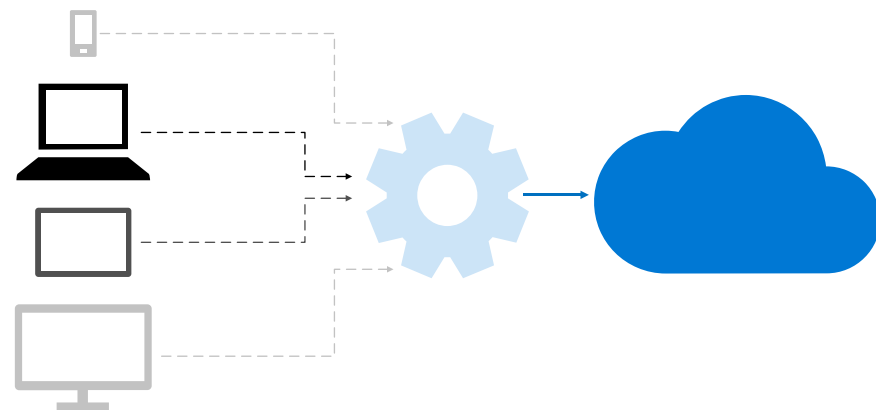


# Intune Enrollment Options

## Enroll your devices into management with Intune

A core component of enterprise-level security includes managing and protecting devices. Whether you're building a Zero Trust security architecture, hardening your environment against ransomware, or building in protections to support remote workers, managing devices is part of the strategy. While Microsoft 365 includes several tools and methodologies for managing and protecting devices, Intune provides optimal integration. This guidance helps you decide which Intune enrollment option is best for your endpoints.



## Which enrollment option is best for your devices?

This guidance helps you decide which enrollment option is best for your endpoints, including:

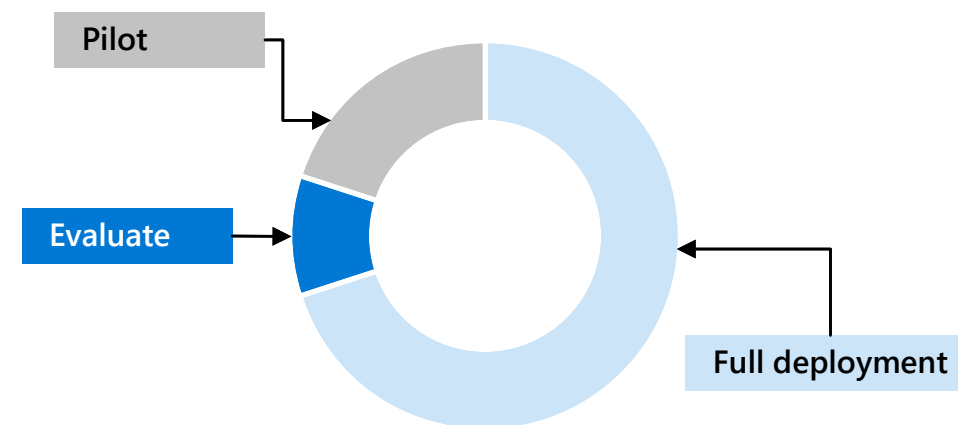
- Windows devices
- macOS
- iOS/iPad
- Android

These lists include organization-owned devices and user-owned devices (BYOD or personal devices). Select the option that best meets your organization requirements.

## Enroll devices in stages

A staged approach is a method of identifying a set of devices to enroll and verifying that certain criteria is met before proceeding to enroll a larger set of devices. You can define the exit criteria for each stage and ensure that these are satisfied before moving on to the next stage.

Adopting a staged-based deployment helps reduce potential issues that can arise while enrolling devices. By evaluating and then piloting a certain number of devices first, you can identify potential issues and mitigate potential risks that might arise.



