Getting Started with Intune Migrations

Microsoft Intune Migration Guide - Microsoft Corporation
Published: October 2023
Version: v1.1

Authors: Dionisio Rocha, Bilal Baydoun, Ricardo Siqueira, Greg Nottage, Aaron Hamilton, Courtenay Bernier, Jamin Almond
Contributors: Jason Roszak

Abstract

This document provides general guidance and information on Microsoft Intune, and recommended processes for migration from 3rd party management solutions to Intune. This guide can help determine the scope, scale, and effort that will be required to migrate between platforms.

Contents

Intune Migration Guide Overview

This guide is designed to help customers who are planning to migrate to Microsoft Intune from existing management solutions or want to migrate to a more cloud native management approach. It will provide high level information on architectural differences that customers need to consider when migrating, and the framework and processes that Microsoft has developed through thousands of migrations with enterprise customers.

Project Managers, Architects, Administrators will find the guide helpful in understanding the major architectural differences between Intune device management and other solutions, and what areas might create a need to change their current processes and procedures. Additionally, the guide provides a list of the major stages of migration planning along with recommended steps to execute in each phase.

Customers should review the guide, evaluate their current environment, and then evaluate if they have sufficient resources and expertise to run a migration project. In many cases customers engage partners or Microsoft Services for assistance to help increase the speed at which they can migrate. A simple one-pager document is available for you to download here to help you understand all required steps and activities in this type of migration projects.

To simplify the learning and adoption curve we also have a list of common terms used in the guide and documentation with a brief explanation and comparable terminology used in other solutions here.

Before you get started: Intune App Protection Policies

Before you start planning your MDM migration you should familiarize yourself with Intune Application Protection Policies (APP). APP can ensure that your data remains safe and protected within your Intune enabled 1st party applications like

Outlook Mobile, Microsoft Office, Microsoft Teams, and Intune SDK enabled Line of Business apps regardless of the management state and platform. App Protection Policies can easily coexist with your existing management system, and even offer protection to apps on devices you're not managing.

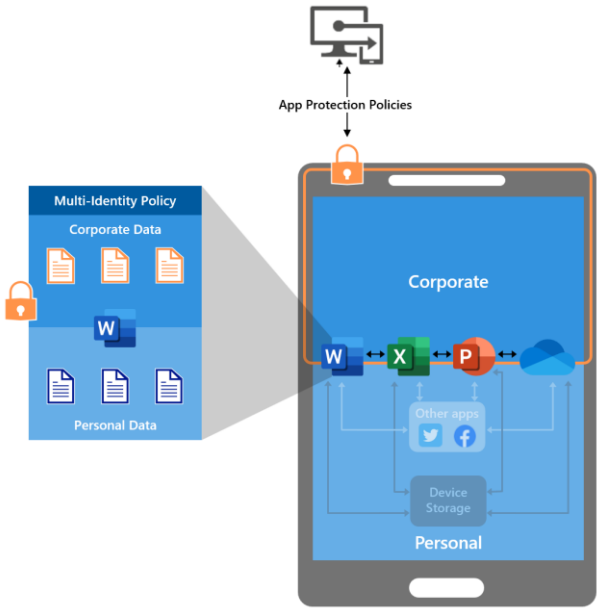
App Protection Policies can be deployed to existing devices and application deployments with little to no interruption to your users, and dramatically reduce the risk of data leaks and use of your data on compromised devices. With or without management you can ensure that users devices are not jailbroken or rooted, that your data is encrypted, and that the user must provide a PIN or biometric to access the app and corporate data.

Many customers have decided to add this additional protection to their existing deployment, and then continue with their long-term migration planning. Very often customers also decide that APP is sufficient for their BYO users who don't need fully managed devices but still want to protect their apps and data. This can both immediately increase your security posture and decrease the complexity of your migration by simplifying your deployment for your BYO devices.

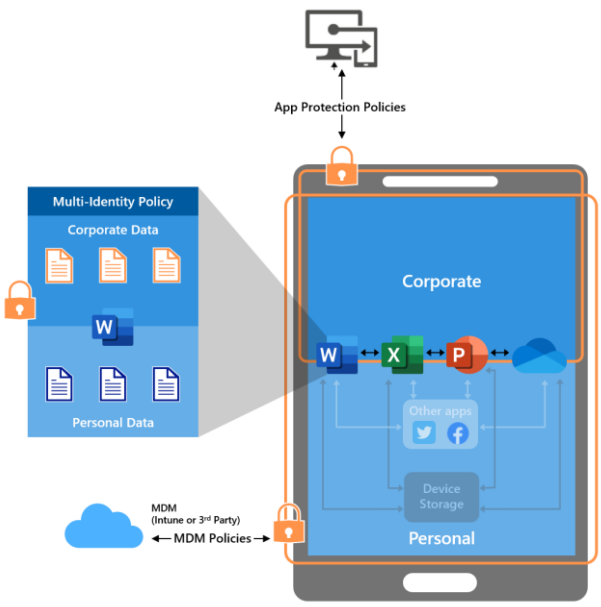
How App Protection Policies Work

As a user logs into APP enabled applications Intune automatically delivers policy targeted to users and then applies the settings specific by the administrator. Most often policies include securing access through Biometric/PIN, encrypting data, and check to see that the device is secure. User's personal data is also separated from their corporate data.

App Protection only



App Protection with MDM (Intune or 3rd Party)



Because of its architecture, APP can be deployed easily in either scenario. As a new user logs into the app, they'll automatically receive policy before they use the application, and your existing users will also start receiving policy as they open and use protected apps.

Finally, the applications can still be securely wiped, and corporate data removed using the same types of processes in you use today. Admins can trigger the wipe from the console, or it could be triggered automatically when a user's account is disabled. In both scenarios the user's personal data will remain intact when the wipe occurs.

Introduction to the Microsoft Intune Service

Microsoft Intune is a cloud-based endpoint management solution. It provides a unified experience for managing your endpoints, applications, and user access to corporate resources. Intune can support the full spectrum of scenarios starting with your unmanaged BYO devices with managed applications, to your corporate owned devices with fully managed applications and device settings.

Intune supports direct management of Windows, iOS/iPadOS, macOS, Android Enterprise, Android Open-Source Project (AOSP), and Linux devices. Additionally basic capabilities for Chrome OS (Inventory, Restart, Lost Mode, Wipe, and Deprovision) can be achieved through configuration of the Chrome Enterprise connector.

Intune is a cloud-based Software as a Service (SaaS) solution that runs on Microsoft Azure. While there are some connectors and optional components you may deploy on-premises (certificate connectors, VPN servers) the Intune service itself exists entirely in the cloud as a multitenancy service.

Microsoft updates the Intune service on a monthly release cycle and customers are notified as updates are deployed and what new features are included in each update: What's new in Microsoft Intune | Microsoft Learn Customers cannot defer or otherwise control the update processes.

Intune does not offer offline or on-premises management offerings. All applications and devices that are managed by Intune require access to cloud based endpoints for enrollment and ongoing management. If you have Microsoft Configuration Manager deployed, you can integrate Configuration with Intune via co-management as a strategy to start your migration to cloud based management. Co-management allows to leverage your existing deployment of Configuration Manager and then migrate workloads to Intune when you're ready: Co-management for Windows devices - Configuration Manager | Microsoft Learn

Intune vs traditional device management

In addition to Intune being a cloud-based service Intune has other differences from traditional device management solutions that administrators should be aware of when planning a migration.

Cloud based user and device identities.

Intune relies on Azure Active Directory (Entra ID or AAD) for its identity management and most of its grouping and targeting abilities. This means that all your users and devices will need to exist in Entra ID to be managed by Intune. Users who exist in your on-premises Active Directory will need to have their identities synchronized to the cloud so that they can enroll devices, be targeted by policies, and access resources that are protected by Microsoft 365. If you have users or devices that typically run in an offline or otherwise disconnected state, you will need to plan alternate solutions for their management: Entra ID Connect sync: Understand and customize synchronization - Microsoft Entra | Microsoft Learn

Grouping and Targeting

Many traditional device management solutions have their own grouping and targeting mechanisms for targeting policies to users and devices. Intune relies on Entra ID (AAD) to provide mechanisms for grouping users and devices. To target a user, a device, or a group of users/devices they need to exist in AAD. AAD supports static and dynamic groups for users and devices. Static groups require an administrator to directly assign members to the group, and dynamic groups allow an administrator to specify rules that will determine what objects exist in the group. For a detailed overview of AAD groups review the following article: Learn about groups and group membership - Microsoft Entra | Microsoft Learn

In addition to basic grouping and targeting provided by AAD Intune also supports filtering rules. Filters allow administrators to further refine their targeting by allowing administrators to include or exclude devices based on additional attributes. For example, an administrator could target a VPN policy to all their iOS devices or users, then use a filter to ensure that the policy is further restricted to only corporate devices. Filters support a wide variety of attributes that can be used in conjunction with AAD groups. For a detailed overview of filters review the following article: Create filters in Microsoft Intune | Microsoft Learn

Hierarchical targeting structure is currently not supported by Intune or AAD. Administrators should review their current targeting structure and design appropriately.

Conditional Access

Intune is part of the Microsoft 365 stack. It provides device management and can help ensure that your devices are up to date and compliant with your corporate policies. Azure Active Directory (AAD) and Intune work together to limit access to your corporate resources using Conditional Access policies. Conditional Access policies allow Administrators to build rules to ensure users accessing corporate resources meet access criteria set by the administrator. These criteria can include controls like Multi-Factor Authentication (MFA), that a device is enrolled and compliant, or that user is using approved apps to access services. Most often administrators rely on Intune to provide signals to confirm a device is enrolled and fully compliant with corporate policies. For a detailed overview of Conditional access review the following article: What is Conditional Access in Azure Active Directory? - Microsoft Entra | Microsoft Learn

On-Premises Resource Access

Intune can provide on-premises resources access through integration with existing VPN solutions or through Microsoft Tunnel Gateway. To support 3rd party VPN solutions, you will need to enroll your devices and deploy configuration profiles and in some cases client apps. For a detailed overview of supported 3rd party VPN solutions and configuration review the following article: Add VPN settings to devices in Microsoft Intune | Microsoft Learn

Intune includes Microsoft Tunnel Gateway (MTG) which provides a standalone VPN solution for iOS and Android devices. MTG is a container-based solution that runs on a Linux server. Administrators will deploy MTG on Linux servers either on-premises or in the cloud, then deploy the Tunnel client and VPN configuration to Intune managed devices.

