✓ 100 XP ▶

Managing Windows devices with Intune

10 minutes

Intune lets you manage your workforce’s devices and apps and how they access your company data. To use this Mobile Device Management (MDM) system, the devices must first be enrolled in the Intune service. Several methods exist to enroll your workforce’s devices. Each method depends on the device's ownership (personal or corporate), device type (iOS, Windows, Android), and management requirements (resets, affinity, locking).

By default, devices for all platforms can enroll in Intune. However, you can restrict devices by platform.

Device management lifecycle

Managing mobile devices, like most IT management activities, follows a lifecycle. The mobile device management lifecycle contains four phases:

- **Enroll**. In the Enroll phase, devices register with the mobile device management solution. With Intune, you can enroll both mobile devices, such as phones, and Windows PCs.
- **Configure**. In the Configure phase, you help to ensure that the enrolled devices are secure and that they comply with any configuration or security policies. You can also automate common administrative tasks, such as configuring Wi-Fi.
- **Protect**. In the Protect phase, the mobile device management solution provides ongoing monitoring of the settings established in the Configure phase. During this phase, you also use the mobile device management solution to help keep devices compliant through the monitoring and deployment of software updates.
- **Retire**. When a device is no longer needed, when it’s lost, or when it’s stolen, you should help to protect the data on the device. You can remove data by resetting the device, performing a full wipe, or performing a selective wipe that removes only corporation-owned data from the device.

Automatic MDM Enrollment

Automatic enrollment lets users enroll their Windows 10 devices in Intune without assistance from IT. Administrators can use the **Azure Active Directory (AAD)** portal to enable automatic enrollment for all users or members of specific groups.

To enroll their devices, 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 and can be managed with Intune through the AAD portal.

Enrolling Windows 10 devices

There are many ways to enroll Windows 10 devices into Microsoft Intune for device management. Some are user-driven and some controlled by IT administrators. Some exist to support BYOD programs and others to streamline modern provisioning scenarios and management for corporate-owned devices. Each enrollment method can have different setup requirements and behaviors.

The following methods, that can be used to enroll in Intune are:

Method	Description
Method 1: Add work or school account	This enrollment method will add the device to the domain by using Azure AD join. If you have Azure AD Premium licenses and your Azure AD tenant has auto-enrollment for Intune configured, your device will also be enrolled into Intune during as well. This method is the preferred method when Autopilot is not used in the environment.
Method 2: Enroll in MDM only (user driven)	This enrollment method will only enroll the device in Intune and not Azure AD join the device. You will only use this form of enrollment in environments that do not have Azure AD Premium licenses that are required to enable auto-enrollment of devices into Intune.
Method 3: Azure AD join (OOBE)	This enrollment method is essentially the same as method 1, with one exception: the device is enrolled during the Out of Box Experience (OOBE). If you have Azure AD Premium licenses and your Azure AD tenant has auto-enrollment for Intune configured, your device will also be enrolled into Intune during as well.
Method 4: Azure AD join (autopilot – user-driven deployment mode)	This enrollment method is essentially the same as method 2, with a few exceptions. The device is enrolled during a customized Out of Box Experience (OOBE). Many of the OOBE screens can be skipped to ensure a smoother setup experience for end users. This method is the preferred method for enrolling device in Intune but it requires Azure AD Premium licenses and your Azure AD tenant has auto-enrollment for Intune configured.

Method	Description
Method 5: Azure AD join (autopilot self-deploying mode)	This enrollment method basically does the same as method 4, with one exception. It allows all OOBE screens to be skipped after the device is first powered on. The Azure AD join and Intune enrollment are fully automated without any user interaction. This type of enrollment is primarily for user-less devices such as kiosks, but it can be used for normal users as well. You can pre-assign a user to a device so all the user has to supply is a password. This setup experience is the most streamlined compared to the other methods.
Method 6: Enroll in MDM only (Device Enrollment Manager)	This method of enrollment is very similar to method 3, except it’s performed by IT admins using a special type of account - A Device Enrollment Manager (DEM) account. The DEM would enroll the device, log on to the company portal and install the apps required by the user.
Method 7: System Center Configuration Manager co-management	Co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Intune. It’s a solution that provides a bridge from traditional to modern management and gives you a path to make the transition using a phased approach. Co-management is the preferred way to enroll existing devices, that are already being managed by System Center Configuration Manager (SCCM). Once enabled, the device can be managed by SCCM and Intune, leveraging the best features of both.
Method 8: Azure AD join (bulk enrollment)	Bulk enrollment is an efficient way to set up a large number of devices to be managed by Intune without the need to re-image the devices. You enable bulk enrollment by creating a provisioning package using the Windows Configuration Designer app from the Store.