Deployment stage	Description
<b>Evaluate</b>	Stage 1: Identify 50 endpoints for testing
<b>Pilot</b>	Stage 2: Identify the next 50-100 endpoints in the production environment
<b>Full deployment</b>	Stage 3: Enroll the rest of the endpoints in larger increments

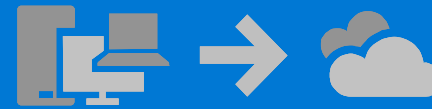
For more guidance, see [aka.ms/IntunePlanningGuide](https://aka.ms/IntunePlanningGuide).














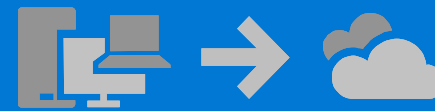
Feature	BYOD: Android Enterprise personally owned devices with a work profile	Android Enterprise dedicated devices	Android Enterprise fully managed	Android Enterprise corporate owned work profile	Android Open Source Project
Use Google Mobile Services (GMS).	✓	✓	✓	✓	✗ Device doesn't support GMS. Some countries don't support GMS.
Devices are personal or BYOD.	✓ You can mark these devices as corporate or personal.	✗ These devices should be enrolled using Android Enterprise personally owned devices with a work profile.	✗ These devices should be enrolled using Android Enterprise personally owned devices with a work profile.	✗ These devices should be enrolled using Android Enterprise personally owned devices with a work profile.	✗ Android Enterprise personally owned devices with a work profile support GMS.
You have new or existing devices.	✓	✓	✓	✓	✓
Need to enroll a few devices, or a large number of devices (bulk enrollment).	✓	✓	✓	✓	✗ Can only enroll one device at a time.
Devices are associated with a single user.	✓	✗ Not recommended. These devices should be enrolled using Android Enterprise fully managed.	✓	✓	✓
You use the optional device enrollment manager (DEM) account.	✓	✗ The DEM account isn't supported.	✗ The DEM account isn't supported.	✗ The DEM account isn't supported.	✗ The DEM account isn't supported.
Devices are managed by another MDM provider.	✗ When a device enrolls, MDM providers install certificates and other files. These files must be removed.	✗ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✗ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✗ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✗ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.
Devices are owned by the organization or school.	✗ Not recommended for organization-owned devices.	✓	✓	✓	✓
Devices are user-less, such as kiosk, dedicated, or shared.	✗ User-less or shared devices should be organization-owned.	✓	✗ User-less devices should be enrolled using Android Enterprise dedicated devices.	✗ User-less devices should be enrolled using Android Enterprise dedicated devices, or an organization administrator.	✓



Automated Device Enrollment (ADE) (supervised)		Apple Configurator enrollment		BYOD: User and Device enrollment	
Feature	Use this enrollment option when	Feature	Use this enrollment option when	Feature	Use this enrollment option when
Devices are personal or BYOD.	Not recommended. These devices should be enrolled using MAM, or User and Device enrollment.	Devices are personal or BYOD.	Not recommended. These devices should be enrolled using MAM, or User and Device enrollment.	Devices are personal or BYOD.	
You have new or existing devices.	Applicable with new devices. Existing devices should be enrolled using Apple Configurator.	You have new or existing devices.		You have new or existing devices.	
Need to enroll a few devices, or a large number of devices.	If you have a large number of devices, then this method will take some time.	Need to enroll a few devices, or a large number of devices.	If you have a large number of devices, then this method will take some time.	Need to enroll a few devices, or a large number of devices.	If you have a large number of devices, then this method will take some time.
Devices are associated with a single user.		Devices are associated with a single user.		Devices are associated with a single user.	
You use the optional device enrollment manager (DEM) account.	The DEM account isn't supported.	You use the optional device enrollment manager (DEM) account.	The DEM account isn't supported.	You use the optional device enrollment manager (DEM) account.	
Devices are managed by another MDM provider.	Users must unenroll from the current MDM provider, then enroll in Intune. With organization-owned devices, we recommend enrolling in Intune.	Devices are managed by another MDM provider.	Users must unenroll from the current MDM provider, then enroll in Intune. With organization-owned devices, we recommend enrolling in Intune.	Devices are managed by another MDM provider.	When a device enrolls, MDM providers install certificates and other files. These files must be removed. You must unenroll, reset the devices, or contact the MDM provider.
Devices are owned by the organization or school.		Devices are owned by the organization or school.		Devices are owned by the organization or school.	Not recommended. Organization-owned devices should be enrolled using Automated Device Enrollment or Apple Configurator.
Devices are user-less, such as kiosk, dedicated, or shared.		Devices are user-less, such as kiosk, dedicated, or shared.		Devices are user-less, such as kiosk, dedicated, or shared.	Typically, user-less or shared devices are organization-owned. These devices should be enrolled using Automated Device Enrollment or Apple Configurator.
You want supervised mode.	Supervised mode deploys software updates, restricts features, allows and blocks apps, and more.	Your team doesn't want to use the ABM or ASM portals, to set up requirements.	The idea of <i>not</i> using the ABM or ASM portals is to give administrators less control.	You want to help protect a specific feature on the device, such as per-app VPN.	
		You need a wired connection, or are having a network issue.			
		A country doesn't support Apple Business Manager or Apple School Manager.	If your country supports ABS or ASM, then devices should be enrolled using Automated Device Enrollment.		