MTG integrates with Conditional Access and can automatically limit VPN access to devices based on their compliance state. For a detailed overview of Microsoft Tunnel Gateway review the following article: Learn about the Microsoft Tunnel VPN solution for Microsoft Intune | Microsoft Learn There is also a premium version of Microsoft Tunnel that provides VPN connection to unmanaged devices that is available as part of the Microsoft Intune Suite or Intune P2 offerings. For more information on MTG for Application Management review the following article: Learn about using Microsoft Tunnel with Mobile Application Management | Microsoft Learn

In addition to Microsoft Tunnel Gateway Administrators can evaluate usage of the Azure Active Directory Application Proxy (AAD App Proxy) for publishing their internal web applications. AAD App Proxy provides secure remote access to on-premises web applications. After a single sign-on to Entra ID, users can access both cloud and on-premises applications through an external URL or an internal application portal.

For a detailed overview of AAD App Proxy review the following article: Remote access to on-premises apps - Entra ID Application Proxy - Microsoft Entra | Microsoft Learn

Administrators should consider the following key points when consider MTG and Entra ID App Proxy:

- MTG provides a traditional socket-based VPN which can provide access to any/all applications and resources on-premises. It will require you deploy MTG servers on-premises, and any other applications required for your scenarios.
- AAD App Proxy provides HTTP/HTTPS publishing and only supports web applications. You will deploy Azure App Proxy connectors on-premises, but you will not need to install additional applications. Clients only need a supported web browser to access published resources.

Network Requirements

As a cloud service Intune requires that administrators, users, and devices have access to a variety of cloud endpoints to function. Administrators will need to be able to access the console. Devices will need to be able to access services to support enrollment and management. And finally, end users will need to be able to access the service through the Company Portal app and web to support self service capabilities. Microsoft maintains a full list of the required endpoints and associated services here: Network endpoints for Microsoft Intune | Microsoft Learn

Note that SSL break and inspect is not recommended for performance and reliability reasons, and some endpoints will be unable to function if SSL inspection is enabled due to certificate pinning. This limitation is documented in the above article.

3rd Party Integration with Intune

In addition to core device and application management Intune supports integration with other 3rd party solutions. Administrators should review their current deployment during the assessment phase of a migration and understand where they can take advantage of integration with the following:

- Service Now or other asset management tools
- JAMF integration for compliance and other device compliance partners
- Mobile Threat Defense solutions
- Network Access Control (802.1X authentication/access solutions from HP, Cisco, etc.)
- Certificate deployment (NDES/SCEP integration)
- Zero touch deployment services: Autopilot, Android Zero Touch, Samsung Knox Mobile Enrollment, Apple Business Manager, Apple School Manager
- App deployment services: Managed Google Play, Apple VPP

Graph API Integration

Intune provides access to nearly every action and object in the console via the Microsoft Graph API. You can use the Intune API in Microsoft Graph to manage devices, apps, and even configure Intune while using your preferred tools. This flexibility allows customers to go beyond capabilities currently in console and setup complex integration and automation that ties in your existing environment.

Working with Intune in Microsoft Graph - Microsoft Graph v1.0 | Microsoft Learn

Microsoft 365 Integration

One of the largest benefits of the Microsoft 365 Solution is the out of box integration between the service offerings. Administrators should review their current portfolio and see where they can reduce complexity, decrease cost, and improve security posture. Intune supports easy integration with the following components and benefits:

- Office 365 – Office 365 can be easily deployed and updated using built in applications and update policies.
- Azure Active Directory – Conditional Access can use Intune device enrollment, compliance policies, and application control policies to limit access to secure devices and applications.
- Microsoft Defender – Easily deploy security policies from Microsoft Intune and integrate device compliance, health, and risk signal into and Conditional Access rules. This includes native support for Windows and first party clients for mobile, macOS, Linux, and mobile devices.

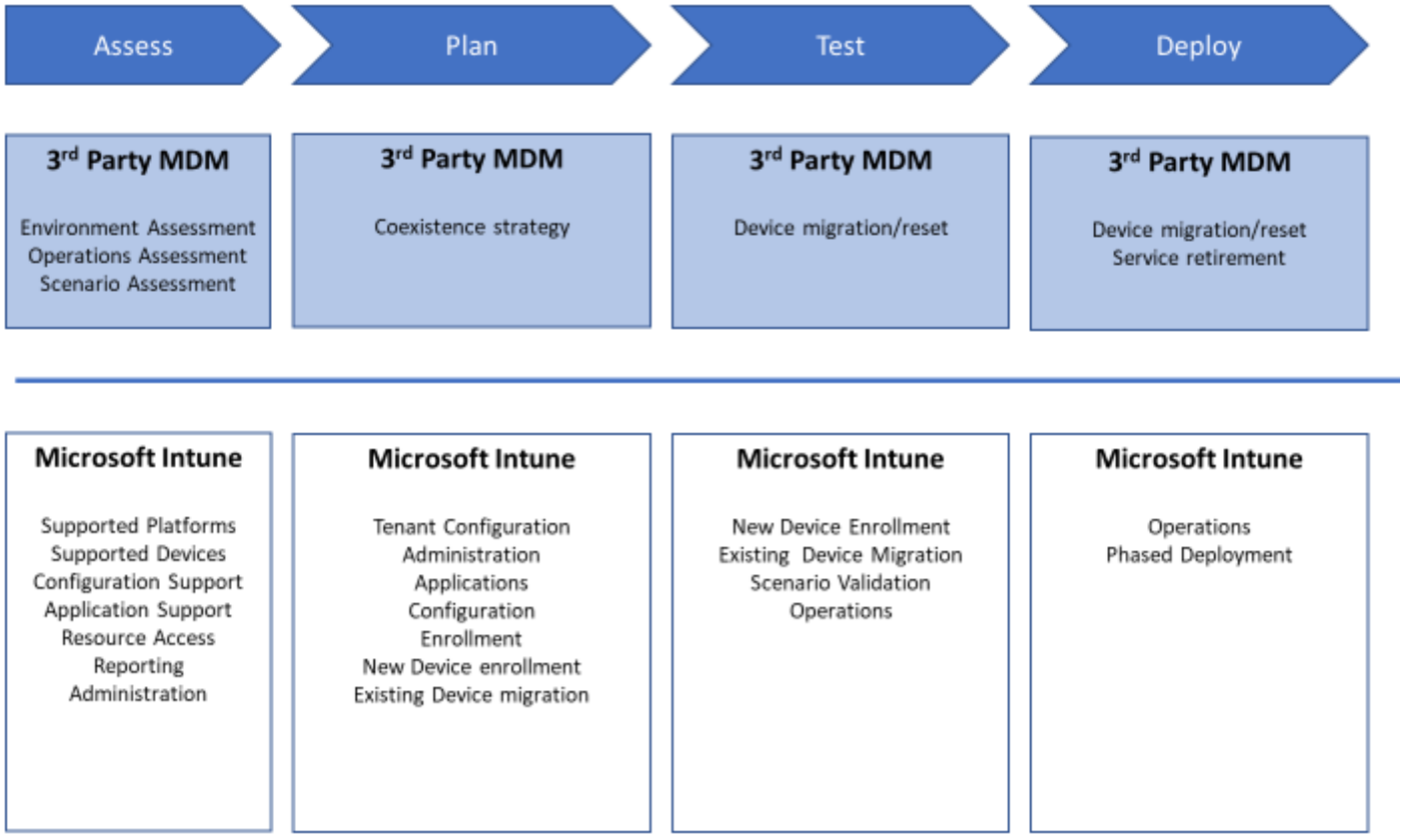
Microsoft Intune App SDK

The Intune App SDK, available for both iOS and Android, enables your app to support Intune app protection policies. When your app has app protection policies applied to it, it can be managed by Intune and is recognized by Intune as a managed app. The SDK strives to minimize the amount of code changes required from the app developer. You'll find that you can enable most of the SDK's features without changing your app's behavior. For enhanced end-user and IT administrator experience, you can utilize the SDK's APIs to customize your app behavior to support features that require your app participation. (Benefits of Intune App SDK - Microsoft Intune | Microsoft Learn)

Where to start

Microsoft recommends that customers simplify their initial deployment and migration to Intune by ensuring the migration planning always starts with assessment and definition of the scenarios and personas the business needs to support. Once the scenarios are defined the administrators should spend time evaluating each one and determine its overall complexity. Microsoft recommends that administrators focus on onboarding the scenarios that have the simplest requirements and the fastest time to value for the business with the least disruption. Do not start with your mission critical devices, your executives, or other areas where minor changes or new experiences has immediate and dramatic impact to the business.

Once you've identified those scenarios you can start thinking through the migration which can be broken down into the following four phases:



Some sample scenarios and high-level configuration steps are outlined below. These samples could be used for a simple POC/Test migration, and the larger guide can provide additional guidance for your production efforts.

Sample Starter Scenarios and high-level requirements:

Scenario 1: Secure access to email and Teams for BYOD mobile devices

In the first scenario the administrator would like to use Intune to provide secure access to Office 365 using the first party productivity applications. They do not intend to fully manage the user's device and simply want to manage Outlook, Teams, and Office. They additionally want to ensure that only secured apps can access Office 365.

Requirements:

- App Protection policies for all Office Applications.
- Limit access to O365 to only approved and protected mobile applications.

Configuration steps

1. Create App Protection Policies for your mobile apps and assign them to approved user groups in your tenant.
2. Create a Conditional Access policy that requires App Protection and assign it to all users.

The steps outlined above will create an experience that provides secure managed apps with access to common productivity services. Your users can install the apps from the public store and when they login with their corporate credentials. Any users not approved and included in your targeting groups won't receive the policies and will be unable to access the services, and any existing users (MDM managed or unmanaged) will automatically receive the policies.

Scenario 2: Mobile Sales Staff PCs

In the second scenario the administrator would like to use Intune to deploy new PCs to the remote sales force. The sales force primarily uses office and a few SaaS applications. The security team requires that the devices be encrypted, have antivirus enabled, and stay up to date with the latest Windows updates within two weeks of release.

Requirements:

- Autopilot enrolled devices
- Entra ID joined
- Office 365 apps
- Basic device configuration including disk encryption, and configuration for Microsoft Defender
- Windows Update For Business

Configuration steps

1. Register the devices with the Auto Pilot Service and create profile
2. Deploy built-in Office 365 Apps to device
3. Build and deploy device configuration policies
4. Configure Windows Update for Business

Starting with simpler, more focused scenarios like the ones above will allow administrators, support staff, and end users to become familiar with the product in simple scenarios and test operations end to end. As knowledge and operational efficiency increases Administrators can then tackle the more complex workloads at a faster pace and with less disruption to support staff and end users.

High Level Intune Migration Process for 3rd party solutions

If you are planning to migrate or evaluating a move from a non-Microsoft management solution to Microsoft Intune, the outline below provides a high-level overview of the process. Depth guidance for migration including technology changes, assessment, planning, testing, and deployment phases are also included later in the guide.

