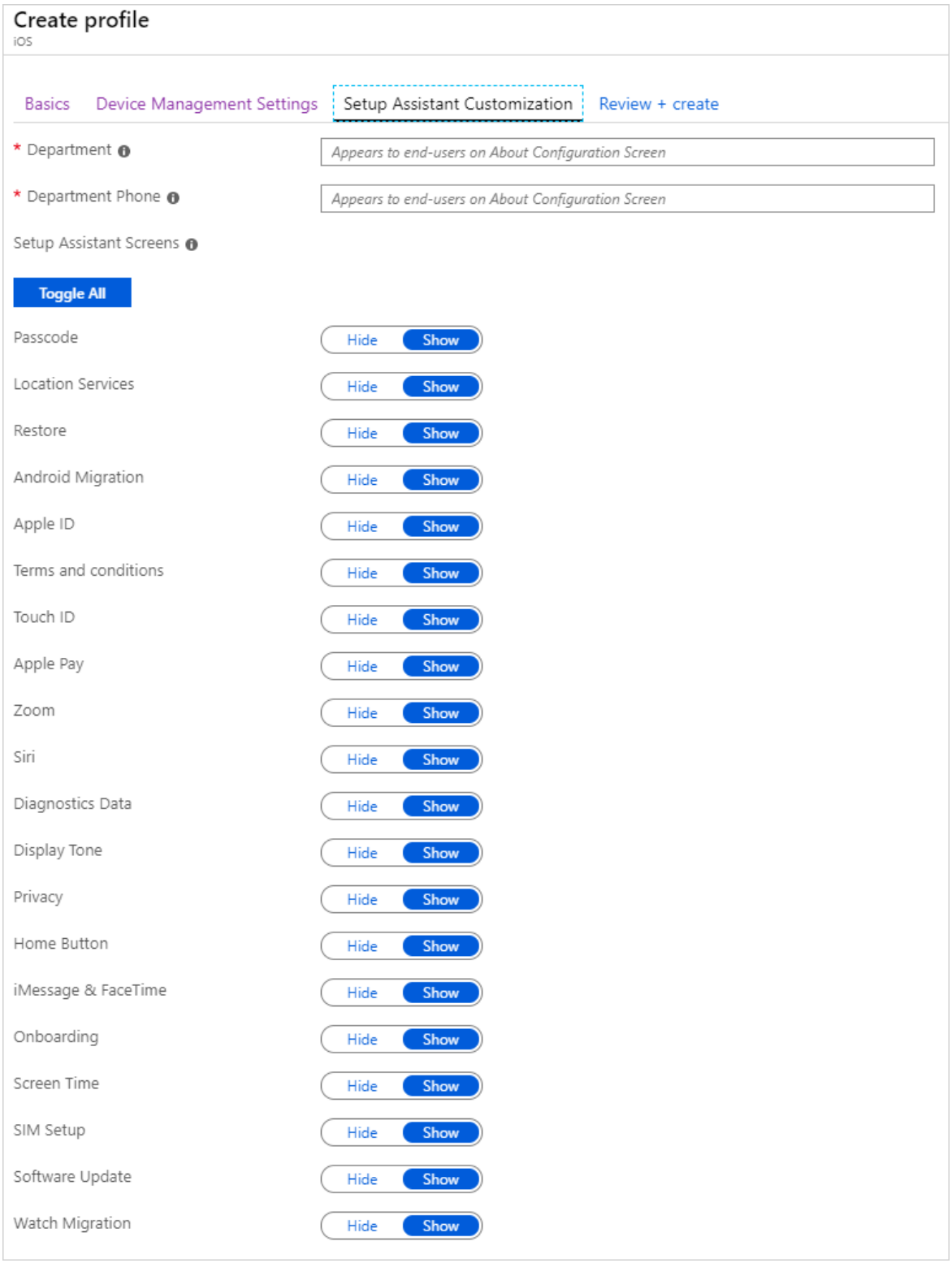
especially for organizations that are deploying large numbers of iOS/iPadOS devices.

Users are notified that their devices are supervised in two ways:

- The lock screen says: "This iPhone is managed by Contoso."
- The **Settings** > **General** > **About** screen says: "This iPhone is supervised. Contoso can monitor your Internet traffic and locate this device."

> **NOTE**
> A device enrolled without supervision can only be reset to supervised by using the Apple Configurator. Resetting the device in this manner requires connecting an iOS/iPadOS device to a Mac with a USB cable. Learn more about this on Apple Configurator docs.

7. Choose if you want locked enrollment for devices using this profile. **Locked enrollment** disables iOS/iPadOS settings that allow the management profile to be removed from the **Settings** menu. After device enrollment, you can't change this setting without wiping the device. Such devices must have the **Supervised** Management Mode set to *Yes*.
8. You can let multiple users sign on to enrolled iPads by using a managed Apple ID. To do so, choose **Yes** under **Shared iPad** (this option requires **Enroll without User Affinity** and **Supervised** mode set to **Yes**.) Managed Apple IDs are created in the Apple School Manager portal. Learn more about shared iPad and Apple's shared iPad requirements.
9. Choose if you want the devices using this profile to be able to **Sync with computers**. **Deny All** means that all devices using this profile won't be able to sync with any data on any computer. If you choose **Allow Apple Configurator by certificate**, you must choose a certificate under **Apple Configurator Certificates**.
10. If you chose **Allow Apple Configurator by certificate** in the previous step, choose an Apple Configurator Certificate to import.
11. You can specify a naming format for devices that is automatically applied when they enroll. To do so, select **Yes** under **Apply device name template**. Then, in the **Device Name Template** box, enter the template to use for the names using this profile. You can specify a template format that includes the device type and serial number.
12. Choose **OK**.
13. Choose **Setup Assistant Settings** to configure the following profile settings:



SETTING	DESCRIPTION
Department Name	Appears when users tap **About Configuration** during activation.
Department Phone	Appears when the user clicks the **Need Help** button during activation.
Setup Assistant Options	The following optional settings can be set up later in the iOS/iPadOS **Settings** menu.

SETTING	DESCRIPTION
Passcode	Prompt for passcode during activation. Always require a passcode for unsecured devices unless access is controlled in some other manner (like kiosk mode that restricts the device to one app).
Location Services	If enabled, Setup Assistant prompts for the service during activation.
Restore	If enabled, Setup Assistant prompts for iCloud backup during activation.
iCloud and Apple ID	If enabled, Setup Assistant prompts the user to sign in an Apple ID and the Apps & Data screen will allow the device to be restored from iCloud backup.
Terms and Conditions	If enabled, Setup Assistant prompts users to accept Apple's terms and conditions during activation.
Touch ID	If enabled, Setup Assistant prompts for this service during activation.
Apple Pay	If enabled, Setup Assistant prompts for this service during activation.
Zoom	If enabled, Setup Assistant prompts for this service during activation.
Siri	If enabled, Setup Assistant prompts for this service during activation.
Diagnostic Data	If enabled, Setup Assistant prompts for this service during activation.

14. Choose **OK**.
15. To save the profile, choose **Create**.

Connect School Data Sync

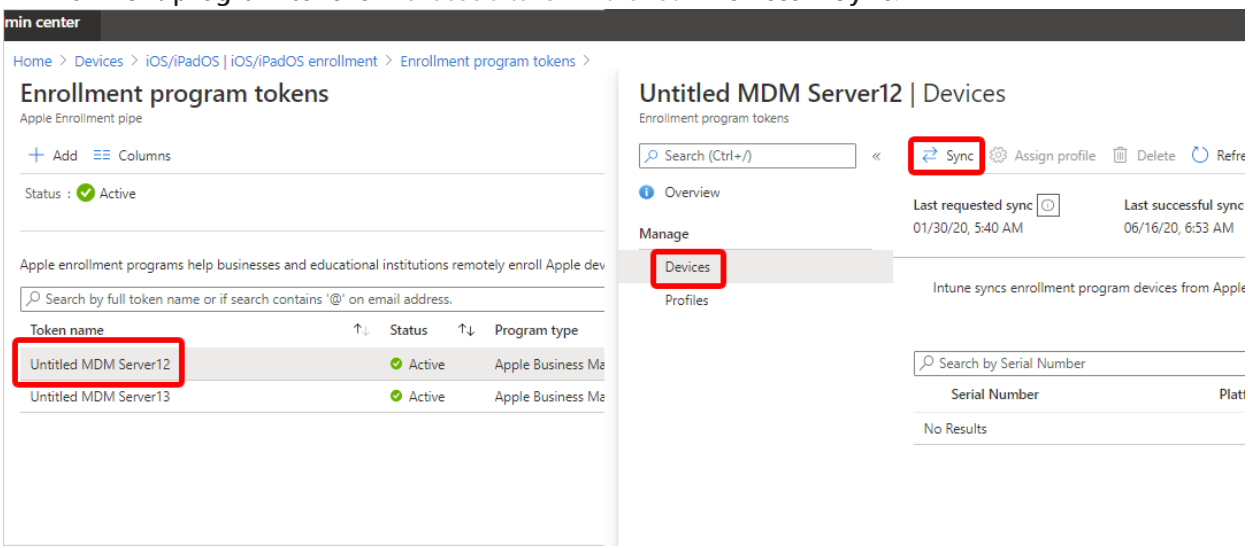
(Optional) Apple School Manager supports synchronizing class roster data to the Azure Active Directory (AD) using Microsoft School Data Sync (SDS). You can only sync one token with SDS. If you set up another token with School Data Sync, SDS will be removed from the token that previously had it. A new connection will replace the current token. Complete the following steps to use SDS to sync school data.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment program tokens**.
2. Select an Apple School Manager token and then choose **School Data Sync**.
3. Under **School Data Sync**, choose **Allow**. This setting allows Intune to connect with SDS in Microsoft 365.
4. To enable a connection between Apple School Manager and Azure AD, choose **Set up Microsoft School Data Sync**. Learn more about how to set up School Data Sync.
5. Click **Save** > **OK**.

Sync managed devices

After Intune has been assigned permission to manage your Apple School Manager devices, synchronize Intune with the Apple service to see your managed devices in Intune.

In the Microsoft Endpoint Manager admin center), choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment program tokens** > choose a token in the list > **Devices** > **Sync**.



To follow Apple's terms for acceptable enrollment program traffic, Intune imposes the following restrictions:

- A full sync can run no more than once every seven days. During a full sync, Intune refreshes every Apple serial number assigned to Intune. If a full sync is attempted within seven days of the previous full sync, Intune only refreshes serial numbers that aren't already listed in Intune.
- Any sync request is given 15 minutes to finish. During this time or until the request succeeds, the **Sync** button is disabled.
- Intune syncs new and removed devices with Apple every 24 hours.

> **NOTE**
> You can also assign Apple School Manager serial numbers to profiles from the **Enrollment Program Devices** blade.

Assign a profile to devices

Apple School Manager devices managed by Intune must be assigned an enrollment profile before they're enrolled.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Enrollment program tokens** > choose a token in the list.
2. Choose **Devices** > choose devices in the list > **Assign profile**.
3. Under **Assign profile**, choose a profile for the devices, and then choose **Assign**.

Distribute devices to users

You have enabled management and syncing between Apple and Intune, and assigned a profile to let your Apple School devices enroll. You can now distribute devices to users. When an iOS/iPadOS Apple School Manager device is turned on, it's enrolled for management by Intune. Profiles can't be applied to activated devices currently in use until the device is wiped.

Set up iOS/iPadOS device enrollment with Apple Configurator

9/23/2022 • 8 minutes to read • Edit Online

Intune supports the enrollment of iOS/iPadOS devices using Apple Configurator running on a Mac computer. Enrolling with Apple Configurator requires that you USB-connect each iOS/iPadOS device to a Mac computer to set up corporate enrollment. You can enroll devices into Intune with Apple Configurator in two ways:

- **Setup Assistant enrollment** - Wipes the device and prepares it to enroll during Setup Assistant.
- **Direct enrollment** - Does not wipe the device and enrolls the device through iOS/iPadOS settings. This method only supports devices with **no user affinity**.

Apple Configurator enrollment methods can't be used with the device enrollment manager.

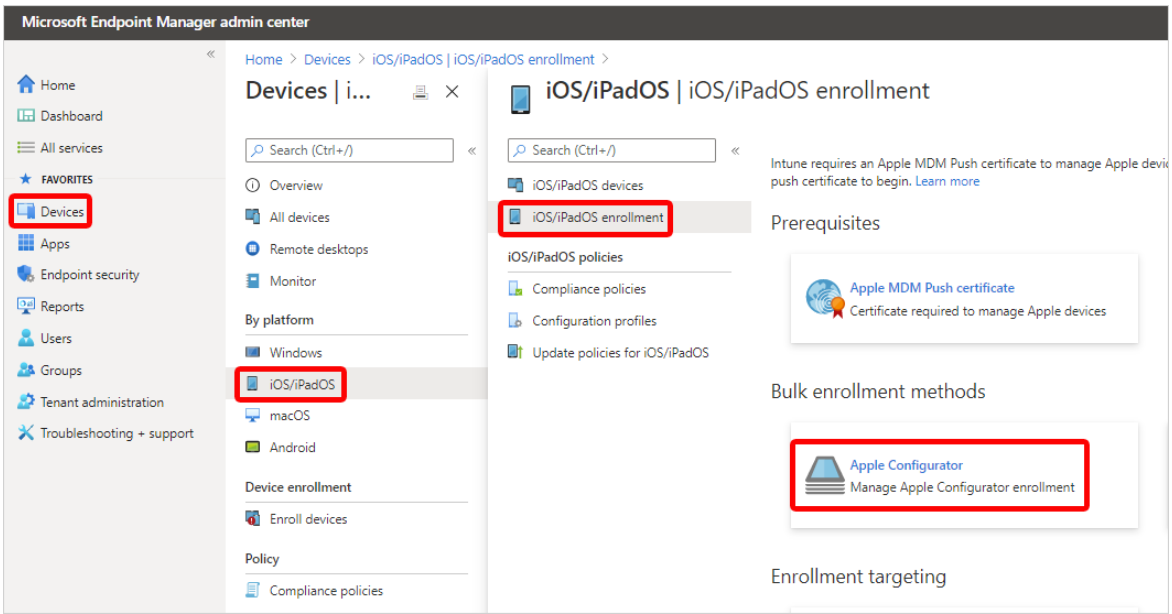
Prerequisites

- Physical access to iOS/iPadOS devices
- Set MDM authority
- An Apple MDM push certificate
- Device serial numbers (Setup Assistant enrollment only)
- USB connection cables
- macOS computer running Apple Configurator 2.0

Create an Apple Configurator profile for devices

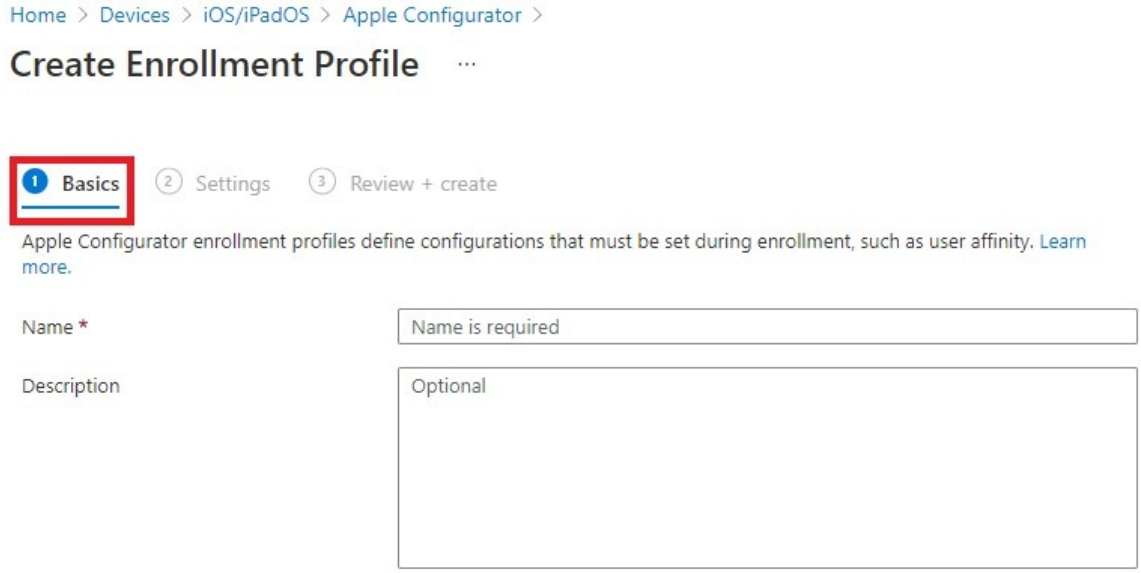
A device enrollment profile defines the settings applied during enrollment. These settings are applied only once. Follow these steps to create an enrollment profile to enroll iOS/iPadOS devices with Apple Configurator.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Apple Configurator**.



