

# Migration guide: Set up or move to Microsoft Intune

Article • 03/03/2025

After you [planned for the move to Microsoft Intune](#), the next step is to choose the migration approach that's right for your organization. These decisions depend on your current mobile device management (MDM) environment, business goals, and technical requirements.

This migration guide lists and describes your options to adopt or move to Intune, which include.

- You don't use a mobile device management solution
- You use a third party partner MDM solution
- You use Configuration Manager
- You use on-premises group policy
- You use Microsoft 365 Basic Mobility and Security

Use this guide to determine the best migration approach, and get some guidance & recommendations.

## Tip

- This guide is a living thing. So, be sure to add or update existing tips and guidance you've found helpful.
- As a companion to this article, the Microsoft 365 admin center also has some setup guidance. The guide customizes your experience based on your environment. To access this deployment guide, go to the [Microsoft Intune setup guide in the Microsoft 365 admin center](#) , and sign in with the **Global Reader** (at a minimum). For more information on these deployment guides and the roles needed, go to [Advanced deployment guides for Microsoft 365 and Office 365 products](#).

To review best practices without signing in and activating the automated setup features, go to the [Microsoft 365 Setup portal](#) .

## Before you begin

- Microsoft Intune is a cloud native solution that helps manage identities, devices, and apps. If your goal is to become cloud native, then you can learn more at the following articles:
  - [Learn about cloud-native endpoints](#)
  - [What is Intune?](#)
- Your Intune deployment might be different from a previous MDM deployment. Intune uses identity-driven access control. It doesn't require a network proxy to access organization data from devices outside your network.



## Currently don't use anything

If you currently don't use any MDM or mobile application management (MAM) provider, then you have some options:

- **Microsoft Intune:** If you want a cloud solution and are ready for full device management, then go straight to Intune. You can use Intune to check for compliance, configure device features, deploy apps, and install system & app updates. You also get the benefits of the [Microsoft Intune admin center](#), which is a web-based console.
  - [Get started with Intune](#)
  - [Step 1 - Set up Intune](#)
  - [Step 2 - Add, configure, and protect apps with Intune](#)
  - [Step 3 - Plan for compliance policies](#)
  - [Step 4 - Create device configuration profiles to secure devices](#)
  - [Step 5 - Enroll devices](#)
- **Configuration Manager:** If you want the features of Configuration Manager (on-premises) combined with Intune (cloud), then consider [tenant attach](#) (in this article) or [co-management](#) (in this article).

Configuration Manager can:

- Manage [on-premises Windows Server and some client devices](#).
- Manage [partner or third party software updates](#).
- Create [custom task sequences](#) when deploying the Windows operating system.
- [Deploy and manage many app types](#).

## Currently use a third party MDM provider

Devices should only have one MDM provider. If you use another MDM provider, like Workspace ONE (previously called AirWatch), MobileIron, or MaaS360, then you can move to Intune.

Users must unenroll their devices from the current MDM provider before they enroll in Intune.

1. **Set up Intune**, including setting the MDM Authority to Intune.

For more information, go to:

- [Get started with your Microsoft Intune deployment](#)
- [Step 1 - Set up Intune.](#)

2. **Deploy apps and create app protection policies.** The idea is to help protect organization data in your apps during the migration and until devices are enrolled & managed by Intune.

For more information, go to [Step 2 - Add, configure, and protect apps with Intune.](#)

3. **Unenroll devices** from the current MDM provider.

When devices are unenrolled, they aren't receiving your policies, including policies that provide protection. The devices are vulnerable until they enroll in Intune and start receiving your new policies.

Give users specific unenroll steps. Include guidance from your existing MDM provider on how to unenroll devices. Clear and helpful communication minimizes end user downtime, dissatisfaction, and helpdesk calls.

4. Optional, but recommended. If you have Microsoft Entra ID P1 or P2, also use **Conditional Access** to block devices until they enroll in Intune.

For more information, go to [Step 3 – Plan for compliance policies.](#)

5. Optional, but recommended. Create a baseline of compliance and device settings that all users and devices must have. These policies can be deployed when users enroll in Intune.

For more information, go to:

- [Step 3 – Plan for compliance policies](#)
- [Step 4 - Configure device features and settings to secure devices and access resources](#)
- [Levels of protection and configuration in Microsoft Intune](#)

6. **Enroll in Intune.** Be sure you give users specific enrollment steps.