The most important part of any migration to Intune is the initial assessment of your current deployment. Ensuring that you accurately assess your current deployment allows you to confirm your use cases, requirements, and determine how to best achieve a solid initial deployment with Intune.

The phases of the migration process:

Phase	Description
Assess	In the assessment phase you will review your current deployment and build a list of all your scenarios and their requirements. This is achieved through reviewing device inventory, applications, configuration, and operational requirements. Once you have this list in hand you can then validate it against what Intune can support to identify any potential gaps or changes that you will need to undertake for a successful deployment. Review current existing management solution state: 1. Device Inventory 2. Application Inventory 3. Content Distribution

	4. Configuration Inventory 5. Users and Groups review 6. Report Inventory 7. Integration Inventory 8. Operations Review 9. Review current state of Entra ID and Intune tenant
Design & Plan	In the planning phase you will take your assessment information and begin planning your deployment. This will be focused on the basics of your initial Intune tenant configuration and converting the information from your assessment into concrete requirements, your deployment strategies, and execution plan. 1. Complete initial tenant configuration 2. Per platform scenario design and implementation planning 3. Per platform enablement or restriction 4. Per platform automated enrollment configuration 5. Configuration engineering 6. Migration scenario validation
Test	In the test phase you will implement the outputs of the planning phase in one or more tenants and then complete testing to validate your scenarios and general operations. This will help you develop the processes and procedures to enroll new devices, migrate existing devices, a develop your operational run books – i.e. device lifecycle management. 1. Enrollment validation 2. Migration validation 3. Scenario validation 4. Operations validation 5. Device decommission validation
Deploy	In the deployment phase you will be repeating the processes developed in your test phase, but now in production across active users and devices. Most often customers will choose to deploy individual platforms or scenarios in small production groups and then slowly increase the size of the groups until they are fully migrated. 1. Deploy scenario with initial production validation groups 2. Expand deployment in phases

High Level Intune Migration Process for Configuration Manager

In addition to Mobile device migration many customers are also evaluating migration of the Windows devices as well. This is often Microsoft Configuration Manager (often referred to as SCCM, or CM). Transitioning from CM to Microsoft Intune might sound challenging, especially for larger organizations with intricate infrastructures. But worry not! By following the streamlined steps listed below, this process can be transformed into a manageable, well-organized, and exciting endeavor. Let's explore how we can make this transition smooth and efficient. Ensuring you review and plan your organizations approach to Co-management/Cloud Management Gateway.

The migration process:

Phase	Description
Assess	Evaluate your current CM infrastructure, identify all the applications, policies, and configurations that are currently managed via CM. This is also a good time to identify any legacy applications, policies, configurations or procedures that need to be altered for a cloud first environment. 1. Evaluate the current CM infrastructure 2. Identify all applications, policies, and configurations managed via CM

	3. Identify any legacy applications or procedures that need to be updated for the new environment
Design & Plan	During the planning phase, the data obtained from your evaluation of Configuration Manager will be harnessed to map out the transition to Intune. This stage is devoted to transposing the established structure and functionalities of your CM setup into your Intune implementation. A pivotal aspect of this phase is to determine which workloads will be migrated to Intune, which will be subject to pilot testing within the new environment, and which will remain under the jurisdiction of Configuration Manager. This deliberate approach ensures a balanced, smooth, and efficient migration process, designed to minimize disruption, and optimize integration. 1. Complete initial tenant configuration for Intune 2. Establish platform enablement or restriction 3. Evaluate Co-Management enablement 4. Identify workloads to be migrated to Intune and those to remain with CM 5. Determine whether Collection synchronization is required 6. Design policies, apps, profiles, and compliance/configuration policies for Intune 7. Define the migration plan: a big bang approach or a phased migration 8. Validate workload migration scenarios
Test	Now that your migration plan is established, a comprehensive testing plan is required to validate the migration scenarios and ensure a smooth transition. This plan will highlight key areas of testing to identify and resolve potential issues before they affect your production environment. 1. Set up Intune and connect it with Entra ID 2. Conduct training for the IT team on Intune's functionalities 3. Enable automatic enrollment 4. Configure Intune based on the organization's migration plan 5. Conduct a pilot test with a small set of devices and users 6. If applicable validate that the pilot devices are enrolled in both CM and Intune (co-management) 7. Test the migration of applications and policies to Intune 8. Ensure that migrated policies and applications work as expected on pilot devices
Deploy	The deployment phase in the transition from CM to Intune involves transferring workloads, devices, applications, and policies based on the organizations previous phases. Co-management capabilities are often used during this phase, allowing workloads to be shared between CM and Intune, and facilitating a more balanced, smooth transition. Throughout this phase, constant monitoring is essential to swiftly address any issues that arise, minimizing potential disruptions. Moreover, regular communication with end-users is crucial to keep them informed about progress and changes they might encounter. 1. Migrate workloads from CM to Intune as per the migration plan 2. Continually monitor the migration and address any issues that arise 3. Regularly communicate with users about the migration progress and any changes they might encounter 4. Validate the successful migration of all workloads to Intune 5. Conduct testing to ensure that all devices, applications, and policies are working as expected in Intune 6. Troubleshoot and resolve any issues that occurred during the migration process

	7. Monitor the Intune environment continuously and fine-tune settings to optimize performance
Decommission	1. Validate all workloads are successfully migrated to Intune 2. Ensure you have a proper plan for migrating any relevant data 3. Build a plan for decommissioning/removing the Configuration Manager client 4. Communicate the timeline for decommissioning Configuration Manager 5. Update all internal process related documentation 6. Refer to this link to uninstall Configuration Manager Uninstall sites - Configuration Manager | Microsoft Learn

Assess – Assess and inventory Intune & existing management solution systems

In the assessment phase you will review your current deployment and build a list of all your requirements. It is important to note that this assessment will help with 2 main objectives later during the migration: **migrating the platform** (applications, configurations, delegation model, etc.) and then **migrating the devices**. The assessment is usually done using the following two steps: Reviewing current third-party MDM state and then reviewing current Microsoft Intune & Entra ID state.

Before you begin:

- Confirm that you are aware of all systems in use. Some environments have multiple instances of the same solution or have different providers for specific platforms.
- Ensure that you or another person has direct access to the environment, full permission to view all objects. Assessing your current systems requires that you have full access to the existing environment and a full understanding of the scenarios it supports.

Reviewing current third-party MDM state

a. **Device inventory**: It is necessary to have clear list of devices that you need to migrate including information about Operating systems version, management mode, ownership (personal, corporate, shared), integration in Zero touch solutions (like Apple Business Manager, Android Zero Touch, Samsung Know Mobile Enrollment, Windows Autopilot), assigned user, last contact date. Each information you collect about your devices will help you define a more precise target and migration strategy. For example:

   i. **Operating System version** will help you know if the device is compatible with OS minimum requirements. If not, you can choose to either update that device (if possible) or replace it with a newer device.
   ii. **Management mode** will help you understand how that device will need to be migrated. Some Management modes need a full device reset and some others need only to unenroll and enroll in Intune.
   iii. **MAM vs MDM –** Depending on your use cases/scenarios some devices might not need management and only need to have protected apps through App Protection Policies. This can greatly simplify your deployment.
   iv. **Zero Touch solutions** will require you to move devices from your current MDM to Microsoft Intune in each portal. Those solutions are highly recommended to simplify the migration process.
   v. **Ownership** will help you with communication strategy as you will probably not manage and communicate the same way the migration for personal, corporate, and shared devices.
   vi. **Assigned user** will need to have all requirements to enroll his device in Intune like an Entra ID account, an Intune license, group memberships, assignments, etc.
   vii. **Last contact date** can help you decide if the device needs to be migrated, wiped, or have a special care for migration.

b. **Applications**: you will need to have a list of all your public, private and web applications for all platforms you need to migrate. It is crucial that you have all the following information to have a smooth migration for your applications:
    i. For private applications only: source files of your application (examples: APK, IPA, EXE, DMG, PKG, MSI files), application icon if required.
    ii. For private Android Enterprise applications only: note if the app is deployed using the MDM directly, the Google Play dev console or using the Managed google Play integrated in your current MDM.
    iii. For web applications only: URL to your application
    iv. For all applications: Name of the application, application assignments (dynamic and static groups), version of the application, application category, applications blacklist or whitelist, etc.
    v. *Important note: Intune does not support direct distribution of APK files. Managed Google Play must be used*

c. **Content distribution**: if you are using content distribution for files, eBooks or others you will need to reference all those types of content to be distributed to your devices.

d. **Configurations**: you will need to review all configuration and compliance profiles that are assigned in your current MDM. Depending on your organization complexity and MDM administration history, you may want to consider either starting over with a clean configuration baseline, or else migrate relevant profiles. You may also need to consider with regulatory compliance requirements which will be needed during the Design & Plan phase. In either case, it is important to list all current profiles including the following information:
    i. Name of the profile
    ii. Platform and Assignment groups
    iii. Type of profile: restrictions, Wi-Fi profile, VPN profile, certificate profile, etc.
    iv. If you feel it is necessary, reference every parameter in each profile that you want to migrate to Intune.

e. **Groups and users**: depending on your current solution you may be using a 3rd party directory or the third-party MDM's integrated directory for managing your groups and users. As it is a requirement to use Entra ID as the directory for Intune, you can either choose to federate your current directory with Entra ID or else migrate your current groups and users to Entra ID. In case you need to migrate, you will need the following information:
    i. **List of all users:** in most cases, every user needs to have an Entra ID account and an Intune license. Some devices like shared kiosks and shared devices may not require user accounts.
    ii. **List of all MDM administrators:** like for users, your administrators will need to have the proper requirements like an Entra ID account to administer Microsoft Intune and Entra ID
    iii. **List of all users with privileges on the device**: for those users, you may consider using Windows LAPS solution or a solution like Endpoint Privilege Management
    iv. **List of all groups and group members:** you need to have a list of all groups with the following information:
        1. **Group name**
        2. **Group type: dynamic or static, user or devices**
            a. If dynamic: criteria that will be used for group inclusion
            b. If static: list of devices or users

f. **Reporting**: your current MDM solution may offer some reporting capabilities that you want to replicate in Intune. As such, you will need to reference the following:
    i. Report name
    ii. Report owner
    iii. Access control
    iv. Report description
    v. Report headers and type of information required
    vi. Report data update frequency

g. **Integration with other systems**: your current MDM solution may be integrated with other solutions. If you still need those integrations, it is important to understand how to transition them to Microsoft Intune and gather all prerequisites (for example: service accounts, Entra ID application, etc.)
    i. Service Now or other asset management tools
    ii. Jamf integration for compliance and other device compliance partners
    iii. Mobile Threat Defense solutions
    iv. 802.1X authentication/access solutions (HP, Cisco, etc.)
    v. Certificate deployment (NDES/SCEP integration)
    vi. Zero touch deployment services: Autopilot, Android Zero Touch, Samsung Knox Mobile Enrollment, Apple Business Manager, Apple School Manager
    vii. App deployment services: Managed Google Play, Apple VPP
    viii. VPN solution
    ix. Remote control solution

h. **Operational requirements**: migrating to Intune may require some changes in your processes and organization. It is critical to correctly assess your current processes and organization as this will serve to identify gaps and impacts during the design phase.

    i. **Delegation model**: identifying very clearly roles, responsibilities and scopes is one of the most underestimated and less understood topics for a migration project. Take the time to identify your current delegation model and if things need to be changed in the new MDM.
    ii. Enrollment process: depending on your current MDM solution and practices, you may have enrollment processes that need to be changed. You need to gather all documentation explaining every type of enrollment available at your organization. This will be needed to identify gaps and impacts with Microsoft Intune
    iii. **Change control:** How to manage change (approvals etc.), app supersedence, targeting concepts (include/exclude groups), ensure no policy overlaps (no 'order of precedence'), daily/weekly/monthly/quarterly/etc. regular tasks – stale device cleanup etc., possible multi-tenant strategy (TEST > DEV > PROD ??)