2. Choose **Profiles** > **Create**.

3. Under **Create Enrollment Profile**, on the **Basics** tab, type a **Name** and **Description** for the profile for administrative purposes. Users do not see these details. You can use this Name field to create a dynamic group in Azure Active Directory. Use the profile name to define the enrollmentProfileName parameter to assign devices with this enrollment profile. Learn more about Azure Active Directory dynamic groups.



4. Click **Next** to display the **Settings** page.

5. For **User Affinity**, choose whether devices with this profile must enroll with or without an assigned user.

   - **Enroll with user affinity** - Choose this option for devices that belong to users and that want to use the company portal for services like installing apps. The device must be affiliated with a user with Setup Assistant and can then access company data and email. Only supported for Setup Assistant enrollment. User affinity requires WS-Trust 1.3 Username/Mixed endpoint. Learn more.
   - **Enroll without User Affinity** - Choose this option for devices unaffiliated with a single user. Use this for devices that perform tasks without accessing local user data. Apps requiring user affiliation (including the Company Portal app used for installing line-of-business apps) won't work. Required for direct enrollment.

> **NOTE**
>
> When **Enroll with user affinity** is selected, make sure that the device is affiliated with a user with Setup Assistant within the first 24 hours of the device being enrolled. Otherwise enrollment might fail, and a factory reset will be needed to enroll the device.

6. If you chose **Enroll with User Affinity**, you have the option to let users authenticate with Company Portal instead of the Apple Setup Assistant.

> **NOTE**
>
> If you want do any of the following, set **Authenticate with Company Portal instead of Apple Setup Assistant** to **Yes**.
>
> - use multifactor authentication
> - prompt users who need to change their password when they first sign in
> - prompt users to reset their expired passwords during enrollment
>
> These are not supported when authenticating with Apple Setup Assistant.

7. Choose **Create** to save the profile.

Setup Assistant enrollment

Add Apple Configurator serial numbers

1. Create a two-column, comma-separated value (.csv) list without a header. Add the serial number in the left column, and the details in the right column. The current maximum for the list is 5,000 rows. In a text editor, the .csv list looks like this:

   F7TLWCLBX196,device details
   DLXQPCWVGHMJ,device details

   Learn how to find an iOS/iPadOS device serial number.

2. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Apple Configurator** > **Devices** > **Add**.

3. Select an **Enrollment profile** to apply to the serial numbers you're importing. If you want the new serial number details to overwrite any existing details, choose **Overwrite details for existing identifiers**.

4. Under **Import Devices**, browse to the csv file of serial numbers, and select **Add**.

Reassign a profile to device serial numbers

You can assign an enrollment profile when you import iOS/iPadOS serial numbers for Apple Configurator enrollment. You can also assign profiles from two places in the Azure portal:

- **Apple Configurator devices**
- **AC profiles**

Assign from Apple Configurator devices

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Apple Configurator** > **Devices** > choose the serial numbers > **Assign profile**.
2. Under **Assign Profile**, choose the **New profile** you want to assign, and then choose **Assign**.

Assign from profiles

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Apple Configurator** > **Profiles** > choose a profile.
2. In the profile, choose **Devices assigned**, and then choose **Assign**.
3. Filter to find device serial numbers you want to assign to the profile, select the devices, and then choose **Assign**.

Export the profile

After you create the profile and assign serial numbers, you must export the profile from Intune as a URL. You then import it into Apple Configurator on a Mac for deployment to devices.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Apple Configurator** > **Profiles** > choose the profile to export.

2. On the profile, select **Export Profile**.

3. Copy the **Profile URL**. You can then add it in Apple Configurator to define the Intune profile used by iOS/iPadOS devices.

   Next you import this profile to Apple Configurator in the following procedure to define the Intune profile used by iOS/iPadOS devices.

Enroll devices with Setup Assistant

1. On a Mac computer, open **Apple Configurator 2**. In the menu bar, choose **Apple Configurator 2**, and then choose **Preferences**.

   > **WARNING**
   > Devices are reset to factory configurations during the enrollment process. As a best practice, reset the device and turn it on. Devices should be at the **Hello** screen when you connect the device. If the device was already registered with the Apple ID account, the device must be deleted from the Apple iCloud before starting the enrollment process. The prompt error appears as "Unable to activate [Device name]".

2. In the **preferences** pane, select **Servers** and choose the plus symbol (+) to launch the MDM Server wizard. Choose **Next**.

3. Enter the **Host name or URL** and **enrollment URL** for the MDM server under Setup Assistant enrollment for iOS/iPadOS devices with Microsoft Intune. For the Enrollment URL, enter the enrollment profile URL exported from Intune. Choose **Next**.
   You can safely disregard a warning stating "server URL is not verified." To continue, choose **Next** until the wizard is finished.

4. Connect the iOS/iPadOS mobile devices to the Mac computer with a USB adapter.

5. Select the iOS/iPadOS devices you want to manage, and then choose **Prepare**. On the **Prepare iOS/iPadOS Device** pane, select **Manual**, and then choose **Next**.

6. On the **Enroll in MDM Server** pane, select the server name you created, and then choose **Next**.

7. On the **Supervise Devices** pane, select the level of supervision, and then choose **Next**.

8. On the **Create an Organization** pane, choose the **Organization** or create a new organization, and then choose **Next**.

9. On the **Configure iOS/iPadOS Setup Assistant** pane, choose the steps to be presented to the user, and then choose **Prepare**. If prompted, authenticate to update trust settings.

10. When the iOS/iPadOS device finishes preparing, disconnect the USB cable.

Distribute devices

The devices are now ready for corporate enrollment. Turn off the devices and distribute them to users. When users turn on their devices, Setup Assistant starts.

After users receive their devices, they must complete Setup Assistant. Devices configured with user affinity can install and run the Company Portal app to download apps and manage devices.

Direct enrollment

When you directly enroll iOS/iPadOS devices with Apple Configurator, you can enroll a device without acquiring the device's serial number. You can also name the device for identification purposes before Intune captures the device name during enrollment. The Company Portal app is not supported for directly enrolled devices. This method does not wipe the device.

Apps requiring user affiliation, including the Company Portal app used for installing line-of-business apps, cannot be installed.

Export the profile as .mobileconfig to iOS/iPadOS devices

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **iOS/iPadOS** > **iOS/iPadOS enrollment** > **Apple Configurator** > **Profiles** > choose the profile to export > **Export Profile**.

2. Under **Direct enrollment**, choose **Download profile**, and save the file. An enrollment profile file is

only valid for two weeks at which time you must re-create it.

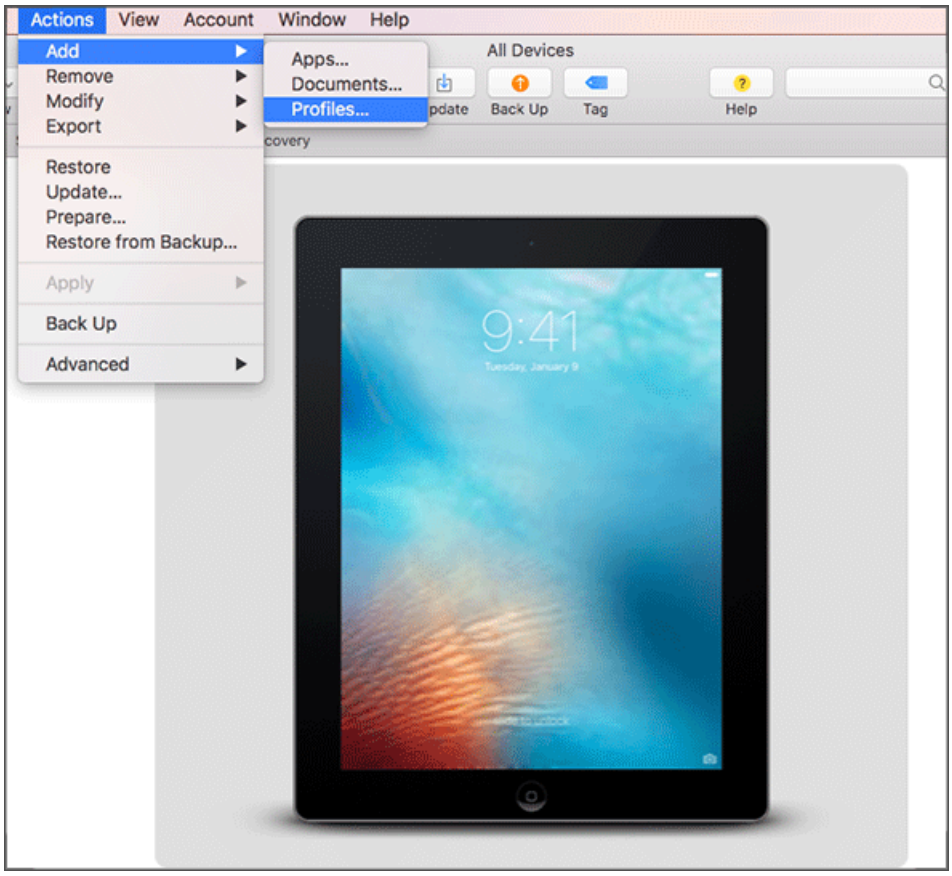
3. Transfer the file to a Mac computer running Apple Configurator to push directly as a management profile to iOS/iPadOS devices.

4. Prepare the device with Apple Configurator by using the following steps:

   a. On a Mac computer, open Apple Configurator 2.0.

   b. Connect the iOS/iPadOS device to the Mac computer with a USB cord. Close Photos, iTunes, and other apps that open for the device when the device is detected.

   c. In Apple Configurator, choose the connected iOS/iPadOS device, and then choose the **Add** button. Options that can be added to the device appear in the drop-down list. Choose **Profiles**.



   d. Use the file picker to select the .mobileconfig file that you exported from Intune, and then choose **Add**. The profile is added to the device. If the device is Unsupervised, the installation requires acceptance on the device.

5. Use the following steps to install the profile on the iOS/iPadOS device. The device must have already completed the Setup Assistant and be ready to use. If enrollment entails app deployments, the device should have an Apple ID set up because the app deployment requires that you have an Apple ID signed in for the App Store.

   a. Unlock the iOS/iPadOS device.
   b. In the **Install profile** dialog box for **Management profile**, choose **Install**.
   c. Provide the Device Passcode or Apple ID, if necessary.
   d. Accept the **Warning**, and choose **Install**.
   e. Accept the **Remote Warning**, and choose **Trust**.
   f. When the **Profile Installed** box confirms the profile as Installed, choose **Done**.

6. On the iOS/iPadOS device, open **Settings** and go to **General** > **Device Management** > **Management Profile**. Confirm that the profile installation is listed, and check the iOS/iPadOS policy restrictions and

installed apps. Policy restrictions and apps might take up to 10 minutes to appear on the device.

7. Distribute devices. The iOS/iPadOS device is now enrolled in Intune and managed.

Next steps

- Manage enrolled devices in Microsoft Endpoint Manager by using the actions and features available in the admin center. For more information about accessing device management actions and device details in the admin center, see What is Microsoft Intune device management?
- For information about enrolling macOS devices via direct enrollment with Apple Configurator, see Use Direct Enrollment for macOS devices.

iOS/iPadOS Enterprise security configuration framework

9/23/2022 • 2 minutes to read • Edit Online

The iOS/iPadOS security configuration framework is a series of recommendations for device compliance and configuration policy settings. These recommendations help you tailor your organization's mobile device security protection to your specific needs.

Security conscious organizations look at ways to ensure corporate data on mobile devices are protected. One method used to protect that data is through device enrollment. Device enrollment helps organizations:

- deploy compliance policies (like PIN strength, jailbreak/root validation, and so on).
- deploy configuration policies (like WIFI, certificates, VPN).
- manage the app lifecycle.

To help you set up a complete security scenario, Microsoft introduced a new taxonomy for security configurations in Windows 10. Intune is using a similar taxonomy for this security configuration framework. They include recommended device compliance and device restriction settings for basic, enhanced, and high security. This taxonomy is explained in the following articles:

- iOS/iPadOS framework deployment methodology: A recommended methodology for deploying the security configuration framework.
- Set app configuration policies for iOS/iPadOS devices: Configure apps on the devices to disallow personal accounts.
- iOS/iPadOS device compliance security settings: Specific configuration settings for ensuring personally owned and corporate owned devices are healthy and compliant.
- iOS/iPadOS personal device security settings: Specific configuration settings for basic, enhanced, and high security on personally owned devices.
- iOS/iPadOS supervised device security settings: Specific configuration settings for basic, enhanced, and high security on corporate owned supervised devices.

iOS/iPadOS enrollment modes

iOS/iPadOS supports several enrollment scenarios, two of which are covered as part of this framework:

- Device enrollment for personally owned devices: These devices are personally owned and used for both work and personal use.
- Supervised automated device enrollment for corporate-owned devices: These devices are corporate-owned, associated with a single user, and used exclusively for work and not personal use.

Next steps

iOS/iPadOS framework deployment methodology

iOS/iPadOS framework deployment methodology

9/23/2022 • 2 minutes to read • Edit Online

Before deploying the framework, Microsoft recommends using a ring methodology for testing validation. Defining deployment rings is generally a one-time event (or at least infrequent). However, IT should revisit these groups to ensure that the sequencing is still correct.

Deployment ring approach

Microsoft recommends the following deployment ring approach for the framework:

DEPLOYMENT RING	TENANT	ASSESSMENT TEAMS	OUTPUT	TIMELINE
Quality Assurance	Pre-production tenant	Mobile capability owners, Security, Risk Assessment, Privacy, UX	Functional scenario validation, draft documentation	0-30 days
Preview	Production tenant	Mobile capability owners, UX	End-user scenario validation, user facing documentation	7-14 days, post Quality Assurance
Production	Production tenant	Mobile capability owners, IT help desk	N/A	7 days to several weeks, post Preview

All policy setting changes should be first applied in a pre-production environment to understand the policy setting implications. After testing is complete, move the changes into production and apply them to a subset of production users, the IT department, and other applicable groups. Finally, the complete the rollout to the rest of the mobile user community. Roll out to production may take longer depending on the changes' scale of impact. If there's no user impact, the change should roll out quickly. If there is user impact, rollout may need to go slower because of the need to communicate changes to the user population.

When testing changes to iOS/iPadOS devices, be aware of the delivery timing. The status of compliance policies for devices can be monitored. For more information, see Monitor Intune device compliance policies and Monitor device profiles in Microsoft Intune.