For more information, go to:

- [Step 5 – Enroll devices in Microsoft Intune](#)
- [Intune enrollment deployment guide](#)

### Important

Don't configure Intune and any existing third party MDM solution simultaneously to apply access controls to resources, including Exchange or SharePoint.

#### Recommendations:

- If you're moving from a partner MDM/MAM provider, then note the tasks you're running and the features you use. This information gives an idea of what tasks to also do in Intune.
- Use a phased approach. Start with a small group of pilot users, and add more groups until you reach full scale deployment.
- Monitor the helpdesk load and enrollment success of each phase. Leave time in the schedule to evaluate success criteria for each group before migrating the next group.

Your pilot deployment should validate the following tasks:

- Enrollment success and failure rates are within your expectations.
- User productivity:
  - Corporate resources are working, including VPN, Wi-Fi, email, and certificates.
  - Deployed apps are accessible.
- Data security:
  - Review compliance reports, and look for common issues and trends. Communicate issues, resolutions, and trends with your help desk.
  - Mobile app protections are applied.
- When you're satisfied with the first phase of migrations, repeat the migration cycle for the next phase.
  - Repeat the phased cycles until all users are migrated to Intune.
  - Confirm the helpdesk is ready to support end users throughout the migration. Run a voluntary migration until you can estimate the support call workload.
  - Don't set deadlines for enrollment until your helpdesk can handle all remaining users.

#### Helpful information:

- [Get started with Intune](#)
- [Intune enrollment deployment guide](#)
- [Step 1 - Set up Intune and your tenant](#)

# Currently use Configuration Manager

Configuration Manager supports Windows Servers, and Windows & macOS client devices. If your organization uses other platforms, you might need to reset the devices, and then enroll them in Intune. Once enrolled, they receive the policies and profiles you create. For more information, see the [Intune enrollment deployment guide](#).

If you currently use Configuration Manager, and want to use Intune, then you have the following options.



## Option 1 - Add tenant attach

Tenant attach allows you to upload your Configuration Manager devices to your organization in Intune, also known as a **tenant**. After you attach your devices, you use the [Microsoft Intune admin center](#) to run remote actions, like sync machine and user policy. You can also see your on-premises servers, and get OS information.

Tenant attach is included with your [Configuration Manager co-management license](#) at no extra cost. It's the easiest way to integrate the cloud (Intune) with your on-premises Configuration Manager setup.

For more information, see [enable tenant attach](#).

## Option 2 - Set up co-management

This option uses Configuration Manager for some workloads, and uses Intune for other workloads.

1. In Configuration Manager, set up [co-management](#).
2. In Intune, [set up Intune](#), including setting the MDM Authority to Intune.

Devices are ready to be enrolled in Intune, and receive your policies.

Helpful information:

- [What is co-management?](#)
- [Co-management workloads](#)
- [Switch Configuration Manager workloads to Intune](#)
- [Configuration Manager product and licensing FAQ](#)

## Option 3 - Move from Configuration Manager to Intune

Most existing Configuration Manager customers want to keep using Configuration Manager. It includes services that are beneficial for on-premises devices.

These steps are an overview, and are only included for those users who want a 100% cloud solution. With this option, you:

- Register existing on-premises Active Directory Windows client devices as devices in Microsoft Entra ID.
- Move your existing on-premises Configuration Manager workloads to Intune.



This option is more work for administrators, but can create a more seamless experience for existing Windows client devices. For new Windows client devices, we recommend you [start from scratch with Microsoft 365 and Intune](#) (in this article).

1. In Microsoft Entra, set up [hybrid Active Directory and Microsoft Entra ID](#) for your devices. Microsoft Entra hybrid joined devices are joined to your on-premises Active Directory, and registered with your Microsoft Entra ID. When devices are in Microsoft Entra ID, they're also available to Intune.

Hybrid Microsoft Entra ID supports Windows devices. For other prerequisites, including sign-in requirements, see [Plan your Microsoft Entra hybrid join implementation](#).

2. In Configuration Manager, set up [co-management](#).
3. In Intune, [set up Intune](#), including setting the MDM Authority to Intune.
4. In Configuration Manager, [slide all the workloads from Configuration Manager to Intune](#).
5. On the devices, uninstall the Configuration Manager client. For more information, see [uninstall the client](#).

Once Intune is set up, you can create an Intune app configuration policy that uninstalls the Configuration Manager client. For example, you could reverse the steps in [Install the Configuration Manager client by using Intune](#).