Reviewing current Microsoft Intune & Entra ID state

As you will migrate to Microsoft Intune, it is important to assess how your platform is already configured. If your Intune & Entra ID instances have been set up recently and not touched before the migration process, you will need to implement some basic Intune and Entra ID features during the project. If not, it is important to understand how Intune and Entra ID are currently used. For example, you may already have Windows devices managed by Intune and you want to migrate your mobile devices from a third-party MDM to Intune. In that case, you need to be extra careful not to impact existing implementation and devices in production. Here are some of the things to look out for in your Microsoft Intune environment:

a. Entra ID accounts
b. Terms and conditions
c. Apple Push certificate configuration
d. Apple Business Manager integration and Apple VPP
e. Managed Google Play integration
f. Company portal customizations
g. Enrollment restrictions
h. All policies: configuration, compliance, conditional access
i. Licensing
j. Conditional access policies

Once you have completed all the assessments, you can then validate your current MDM configurations against what Intune can support to identify any potential gaps or changes that you will need to undertake for a successful deployment. For each item covered in section 1 – Reviewing current third-party MDM state, verify first what you need to migrate and if it is covered by Intune. Once you have that matrix, you can move to the Design & Plan phase.

Design & Plan – Intune design and implementation planning

In the design and plan phase you will begin mapping out your implementation and migration to Intune. This includes taking the outputs of your assessment and aligning them to your business scenarios, defining your migration strategy, identifying infrastructure requirements, and building a plan.

Before you begin:

- Confirm that you've completed the assessment phase and have all your requirements documented.
- Ensure that you or another person has direct access to the environment, full permission to view all objects. Assessing your current systems requires that you have full access to the existing environment and a full understanding of the scenarios it supports.

Based on the outputs of your assessment phase you can start planning your implementation and migration to Intune. If you have a new Intune instance you should review the general setup documentation for Intune here: [Set up Intune - Microsoft Intune | Microsoft Learn]

The most common items that administrators need to configure are:

- Customization/Branding – Tenant wide customization for colors, logos, contact information
- Enrollment customization – Customizing the enrollment experiences, prompts, and platforms
- Assigning licenses – Users need licenses assigned to enroll devices

When you have confirmed your basic tenant configuration is complete the Design & Plan phase can now begin. This part is usually split per platform (for example: mobile devices, Windows) as this may require people with different skills. It is important still to have a core team that will manage the design of common features like RBAC, certificate deployments, 3rd party integrations, etc.

As you will begin working on a platform, you need to distinguish two use-cases:

- Onboarding new or unmanaged devices to Intune
- Migrating existing devices from a existing management solution to Intune

This distinction is important for planning purposes, since existing devices migrating from an existing management system to Intune can be understood as going through two phases, first leaving the current management system, and then onboarding into Intune. While the former depends on the nature of the existing solution, the latter follows the same process as a new device use case. By separating both use cases, you can speed up testing and validating your Intune configuration.

As you enter the Design & Plan stage of the migration, it is important to determine which platforms will be migrating to Intune. Each platform has different target management modes, enrollment prerequisites and strategies etc., and as such the Design & Plan phase is best done *per platform*.

Another important concept of a successful migration plan is the *flip the switch* moment. This is the day from which all new and recently reset (with or without automatic enrollment) devices will be enrolled by default to your new Intune tenant. Only the first use case is needed for this date to be set, and it will reduce the number of devices yet to be migrated.

When you start using your new Intune and Entra ID infrastructure, you will need to define a coexistence plan. Since your migration project will probably a few weeks or months depending on the volume, devices managed by the existing management system and Intune devices need both to access your services and be properly managed and secured. This will have an impact on your design plan and on the workload of some of your teams (device management teams, helpdesk, etc.).

Design and implement Use Case A: new or unmanaged devices

Onboarding strategy

When designing an onboarding strategy, the most important information to consider is the Target Management Mode. Different platforms allow for different Management Modes, and each one has a different associated Enrollment Method. Currently, Intune is currently able to cover the following device platforms:

- Android: corporate and user owned
- Apple: corporate and user owned
- Windows: corporate and user owned
- Linux: user owned

In broad strokes, each device platform can be managed in multiple ways:

- Corporate-owned devices without personal usage
- Corporate-owned devices allowing for personal usage
- Corporate-owned kiosk or userless devices
- Personally-owned devices (including MAM)

Additionally, corporate-owned devices can each be set up for automated enrollment, which we recommend. This includes mainly Android Zero Touch, Samsung KME, Apple Business/School Manager and Windows Autopilot, but other providers might also deliver this feature.

Thus, to determine the overall onboarding strategy, a list of target management modes per device platform must be decided before the rest of the design steps. Communication and support strategy will be closely derived from the choices made concerning the management mode and enrollment methods:

- Does the user need any type of information (QR code, authentication details, etc) to start enrollment or is it automated?
- Are personal devices enabled and, if so, what are the platforms and versions allowed to be enrolled?
- Is the support material ready for when the end user contacts support and how can they distinguish between the different possibilities?

These and further questions must be defined during this phase, for each device platform, management mode and enrollment method.

At the end of this step, a table of use cases to be covered can be drawn, per platform. Below is an **example** of this output:

Platform	Target Management Mode	Enrollment Method
Android	Corporate-owned without personal usage	Automated enrollment
Android	Personally-owned (MAM)	No enrollment needed
Apple	Corporate-owned allowing for personal usage	User-initiated enrollment
Apple	Personally-owned (MAM)	No enrollment needed
Windows	HAAD-joined + Intune	Automated enrollment

Onboarding engineering

Setting up the multiple onboarding engineering requirements, per platform, is best done by going through the table generated in the last step. Doing so will provide line-by-line guidance for the prerequisites that need to be enabled and configured for each platform. The objective for each line should be to have an enrolled device, without further configuration, within the limitations of the use case itself.

Each integration will be different based on use case goals, but the high-level steps can be listed as follows:

1. Configure *Device Platform Restrictions*, allowing the target platform to be enrolled, as well as allowing *Personally owned* devices to enroll to Intune if applicable. You can choose to target specific user groups in this step, in order to restrict testing/deployment to a limited amount of users
2. Integrate or configure *automated enrollment providers* (Android Zero Touch, Samsung KME, Apple Business/School Manager, Windows Autopilot, …) if this is part of the use case. At this step, implement the prerequisites for each specific provider:
    a. **Apple devices**
        i. Upload an Apple MDM Push Certificate to Intune
        ii. Add Intune as an MDM server to Apple Business/School Manager and get an Apple enrollment program token (iOS/iPadOS or macOS)
        iii. Upload the MDM server token obtained and create an Apple Enrollment Profile
        iv. Assign the profile to your devices
        v. If you are using VPP in the ADE portal create a new VPP token for your Intune instance and purchase or transfer licenses, then upload the token to Intune.
    b. **Android devices**
        i. Connect Intune to your Managed Google Play account. If the account is already used for your current existing management solution provider, creating a new account will be needed in order to link Intune
        ii. Prepare and assign a new *Zero-Touch Enrollment* profile in Samsung KME or Android Zero-Touch, targeting your Intune environment, depending on the chosen use cases
    c. **Windows devices**
        i. Manually register your devices to Autopilot by uploading the device hashes (locally generated) to Intune or integrating your vendor to your tenant's Autopilot
        ii. Create an Entra ID group and either manually or dynamically include your Autopilot devices on it
        iii. Create an Autopilot profile and deploy it to the Entra ID group containing your target devices
        iv. (Optional) Create an Enrollment Status Page (ESP) profile and assign it to the target users
    d. **Linux devices**
        i. No prerequisites need to be setup in your tenant to enroll Linux devices
3. Configure *user-initiated enrollment* where applicable, generating the required information (e.g. QR codes) to distribute to end users
4. Test each use case individually, taking notes of the enrollment process for support and communication requirements, as well as adjusting enrollment configuration as needed

By the end of this step, you should have a few enrolled devices (either automatically or manually enrolled) corresponding to every use case listed by the end of the *Onboarding Strategy* step. The devices should appear in your Intune *Devices* panel, along with their information.

Configuration engineering

With the validation of the enrollment process for each use case, target configuration must be designed in order to be pushed for each type of device. Depending on the choices made earlier concerning current existing management solution configuration you might have a list of profiles and parameters already in place. If not and you're starting over with a clean configuration baseline, please take note of regulatory compliance and internal security requirements before starting this phase of the migration.

Microsoft provides security configuration guidance for a variety of use-cases. If you're starting from scratch, it's a good starting point before adding company-specific configurations.

Broadly, device configuration can be split between two types:

1. Device-targeted configuration: targeted using *Filters*, this type of configuration is typically used to cover security and baseline settings for entire device platforms, with some distinction based on use cases (corporate vs personal, user vs user-less devices)
2. User-targeted configuration: targeted using *Entra ID groups*, this type of configuration depends on which user is connected to the device, and usually targets specific needs for a subset of users

In general, we recommend adopting a multi-tiered design for your configuration engineering:

1. Baseline configuration: including security configuration, this baseline is applied to all device platforms, with platform-specific and use-case specific settings being determined through the use of filters. This allows for all managed devices to have a common set of policies that are consistent across platforms, for all users. These settings will seldom change over the life of a device.
2. Use-case specific configurations: configurations that fall out of scope of the baseline settings, such as restrictions or additional settings for use-case specific devices will be configured separately, equally through the usage of filters, allowing for more flexibility over the lifecycle of a device (e.g. different set of applications for a Dedicated Android device).
3. User specific configurations: this last tier contains settings that depend on the user connected to the device (which department, which role, etc) and will tailor it to their specific usage. This targets the user rather than the device and gives the most flexibility for changes in implementation.