Next steps

Set app configuration policies for iOS/iPadOS devices

iOS/iPadOS security configuration framework app configuration policies

9/23/2022 • 2 minutes to read • Edit Online

As part of the iOS/iPadOS security configuration framework, you must properly set app configuration policies for iOS/iPadOS devices.

iOS/iPadOS supervised devices are designed to be used for work or school data only. So, Microsoft apps deployed on these devices must be configured to disallow personal accounts.

Disallow personal accounts for Microsoft apps on iOS/iPadOS devices

1. Add the iOS apps so that they can be deployed to the device. For more information, see Add iOS store apps to Microsoft Intune.
2. Create a policy for each Microsoft app as described in Add app configuration policies for managed iOS/iPadOS devices.
3. Create the following single key in each policy:

KEY	VALUES
IntuneMAMAllowedAccountsOnly	**Enabled**: The only account allowed is the managed user account defined by theIntuneMAMUPNkey. **Disabled**(or any value that is not a case insensitive match to**Enabled**): Any account is allowed.
IntuneMAMUPN	UPN of the account allowed to sign into the app. For Intune enrolled devices, the{{userprincipalname}}token may be used to represent the enrolled user account.

Next steps

Apply iOS/iPadOS device compliance security configuration settings.

iOS/iPadOS device compliance security configurations

9/23/2022 • 3 minutes to read • Edit Online

As part of the iOS/iPadOS security configuration framework, apply the following device compliance settings to mobile users using personal and supervised devices. For more information on each policy setting, see Device Compliance settings for iOS/iPadOS in Intune.

When choosing your settings, be sure to review and categorize usage scenarios. Then, configure users following the guidance for the chosen security level. You can adjust the suggested settings based on the needs of your organization. Make sure to have your security team evaluate the threat environment, risk appetite, and impact to usability.

Administrators can incorporate the below configuration levels within their ring deployment methodology for testing and production use by importing the sample iOS/iPadOS Security Configuration Framework JSON templates with Intune's PowerShell scripts.

> **NOTE**
> Due to the limited number of settings available for device compliance, there is no basic security (level 1) offering.

Enhanced security (Level 2)

Level 2 is the recommended minimum security configuration for iOS/iPadOS devices where users access work or school data. This configuration is applicable to most mobile users accessing work or school data on a device.

To simplify the table below, only configured settings are listed. Undocumented device compliance settings are not configured.

SECTION	SETTING	VALUE	NOTES
Device Health	Jailbroken devices	Block	
Device Properties	Minimum OS version	Format: Major.Minor Example: 14.8	Microsoft recommends configuring the minimum iOS major version to match the supported iOS versions for Microsoft apps. Microsoft apps support a N-1 approach where N is the current iOS major release version. For minor and build version values, Microsoft recommends ensuring devices are up to date with the respective security updates. For Apple's latest recommendations, see Apple security updates.

SECTION	SETTING	VALUE	NOTES
System Security	Require a password to unlock mobile devices	Require	
System Security	Simple passwords	Block	
System Security	Minimum password length	6	Organizations may need to update this setting to match their password policy.
System Security	Required password type	Numeric	Organizations may need to update this setting to match their password policy.
System Security	Maximum minutes after screen lock before password is required	5	Organizations may need to update this setting to match their password policy.
System Security	Maximum minutes of inactivity until screen locks	5	Organizations may need to update this setting to match their password policy.
Actions for noncompliance	Mark device noncompliant	Immediately	By default, the policy is configured to mark the device as noncompliant. Additional actions are available. For more information, seeConfigure actions for noncompliant devices in Intune.

High security (Level 3)

Level 3 is the recommended configuration for both:

- Organizations with large and sophisticated security organizations.
- Specific users and groups who will be uniquely targeted by adversaries. Such organizations are typically targeted by well-funded and sophisticated adversaries.

This configuration expands upon Level 2 by:

- Increasing the minimum operating system version.
- Ensuring that the device is compliant by enforcing the most secure Microsoft Defender for Endpoint or mobile threat defense level.
- Enacting stronger password policies.

The policy settings enforced in level 3 include all the policy settings recommended for level 1. The settings listed below include only those that have been added or changed. These settings may have significant impact to users or applications. They enforce a level of security more appropriate for risks facing targeted organizations.

SECTION	SETTING	VALUE	NOTES
Device Health	Require the device to be at or under the Device Threat Level	Secured	This setting requires a mobile threat defense product. For more information, seeMobile Threat Defense for enrolled devices. Customers should consider implementing Microsoft Defender for Endpoint or a mobile threat defense solution. It is not necessary to deploy both.
Device Properties	Minimum OS version	Format: Major.Minor Example: 15.0	Microsoft recommends configuring the minimum iOS major version to match the supported iOS versions for Microsoft apps. Microsoft apps support a N-1 approach where N is the current iOS major release version. For minor and build version values, Microsoft recommends ensuring devices are up to date with the respective security updates. For Apple's latest recommendations, see Apple security updates.
Microsoft Defender for Endpoint	Require the device to be at or under the machine risk score	Clear	This setting requires Microsoft Defender for Endpoint. For more information, see Enforce compliance forMicrosoft Defender for Endpoint with Conditional Access in Intune. Customers should consider implementing Microsoft Defender for Endpoint or a mobile threat defense solution. It is not necessary to deploy both.
System Security	Password expiration (days)	365	
Actions for noncompliance	Mark device noncompliant	Immediately	By default, the policy is configured to mark the device as noncompliant. Additional actions are available. For more information, seeConfigure actions for noncompliant devices in Intune.

Next steps

Apply iOS/iPadOS personal device security configurations or iOS/iPadOS supervised device security configurations.

iOS/iPadOS personal device security configurations

9/23/2022 • 4 minutes to read • Edit Online

As part of the iOS/iPadOS security configuration framework, apply the following device compliance settings to mobile users using personal devices. For more information on each policy setting, see iOS/iPadOS device settings in Microsoft Intune.

When choosing your settings, be sure to review and categorize usage scenarios. Then, configure users following the guidance for the chosen security level. You can adjust the suggested settings based on the needs of your organization. Make sure to have your security team evaluate the threat environment, risk appetite, and impact to usability.

Administrators can incorporate the below configuration levels within their ring deployment methodology for testing and production use by importing the sample iOS/iPadOS Security Configuration Framework JSON templates with Intune's PowerShell scripts.

Personal basic security (Level 1)

Level 1 is the recommended minimum security configuration for iOS/iPadOS personal devices where users access work or school data.

The policies in level 1 enforce a reasonable data access level while minimizing the impact to users. This is done by enforcing password policies, device lock characteristics, and disabling certain device functions (e.g., untrusted certificates).

To simplify the table below, only configured settings are listed. Undocumented device restrictions are not configured.

Device restrictions

SECTION	SETTING	VALUE	NOTES
App Store, Doc Viewing, Gaming	Treat AirDrop as an unmanaged destination	Yes	
Built-in Apps	Block Siri while device is locked	Yes	
Built-in Apps	Require Safari fraud warnings	Yes	
Cloud and Storage	Force encrypted backup	Yes	
Cloud and Storage	Block managed apps from storing data in iCloud	Yes	
Connected Devices	Force Apple Watch wrist detection	Yes	
General	Block untrusted TLS certificates	Yes	

SECTION	SETTING	VALUE	NOTES
General	Block trusting new enterprise app authors	Yes	
Locked Screen Experience	Block Notification Center access in lock screen	Yes	
Locked Screen Experience	Block Today view in lock screen	Yes	
Password	Require a password	Yes	
Password	Block simple passwords	Yes	
Password	Required password type	Numeric	
Password	Minimum password length	6	Organizations may need to update this setting to match their password policy.
Password	Number of sign-in failures before wiping the device	10	Organizations may need to update this setting to match their password policy.
Password	Maximum minutes after screen lock before password is required	5	Organizations may need to update this setting to match their password policy.
Password	Maximum minutes of inactivity until screen locks	5	Organizations may need to update this setting to match their password policy.

Personal enhanced security (Level 2)

Level 2 is the recommended configuration for personal devices where users access more sensitive information. These devices are a natural target in enterprises today. These settings don't assume a large staff of highly skilled security personnel. Therefore, they should be accessible to most enterprise organizations. This configuration is applicable to most mobile users accessing work or school data on a device.

This configuration expands upon the configuration in Level 1 by enacting data sharing controls.

The level 2 settings include all the policy settings recommended for level 1. However, the settings listed below include only those settings that have been added or changed. These settings may have a slightly higher impact to users or to applications. They enforce a level of security more appropriate for risks facing users with access to sensitive information on mobile devices.

Device restrictions

SECTION	SETTING	VALUE	NOTES
App Store, Doc Viewing, Gaming	Block viewing corporate documents in unmanaged apps	Yes	
App Store, Doc Viewing, Gaming	Block viewing non-corporate documents in corporate apps	Not configured	Enabling this device restriction blocks Outlook for iOS's ability to export contacts. This setting is not recommended if using Outlook for iOS. For more information, see Support Tip: Enabling Outlook iOS Contact Sync with iOS12 MDM Controls.
App Store, Doc Viewing, Gaming	Allow managed apps to write contacts to unmanaged contacts accounts	Yes	This setting is needed to allow Outlook for iOS to export contacts when **Block viewing corporate documents in unmanaged apps** is set to *Yes*. For more information, see Support Tip: Enabling Outlook iOS Contact Sync with iOS12 MDM Controls.
App Store, Doc Viewing, Gaming	Allow copy/paste to be affected by managed open-in	Not configured	Enabling this setting will block personal accounts within managed Microsoft apps from sharing data to unmanaged apps.
Built-in Apps	Block Siri for dictation	Yes	
Built-in Apps	Block Siri for translation	Yes	
Cloud Storage	Block backup of enterprise books	Yes	
Cloud Storage	Block notes and highlights sync for enterprise books	Yes	
General	Block sending diagnostic and usage data to Apple	Yes	

Personal high security (Level 3)

Level 3 is the recommended configuration for both:

- Organizations with large and sophisticated security organizations.
- Specific users and groups who will be uniquely targeted by adversaries. Such organizations are typically targeted by well-funded and sophisticated adversaries.

This configuration expands upon Level 2 by:

- Enacting stronger password policies.

- Disabling device functionality (e.g., screenshots and screen recordings).
- Enforcing additional data transfer restrictions (e.g., blocking Handoff).

The policy settings enforced in level 3 include all the policy settings recommended for level 2. The settings listed below include only those that have been added or changed. These settings may have significant impact to users or applications. They enforce a level of security more appropriate for risks facing targeted organizations.

Device restrictions

SECTION	SETTING	VALUE	NOTES
Cloud and Storage	Block Handoff	Yes	
Connected Devices	Require AirPlay outgoing requests pairing password	Yes	
Connected Devices	Block Apple Watch auto unlock	Yes	
General	Block screenshots and screen recording	Yes	
Password	Number of sign-in failures before wiping the device	5	Organizations may need to update this setting to match their password policy.
Password	Password expiration (days)	365	Organizations may need to update this setting to match their password policy.
Password	Prevent reuse of previous passwords	5	Organizations may need to update this setting to match their password policy.
Wireless	Block voice dialing while device is locked	Yes	

Next steps

Administrators can incorporate the above configuration levels within their ring deployment methodology for testing and production use by importing the sample iOS/iPadOS Security Configuration Framework JSON templates with Intune's PowerShell scripts.

iOS/iPadOS supervised device security configurations

9/23/2022 • 6 minutes to read • Edit Online

As part of the iOS/iPadOS security configuration framework, apply the following device compliance settings to mobile users using supervised devices. For more information on each policy setting, see iOS/iPadOS device settings in Microsoft Intune.

When choosing your settings, be sure to review and categorize usage scenarios. Then, configure users following the guidance for the chosen security level. You can adjust the suggested settings based on the needs of your organization. Make sure to have your security team evaluate the threat environment, risk appetite, and impact to usability.

Administrators can incorporate the below configuration levels within their ring deployment methodology for testing and production use by importing the sample iOS/iPadOS Security Configuration Framework JSON templates with Intune's PowerShell scripts.

Supervised basic security (Level 1)

Level 1 is the minimum security configuration for an enterprise mobile device owned by the organization.

The policies in level 1 enforce a reasonable data access level while minimizing the impact to users by:

- Enforcing password policies.
- Enabling certain device lock characteristics.
- Disabling certain device functions (like untrusted certificates).

To simplify the table below, only configured settings are listed. Undocumented device restrictions are not configured.

Device restrictions

SECTION	SETTING	VALUE	NOTES
App Store, Doc Viewing, Gaming	Treat AirDrop as an unmanaged destination	Yes	
Built-in Apps	Block Siri while device is locked	Yes	
Built-in Apps	Require Safari fraud warnings	Yes	
Cloud and Storage	Force encrypted backup	Yes	
Cloud and Storage	Block managed apps from storing data in iCloud	Yes	
Cloud and Storage	Block iCloud Keychain sync	Yes	

SECTION	SETTING	VALUE	NOTES
Connected Devices	Force Apple Watch wrist detection	Yes	
Connected Devices	Block storage of AirPrint credentials in Keychain	Yes	
Connected Devices	Require AirPrint to destinations with trusted certificates	Yes	
Connected Devices	Block iBeacon discovery of AirPrint printers	Yes	
Connected Devices	Block setting up new nearby devices	Yes	
General	Block untrusted TLS certificates	Yes	
General	Block trusting new enterprise app authors	Yes	
General	Allow activation lock	Yes	
Locked Screen Experience	Block Notification Center access in lock screen	Yes	
Locked Screen Experience	Block Today view in lock screen	Yes	
Password	Require a password	Yes	
Password	Block simple passwords	Yes	
Password	Required password type	Numeric	
Password	Minimum password length	6	Organizations may need to update this setting to match their password policy.
Password	Number of sign-in failures before wiping the device	10	Organizations may need to update this setting to match their password policy.
Password	Maximum minutes after screen lock before password is required	5	Organizations may need to update this setting to match their password policy.

SECTION	SETTING	VALUE	NOTES
Password	Maximum minutes of inactivity until screen locks	5	Organizations may need to update this setting to match their password policy.
Password	Block password proximity requests	Yes	
Password	Block password sharing	Yes	
Password	Require Touch ID or Face ID authentication for AutoFill of password or credit card information	Yes	

Supervised enhanced security (Level 2)

Level 2 is the recommended configuration for supervised devices where users access more sensitive information. These devices are a natural target in enterprises today. These settings don't assume a large staff of highly skilled security personnel. Therefore, they should be accessible to most enterprise organizations. This configuration is applicable to most mobile users accessing work or school data on a device.

This configuration expands upon the configuration in Level 1 by enacting data transfer controls and blocking access to USB devices.

The level 2 settings include all the policy settings recommended for level 1. However, the settings listed below include only those settings that have been added or changed. These settings may have a slightly higher impact to users or to applications. They enforce a level of security more appropriate for risks facing users with access to sensitive information on mobile devices.

Device restrictions

SECTION	SETTING	VALUE	NOTES
App Store, Doc Viewing, Gaming	Block viewing corporate documents in unmanaged apps	Yes	
App Store, Doc Viewing, Gaming	Block viewing non-corporate documents in corporate apps	Not configured	Enabling this device restriction blocks Outlook for iOS's ability to export contacts. This setting is not recommended if using Outlook for iOS. For more information, see Support Tip: Enabling Outlook iOS Contact Sync with iOS12 MDM Controls.