Devices are ready to be enrolled in Intune, and receive your policies.

#### Important

Hybrid Microsoft Entra ID supports only Windows devices. Configuration Manager supports Windows and macOS devices. For macOS devices managed in Configuration Manager, you can:

1. Uninstall the Configuration Manager client. When you uninstall, the devices aren't receiving your policies, including policies that provide protection. They're vulnerable until they enroll in Intune and start receiving your new policies.
2. Enroll the devices in Intune to receive policies.

To help minimize vulnerabilities, move macOS devices after Intune is set up, and when your enrollment policies are ready to be deployed.

## Option 4 - Start from scratch with Microsoft 365 and Intune

This option applies to Windows client devices. If you use Windows Server, such as Windows Server 2022, then don't use this option. Use Configuration Manager.

To manage your Windows client devices:

1. [Deploy Microsoft 365](#), including creating users and groups. Don't use or configure Microsoft 365 Basic Mobility and Security.

Helpful links:

- [Microsoft 365 Enterprise deployment guide](#)
- Set up [Microsoft 365 Business](#)

2. [Set up Intune](#), including setting the MDM Authority to Intune.
3. Uninstall the Configuration Manager client on existing devices. For more information, see [uninstall the client](#).

Devices are ready to be enrolled in Intune, and receive your policies.

## Currently use on-premises group policy

In the cloud, MDM providers, like Intune, manage settings and features on devices. Group policy objects (GPO) aren't used.

When you manage devices, Intune device configuration profiles replace on-premises GPO. Device configuration profiles use settings exposed by Apple, Google, and Microsoft.

Specifically:

- On Android devices, these profiles use the Android [Management API](#) and [EMM API](#).
- On Apple devices, these profiles use the [Device management payloads](#).
- On Windows devices, these profiles use the [Windows configuration service providers \(CSPs\)](#).

When moving devices from group policy, use [Group policy analytics](#). Group Policy analytics is a tool and feature in Intune that analyzes your GPOs. In Intune, you import your GPOs, and see which policies are available (and not available) in Intune. For the policies that are available in Intune, you can create a settings catalog policy using the settings you imported. For more information on this feature, go to [Create a Settings Catalog policy using your imported GPOs in Microsoft Intune](#).



Next, [Step 1: Set up Microsoft Intune](#).

## Currently use Microsoft 365 Basic Mobility and Security

If you created and deployed Microsoft 365 Basic Mobility and Security policies, then you can migrate the users, groups, and policies to Microsoft Intune.

For more information, go to [Migrate from Microsoft 365 Basic Mobility and Security to Intune](#).

## Tenant to tenant migration

A tenant is your organization in Microsoft Entra ID, like Contoso. It includes a dedicated Microsoft Entra service instance that Contoso receives when it gets a Microsoft cloud service, like Microsoft Intune or Microsoft 365. Microsoft Entra ID is used by Intune and Microsoft 365 to identify users and devices, control access to the policies you create, and more.

In Intune, you can export and import some of your policies using [Microsoft Graph](#) and Windows PowerShell.

For example, you create a Microsoft Intune trial subscription. In this subscription trial tenant, you have policies that configure apps and features, check compliance, and more. You'd like to move these policies to another tenant.

This section shows how to use the Microsoft Graph scripts for a tenant to tenant migration. It also lists some policy types that can or can't be exported.





- These steps use the [Intune beta Graph samples](#) on GitHub. The sample scripts make changes to your tenant. They're available as-is, and should be validated using a non-production or "test" tenant account. Be sure the scripts meet your organization security guidelines.
- The scripts don't export and import every policy, such as certificate profiles. Expect to do more tasks than what's available in these scripts. You will have to recreate some policies.
- Users must unenroll the device from the old tenant, and then re-enroll in the new tenant.

## Download the samples, and run the script

This section includes an overview of the steps. Use these steps as guidance, and know that your specific steps might be different.

1. Download the samples, and use Windows PowerShell to export your policies:
  - a. Go to [microsoftgraph/powershell-intune-samples](#) , select **Code** > **Download ZIP**. Extract the contents of the .zip file.
  - b. Open the Windows PowerShell app as administrator, and change the directory to your folder. For example, enter the following command:

```
cd C:\psscripts\powershell-intune-samples-master
```

- c. Install the AzureAD PowerShell module:

```
Install-Module AzureAD
```

Select **Y** to install the module from an untrusted repository. The install can take a few minutes.