Over the creation of every profile, we recommend adding them to each use case defined in the previous step. Once all the targeted use cases have been given targeted configuration profiles, line-by-line testing should be done to validate each profile – and thus validating the whole use case.

Design and implement Use Case B: device migration

Migration strategy

Once the first use case has been designed and planned, we can address the device migration strategy. While not mandatory, this process allows for target enrollment and management definition before addressing the migration itself, which significantly saves time in most cases.

Source and target management mode

The basis of the migration strategy is a complete list of source and target device management modes. Using the table defined during the *Onboarding Strategy* step of the *New and unmanaged devices* use case, you can align the current (or source) management modes with a target mode. This alignment will determine enrollment methods available for each line, as well as user impact such as wiping the devices.

By the end of this step, a new table should have been created, based on source and target enrollment modes. Below is an **example** of this output, based on the table defined earlier:

Platform	Source Management Mode	Target Management Mode	Enrollment Method	Wipe needed?

Android	Device Administrator	Corporate-owned without personal usage	Automated enrollment	Yes
Android	Personally-owned with Work Profile	Personally-owned (MAM)	No enrollment needed	Corporate data only
Apple	Corporate-owned allowing for personal usage	Corporate-owned allowing for personal usage	User-initiated enrollment	Corporate data only
Apple	Non-existent	Personally-owned (MAM)	No enrollment needed	No
Windows	HAAD-joined + existing management solution	HAAD-joined + Intune	Automated enrollment	Yes

This table should be used as the reference for the rest of the design and planning process, with prerequisites and testing phases for each line. The enrollment methods should be configured as required, each platform having their own prerequisites and workflows.

Enrollment methods

The available enrollment methods depend on the target management mode as well as device platform, and each require a different set of prerequisites (or none). We recommend that the table created in the step above be completed with the enrollment methods, giving special attention to the wiping requirements. More information about all available enrollment methods is available here.

Timeline, communication, and support strategy

Creating a clear timeline for the migration process is the cornerstone of a successful migration. Since it will involve multiple teams (engineering, support, change management, leadership sponsors, …), everyone must understand what will happen and when.

We recommend creating a dynamic timeline that covers both the process itself and the expected actions from every stakeholder, validating each step only when every stakeholder is ready to move forward. Below is an list-based example of such a timeline, taking into account a common responsibility split (engineering, support and change management):

- **Design & Plan (Month 1)**
  - Engineering
    - Actions: design and engineering of the solution, across all expected use cases (this document)
    - Validation needed: design is finished and implemented
  - Support
    - Actions: interfaces with the engineering team to understand how Intune works and their role in the console (see RBAC) and, if applicable, what are the impacts of new use cases being designed (e.g. BYOD)
    - Validation needed: None
  - Change management
    - Actions: interfaces with the engineering team to understand how Intune works and what are the probable impacts of the migration, as well as giving feedback concerning user needs and limitations
    - Validation needed: None
- **Technical testing (Month 2)**
  - Engineering

        - Actions: validate and adjust, if needed, each use case. Feedback from support and change management teams is important during this phase in order to minimize user impact during the migration process
        - Validation needed: design is fully tested and validated by all stakeholders
    - Support
        - Actions: ideally part of the technical testing process, the support team will identify roadblocks and user experience inconveniences of each use case to be migrated, giving this feedback to the engineering team. This can also be a good opportunity to prepare user-support documentation for the pilot and the rollout
        - Validation needed: all use cases have been tested by the support team and the documentation reflects each one accurately
    - Change management
        - Actions: ideally part of the technical testing process, the change management team will create the material needed for the pilot and rollout phases during the test phase, as well as give feedback to the engineering team concerning user impact
        - Validation needed: all use cases have been tested by the change management team and the material reflects each one accurately
- **Pilot (Months 3 and 4)**
    - Engineering
        - Actions: if needed, adjust each use case depending on user feedback. Ideally, the whole engineering team is part of the pilot users
        - Validation needed: all use cases have been validated by the pilot users
    - Support
        - Actions: validate the support process for each use case, from start to finish. List the most common causes of failure and ticket creation and share them with the engineering team for adjustments; Ideally, the support team dedicated to the migration is part of the pilot users
        - Validation needed: all use cases and their accompanying support material have been validated
    - Change management
        - Actions: validate the migration material that will be provided to the end user, adjusting its content where needed. Ideally, the change management team is part of the pilot users
        - Validation needed: all use cases and their accompanying material have been validated
- **Rollout (Months 5 and 6)**
    - All teams
        - Actions: create and migrate all end users to Intune, across all use cases. If the pilot has been run on a representative amount of users (across all target use cases), technical and support adjustments should be kept at a minimum, but the teams must be ready to adapt technical implementation if that isn't the case
        - Validation needed: all users have been migrated. Otherwise, see the *Migration enforcement methodology* section

Migration enforcement methodology

While a successful communication and support strategy, accompanied by a robust implementation, help with user adoption, it is the case that most migrations will have a tail end with users unwilling to migrate. Determining in advance the strategy to reduce or ideally eliminate this situation is part of the planning phase.

There are multiple alternatives that help with this issue, and their applicability is different depending on the company. They include:

1. Cut-off dates per migration wave or globally: each wave will include a date where the previous service will be cutoff, either through a remote wipe of the devices or losing access to enterprise data. This can also be applied globally to all non-migrated users. It is very important to communicate clearly about this procedure

2. Rolling refresh or replacement of older devices: if the migration more complex or impossible on older devices (their identification being part of the design phase), they can be addressed by a device refresh rollout with the target MDM already configured (see New Device use case)

3. Identifying inactive users on the previous MDM solution: while most active users will in time migrate, persons who do not active use their devices are likely to ignore the communications. They can be identified on the previous MDM solution and be either remotely wiped or targeted with a specific communication template

It is likely that a combination of these and other strategies will be the best for your company, no single solution being both cost sensitive and able to target 100% of users.

Coexistence strategy

No migration happens in a day, and you will need to manage both environments during the transition between your current management solution and Intune. There are several major areas that you will need to ensure you have plans and processes in place to handle.

Operations

Your teams (helpdesk, administrators, etc.) will need to continue operations on the old management system while the migration is not finished and run the Intune platform. This means you need to have a clear escalation and ticketing process to handle specific situations to the project and regular incidents and requests.

New Device Enrollment

Also, during the transition phase, you need to have a clear strategy on which UEM platform needs to be used for new enrollments. This might be a global strategy or be more granular per entity, per persona, etc.

Resource Access

Most companies require devices to be managed and compliant for access to corporate resources. If you're using any *system* which is checking device compliance or any information coming from the MDM, you need to make sure those systems can handle both Intune-managed devices and 3rd-party-managed devices. The most common systems that need to be reviewed are Conditional Access, Wi-Fi networks, and VPN solutions.

Each of these can vary based on your implementation generally you should consider the following for each.

- Conditional Access: Conditional Access (CA) will block targeted users who cannot meet the compliance requirements of the rules that administrators configure. This is typically either using a known/compliant device or approved and managed apps. To avoid having your existing users and devices blocked you will need to set up the Intune partner compliance integration for your existing solution. This will allow your existing devices to be registered for compliance status and for Conditional Access to allow the users and devices to access resources. Then as you complete your migration you can decommission the connector. For a list of supported compliance partners and the steps to configure please read the following article: Device compliance partners in Microsoft Intune | Microsoft Learn
- Wi-Fi Networks: Frequently Wi-Fi networks require certificates and compliance information before granting users and devices access to the network. You will need to ensure that your existing systems are configured to support the certificates issued by Intune and to use the compliance information stored in Entra ID. Intune provides integration for Network Access Control (NAC) via an API that allows your systems to query a devices compliance status and determine if the device should be granted access. For supported providers and more

information please read the following article: Network access control integration with Microsoft Intune | Microsoft Learn

- VPN Solutions: You will need to test and evaluate the steps required to integrate your existing VPN solution with your new Intune endpoints. Often the VPN solution are supported out of the box and will simply require that you deploy the VPN client, configuration profiles, and optionally certificates depending on your configuration. A full list of supported VPN solutions and the steps to deploy can configure can be found here: Add VPN settings to devices in Microsoft Intune | Microsoft Learn If migrating your devices means that you will be also retiring your existing VPN solution then you will need to evaluate deploy of Microsoft Tunnel Gateway for your mobile devices. Microsoft Tunnel provides a Layer 3 VPN solution for iOS and Android and runs on physical or virtual Linux servers that you provision either on-premises or in the cloud. Tunnel for MDM enrolled devices is included in the base Intune licensing. For additional information please read the following article: Learn about the Microsoft Tunnel VPN solution for Microsoft Intune | Microsoft Learn
  Alternatively if your on-premises resource access requirements are limited strictly to web based applications you can evaluate deployment of the Entra ID Application proxy which can provide secure access and SSO to your internal web applications. For additional information on Entra ID Application proxy please read the following article: Remote access to on-premises apps - Entra ID Application Proxy - Microsoft Entra | Microsoft Learn

Migration engineering

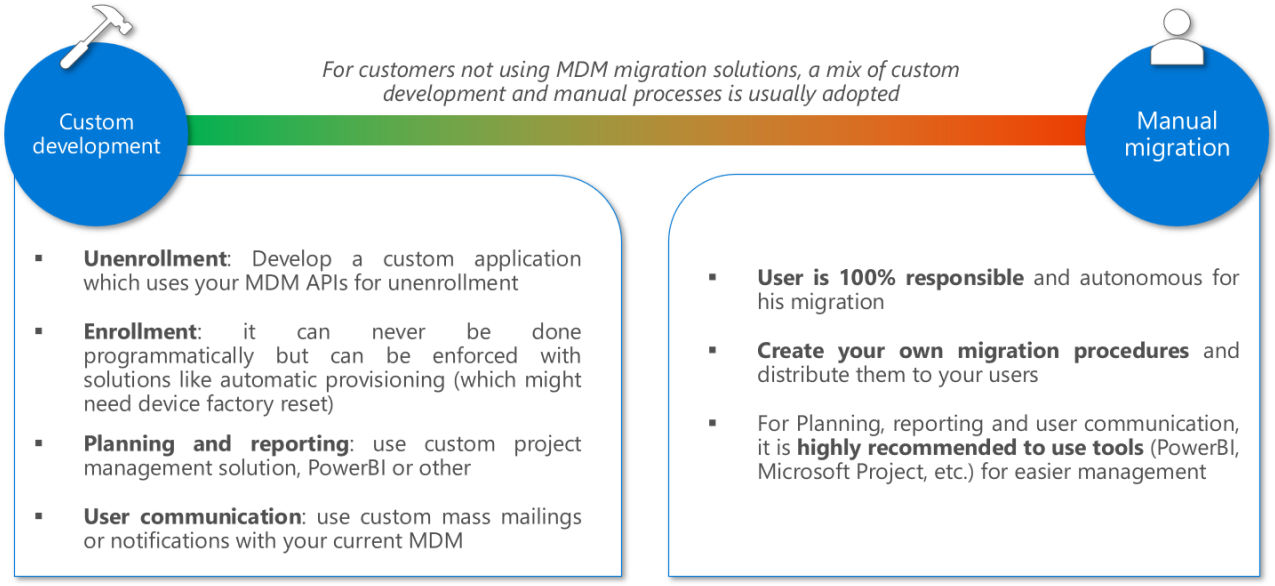
Now that you have defined your migration strategy, you need to define how you are going to execute it. Depending on the platform and management mode, you may be able to automate some steps of the migration.