Device and user profiles

Microsoft Intune includes settings and features that you can enable or disable on different devices within your organization. These settings and features are managed using profiles. Some profile examples include:

- A Wi-Fi profile that gives different devices access to your corporate Wi-Fi.
- A VPN profile that gives different devices access to your VPN server within your corporate network.

The following profiles are available in Intune:

Profile	Description
Device features (iOS and macOS)	Device features control features on iOS and macOS devices, such as AirPrint, notifications, and shared device configurations.
Device restrictions	Device restrictions control security, hardware, data sharing, and more settings on the devices. For example, create a device restriction profile that prevents iOS device users from using the device camera.
Endpoint protection	Endpoint protection settings for Windows 10 configure BitLocker and Windows Defender settings for Windows 10 devices.
Identity Protection	Identity protection controls the Windows Hello for Business experience on Windows 10 and Windows 10 Mobile devices. Configure these settings to make Windows Hello for Business available to users and devices, and to specify requirements for device PINs and gestures.
Kiosk	The kiosk settings profile configures a device to run one app or run multiple apps. You can also customize other features on your kiosk, including a start menu and a web browser.
Email	The email settings profile creates, assigns, and monitors Exchange ActiveSync email settings on the devices. Email profiles help ensure consistency, reduce support calls, and let end-users access company email on their personal devices, without any required setup on their part.
VPN	VPN settings assign VPN profiles to users and devices in your organization, so they can easily and securely connect to the network. Virtual private networks (VPNs) give users secure remote access to your company network. Devices use a VPN connection profile to start a connection with your VPN server.
Wi-Fi	Wi-Fi settings assign wireless network settings to users and devices. When you assign a Wi-Fi profile, users get access to your corporate Wi-Fi without having to configure it themselves.
eSIM cellular (public preview)	eSIM cellular profiles provide the ability to configure cellular data plans on your managed devices for internet and data access. After getting activation codes from your mobile operator, you can use Intune to import these activation codes, and then assign to your eSIM capable devices.

Profile	Description
Education	- **Education settings - Windows 10:** configure options for the Windows Take a Test app. When you configure these options, no other apps can run on the device until the test is complete. - **Education settings – iOS:** uses the iOS Classroom app to guide learning, and control student devices in the classroom. You can configure iPad devices to multiple students can share a single device.
Edition upgrade	Windows 10 edition upgrades automatically upgrade devices that run some versions of Windows 10 to a newer edition.
Update policies	iOS update policies show you how to create and assign iOS policies to install software updates on your iOS devices. You can also review the installation status.
Certificates	Certificates configure trusted, Simple Certificate Enrollment Protocol (SCEP), and Public Key Cryptography Standards (PKCS) certificates that can be assigned to devices, and used to authenticate Wi-Fi, VPN, and email profiles.
Windows Information Protection profile	Windows Information Protection helps protect against data leakage without interfering with the employee experience. It also helps to protect enterprise apps and data against accidental data leaks on enterprise-owned devices and personal devices that employees use at work. It does this without requiring changes to your environment or other apps.
Custom profile	Custom settings include the ability to assign device settings that are not built-into Intune. For example, on Android devices, you can enter Open Mobile Alliance Uniform Resource Identifier (OMA-URI) values. For iOS devices, you can import a configuration file you created in the Apple Configurator. Custom profiles will be explained in detail in a later topic.

User profiles

The Windows 10 operating system requires each user to have a user profile. User profiles are created during a user’s first sign-in, and they are stored in the Users folder. User profiles are created based on the content in the Default profile in the Users folder. The three different types of user profiles are:

- **Local:** This type is available on a single computer only.
- **Roaming:** This type can roam between computers that are domain members.
- **Mandatory:** This is a special type of preconfigured user profile that does not store user changes between sign-ins.

- **Temporary User Profiles:** A temporary profile is issued each time that an error condition prevents the user's profile from loading.

Learn more

- Plan for device Compliance
- Design and create Conditional Access Policies
- Configure device compliance policy
- Manage Conditional Access Policies
- Microsoft Intune device reports

Next unit: Summary and knowledge check

Continue >