- d. Change the directory to the folder with the script you want to run. For example, change the directory to the CompliancePolicy folder:

```
cd C:\psscripts\powershell-intune-samples-master\powershell-intune-samples-master\CompliancePolicy
```

- e. Run the export script. For example, enter the following command:

```
.\CompliancePolicy_Export.ps1
```

Sign in with your account. When prompted, enter the path to put the policies. For example, enter:

```
C:\psscripts\ExportedIntunePolicies\CompliancePolicies
```

In your folder, the policies are exported.

2. Import your policies in your new tenant:



- a. Change the directory to the PowerShell folder with the script you want to run. For example, change the directory to the CompliancePolicy folder:

```
cd C:\psscripts\powershell-intune-samples-master\powershell-intune-samples-master\CompliancePolicy
```

- b. Run the import script. For example, enter the following command:

```
.\CompliancePolicy_Import_FromJSON.ps1
```


Sign in with your account. When prompted, enter the path to the policy .json file you want to import. For example, enter:

```
C:\psscripts\ExportedIntunePolicies\CompliancePolicies\PolicyName.json
```

3. Sign in to the [Intune admin center](#) . The policies you imported are shown.

# What you can't do

There are some policy types that can't be exported. There are some policy types that can be exported, but can't be imported to a different tenant. Use the following list as a guide. Know there are other policy types that aren't listed.

 Expand table

Policy or profile type	Information
Applications	
Android line-of-business apps	<div><div>✗ Export</div><div>✗ Import</div></div>

Policy or profile type	Information
	To add your LOB app to a new tenant, you also need the original .apk application source files.
Apple – Volume Purchase Program (VPP)	<p>❌ Export ❌ Import</p> <p>These apps are synced with the Apple VPP. In the new tenant, you add your VPP token, which shows your available apps.</p>
iOS/iPadOS line-of-business apps	<p>❌ Export ❌ Import</p> <p>To add your LOB app to a new tenant, you also need the original .ipa application source files.</p>
Managed Google Play	<p>❌ Export ❌ Import</p> <p>These apps and weblinks are synced with Managed Google Play. In the new tenant, you add your Managed Google Play account, which shows your available apps.</p>
Microsoft Store for Business	<p>❌ Export ❌ Import</p> <p>These apps are synced with the Microsoft Store for Business. In the new tenant, you add your Microsoft Store for Business account, which shows your available apps.</p>
Windows app (Win32)	<p>❌ Export ❌ Import</p> <p>To add your LOB app to a new tenant, you also need the original .intunewin application source files.</p>
<b>Compliance policies</b>	
Actions for Non-Compliance	<p>❌ Export ❌ Import</p> <p>It's possible there could be a link to an e-mail template. When you import a policy that has non-compliance actions, the default actions for non-compliance are added instead.</p>
Assignments	<p>✅ Export ❌ Import</p>

Policy or profile type	Information
Assignments are targeted to a group ID. In a new tenant, the group ID is different.	
<b>Configuration profiles</b>	
Email	<p>✅ Export</p> <p>✅ If an email profile doesn't use certificates, then the import should work.  ❌ If an email profile uses a root certificate, then the profile can't be imported to a new tenant. The root certificate ID is different in a new tenant.</p>
SCEP certificate	<p>✅ Export</p> <p>❌ Import</p> <p>SCEP certificate profiles use a root certificate. The root certificate ID is different in a new tenant.</p>
VPN	<p>✅ Export</p> <p>✅ If a VPN profile doesn't use certificates, then the import should work.  ❌ If a VPN profile uses a root certificate, then the profile can't be imported to a new tenant. The root certificate ID is different in a new tenant.</p>
Wi-Fi	<p>✅ Export</p> <p>✅ If a Wi-Fi profile doesn't use certificates, then the import should work.  ❌ If a Wi-Fi profile uses a root certificate, then the profile can't be imported to a new tenant. The root certificate ID is different in a new tenant.</p>
Assignments	<p>✅ Export</p> <p>❌ Import</p> <p>Assignments are targeted to a group ID. In a new tenant, the group ID is different.</p>
<b>Endpoint Security</b>	
Endpoint detection and response	<p>❌ Export</p> <p>❌ Import</p> <p>This policy is linked to Microsoft Defender for Endpoint. In the new tenant, you configure Microsoft Defender for Endpoint, which automatically includes the <b>Endpoint detection and response</b> policy.</p>

## Related articles

- [Get started with Intune](#)
- [Enrollment deployment guides](#)