Automation tools

Migrating from a existing management solution to Intune is a project that has impacts on end users and you should anticipate user change management and communication strategy. Even if some of the tools mentioned below will help automating some tasks, the user will almost always have some actions during the migration process.

When working on automating steps, companies can have different approaches:

1. Do not automate at all – just document all migration steps and let the user or a technician handle the migration
2. Build your own automation tools
3. Use 3rd party migration tools



If you choose to build your own automation tools, you need to have skilled developers who know how to use the existing management solution APIs and Microsoft Graph APIs for Intune.

If you are looking for a 3rd party migration tool to help you automate some migration steps, you should look out for the following capabilities: automating unenrollment in existing management solution, enrollment in Intune, planning, reporting and user communication.

For your reference, there are a few migration tools available on the market for migrating mobile devices like EBF Onboarder

As for Windows migrations, there are many ways to automate migrations. If you're looking for additional assistance in that space, you can contact your Microsoft contacts or partners.

Tips for simplifying migrations

On top of using automation tools, there are a few tips you can use to simplify the migration process.

For example, for mobile devices, you can:

1. Remove any restrictions preventing the user to unenroll himself when he is eligible for migration. This can help your users manually trigger the migration themselves if automated unenrollment failed
2. If your device does not need to be wiped, deploy the Company portal in advance with your existing management solution and choose the option not to remove it after unenrollment.
3. Choose not to remove some key applications after unenrollment like Microsoft Authenticator if you're using Azure MFA
4. Instruct your users to backup their Microsoft authenticator application for an easier restore process

For example, for Windows devices, you can:

1. Enable OneDrive Known Folders move, OneDrive silent sign-in and Files on-demand. Those features will make it much easier for your end users to retrieve their data after migration, especially if your migration plan includes creating a new user profile in windows
2. Enable Microsoft edge profile sync and automatic sign-in. That will help your end users retrieve their browser favorites, passwords, etc.

Design and implement Common Infrastructure

In parallel of designing and building your device platforms onboarding and migration, you need to plan for implementing common foundations in Intune. Also, you need to be extra careful if those common infrastructures are shared between the existing management solution and Intune, like for example a PKI, Entra ID conditional access, Zero touch solutions, etc.

Migration between Zero Touch providers and application stores (MDM connection)

If you already have a Zero Touch provider configured with your existing management solution, some precautions must be taken, depending on the provider:

- Windows Autopilot
    - A device can only be associated with a single tenant. When moving from one Intune tenant to another, you'll need to remove the devices from the *source* Autopilot and add them to the *target* Autopilot.
    - However, note that the Autopilot registration cannot be removed if the device is currently enrolled. You'll need to delete the Intune device (and wipe it) then remove the Autopilot registration.
- Android Zero Touch (AZT) and Samsung Knox Mobile Enrollment (KME)
    - You will need to create new Device profiles that include Intune enrollment tokens.
    - Once the profiles are created, you will be able to change the device profile of the target devices for migration.
- Apple Business Manager/Apple School Manager
    - You can generate an Apple enrollment program token in your current ABM/ASM portal, in order to link Intune to it. Your existing management solution can coexist with Intune in the Apple portal
    - However, a device can only be managed by one MDM. In order for the migration to work, the device needs to be wiped and then changed from the existing management solution to Intune. Once reenrolled,

it'll be managed by Intune. For more information on migrating supervised devices please follow that link: Migrating ADE iOS Devices to Intune - Microsoft Community Hub

Role-Based Access Control (RBAC)

When you're configuring your Intune environment to migrate your devices, you might encounter an existing delegation model that you will need to adapt. Let's assume you are already using Intune to manage Windows devices and now you need to migrate mobile devices from your other management solution platform to Intune, then you will need to properly design your delegation model so that you don't interfere with Windows devices.

In this case, the RBAC model should be thought to fit your needs during the migration project and afterwards during regular operations. That means, you might need to provide access to project team members during the migration project. All choices regarding RBAC are sensitive and need to be discussed with Operations team well in advance.

Certificate deployment

You can use certificates with Intune to authenticate your users to applications and corporate resources through VPN, Wi-Fi, or email profiles. When you use certificates to authenticate these connections, your end users won't need to enter usernames and passwords, which can make their access seamless. Certificates are also used for signing and encryption of email using S/MIME.

It is likely that you already have certificate-issuing infrastructure, and these can be moved to Intune without impacting user experience. Intune supports Simple Certificate Enrollment Protocol (SCEP), Public Key Cryptography Standards (PKCS), and imported PKCS certificates as methods to provision certificates on devices.

In addition to these three certificate types, you'll also need to issue a trusted root certificate from a trusted Certification Authority (CA) – it can be an on-premises Microsoft CA or a 3rd party CA. This is done with a Trusted Certificate profile that must be distributed to the devices before the SCEP/PKCS/Imported PKCS profiles.

Choosing which certificate type to deploy goes beyond the scope of this guide, but if an existing certificate delivery infrastructure already exists, you'll need to:

- Determine if the infrastructure is based on a Microsoft CA or a 3rd party CA:
    - If you have a Microsoft CA:
        - Install the Certificate Connector for Microsoft Intune
        - If you wish to deploy SCEP certificates, setup an NDES server
    - If you have a 3rd party CA:
        - If you wish to deploy SCEP certificates, Integrate the 3rd party CA with Intune if supported, then create an Application registration in Entra ID with the rights delegation
        - If you wish to deploy a PKCS imported certificate, install the Certificate Connector for Microsoft Intune
- In both cases, a *Trusted Certificate Profile* will need to be deployed with the Root CA certificate

i. 3rd party integrations
ii. Network infrastructure (VPN, NAC, proxy, …)
iii. On-premises resource access
iv. Define RBAC model
v. Define Operational support model (DEV >TEST >PROD?):
    1. Define update/release rings
    2. App/package updates
    3. OS update release cycle
    4. Security Baselines

Test and verify

After completing the design phase, we move on to testing. The testing phase is used to develop test plans for use cases across each platform being managed by Intune.

The goal is to identify any issues with device management and provide the necessary learning needed to effectively manage devices across your organization. Testing provides information about use cases to admins before a full organization wide deployment is started. We recommend testing various scenarios to ensure Intune meets the requirements for device management across networks, locations, and platforms including different OS versions.

Before you begin:

- Confirm that you've completed the assessment and planning phases.
- You should have a list of the scenarios you're going to support and the requirements for each.
- You should know the migration strategies you will be testing.
- Ensure that you have test devices for each platform.
- Ensure that you or another person has direct access to the environment, full permission to view all objects.

The main objective of this phase is making sure that the migration and enrollment processes work in your own environment. For that reason, it is important to test in target conditions. For example, testing on a virtual machine or testing with your private 4G connection might not give you the same results as if you were testing in your organization's network with a physical device.

As a best practice, follow this plan to test efficiently all your scenarios in your environment:

1. **Unit testing**: Test Entra ID and Intune management capabilities for all platforms and management modes you will encounter. Those tests need to be done on new devices that have not been enrolled with any previous management solution. Once every functionality is validated in your environment, move on to next phase.

2. **Integration and migration testing**: Assign all target functionalities to your test device (applications, profiles, etc.) and then validate that the migration tool and process works in all the conditions users might encounter (migrating at home, migrating at work, etc.)

Unit testing: Testing Entra ID and Intune management capabilities per platform

Android

When managing Android devices, there are several areas that should be tested to ensure the device is managed as expected and to identify any potential issues that need to be addressed. Some of the key areas to focus on during testing include:

- Device Configuration: Ensure that the device is correctly configured with the appropriate settings, such as network settings, display settings, and device security policies.

- Device Performance: Test the device's performance by running applications and performing common tasks to ensure that the device operates smoothly and quickly.

- Application Management: Test the ability to manage applications on the device, including installation, updates, and removal of apps.

- Security Management: Test the security features of the device, such as screen locks, password policies, and encryption.

- Remote Management: Test the ability to remotely manage the device, such as remotely wiping the device, locking the device, or pushing software updates.

- Device Compatibility: Test the device's compatibility with various applications, peripherals, and networks to ensure that the device can function in various environments.

- Device Compliance: Test the device's compliance with organizational policies, industry standards, and regulatory requirements.

- Device Customization: Test the ability to customize the device with custom settings, wallpapers, and themes.

- Geographical management: Test device management across different geographical locations.

By testing these areas, you can ensure that Android devices are fully operational and secure meeting, your organization's requirements.

Test case scenario overview

Device enrollment

1. BYOD – Work Profile
    a. Test enrollment of a personal Android device
2. Android Enterprise corporate owned
    a. Test enrollment of a Corporate Owned device scenarios via QR code, Zero Touch either through Google ZTE and/or Samsung Knox Mobile Enrollment (KME)
3. AOSP
    a. Test enrollment of user assigned and userless device enrollments such as Oculus, HTC VR, or RealWear.

Device compliance

1. Create compliance policy
2. Verify device is compliant with compliance policies after enrollment.

Conditional access

1. Create a conditional access policy.
2. Verify device is blocked and allowed via compliance policies.

Software and OS updates

1. Create software and/or OS update policy.
2. Verify software updates via configuration settings and FOTA settings (where applicable, i.e. Zebra).

App deployment

- Assign a set of applications and verify applications have deployed to the device.
- Unassign applications and verify removal from the device.

App Configuration Policies

- Create and assign an app config policy and verify settings applied on the device.

Policy deployment

- Create and assign policies that meet your organization's requirements and verify settings applied on the device.