	BYOD: Device enrollment	Automated Device Enrollment (ADE) (supervised)	Direct enrollment
Feature	Use this enrollment option when	Use this enrollment option when	Use this enrollment option when
 Devices are personal or BYOD.	✓	✗ Not recommended. BYOD or personal devices should be enrolled using Device enrollment.	✗ Not recommended. BYOD or personal devices should be enrolled using Device enrollment.
 You have new or existing devices.	✓	<ul style="list-style-type: none"> <li>✓ Applicable with new devices.</li> <li>✓ To enroll existing devices, see Enroll your macOS device registered in ABM/ASM with Automated Device Enrollment after Setup Assistant.</li> </ul>	✓
 Need to enroll a few devices, or a large number of devices.	✓	✓	✓ If you have a large number of devices, then this method will take some time.
 Devices are associated with a single user.	✓	✓	✗ Not recommended. Devices that need user affinity should be enrolled using Automated device enrollment (ADE).
 You use the optional device enrollment manager (DEM) account.	<ul style="list-style-type: none"> <li>✓ Be aware of impact and any limitations using DEM account.</li> </ul>	✗ The DEM account isn't supported.	✗ The DEM account isn't supported.
 Devices are managed by another MDM provider.	✗ When a device enrolls, MDM providers install certificates and other files. These files must be removed. You must unenroll, reset the devices, or contact the MDM provider.	✗ To be fully managed by Intune, users must unenroll from the current MDM provider, and then enroll in Intune. Or, you can use Device enrollment to manage specific apps on the device. Since these devices are organization-owned, it's recommended to enroll in Intune.	✗ To be fully managed by Intune, users must unenroll from the current MDM provider, and then enroll in Intune. Or, you can use Device enrollment to manage specific apps on the device. Since these devices are organization-owned, it's recommended to enroll in Intune.
 Devices are owned by the organization or school.	✗ It's recommended that organization-owned devices should be enrolled using Automated Device Enrollment or Apple Configurator.	✓	✓
 Devices are user-less, such as kiosk, dedicated, or shared.	✗ These devices are organization-owned. User-less devices should be enrolled using Automated Device Enrollment or Apple Configurator.	✓	✓
 You need a wired connection, or are having a network issue.	<ul style="list-style-type: none"> <li>✓ A wired connection isn't needed, but can be used.</li> <li>✗ If there's a network issue, you can use Direct enrollment.</li> </ul>	<ul style="list-style-type: none"> <li>✓ A wired connection isn't needed, but can be used.</li> <li>✗ If there's a network issue, you can use Direct enrollment.</li> </ul>	✓
 Your team doesn't want to use the ABM or ASM portals, to set up requirements.	✗ Use Direct enrollment.	✗ Use Direct enrollment.	✓ The idea of <i>not</i> using the ABM or ASM portals is to give administrators less control.
 A country doesn't support Apple Business Manager or Apple School Manager.	✗ Use Direct enrollment.	✗ Use Direct enrollment.	✓ If your country supports ABS or ASM, then devices should be enrolled using Automated Device Enrollment.