SECTION	SETTING	VALUE	NOTES
App Store, Doc Viewing, Gaming	Allow managed apps to write contacts to unmanaged contacts accounts	Yes	This setting is needed to allow Outlook for iOS to export contacts when **Block viewing corporate documents in unmanaged apps** is set to *Yes*. For more information, see Support Tip: Enabling Outlook iOS Contact Sync with iOS12 MDM Controls.
App Store, Doc Viewing, Gaming	Allow copy/paste to be affected by managed open-in	Yes	Enabling this setting will block personal accounts within managed Microsoft apps from sharing data to unmanaged apps.
Built-in Apps	Block Siri for dictation	Yes	
Built-in Apps	Block Siri for translation	Yes	
Cloud Storage	Block backup of enterprise books	Yes	
Cloud Storage	Block notes and highlights sync for enterprise books	Yes	
Cloud Storage	Block iCloud document and data sync	Yes	
Connected Devices	Block access to USB in Files app	Yes	
General	Block sending diagnostic and usage data to Apple	Yes	

Supervised high security (Level 3)

Level 3 is the recommended configuration for both:

- Organizations with large and sophisticated security organizations.
- Specific users and groups who will be uniquely targeted by adversaries. Such organizations are typically targeted by well-funded and sophisticated adversaries.

This configuration expands upon Level 2 by:

- Enacting stronger password policies.
- Disabling device functionality (like AirPrint).
- Requiring app installation through Apple's volume purchase program. For more information, see How to manage iOS and macOS apps purchased through Apple Business Manager with Microsoft Intune.
- Enforcing additional data transfer restrictions (like blocking iCloud backup).

The policy settings enforced in level 3 include all the policy settings recommended for level 2. The settings listed below include only those that have been added or changed. These settings may have significant impact to users

or applications. They enforce a level of security more appropriate for risks facing targeted organizations.

Device restrictions

SECTION	SETTING	VALUE	NOTES
App Store, Doc Viewing, Gaming	Block App store	Yes	
App Store, Doc Viewing, Gaming	Block playback of explicit music, podcast, and iTunes U	Yes	
App Store, Doc Viewing, Gaming	Block adding Game Center friends	Yes	
App Store, Doc Viewing, Gaming	Block Game Center	Yes	
App Store, Doc Viewing, Gaming	Block multiplayer gaming	Yes	
App Store, Doc Viewing, Gaming	Block access to network drive in Files app	Yes	
Built-in Apps	Block Siri	Yes	
Built-in Apps	Block iTunes store	Yes	
Built-in Apps	Block Find My Friends	Yes	
Built-in Apps	Block user modification to the Find My Friends settings	Yes	
Built-in Apps	Block Safari Autofill	Yes	
Cloud and Storage	Block Handoff	Yes	
Cloud and Storage	Block iCloud backup	Yes	
Connected Devices	Require AirPlay outgoing requests pairing password	Yes	
Connected Devices	Block Apple Watch auto unlock	Yes	
Connected Devices	Block AirDrop	Yes	
Connected Devices	Block pairing with non-Configurator hosts	Yes	
Connected Devices	Block AirPrint	Yes	

SECTION	SETTING	VALUE	NOTES
Connected Devices	Allow users to boot devices into recovery mode with unpaired devices	Not configured	
General	Block screenshots and screen recording	Yes	
General	Block modification of account settings	Yes	
General	Block use of erase all content and settings	Yes	
General	Block configuration profile changes	Yes	
General	Block removing apps	Yes	
General	Force automatic data and time	Yes	
General	Block VPN creation	Yes	
General	Block modification of eSIM settings	Yes	
Password	Number of sign-in failures before wiping the device	5	Organizations may need to update this setting to match their password policy.
Password	Password expiration (days)	365	Organizations may need to update this setting to match their password policy.
Password	Prevent reuse of previous passwords	5	Organizations may need to update this setting to match their password policy.
Password	Block password AutoFill	Yes	
Wireless	Block voice dialing while device is locked	Yes	

SECTION	SETTING	VALUE	NOTES
Wireless	Require joining Wi-Fi networks only using configuration profiles	Not configured	Care should be taken when using this setting as this could affect your ability to connect to the device if the specified Wi-Fi Networks are unavailable or if the setting is configured incorrectly. This could result in a situation where you are locked out of the device and unable to remotely reset the device.

Next steps

Administrators can incorporate the above configuration levels within their ring deployment methodology for testing and production use by importing the sample iOS/iPadOS Security Configuration Framework JSON templates with Intune's PowerShell scripts.

Set up enrollment for macOS devices in Intune

9/23/2022 • 7 minutes to read • Edit Online

Microsoft Intune supports enrollment on personal and company-owned devices. This article describes the methods and features you can use to enroll personal, company-owned, and VM devices in Intune.

Enable enrollment in Microsoft Intune

Complete these steps first to enable enrollment in your Microsoft Intune tenant.

1. Verify that devices are eligible for Apple device enrollment
2. Configure domains
3. Set the MDM Authority
4. Get an Apple MDM push certificate
5. Assign user licenses in the Microsoft 365 admin center
6. Create groups
7. Configure the Company Portal app

Enroll devices

After you enable enrollment, use one of the supported methods described in this section to enroll user-owned and company-owned devices.

User-owned macOS devices (BYOD)

Intune supports *bring-your-own-device*, or *BYOD*, which lets people enroll their personal devices themselves. To finish setting up enrollment for BYOD scenarios, tell your licensed users to use one of these options to enroll devices:

- Sign in to Company Portal website and follow on-screen instructions to add device.
- Install Company Portal app for Mac at aka.ms/EnrollMyMac and follow-on screen instructions to add device.

Company-owned macOS devices

Intune supports the following enrollment methods for company-owned macOS devices. Select a hyperlinked method to open its setup steps.

- Apple Automated Device Enrollment: Use this method to automate the enrollment experience on devices purchased through Apple Business Manager or Apple School Manager. Automated device enrollment deploys the enrollment profile over-the-air, so you don't need to have physical access to devices.
- Device enrollment manager (DEM): Use this method for large-scale deployments and when there are multiple people in your organization who can help with enrollment setup. Someone with device enrollment manager (DEM) permissions can enroll up to 1,000 devices with a single Azure Active Directory account. This method uses the Company Portal app or Microsoft Intune app to enroll devices. You can't use a DEM account to enroll devices via Automated Device Enrollment.
- Direct enrollment: Direct enrollment enrolls devices with no user affinity, so this method is best for devices that aren't associated with a single user. This method requires you to have physical access to the Macs you're enrolling.

Bootstrap tokens

Intune supports the use of bootstrap tokens on enrolled Macs running macOS 10.15 or later. Bootstrap tokens

grant volume ownership status to local user and guest accounts so that non-admin users can approve important operations that an admin would otherwise need to do. Operations such as:

- User-initiated software updates
- Kernel extension installation on Apple silicon

You can utilize bootstrap tokens on supervised Macs, and Macs enrolled via macOS automated device enrollment.

Get bootstrap token

The bootstrap token is automatically generated when:

- A newly enrolled Mac checks in with Intune and
- A secure token-enabled user (typically an Intune administrator) signs in to the Mac with their cleartext password

The token is then automatically escrowed to Microsoft Intune. You can use a command line tool to manually view, generate, and escrow a bootstrap token on supported macOS devices, if needed. For more information about commands, see Use secure token, bootstrap token, and volume ownership in deployments on Apple Support.

Monitor bootstrap escrow status

You can monitor the escrow status for any enrolled Mac in the admin center. The *Bootstrap token escrowed* hardware property reports whether or not the bootstrap token has been escrowed in Intune. Intune reports **Yes** when the token has been successfully escrowed and **No** when the token has not been escrowed.

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select **Devices** > **macOS**. All macOS devices are shown in a table.
3. Select a device.
4. Select **Hardware**.
5. In your hardware details, scroll down to **Conditional access** > **Bootstrap token escrowed**.

Manage kernel extensions and software updates

A bootstrap token can be used to approve the installation of both kernel extensions and software updates on a Mac with Apple silicon.

User-initiated software updates can be carried out with a bootstrap token on Macs that are running macOS, version 11.1, and enrolled via automated device enrollment. To authorize user-initiated software updates on a device that isn't enrolled via automated device enrollment, you must restart the Mac in recovery mode and downgrade its security settings. You can also utilize the bootstrap token for software updates on Macs running macOS 11.2 and later, with the only requirement being that the device needs to be supervised.

Kernel extension management is automatically available on Macs running macOS 11 or later and enrolled via automated device enrollment. To authorize the remote management of kernel extensions on a device that isn't enrolled via automated device enrollment, you must restart the Mac in recovery mode and downgrade its security settings.

For more information about changing security settings, see Change security settings on the startup disk of a Mac with Apple silicon on Apple Support.

Block macOS enrollment

By default, Intune lets macOS devices enroll. To block macOS devices from enrollment, see Set device type restrictions.

Enroll virtual macOS machines for testing

> **NOTE**
> Intune supports macOS virtual machines for testing purposes only. Don't use macOS virtual machines as official devices for employees or students.

Intune supports virtual machines running:

- Parallel Desktop
- VMware Fusion
- Apple Silicon

Intune needs to know the VM's hardware model and serial number to recognize and enroll it as a device. If you try to enroll a VM without providing those details, enrollment fails. This section provides more information about how to satisfy this requirement before enrollment.

Parallels Desktop

Modify the VM's configuration settings to add or change a VM serial number and hardware model identifier. Enter any string of alphanumeric characters for the serial number. For hardware model, we recommend using the model of the device that's running the VM. To find your Mac's hardware model, select the Apple menu and go to **About This Mac** > **System Report** > **Model Identifier**.

For more information, see the following topics in the Parallels knowledge base:

- How to enroll a macOS VM in Parallels Desktop using Intune
- How to find and change the serial number

VMware Fusion

Add the following lines to your .vmx file to set the VM's hardware model and serial number. The values shown in this sample are examples.

```
serialNumber = "ABC123456789"
hw.model = "MacBookAir10,1"
```

Enter any string of alphanumeric characters for the serial number. For hardware model, we recommend using the model of the device that's running the VM. To find your Mac's hardware model, select the Apple menu and go to **About This Mac** > **System Report** > **Model Identifier**.

See the VMware customer connect website for more information about editing the .vmx file for your VMware Fusion VM.

Apple Silicon

No changes are required for virtual machines running on Apple Silicon hardware. Parallels Desktop and VMware Fusion are supported on Macs with Apple Silicon, so if you set up a VM this way, you don't need to modify the hardware model ID or serial number.

User-approved enrollment

All Mac enrollments in Intune are considered user-approved. User-approved enrollment lets you manage macOS devices that aren't part of Apple School Manager or Apple Business Manager. It provides the same level of control as supervised macOS devices enrolled using Automated Device Enrollment or Apple Configurator.

Intune automatically turns on supervision for user-approved devices running macOS 11 and later. It also does this for enrolled devices that later update to macOS 11 or later.

> **NOTE**
>
> Intune announced support for user approved enrollment in June 2020. BYOD enrollments that occured before that time may not be user-approved. For more information about Apple devices becoming user approved, see User approved MDM enrollment on the Apple Support website.

User experience

The device user signs in to the Company Portal app to initiate enrollment. Company Portal then opens the device's system preferences and prompts the user to install the management profile. Company Portal provides in-app instructions to help users find the profile. Users go to **System Preferences** > **Profiles** to approve the management profile installation. Device users that don't provide approval during enrollment can return to system preferences later to give approval.

Find out if device is user approved

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Choose **Devices** > **All devices**.
3. Choose a macOS device.
4. From the side menu, select **Hardware**.
5. Check the value next to **User approved enrollment**.

Next steps

- For user-help documentation, which provides step-by-step enrollment instructions for device users, see Enroll your macOS device in Intune. You can also create your own instructions if you prefer to capture your organization's branded or customized enrollment experience.
- After macOS devices are enrolled, you can create custom settings for macOS devices.

Automatically enroll macOS devices with the Apple Business Manager or Apple School Manager

9/23/2022 • 13 minutes to read • Edit Online

IMPORTANT

Apple recently changed from using the Apple Device Enrollment Program (DEP) to Apple Automated Device Enrollment (ADE). Intune is in the process of updating the Intune user interface to reflect that. Until such changes are complete, you'll continue to see *Device Enrollment Program* in the Intune portal. Wherever that is shown, it now uses Automated Device Enrollment.

You can set up Intune enrollment for macOS devices purchased through Apple's Apple Business Manager or Apple School Manager. You can use either of these enrollments for large numbers of devices without ever touching them. You can ship macOS devices directly to users. When the user turns on the device, Setup Assistant runs with preconfigured settings and the device enrolls into Intune management.

To set up enrollment, you use both the Intune and Apple portals. You create enrollment profiles containing settings that applied to devices during enrollment.

Neither Apple Business Manager enrollment or Apple School Manager work with the device enrollment manager.

Prerequisites

- Devices purchased in Apple School Manager or Apple's Automated Device Enrollment
- A list of serial numbers or a purchase order number.
- MDM Authority
- Apple MDM Push certificate

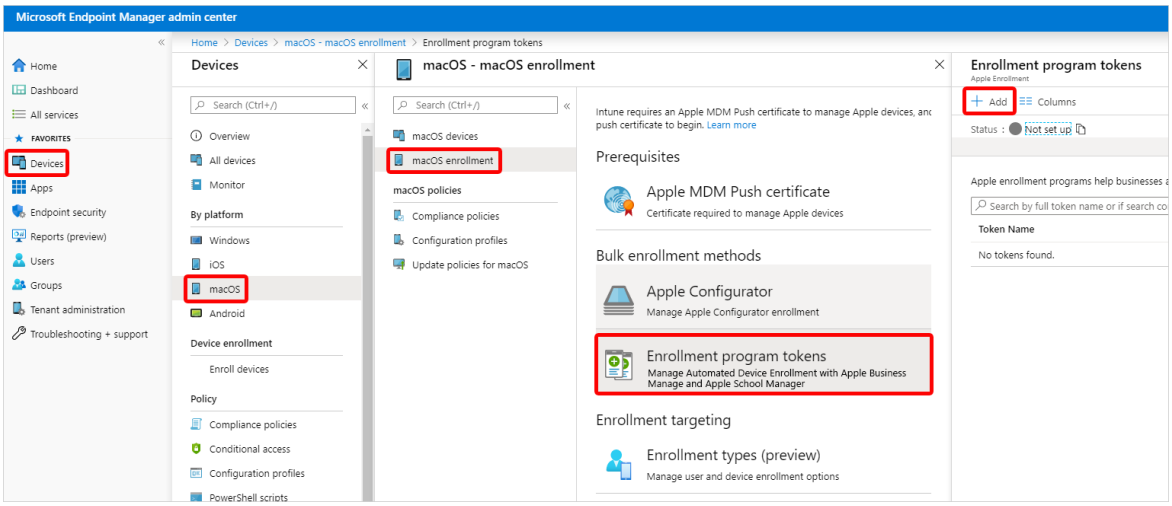
Get an Apple ADE token

Before you can enroll macOS devices with ADE or Apple School Manager, you need a token (.p7m) file from Apple. This token lets Intune sync information about the devices that your organization owns. It also lets Intune upload enrollment profiles to Apple and assign these profiles to devices.