Remote actions

Test and verify remote actions for device management:

1. Wipe
2. Retire
3. Reset passcode
4. Device rename
5. Remote lock
6. Restart
7. Shutdown
8. Remote assistance (where applicable)
9. Play lost device sound (where applicable)

Apple

When managing Apple devices, there are several areas that should be tested to ensure the device is managed as expected and to identify any potential issues that need to be addressed. Some of the key areas to focus on during testing include:

- Device Configuration: Ensure that the device is correctly configured with the appropriate settings, such as network settings, display settings, and device security policies.
- Device Performance: Test the device's performance by running applications and performing common tasks to ensure that the device operates smoothly and quickly.
- Application Management: Test the ability to manage applications on the device, including installation, updates, and removal of apps.
- Security Management: Test the security features of the device, such as screen locks, password policies, and encryption.
- Remote Management: Test the ability to remotely manage the device, such as remotely wiping the device, locking the device, or pushing software updates.
- Device Compatibility: Test the device's compatibility with various applications, peripherals, and networks to ensure that the device can function in various environments.
- Device Compliance: Test the device's compliance with organizational policies, industry standards, and regulatory requirements.
- Device Customization: Test the ability to customize the device with custom settings, wallpapers, and themes.
- Geographical management: Test device management across different geographical locations.

By testing these areas, you can ensure that Apple devices are fully operational and secure, meeting your organization's requirements.

Test case scenario overview

iOS/iPadOS

Device enrollment

1. BYOD
2. Automated Device Enrollment (ADE)

Device compliance

1. Create compliance policy.
2. Verify device is compliant with compliance policies after enrollment.

Conditional access
1. Create conditional access policy.
2. Verify device is blocked and allowed via compliance policies.

Software and OS updates
1. Create software and/or OS update policy.
2. Verify software updates and update policies via configuration settings.

App deployment
- Assign a set of applications and verify applications have deployed to the device.
- Unassign applications and verify removal from the device.

App Configuration Policies
- Create and assign an app config policy and verify settings applied on the device.

Policy deployment
- Create and assign policies that meet your organization's requirements and verify settings applied on the device.

Remote actions
Test and verify remote actions for device management:
1. Wipe
2. Retire
3. Remove passcode
4. Device rename
5. Remote lock
6. Restart
7. Shutdown

macOS
Device enrollment
1. BYOD
2. Automated Device Enrollment (ADE)

Device compliance
1. Create compliance policy.
2. Verify device is compliant with compliance policies after enrollment.

Conditional access
1. Create conditional access policy.
2. Verify device is blocked and allowed via compliance policies.

Software and OS updates
1. Create software and/or OS update policy.
2. Verify software updates and update policies via configuration settings.

App deployment
- Assign a set of applications and verify applications have deployed to the device.
- Unassign applications and verify removal from the device.

App Configuration Policies

- Create and assign an app config policy and verify settings applied on the device.

Policy deployment
- Create and assign policies that meet your organization's requirements and verify settings applied on the device.

Remote actions
Test and verify remote actions for device management:
1. Wipe
2. Retire
3. Reset passcode
4. Device rename
5. Restart
6. Shutdown

Windows

When managing Windows devices, there are several areas that should be tested to ensure the device is managed as expected and to identify any potential issues that need to be addressed. Some of the key areas to focus on during testing include:

- Device Configuration: Ensure that the device is correctly configured with the appropriate settings, such as network settings, display settings, and device security policies.
- Device Performance: Test the device's performance by running applications and performing common tasks to ensure that the device operates smoothly and quickly.
- Application Management: Test the ability to manage applications on the device, including installation, updates, and removal of apps.
- Security Management: Test the security features of the device, such as screen locks, password policies, and encryption.
- Remote Management: Test the ability to remotely manage the device, such as remotely wiping the device, locking the device, or pushing software updates.
- Device Compatibility: Test the device's compatibility with various applications, peripherals, and networks to ensure that the device can function in various environments.
- Device Compliance: Test the device's compliance with organizational policies, industry standards, and regulatory requirements.
- Device Customization: Test the ability to customize the device with custom settings, wallpapers, and themes.
- Geographical management: Test device management across different geographical locations.

By testing these areas, you can ensure that Windows devices are fully operational and secure, meeting your organization's requirements.

Test case scenario overview

Device enrollment

1. BYOD
2. Autopilot

Device compliance

1. Create compliance policy.
2. Verify device is compliant with compliance policies after enrollment.

Conditional access

1. Create a conditional access policy.
2. Verify device is blocked and allowed via compliance policies.

Software and OS updates

1. Create software and/or OS update policy.
2. Verify software updates via configuration settings.

App deployment

- Assign a set of applications and verify applications have deployed to the device.
- Unassign applications and verify removal from the device.

App Configuration Policies

- Create and assign an app config policy and verify settings applied on the device.

Policy deployment

- Create and assign policies that meet your organization's requirements and verify settings applied on the device.

Remote actions

Test and verify remote actions for device management:

1. Wipe
2. Retire
3. Reset passcode
4. Device rename
5. Restart
6. Shutdown
7. Remote help

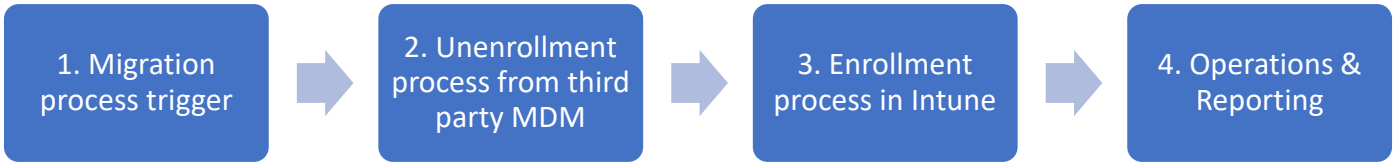
Platform administration and common foundations

In this section, you will need to test all common foundations and administration for your Intune platform, for example:

1. Group management
2. Certificate distribution
3. RBAC model
4. Network components
5. Reporting
6. 3rd party integrations if any

Integration and migration testing

When you execute a migration project, there are several moving pieces you need to verify in an end-to-end migration scenario.



1. Migration process trigger

In this step, either you are allowing the end-user to control the launch of the migration process or you are doing it centrally. In both cases, you need to make sure that the trigger works as expected and that the migration launch is reported in your tools.

2. Unenrollment process from third party MDM

In this case, depending on the platform you are migrating, you could either be in a "wipe and reinstall" process or just a "unenroll and enroll" process. In either cases, you will need to make sure that the device is effectively unenrolled from the previous third party MDM, either using a manual migration by the end-user or using a migration tool.

3. Enrollment process in Intune

When the device is ready for enrollment, either manually or using a migration tool, you need to verify that all your requirements for your target solution are met at the end of the enrollment: application installations, configuration, compliance, conditional access, network access, etc.

4. Operations & Reporting

This area needs to be tested thoroughly, especially if you have a complex organization. Making sure that all L1/L2/L3 operators have the right privileges and access is key for IT change management. Also, you need to make sure the reporting to follow-up on which devices have started, are in progress or have finished their migration is working correctly.

Deploy

Deployment can begin once you've completed the assessment, design & planning, and test phases for a platform. Most companies start their deployments focused on specific scenarios or business units and will deploy with a few smaller sets of users/devices and then deploy increasingly larger waves until all users and devices are migrated. For example, starting with BYO devices but only for the IT department or only a subset of kiosks at a specific store.

Communication with your support staff, end users, and all stakeholders is critical during deployment. All parties involved need to understand when the changes are going to happen, what actions they will need to take, and how to confirm that the deployment or migration of a device is complete and successful.

Microsoft has created the Intune Adoption Kit to help provide examples of the type of information and communications typically used: [Download Intune Adoption Kit from Official Microsoft Download Center]

Before you begin:

- Confirm that you've completed the assessment, planning, and test phases.
- Confirm that you have a communication strategy ready.
- Confirm that your stakeholders are aware of the migration and have approved the timeline.
- Confirm you have a roll back plan for users, device, services if an issue is found that didn't surface during testing.

Automatic Enrollment Registration Migration

For corporate Windows, iOS, macOS, and Android devices, administrators can leverage automatic enrollment to simplify enrollment of corporate devices into Intune. Administrators must have a plan for updating the registration for any devices configured for automatic enrollment. Review the following table and ensure you have registered your Intune instance with the enrollment provider and that prior to deployment or migration the devices are configured to enroll with Intune.

Platform	Enrollment system	Steps to prepare for device migration
iOS/iPadOS	Automated Device Enrollment	Ensure that your Intune instance is configured as a server and devices are assigned to the new server.
macOS	Automated Device Enrollment	Ensure that your Intune instance is configured as a server and devices are assigned to the new server.
Android	Google Zero Touch Enrollment	Register your Intune instance in the ZTE portal and update device assignment
Android	Samsung Knox Mobile Enrollment	Add MDM profile(s) for Intune
Windows	Autopilot	Autopilot devices must be deregistered with current Entra ID tenant and reregistered with new tenant

Migration steps for mobile devices

As mentioned in "Design & Plan" phase, there will be 2 main scenarios you may encounter for migrating existing devices:

- **Wiping the device**

This solution if used usually as a last resort as it is the most destructive. As a prerequisite, you will need to consider how you want to manage user data backup. If needed, you can rely on solutions like OneDrive or the manufacturer's backup tools.

When you are ready to launch a migration wave, you can choose either to wipe devices from your 3rd party in bulk or let your end users wipe their devices themselves when they are ready. Wipe in bulk is usually used as a last resort by IT whenever you need to make sure you meet your project deadlines. We highly recommend you enable your users to wipe their devices themselves when ready.

Once the wipe command has been initiated, the migration process becomes straightforward like a standard onboarding process for a new or unmanaged device. After enrollment, you may need to provide additional guidance to your end users to restore their data. Note that this solution is very similar to replacing an old mobile device with a new one.

- **Unenrolling from existing management solution and enrolling in Intune**

Some management modes do not require wiping the device for the migration process. In that case, you can follow those steps:

1. Push the company portal application using your existing management solution. Important: you need to make sure it won't be uninstalled when the device is unenrolled.
2. Enable your end users to unenroll their devices
3. Optionally but recommended: create a conditional access policy requiring devices to be compliant to access corporate resources. This step can help or accelerate enrollment to Intune. Please be very careful on which groups needs to be assigned to this conditional access policy
4. End users manually enroll their devices using the company portal as would a user with a new or unmanaged device
5. Provide guidance to your users on how to set up back their applications (email client, collaboration tools, etc.)

Migration steps for Windows

Windows migrations are also possible through a couple of different scenarios, both with advantages and disadvantages.