	Windows Automatic enrollment	Windows Autopilot	BYOD: User enrollment	Co-management with Configuration Manager
Feature	Use this enrollment option when	Use this enrollment option when	Use this enrollment option when	Use this enrollment option when
You have Azure AD Premium.	✓	✓ Windows Autopilot uses Automatic enrollment. Automatic enrollment requires Azure AD Premium.	✗ Azure AD Premium isn't required. ✓ If the devices join Azure AD, then they can use Azure AD Premium features.	✓ Depending on your co-management configuration, Azure AD Premium may be required.
You'll use Conditional Access on devices enrolled via bulk enrollment.	✓ Available on Windows 11 and Windows 10 1803+.	Not applicable	Not applicable	✓
You purchase devices from an OEM that supports the Windows Autopilot service.	✗ If your OEM supports Windows Autopilot, then use Windows Autopilot enrollment.	✓	Not applicable	✓
Devices are hybrid Azure AD joined.	✗ Automatic enrollment is available for full Azure AD joined devices (cloud-native endpoints).	✓ Hybrid Azure AD joined devices are joined to your on-premises AD, and registered with your Azure AD. Devices registered in Azure AD are available to Intune.	✓ Users should know that their personal devices might be managed by the organization IT.	✓ Hybrid Azure AD joined devices are joined to your on-premises AD, and registered with your Azure AD. Devices registered in Azure AD are available to Intune.
You have remote workers.	✓	✓ With Windows Autopilot, the OEM can ship devices directly to users.	✓ Users should know that their personal devices might be managed by the organization IT.	✓
Devices are personal or BYOD.	✓	✗ For BYOD or personal devices, use Windows automatic enrollment or a User enrollment option.	✓	✓
You have new or existing devices.	✓	✓ You can update desktops running older Windows versions, e.g. Windows 7 to 10. This option also uses Microsoft Endpoint Configuration Manager.	✓	✓ For devices that aren't running Windows 10/11, such as Windows 7, you'll need to upgrade.
Need to enroll a few devices, or a large number of devices.	✓ Bulk enrollment is available for organization-owned devices, not personal/BYOD.	✓	✓	✓
Devices are associated with a single user.	✓	✓	✓	✓
You use the optional device enrollment manager (DEM) account.	✓	✓	✗ DEM accounts don't apply to User enrollment.	✗ DEM accounts don't apply to co-management.
Devices are managed by another MDM provider.	✗ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✗ To be fully managed by Intune, users need to unenroll from the current MDM provider, and then enroll in Intune.	✓ A device managed by another MDM provider can register in Azure AD. ✗ For Intune, users need to unenroll from the current provider, and then enroll in Intune.	✗ To be co-managed, users need to unenroll from the current MDM provider. They shouldn't be enrolled using the Intune classic agents.
Devices are owned by the organization or school.	✓	✓	✓ You can use User enrollment, but it's recommended to use Windows Autopilot, or Windows Automatic enrollment.	✓
Devices are user-less, such as kiosk, dedicated, or shared.	✓ Requires users to sign in with their organization account and automatically enroll. Then create a kiosk profile, and assign it to this device.	✓ Requires users to sign in with their organization account and automatically enroll. Then create a kiosk profile, and assign it to this device.	✗ Requires a user to sign in with an organization account, and use the Settings app, which isn't common on shared devices.	✓ Requires users to sign in with their organization account and automatically enroll. Then create a kiosk profile, and assign it to this device.
Devices are enrolled in Intune.	Not applicable	Not applicable	Not applicable	✓ You have devices you want to bring to co-management. Devices may have been enrolled using Windows Autopilot, or directly from your hardware OEM.