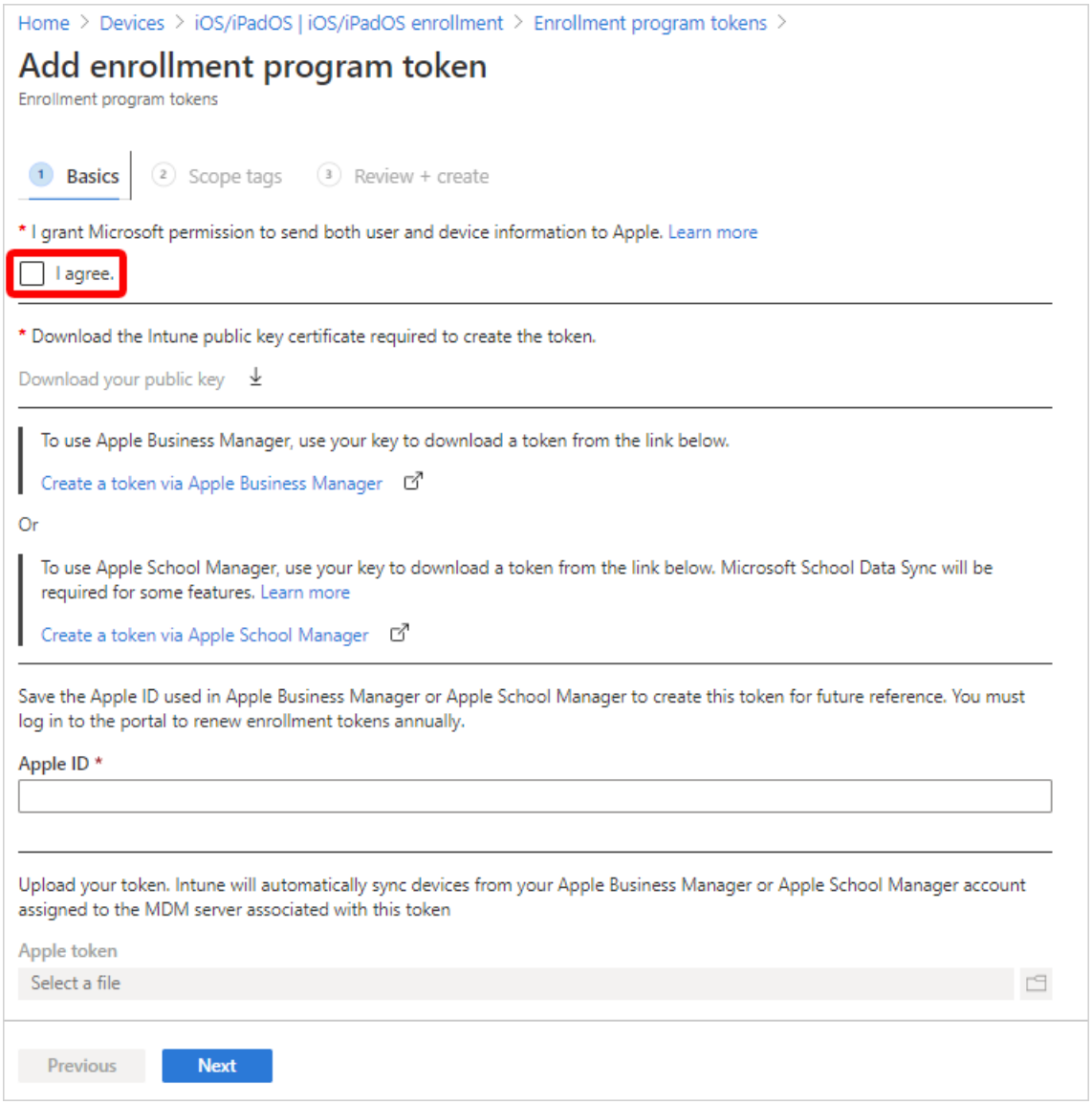
You use the Apple portal to create a token. You also use the Apple portal to assign devices to Intune for management.

Step 1. Download the Intune public key certificate required to create the token

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **macOS** > **macOS enrollment** > **Enrollment Program Tokens** > **Add**.



2. Grant permission to Microsoft to send user and device information to Apple by selecting **I agree**.



3. Choose **Download your public key** to download and save the encryption key (.pem) file locally. The PEM file is used to request a trust-relationship certificate from the Apple portal.

Step 2. Use your key to download a token from Apple

1. Choose **Create a token via Apple Business Manager** or **Create a token via Apple School Manager** to open the Apple portal used by your organization.
2. Sign in to the portal with your company Apple ID. You can use this Apple ID to renew your token.
3. Select your account name to open the portal menu, and then choose **Preferences**.

4. Go to your MDM server assignments.
5. Select the option to add an MDM server.
6. Enter the **MDM Service Name**. The purpose of the server name is to help identify your mobile device management (MDM) server in the portal. It doesn't have to be the actual name or URL of the Microsoft Intune server.
7. Upload your public key file and then save your changes. Then you can download the server token.

Best practices

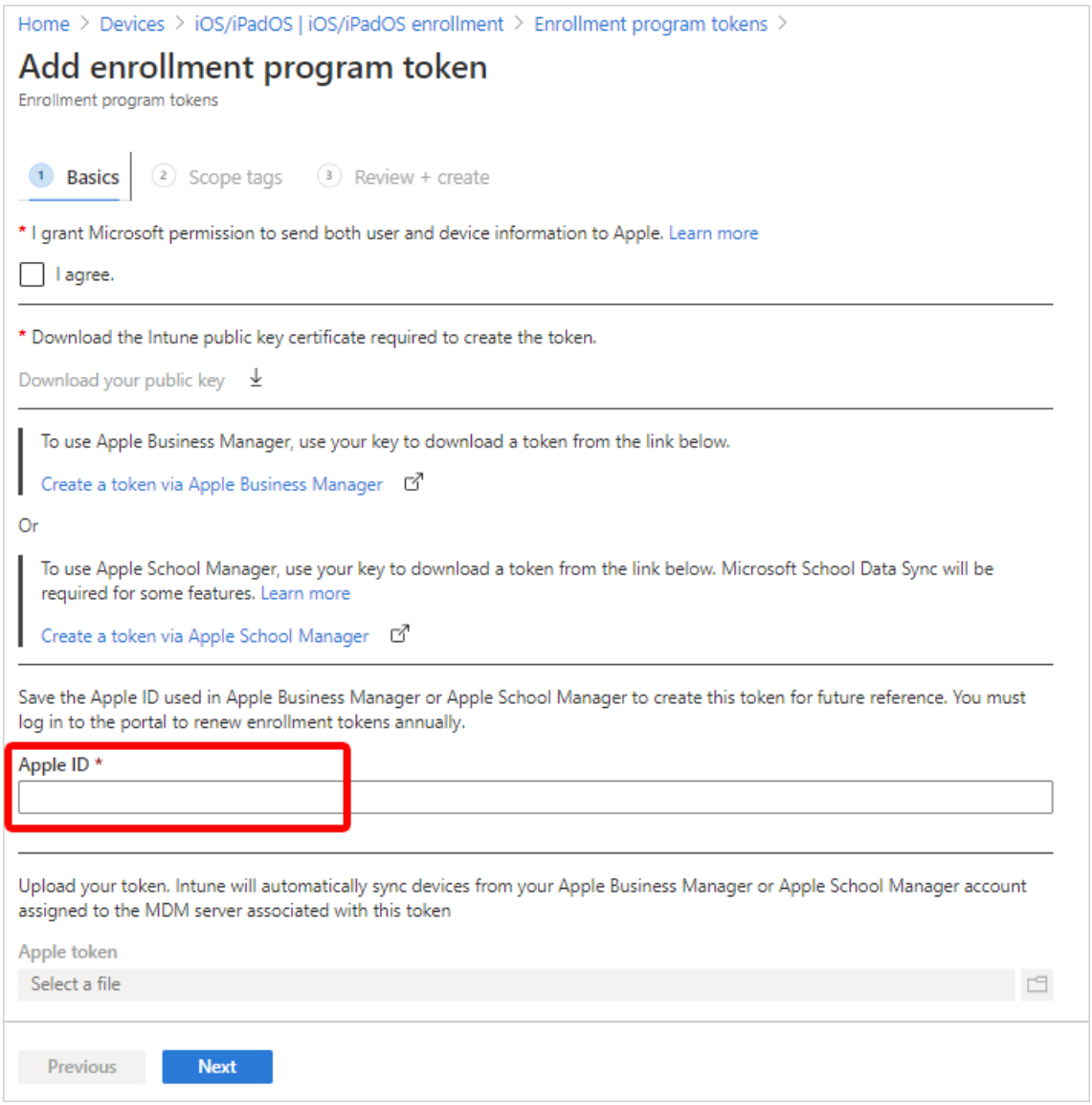
While you're in the Apple portal, you can also apply device filters and assign devices to the MDM server.

- Apply filters: To filter devices before assigning them to your MDM server, go to **Devices** > **Filter**. You can filter devices by:
  - Device management
  - Source
  - Order number
  - Device type
  - Storage size
- Bulk assign devices: You can assign all eligible devices to your new MDM servers at the same time.
  1. Go to **Devices** > **All Devices** or select the devices you want to assign.
  2. Select **Edit MDM Server**.
  3. Select the MDM server you want to use.
  4. Select **Continue**.
  5. When prompted to, confirm your changes. A notification appears to confirm that the devices have been assigned to the new MDM server.

The Apple portal keeps track of your activity and changes. Select **Activity** to view assignment results and download logs.

Step 3. Save the Apple ID used to create this token

Return to the Microsoft Endpoint Manager admin center and enter your Apple ID so that you have record of it for future reference.



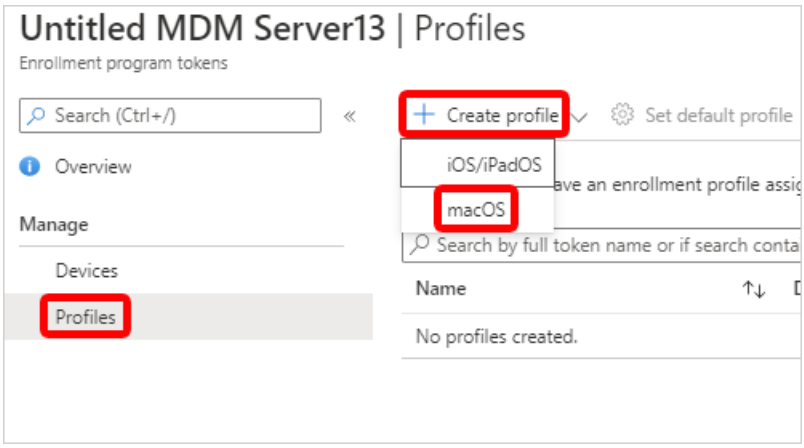
Step 4. Upload your token

In the **Apple token** box, browse to the certificate (.pem) file, choose **Open**, and then choose **Create**. With the push certificate, Intune can enroll and manage macOS devices by pushing policy to enrolled devices. Intune automatically synchronizes with Apple to see your enrollment program account.

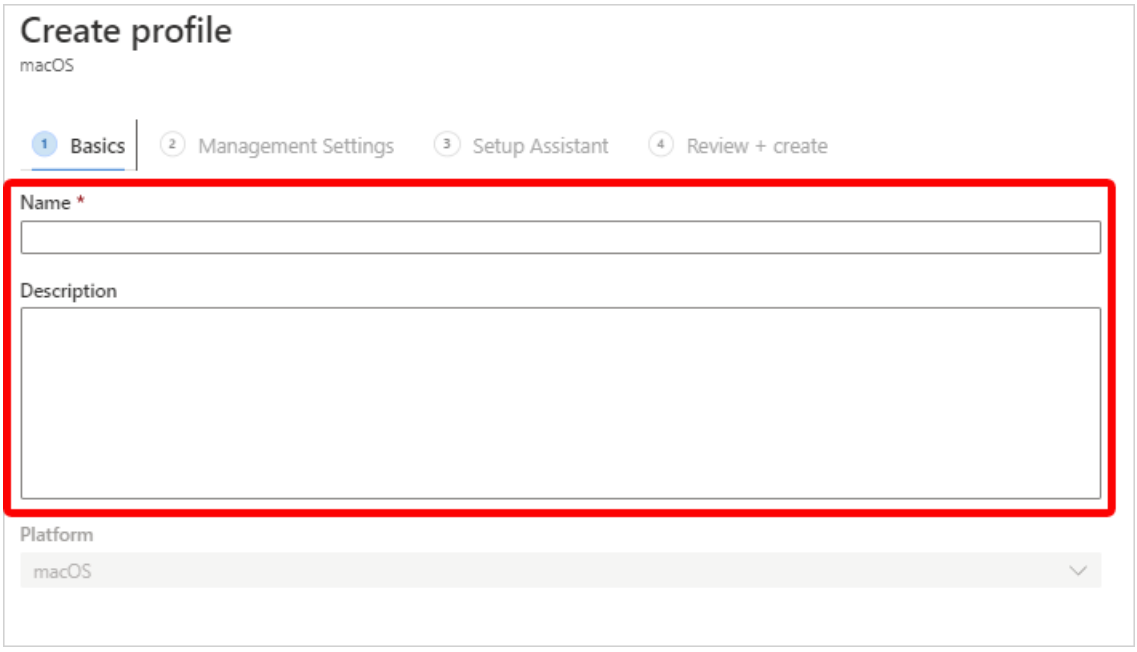
Create an Apple enrollment profile

Now that you've installed your token, you can create an enrollment profile for devices. A device enrollment profile defines the settings applied to a group of devices during enrollment.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **macOS** > **macOS Enrollment** > **Enrollment program tokens**.
2. Select a token, choose **Profiles**, and then choose **Create profile** > **macOS**.



3. On the **Basics** page, enter a **Name** and **Description** for the profile for administrative purposes. Users do not see these details. You can use this **Name** field to create a dynamic group in Azure Active Directory. Use the profile name to define the enrollmentProfileName parameter to assign devices with this enrollment profile. Learn more about Azure Active Directory dynamic groups.



4. For **Platform**, choose **macOS**.
5. Select **Next** to go to the **Management Settings** page.
6. For **User Affinity**, choose whether or not devices with this profile must enroll with or without an assigned user.

   - **Enroll with User Affinity** - Choose this option for devices that belong to users and that want to use the Company Portal app for services like installing apps. If using ADFS, user affinity requires WS-Trust 1.3 Username/Mixed endpoint. Learn more. Choose this option if you need multi-factor authentication (MFA).
   - **Enroll without User Affinity** - Choose this option for device unaffiliated with a single user. Use this for devices that perform tasks without accessing local user data. Apps like the Company Portal app don't work.

7. If you selected **Enroll with User Affinity** for the **User Affinity** field, you now have the option to choose the authentication method to use when authenticating users. For **Authentication method**, select one of the following options:

   - **Setup Assistant (legacy)**: Use the legacy Setup Assistant if you want users to experience the

typical, out-of-box-experience for Apple products. This installs standard preconfigured settings when the device enrolls with Intune management. If you're using Active Directory Federation Services and you're using Setup Assistant to authenticate, a WS-Trust 1.3 Username/Mixed endpoint is required. Learn more.

- **Setup Assistant with modern authentication**: Devices running macOS 10.15 and later can use this method (older macOS devices in this profile will fall back to using the **Setup Assistant (legacy)** process).

  If a conditional access policy that requires multi-factor authentication (MFA) applies at enrollment or at enrollment and during Company Portal sign in, then MFA is required. However, MFA is optional based on the Azure AD settings in the targeted Conditional Access policy.

  After completing all the Setup Assistant screens, the end user lands on the home page (at which point their user affinity is established). However, until the user signs in to the Company Portal using their Azure AD credentials, the device:

  - Won't be fully registered with Azure AD.
  - Won't show up in the user's device list in the Azure AD portal.
  - Won't have access to resources protected by conditional access.
  - Won't be evaluated for device compliance.
  - Will be redirected to the Company Portal from other apps if the user tries to open any managed applications that are protected by conditional access.

  For more information on how to get the macOS Company Portal on the users device, see Add the Company Portal for macOS app.

8. For **Locked enrollment**, choose whether or not you want locked enrollment for devices using this profile. **Yes** disables macOS settings that allow the management profile to be removed from the **System Preferences** menu or through the **Terminal**. After device enrollment, you cannot change this setting without wiping the device.
9. Select **Next** to go to the **Setup Assistant** page.
10. On the **Setup Assistant** page, configure the following profile settings:

DEPARTMENT SETTINGS	DESCRIPTION
Department Name	Appears when users tap **About Configuration** during activation.
Department Phone	Appears when the user clicks the **Need Help** button during activation.

You can choose to show or hide a variety of Setup Assistant screens on the device when the user sets it up.

- If you choose **Hide**, the screen won't be displayed during setup. After setting up the device, the user can still go in to the **Settings** menu to set up the feature.
- If you choose **Show**, the screen will be displayed during setup. The user can sometimes skip the screen without taking action. But they can then later go into the device's **Settings** menu to set up the feature.

SETUP ASSISTANT SCREEN SETTINGS	IF YOU CHOOSE SHOW, DURING SETUP THE DEVICE WILL...

SETUP ASSISTANT SCREEN SETTINGS	IF YOU CHOOSE SHOW, DURING SETUP THE DEVICE WILL...
Location Services	Prompt the user for their location. For macOS 10.11 and later and iOS/iPadOS 7.0 and later.
Restore	Display the Apps & Data screen. This screen gives the user the option to restore or transfer data from iCloud Backup when they set up the device. For macOS 10.9 and later, and iOS/iPadOS 7.0 and later.
Apple ID	Give the user the options to sign in with their Apple ID and use iCloud. For macOS 10.9 and later, and iOS/iPadOS 7.0 and later.
Terms and Conditions	Require the user to accept Apple's terms and conditions. For macOS 10.9 and later, and iOS/iPadOS 7.0 and later.
Touch ID and Face ID	Give the user the option to set up fingerprint identification for the device. For macOS 10.12.4 and later, and iOS/iPadOS 8.1 and later.
Apple Pay	Give the user the option to set up Apple Pay on the device. For macOS 10.12.4 and later, and iOS/iPadOS 7.0 and later.
Siri	Give the user the option to set up Siri. For macOS 10.12 and later, and iOS/iPadOS 7.0 and later.
Diagnostics Data	Display the Diagnostics screen to the user. This screen gives the user the option to send diagnostic data to Apple. For macOS 10.9 and later, and iOS/iPadOS 7.0 and later.
Display Tone	Give the user the option to turn on Display Tone. For macOS 10.13.6 and later, and iOS/iPadOS 9.3.2 and later.
FileVault	Display the FileVault 2 encryption screen to the user. For macOS 10.10 and later.
iCloud diagnostics	Display the iCloud Analytics screen to the user. For macOS 10.12.4 and later.
Registration	Display the registration screen. For macOS 10.9 and later.
iCloud Storage	Display the iCloud Documents and Desktop screen to the user. For macOS 10.13.4 and later.
Appearance	Display the Appearance screen to the user. For macOS 10.14 and later, and iOS/iPadOS 13.0 and later.
Screen Time	Display the Screen Time screen. For macOS 10.15 and later, and iOS/iPadOS 12.0 and later.
Privacy	Display the Privacy screen to the user. For macOS 10.13.4 and later, and iOS/iPadOS 11.3 and later.

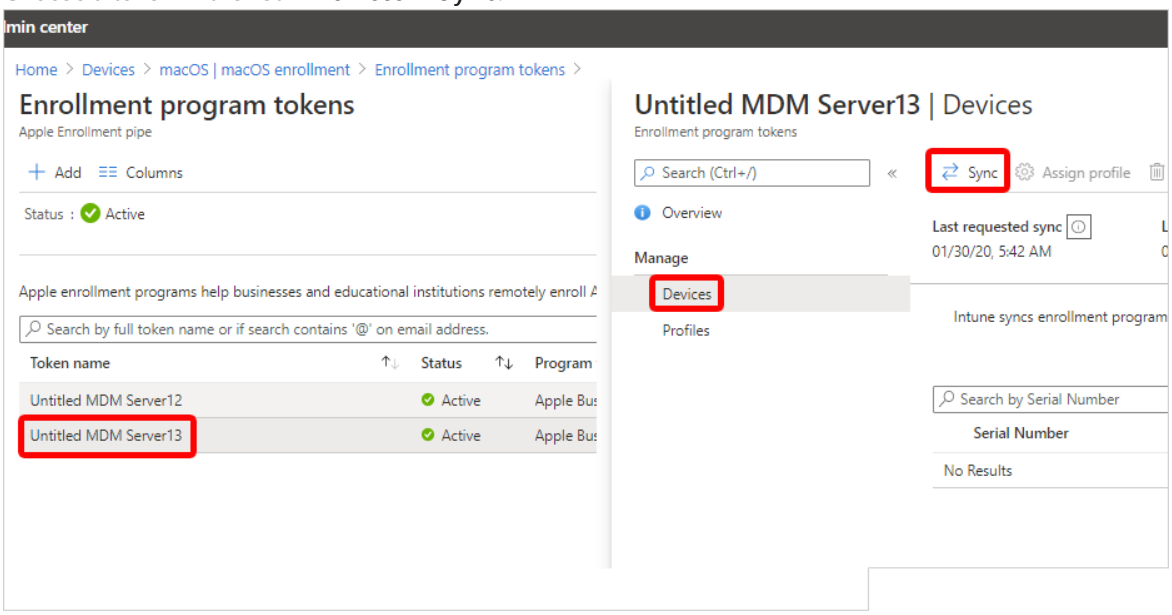
SETUP ASSISTANT SCREEN SETTINGS	IF YOU CHOOSE SHOW, DURING SETUP THE DEVICE WILL...
Accessibility	Display the Accessibility screen to the user. If this screen is hidden, the user won't be able to use the Voice Over feature. Voice Over is supported on devices that: - Run macOS 11. - Are connected to the internet using Ethernet. - Have the serial number appear in Apple School Manager or Apple Business Manager.
Auto unlock with Apple Watch	Give the user an option to use their Apple Watch to unlock their Mac. For macOS 12.0 and later.

11. Select **Next** to go to the **Review + create** page.
12. To save the profile, choose **Create**.

Sync managed devices

Now that Intune has permission to manage your devices, you can synchronize Intune with Apple to see your managed devices in Intune in the Azure portal.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **macOS** > **macOS Enrollment** > **Enrollment program tokens**.
2. Choose a token in the list > **Devices** > **Sync**.



To comply with Apple's terms for acceptable enrollment program traffic, Intune imposes the following restrictions:

- A full sync can run no more than once every seven days. During a full sync, Intune fetches the complete updated list of serial numbers assigned to the Apple MDM server connected to Intune. After an Enrollment Program device is deleted from Intune portal without being unassigned from the Apple MDM server in the Apple portal, it won't be re-imported to Intune until the full sync is run.
- If a device is released from ABM/ASM, it can take up to 45 days for it to be automatically deleted from the devices page in Intune. You can manually delete released devices from Intune one by one if needed. Released devices will be accurately reported as being Removed from ABM/ASM in Intune until they are automatically deleted within 30-45 days.
- A sync is run automatically every 24 hours. You can also sync by clicking the **Sync** button (no more

than once every 15 minutes). All sync requests are given 15 minutes to finish. The **Sync** button is disabled until a sync is completed. This sync will refresh existing device status and import new devices assigned to the Apple MDM server.

Assign an enrollment profile to devices

You must assign an enrollment program profile to devices before they can enroll.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **macOS** > **macOS Enrollment** > **Enrollment program tokens** > choose a token in the list.
2. Choose **Devices** > choose devices in the list > **Assign profile**.
3. Under **Assign profile**, choose a profile for the devices > **Assign**.

Assign a default profile

You can pick a default macOS and iOS/iPadOS profile to be applied to all devices enrolling with a specific token.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **macOS** > **macOS Enrollment** > **Enrollment program tokens** > choose a token in the list.
2. Choose **Set Default Profile**, choose a profile in the drop-down list, and then choose **Save**. This profile will be applied to all devices that enroll with the token.

Distribute devices

You have enabled management and syncing between Apple and Intune, and assigned a profile to let your devices enroll. You can now distribute devices to users. Devices with user affinity require each user be assigned an Intune license. Devices without user affinity require a device license.

Devices registered with ABM/ASM and assigned a profile in Intune can be enrolled:

- During Setup Assistant for new devices or wiped devices.
- After Setup Assistant using the profiles command.

Enroll your macOS device registered in ABM/ASM with Automated Device Enrollment during Setup Assistant

Devices configured in ABM/ASM will automatically enroll into management with Intune during Setup Assistant with a Remote Management prompt.

> **NOTE**
> If the device was assigned to a macOS enrollment profile with user affinity, you must sign in to the Company Portal for Azure AD registration and Conditional Access.

Enroll your macOS device registered in ABM/ASM with Automated Device Enrollment after Setup Assistant

For macOS 10.13 and later devices, you can follow these steps to enroll.

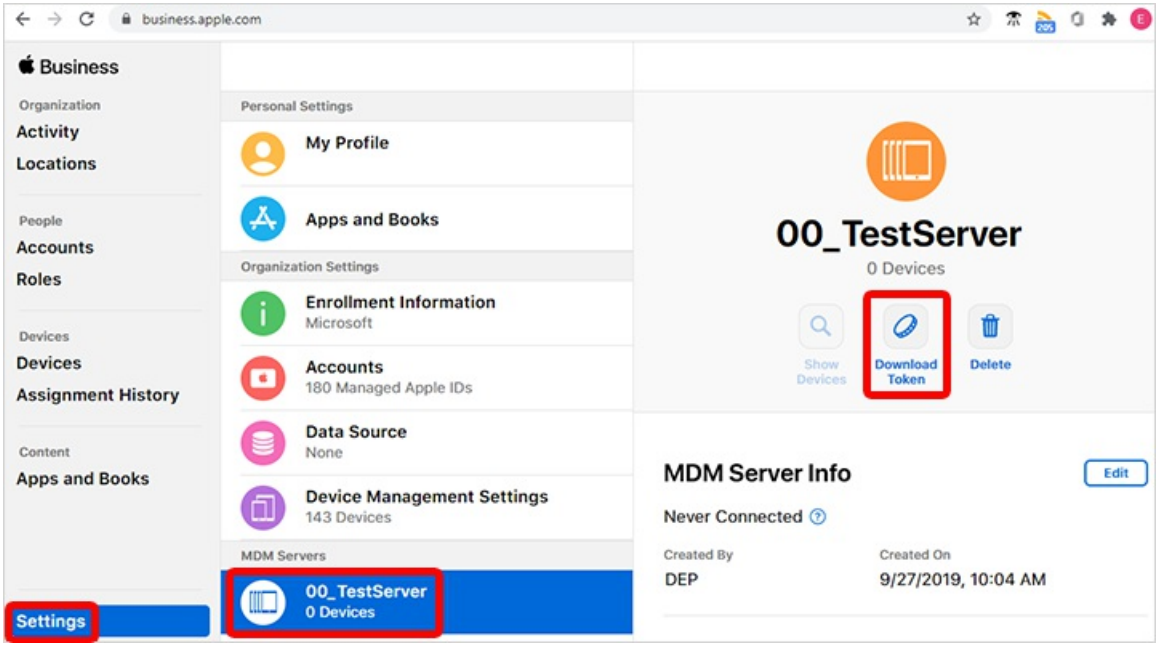
1. In the Apple Business Manager or Apple School Manager portal, import the device.
2. In the Microsoft Endpoint Manager admin center, make sure that the device is assigned a macOS enrollment profile with or without user affinity.
3. Log in to the device as a local administrator account.
4. To trigger enrollment, on the **Home** page, open **Terminal** and run the following command: sudo profiles renew -type enrollment
5. Enter your device password for the local administrator account.
6. In the **Device enrollment** window, choose **Details**.
7. In the **System preferences** window, choose **Profiles**.

8. Follow the prompts that will download the management profile, certs, and policies from Intune. You can view the profiles on the device anytime by going to **System Preferences** > **Profiles**.
9. If the device was assigned to a macOS enrollment profile with user affinity, you must sign in to the Company Portal for Azure AD registration and Conditional Access.

Renew an ADE token

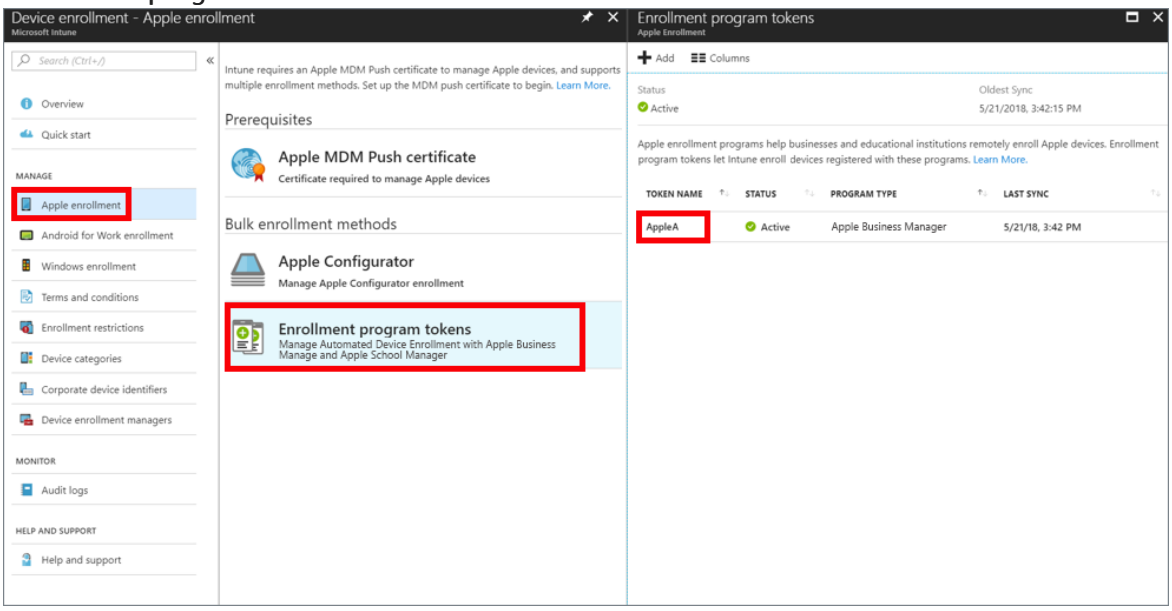
1. Go to business.apple.com and sign in with an account that has the role of Administrator or Device Enrollment Manager.

2. Choose **Settings** > under **MDM Servers** choose your MDM server associated with the token file that you want to renew > **Download Token**.

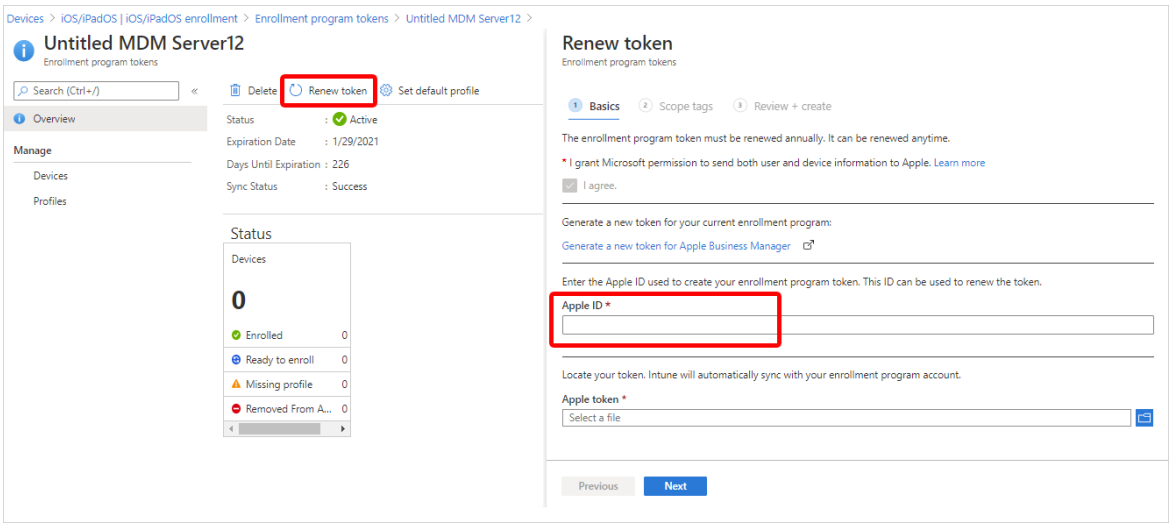


3. Choose **Download Server Token**.

4. In the Microsoft Endpoint Manager admin center, choose **Device enrollment** > **Apple Enrollment** > **Enrollment program tokens** > choose the token.

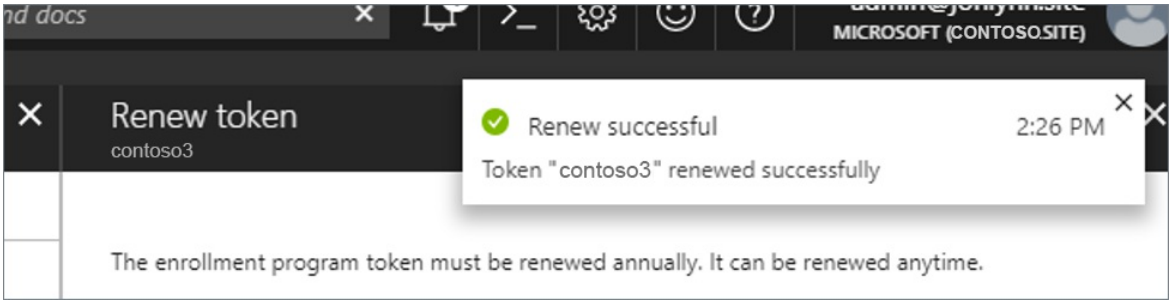


5. Choose **Renew token** and enter the Apple ID used to create the original token.



6. Upload the newly downloaded token.

7. Choose **Renew token**. You'll see the confirmation that the token was renewed.



Next steps

After enrolling macOS devices, you can start managing them.

Use Direct Enrollment for macOS devices

9/23/2022 • 2 minutes to read • Edit Online

Intune supports the enrollment of macOS devices using Direct Enrollment (DE) for corporate devices. Direct Enrollment does not wipe the device. It enrolls the device through macOS settings. This method only supports devices with **no user affinity**.

Prerequisites

- Physical access to macOS devices
- Set MDM authority
- An Apple MDM push certificate
- Administrator rights on the macOS devices you are enrolling

Create an Apple Configurator profile for devices

A device enrollment profile defines the settings applied during enrollment. These settings are applied only once. Follow these steps to create an enrollment profile to enroll macOS devices with Direct Enrollment.

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **Enroll devices** > **Apple enrollment** > **Apple Configurator**.
2. Choose **Profiles** > **Create**.
3. Under **Create Enrollment Profile** on the **Basics** tab, type a **Name** and **Description** for the profile for administrative purposes. Users do not see these details. You can use this Name field to create a dynamic group in Azure Active Directory. Use the profile name to define the enrollmentProfileName parameter to assign devices with this enrollment profile. Learn more about Azure Active Directory dynamic groups.
4. For **User Affinity**, choose **Enroll without User Affinity** - Choose this option for devices unaffiliated with a single user. Use this for devices that perform tasks without accessing local user data. Apps requiring user affiliation (including the Company Portal app used for installing line-of-business apps) won't work. Required for Direct Enrollment.

   > **NOTE**
   > **Enroll with user affinity** is not supported on macOS when using Direct Enrollment. For devices that need user affinity, use Automated Device Enrollment.

5. Choose **Create** to save the profile.

Direct Enrollment

Because Direct Enrollment only supports enrollment without user affinity, the company portal cannot be used to install available applications.

Export the profile and install on macOS devices

1. In the Microsoft Endpoint Manager admin center, choose **Devices** > **Enroll devices** > **Apple enrollment** > **Apple Configurator** > **Profiles** > choose the profile to export > **Export Profile**.
2. Under **Direct enrollment**, choose **Download profile**, and save the file.

> **NOTE**
>
> A downloaded enrollment profile is valid for two weeks after download. You can download as many enrollment profiles using this link as you need. Downloading a new profile does not render the previous one invalid, however it also doesn't extend the previously downloaded file expiry time.

3. Transfer the file to a macOS computer to install it directly.
4. Double-click on the saved **.mobileconfig** to open the file in Profiles.
5. When prompted to install the management profile, select **Install**.
6. Confirm on the next prompt you want to install the management profile by selecting **Install**.
7. Enter the credentials for an admin account on the macOS device and click **OK**.
8. The macOS device is now enrolled in Intune and managed, targeted profiles will begin downloading.

Next steps

After enrolling macOS devices, you can start managing them.

What are enrollment restrictions?

9/23/2022 • 4 minutes to read • Edit Online

Applies to

- Android
- iOS
- macOS
- Windows 10
- Windows 11

Device enrollment restrictions let you restrict enrollment based on device attributes. When restrictions are applied, users on restricted devices or who exceed the device limit are blocked from enrolling in Microsoft Intune. There are two types of device enrollment restrictions you can configure in Microsoft Intune:

- *Device platform restrictions* define which platforms, versions, and management types can enroll. In Intune, you can restrict device platforms, OS versions, manufacturer, and personally owned devices.
- *Device limit restrictions* define how many devices each user can enroll.

Each restriction type comes with one default policy that you can edit and customize as needed. Intune applies the default to all user and userless enrollments until you assign a higher-priority policy.

This article provides an overview of the available enrollment restrictions. When you're ready to create an enrollment restriction policy, see Next steps (in this article).

Available restrictions

You can configure the following restrictions in the admin center:

- Device limit
- Device platform
- OS version
- Device manufacturer
- Device ownership (personally-owned devices)

Device limit

Put a limit on the number of devices a person can enroll. You can set the device limit from 1 to 15.

This configuration is in the admin center under **Enrollment device limit restrictions**.

Device platform

Block devices running on a specific device platform. You can apply this restriction to devices running:

- Android device administrator
- Android Enterprise work profile
- iOS/iPadOS
- macOS
- Windows 10/11

In groups where both Android platforms are allowed, devices that support work profile will enroll with a work profile. Devices that don't support work profile will enroll on the Android device administrator platform. Neither

work profile nor device administrator enrollment will work until you complete all prerequisites for Android enrollment.

This restriction is in the admin center under **Enrollment device platform restrictions**.

OS version

This restriction enforces your maximum and minimum OS version requirements. This type of restriction works with the following operating systems:

- Android device administrator*
- Android Enterprise work profile*
- iOS/iPadOS*
- Windows

* Version restrictions are supported on these operating systems for devices enrolled via Intune Company Portal only.

This restriction is in the admin center under **Enrollment device platform restrictions**.

Device manufacturer

This restriction blocks devices made by specific manufacturers, and is applicable to Android devices only. It is in the admin center under **Enrollment device platform restrictions**.

Personally-owned devices

This restriction helps prevent device users from accidentally enrolling their personal devices, and applies to devices running:

- Android
- iOS/iPad OS
- macOS
- Windows 10/11

This restriction is in the admin center under **Enrollment device platform restrictions**.

Blocking personal Android devices

By default, until you manually make changes in the admin center, your Android Enterprise work profile device settings and Android device administrator device settings are the same.

If you block Android Enterprise work profile enrollment on personal devices, only corporate-owned devices can enroll with personally-owned work profiles.

Blocking personal iOS/iPadOS devices

By default, Intune classifies iOS/iPadOS devices as personally-owned. To be classified as corporate-owned, an iOS/iPadOS device must fulfill one of the following conditions:

- Registered with a serial number or IMEI.
- Enrolled by using Automated Device Enrollment (formerly Device Enrollment Program).

> **NOTE**
> An iOS User Enrollment profile overrides an enrollment restriction policy. For more information, see Set up iOS/iPadOS and iPadOS User Enrollment (preview).

Blocking personal Macs

By default, Intune classifies macOS devices as personally-owned. To be classified as corporate-owned, a Mac must fulfill one of the following conditions:

- Registered with a serial number.
- Enrolled by using Automated Device Enrollment (formerly Device Enrollment Program).

Blocking personal Windows devices

If you block personally owned Windows devices from enrollment, Intune checks to make sure that each new Windows enrollment request has been authorized for corporate enrollment. Unauthorized enrollments are blocked.

The following enrollment methods are authorized for corporate enrollment:

- The enrolling user is using a device enrollment manager account.
- The device enrolls through Windows Autopilot.
- The device is registered with Windows Autopilot but isn't an MDM enrollment only option from Windows Settings.
- The device enrolls through a bulk provisioning package.
- The device enrolls through GPO, or automatic enrollment from Configuration Manager for co-management.

> **NOTE**
> Since a co-managed device enrolls in the Microsoft Intune service based on its Azure AD device token, and not a user token, only the default Intune enrollment restriction will apply to it.

Intune marks devices going through the following types of enrollments as corporate-owned, and blocks them from enrolling because these methods don't offer the Intune administrator per-device control:

- Automatic MDM enrollment with Azure Active Directory join during Windows setup*.
- Automatic MDM enrollment with Azure Active Directory join from Windows Settings*.

Intune also blocks personal devices using these enrollment methods:

- Automatic MDM enrollment with Add Work Account from Windows Settings*.
- MDM enrollment only option from Windows Settings.

* These won't be blocked if registered with Autopilot.

Limitations

- Enrollment restrictions are applied to users. For enrollment scenarios that aren't user-driven, such as Windows Autopilot self-deploying mode, bulk enrollment (WCD), or Azure Virtual desktop, Intune enforces the default policy.
- Device limit restrictions can't be applied to devices in the following Windows enrollment scenarios, because these scenarios utilize shared device mode:
  - Co-managed enrollments
  - Group Policy (GPO) enrollments
  - Azure Active Directory (Azure AD) joined enrollments, including bulk enrollments
  - Windows Autopilot enrollments
  - Device enrollment manager enrollments

  Instead, you can configure a hard limit for these enrollment types in Azure AD. For more information, see Manage device identities by using the Azure portal.

Next steps

Use the table-of-contents to step through each article in the enrollment restrictions how-to guide, or jump to an

article using the following links:

- Create device platform enrollment restrictions
- Create device limit enrollment restrictions
- View enrollment reports

Create device platform restrictions

9/23/2022 • 5 minutes to read • Edit Online

Applies to

- Android
- iOS
- macOS
- Windows 10
- Windows 11

Create a device platform enrollment restriction policy to restrict devices from enrolling in Intune. Available restrictions include:

- Device platform
- OS version
- Manufacturer
- Ownership (personally-owned)

You can create a new device platform restriction policy in the Microsoft Endpoint Manager admin center or use the default policy that's already available. You can have up to 25 device platform restriction policies.

This article describes the device platform restrictions supported in Microsoft Intune and how to configure them in the admin center.

Default policy

Microsoft Intune provides one default policy for device platform restrictions that you can edit and customize as needed. Intune applies the default policy to all user and userless enrollments until you assign a higher-priority policy.

Best practice - Android platform restrictions

Since Intune supports two Android platforms, it's important to understand how OS version restrictions work when used together with device platform restrictions:

- If you allow both platforms for the same group, and then refine it for specific and non-overlapping versions, devices are sent through the Android enrollment flow that's picked for their version.
- If you allow both platforms, but block the same versions, devices running blocked versions can't enroll. Users on these devices are sent through the Android device administrator enrollment flow before they're blocked and prompted to sign out.

Create a device platform restriction

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Go to **Devices** > **Enroll devices** > **Enrollment device platform restrictions**.
3. Select the tab along the top of the page that corresponds with the platform you're configuring. Your options:
   - **Android restrictions**

- **Windows restrictions**
- **MacOS restrictions**
- **iOS restrictions**

4. Select **Create restriction**.
5. On the **Basics** page, give the restriction a name and optional description.
6. Select **Next**.
7. On the **Platform settings** page, configure the restrictions for your selected platform. Your options:
   - **Platform** (Android): Select **Allow** to permit a platform to enroll, and **Block** to restrict it.
   - **MDM** (Windows, macOS, and iOS/iPadOS): Select **Allow** to permit a platform to enroll, and **Block** to restrict it.
   - **Personally-owned**: Select **Allow** to permit devices to enroll and operate as personal devices.
   - **Device manufacturer** (Android): Enter a comma-separated list of the manufacturers that you want to block.
   - **Allow min/max range** (Android, Windows, iOS/iPadOS): Enter the minimum and maximum OS versions allowed to enroll. Supported version formats include:
     - Windows supports major.minor.build.rev for Windows 10 and Windows 11.
     - Android device administrator and Android Enterprise work profile support major.minor.rev.build.
     - iOS/iPadOS supports major.minor.rev.

     > **TIP**
     > The min/max range isn't applicable to Apple devices that enroll with the Device Enrollment Program, Apple School Manager, or the Apple Configurator app. Although Intune doesn't block ADE enrollments that use Company Portal to authenticate, not meeting OS requirements impacts registration because devices can't create the Azure AD device record used to evaluate Conditional Access policies. You can tell that this is the case if a device user receives an error message that says "Couldn't map device record with a user" after they sign in to Company Portal.

8. Select **Next**.
9. Optionally, add scope tags to the restriction. For more information about scope tags, see Use role-based access control and scope tags for distributed IT.

   > **NOTE**
   > If you apply scope tags to a restriction, only Intune users within scope can view and manage the policy. Only people in scope can view and reorder a restriction, or change its priority level. They can also see the relative priority of the restriction, even if they can't see all restrictions.

10. Select **Next**.
11. On the **Assignments** page, select **Add groups** and then use the search box to find and select groups. To assign the restriction to all device users, select **Add all users**. If you don't assign a restriction to at least one group, the restriction won't take effect.
12. Optionally, after you assign groups, select **Edit filter** to restrict the policy assignment further with filters. Filters are available for macOS, iOS, and Windows policies. For more information, see Apply assignment filters (in this article).

13. Select **Next**.
14. Review your policy, and then select **Create** to create it.

You can view the new restriction policy and access its properties in the **Enrollment device platform restrictions** > **Device type restrictions** table. Select and drag the restriction to reposition it in the table and change its priority.

Apply assignment filters

You can use assignment filters to include and exclude additional devices from certain group-targeted policies. Enrollment restrictions and ESP policies both support the use of assignment filters.

For example, you can use a filter to allow personal Windows devices to enroll while blocking devices that run a specific operating system SKU. To achieve this outcome, apply a preconfigured filter to your enrollment restriction assignments. The filter needs to have the `operatingSystemSKU` property in its rules. Example steps:

1. Create a platform enrollment restriction policy for Windows.
2. In the platform settings, select the option that allows personal devices to enroll.
3. In the assignments settings, select the groups you want to assign.
4. Select **Edit filter** and then apply your preconfigured filter that contains the `operatingSystemSKU` property. The applied property blocks devices running Windows 10 Home edition.

For more information about creating filters, see Create a filter.

Supported filter properties

Enrollment restrictions support fewer filter properties than other group-targeted policies. This is because devices aren't yet enrolled, so Intune doesn't have the device info to support all properties. You'll see the limited selection of properties when you:

- Configure a device platform restriction policy for Apple and Windows devices.
- Configure an enrollment status page (ESP) policy for Windows.
- Edit a filter that's in-use in an enrollment restriction or ESP profile.

The following filter properties are always available to use with enrollment policies:

Windows

- OS version
- Operating System SKU
- Enrollment profile name

iOS/iPadOS and macOS

- Manufacturer
- Model
- OS version
- Ownership
- Enrollment profile name

For more information about these properties, see device properties. Filters can't be used with Android enrollment restrictions.

Edit enrollment restrictions

Edits are applied to new enrollments and do not affect devices that are already enrolled.

1. Go to **Enrollment device platform restrictions**.
2. In the **Device type restrictions** table, select the name of the policy you want to change.
3. Select **Properties**.
4. Select **Edit**.
5. Make your changes and select **Review + save**.
6. Review your changes and select **Save**.

Create device limit restrictions in Intune

9/23/2022 • 3 minutes to read • Edit Online

Applies to

- Android
- iOS
- macOS
- Windows 10
- Windows 11

Create a device limit enrollment restriction policy to limit the number of devices a user can enroll in Microsoft Intune. Device limit restrictions work on devices that meet the following criteria:

- Microsoft Intune-managed
- Established contact with Intune within last 90 days
- Not in a registration-pending state for more than 24 hours
- Hasn't failed Apple enrollment
- Hasn't been deleted from Microsoft Intune
- Enrollment type is not in shared mode (check DeviceCountsForDeviceCap for detail)

You can create a new device limit-enrollment restriction policy in the Microsoft Endpoint Manager admin center or use the default policy that's already available. You can have up to 25 device limit restriction policies.

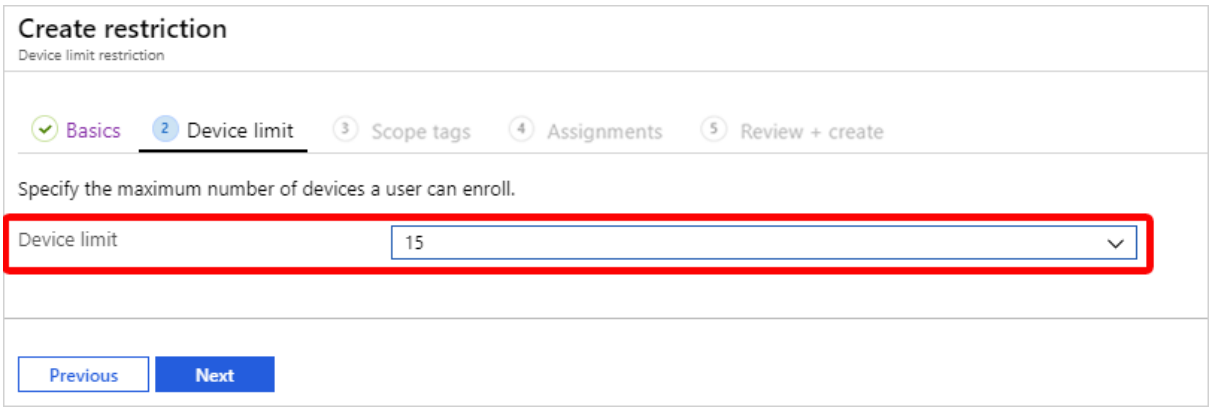
This article describes how to create and configure a device limit-enrollment restriction policy in the admin center.

Default policy

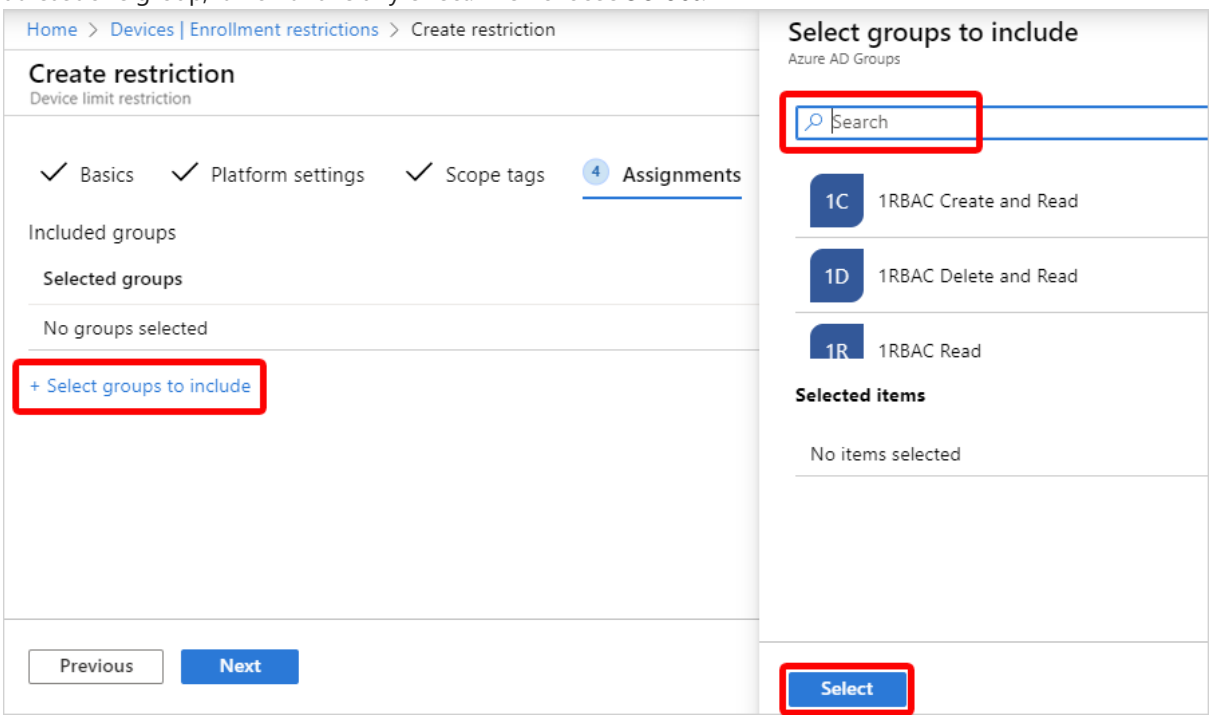
Microsoft Intune provides one default policy for device limit restrictions that you can edit and customize as needed. Intune applies the default policy to all user and userless enrollments until you assign a higher-priority policy.

Create a device limit restriction

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Go to **Devices** > **Enrollment restrictions** > **Create restriction** > **Device limit restriction**.
3. On the **Basics** page, give the restriction a **Name** and optional **Description**.
4. Choose **Next** to go to the **Device limit** page.
5. For **Device limit**, select the maximum number of devices that a user can enroll.



6. Choose **Next** to go to the **Scope tags** page.
7. On the **Scope tags** page, optionally add the scope tags you want to apply to this restriction. For more information about scope tags, see Use role-based access control and scope tags for distributed IT.
8. Choose **Next** to go to the **Assignments** page.
9. Choose **Select groups to include** and then use the search box to find groups that you want to include in this restriction. The restriction applies only to groups to which it's assigned. If you don't assign a restriction to at least one group, it won't have any effect. Then choose **Select**.



10. Select **Next** to go to the **Review + create** page.
11. Select **Create** to create the restriction. The new restriction appears in your list of restrictions and is given a higher priority than the default policy. For information about changing the priority level, see Change restriction priority (in this article).

Edit enrollment restrictions

Edits are applied to new enrollments and don't affect devices that are already enrolled.

1. Go to **Enrollment device limit restrictions** to bring up the list of your policies.
2. Select the name of the policy you want to change.
3. Select **Properties**.
4. Select **Edit**.
5. Make your changes and select **Review + save**.
6. Review your changes and select **Save**.

Change restriction priority

When a group is assigned multiple restrictions, the priority level determines which policy gets applied. The restriction with highest priority (*1* being the highest priority position) is applied and the other restrictions are disregarded. For example:

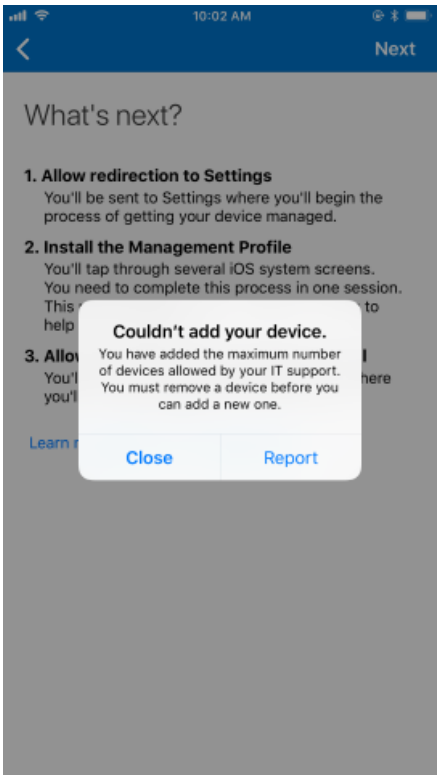
1. Joe belongs to two user groups in Intune: Group A and Group B.
2. Group A is assigned a restriction policy. Its priority level is 5.
3. Group B is assigned a restriction policy. The priority level is 2.
4. Joe is subject only to the priority 2 restrictions.

When you create a restriction, it's added to the list just above the default. You can change the priority of non-default restrictions.

1. Go to **Enrollment device limit restrictions**.
2. Select **Device limit restrictions** to bring up the list of your policies.
3. Hover over the policy in the **Priority** column,and then select and drag the priority to the desired position in the list.

Device user experience

BYOD users who reach their device limit receive a message during enrollment explaining the restriction. To continue enrolling, the device user must unenroll an existing device. Alternatively, as the admin you can increase the device limit in the admin center. For more information about troubleshooting enrollment errors such as this one, see Troubleshoot device enrollment.



View enrollment reports

9/23/2022 • 2 minutes to read • Edit Online

Applies to

- Android
- iOS
- macOS
- Windows 10
- Windows 11

Your can use the following reports in the Microsoft Endpoint Manager admin center to monitor and troubleshoot issues with enrollment restrictions and enrollment status page assignments:

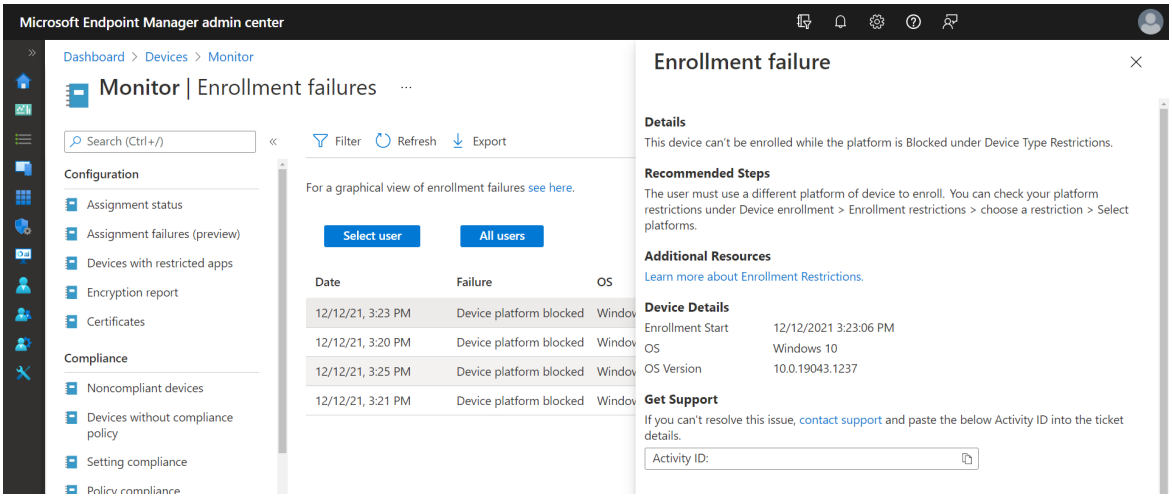
- Enrollment failures report
- Troubleshooting + support page
- Device enrollment page

This article describes each report and how to access them in the admin center.

Enrollment failures report

Use the enrollment failures report to view enrollment failures for all users or for select users. This report shows each failed enrollment attempt along with the date it occurred, reason for failure, OS, OS version, username, and enrollment method.

1. Sign in to the Microsoft Endpoint Manager admin center and select **Devices** > **Monitor** > **Enrollment failures**.
2. Select **All users** or **Select user**, depending on the scenario you're troubleshooting.
3. Select a row in the table for more details about the failure and recommended remediation steps.



Troubleshooting + support page

Use the enrollment failures report on the Troubleshooting + support page to view enrollment failures for a select user. This report shows every failed enrollment attempt the user encountered along with the date it occurred, reason for failure, OS, OS version, username, and enrollment method. You can also view other data

about the user on this page, including all assignments, devices, and app protection statuses they're associated with.

1. Sign in to the Microsoft Endpoint Manager admin center and select **Troubleshooting + support** > **Select user**.
2. Choose a user > **Select**.
3. Under **Enrollment failures**, select a row to view more details about the failure and recommended remediation steps.

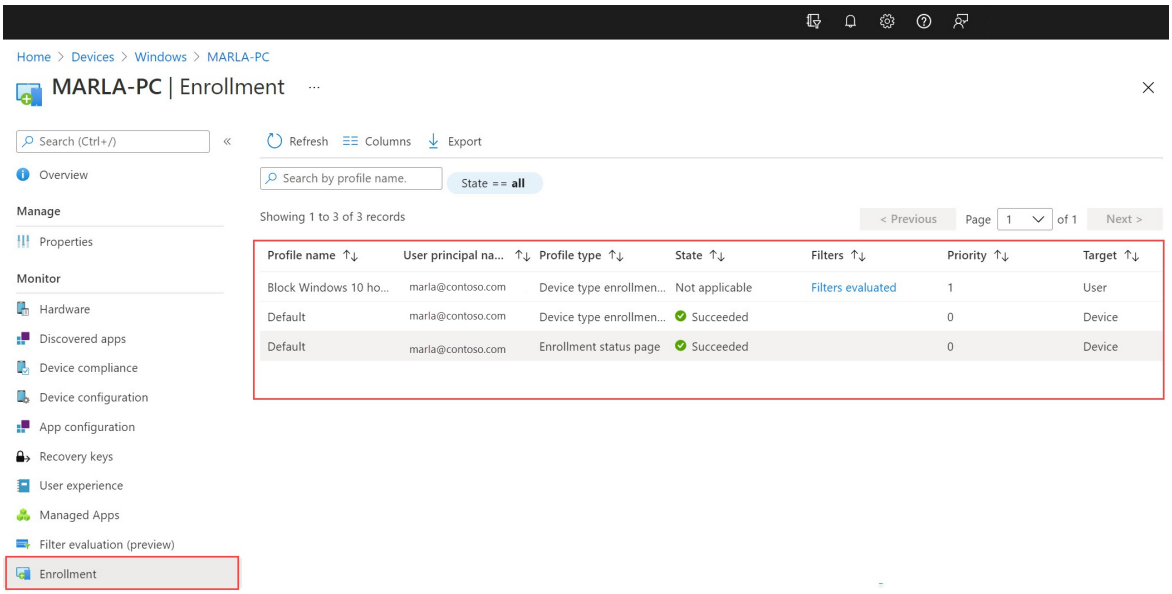
Device enrollment page

The device enrollment page shows the enrollment policies (both enrollment restriction and enrollment status page policies) applied to a device when it was first enrolled in Microsoft Intune. Use this report to help pinpoint the source of the failure, such as an unexpected policy, target, or filter. Data is available for iOS/iPadOS, macOS, and Windows devices, and includes:

- Profile name
- User principal name
- Profile type (either enrollment status page or device type enrollment restriction)
- Priority
- Target (either user or device)
- Filters, with a link to the filter evaluation results (only available if the enrollment policy was assigned using an assignment filter)

To access report data:

1. Sign in to the Microsoft Endpoint Manager admin center and select **Devices** > **All devices**.
2. Select an enrolled iOS/iPadOS, macOS, or Windows device.
3. Under **Monitor**, select **Enrollment**.
4. Review the report data.



NOTE

Report data is only available for devices enrolled after the Microsoft Intune 2112 service release. No results are available for devices enrolled prior to that release.