- Wiping the device

This method involves resetting the device to its original factory state – either by resetting (wiping) it or deploying a fresh operating system image (bare metal restore). In either case, existing data, applications, and settings are removed so any of these items must be preserved and re-applied using another process (if they must be retained).

The advantage of this method is that the device is returned to a pristine state, prior to enrollment into the target environment.

- Unenrolling from existing management platform

It is possible to unenroll the device from the existing management platform and then enroll it into the target environment. However, this is not an automated process and there are inherent risks in leaving remnants of the source environment 'tattooed' to the device.

The advantage of this method though is that it is not data-destructive, so some organizations may prefer this option to preserve existing data and applications – although preservation of existing settings is likely not to transfer as the user profile may well be different after the device is joined to the target environment.

i. Assumptions that target Intune/Autopilot configuration is correct and has been tested prior to device migrations.

It's advisable to ensure you have configured and tested your enrollment configuration thoroughly before performing any migrations. This includes your required applications, packages, scripts and policies. Making sure you have tested this process with devices that are representative of your existing estate is advisable to ensure you are not spending valuable time during a migration troubleshooting issues that can occur through lack of testing.

ii. Ensure functioning push button reset (PBR) on devices to be migrated.

Windows operating system (OS) resets have a dependency on a fully functioning Windows Recovery Environment (WinRE). The Push Button Reset (PBR) process is initiated using the WinRE. If the WinRE is missing or misconfigured, the OS reset will fail. As the migration process is reliant on the OS being reset, having a working WinRE is a critical requirement for success.

iii. Recommend In-Place Upgrade to a supported OS version prior to migration (successful IPU fixes most PBR issues – so successful IPU = working PBR = successful device reset). Newer OS versions have improved reset functionality (like Cloud Download Reset in W10 2004 and above) and better error handling.

One way to ensure your devices have a working WinRE is to complete a successful Windows Feature Upgrade (via an in-place upgrade that is run locally from the device). For the Feature Upgrade to be successful, it too requires a working WinRE – but if it encounters a missing or misconfigured WinRE – the in-place upgrade setup process will recreate a new WinRE at the end of the drive (by dynamically resizing the OS partition and creating a new WinRE partition in the free space). So a good way to confirm your devices are in a state ready to be wiped/reset, is to have successfully completed an in-place upgrade first, which will repair the WinRE (thus ensuring Push Button Reset will work).

Another benefit of the Feature Update is improvements to the Push Button Reset (PBR) process. Newer Windows versions include enhancements to PBR that make the reset process more reliable. An example of this is the Cloud Download Reset functionality added in Windows 10 2004 and above. This enables the operating system to dynamically download the components required to rebuild itself from the Microsoft cloud.

iv. Items to consider:

1. Appropriate user comms – inform about migration (screenshots of what OOBE should look like, branding/messaging etc.), who is responsible for data backup, device must be plugged in on mains power, recommended reboot prior to scheduled migration time,

consider need for a migration booking/scheduling solution, ensure up-to-date contact info for users who are migrating – in-case IT support need to reach out in event of migration issues.

A better experience for your user community involves good communication. This means timely messaging, well in advance of any migrations – and using multiple methods of communication (emails, Teams channel notifications, verbal messaging from managers etc.). You should clearly state what is required from your users prior to any migrations. This should cover at least the following items:

- Who you consider responsible for any data backup (as the OS reset will restore the device to it's original factory condition, thereby removing any user data/applications/settings etc.).
- Expectations around the migration experience – providing a visual explanation, with screenshots of what the migration process will look like.
- Expectations on what actions must be performed during the migration process – so will your users be performing the migrations or will IT personnel complete the process? Ensure devices are on mains power, not battery and have been recently rebooted prior to the migration.
- Ensure user contact information is current and also ensure users have an escalation path and are correctly briefed on who to contact with questions.
- Consider developing a booking system, allowing end users to perform the migrations via a self-service option on a schedule that suits them.

2. Power management policy changes to prevent devices from sleeping prior to migration.

If you have power management policies that enforce energy saving timeouts, consider an override policy for devices that are targeted for migration. This should be configured in the source environment, to ensure devices have the best chance of migrating without going offline due to a sleep timeout.

3. Block enrollment in legacy environments

For devices that are migrating from an existing Intune environment, consider blocking the enrollment of devices in the source tenant. This is to mitigate the risk of devices being wiped/reset then accidentally re-joined to the source environment.

Some areas for consideration in this scenario are:

- Intune Device Enrollment Restriction – *block Windows MDM*
- Disable 'Convert all targeted devices to Autopilot' profile option

v. Potentially deploy persistent provisioning package to existing devices (can be used to control devices during reset process: add a delay etc.).

It is possible to leverage a persistent provisioning package to perform actions that may be required as part of the reset process. A persistent provisioning package is preserved as part of the OS reset and can contain scripts/packages/applications that need to be re-applied during the reset process, prior to the device returning to the Out-Of-Box-Experience (OOBE). An example might be re-installing a required security application, to ensure optimal device compliance or running a script to perform a delay whilst back-end objects are prepared (such as backup/migration of existing Autopilot registration information between source/target tenants).

vi. Harvest Autopilot hardware hashes from existing devices (store in Internet accessible file-share, like Azure blob storage), can be exported from Configuration Manager DB if CM is managing existing devices.

For devices that will be enrolled using Windows Autopilot, a critical dependency is to ensure your device has its hardware hash pre-registered in the target tenant prior to enrollment. Since it is only possible to

register the Autopilot hardware hash to a single tenant at a time, preparation is required. It is not possible to export existing Autopilot hardware hashes from Intune, so provision must be made to harvest this information and store it prior to migration. One possible way to achieve this capture of hardware hashes is to deploy a script that captures the required data and stores it to a datastore (such as an Azure blob store) for later retrieval.

For environments that are using Configuration Manager Current Branch, the required hardware hash data is already captured for each device inside the Configuration Manager database and this can be exported for import into the target environment.

Once the migration is in progress, the existing Autopilot objects can be deleted from the source tenant and then imported into the target tenant. However, this is not an instant process and time must be allowed for successful deletion, import and Autopilot profile assignment before a successful enrollment can be completed. See the recommendation above for the persistent provisioning package as a way to introduce additional time into the OS reset process to help with this.

vii. Issue OS reset (Intune wipe with no options checked, or script pushed from Configuration Manager to poke reset CSP).

The simplest way to migrate from an existing Intune tenant to a new tenant is to issue the wipe from the source Intune tenant. On successful processing of the wipe, Intune will remove the existing device object. This then enables you to remove the associated Autopilot object (which cannot be removed until the corresponding Intune object is removed first). Once this happens at the back end, your devices can be imported into the target environment.

It is also possible to initiate the wipe process by deploying a script to your existing devices that will invoke the required WMI call to connect to the reset CSP.

viii. Cleanup legacy associated device objects (remove Intune > Autopilot > AAD objects – if it's moving from one tenant to another), zap any existing management solution objects

For Intune tenant migrations (with existing Autopilot objects) it is required to remove the existing device objects from the source to enable import into the target environment.

For migrations from other management solutions, it may be necessary to perform cleanup actions specific to the guidance for those respective platforms.

ix. Import Autopilot hardware hashes from blob store.

For devices that are being enrolled using Windows Autopilot – ensure the required hardware hashes are imported prior to any attempts to enroll.

x. Confirm Autopilot profile targeting.

For devices that are being enrolled using Windows Autopilot – successful enrollment is also dependent on the correct targeting of a Windows Autopilot profile. This requires devices to be added to an associated targeting group for that Autopilot profile. So, part of the migration process is to ensure these devices are correctly added to the required group, so that the Autopilot profile can be assigned. Using a static AAD group is usually best for this, since it is not subject to any delays associated with dynamic group membership processing.

xi. Enroll migrated devices using Autopilot (after device is reset to OOBE).

For devices that are being enrolled using Windows Autopilot – once the devices are showing in the list of Autopilot devices in the target tenant and have the status of profile applied, they can be enrolled in the normal way by your end users.

xii. Mop-up activities:

1. Check which devices have enrolled – potentially contact users.
2. May need manual intervention to get the device back to functional state.

Intune Terminology

While the general concepts for device management are consistent across management solutions terminology can at times be different and generate confusion for new administrators and users. The table below lists common terminology and acronyms in Intune that administrators often need some clarification on when migrating.

Term	What it means in Intune	Comparable terms and features
Conditional Access	Microsoft's Zero Trust policy engine that uses if-then statements to grant users access to resources based on signals from various sources. For example, a user must be on an enrolled and compliant device to access email.	One Access, Secure Access
User	A User account in Entra (Entra ID). This account could exist only in the cloud, or it can be synchronized from on premises Active Directory.	User Account, Basic User Account
Device	A device object in Entra (Entra ID). This is the registration record that is created when a device is added to the directory.	Device Record
Assigned Group	A Group in Entra (Entra ID) with users or devices directly added to it.	Static Group
Dynamic Group	A Group in Entra (Entra ID) who's members are added via querying one or more attributes. The administrator must select if the group will be users or devices during the initial creation.	Dynamic Collection, Smart Groups, Query based group
Assignment	The process of targeting an Intune policy or object to a group. For example, "assigning Word to the accounting group".	Smart group, attribute-based targeting
Filter	Filters are a targeting feature in Intune that allows administrators to narrow the assignment the scope of a policy assignment using additional attributes. For example, and administrator might assign Word to accounting users, and then use a filter to limit it to corporate only devices.	Smart Group, Rule Filter
Device Categories	An Intune feature that allows and administrator to assign a label to a device to help categorize the device. This category can then be used to help with targeting and/or reporting.	Labels
App Protection Policy (APP)	App Protection policies provide Mobile Application Management (MAM) polices to Intune SDK enabled applications. App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app.	Mobile Application Management, MAM
App Configuration Policies	App configuration policies allow administrators to send configuration information to applications on devices. For example, configuring the database server for a mobile application.	App Config, MAM
Policy Sets	An Intune feature that allows an administrator to create a virtual bundle of objects (apps, policies) and make a single assignment for these objects. For example, creating an Accounting Devices policy set and	

	then selecting all of the apps and settings for the accounting department.	
App Selective Wipe	An Intune feature that allows an administrator to send a wipe command to applications with an active App Protection Policy. This is supported with or without device management.	MAM Wipe
Microsoft Tunnel Gateway	Microsoft Tunnel is the first party VPN solution from Microsoft for mobile devices.	Mobile Access, Mobile VPN, Secure Access Gateway
Roles	Roles defined permission sets within Intune that grant users the ability perform actions in Intune. They are the foundation for Role Based Access Control (RBAC) and delegated managed in Intune. Roles are used to determine what actions a administrator can take, and on what objects.	Role Based Access, RBAC
Scope Tags	Scope Tags are used to filter what objects an administrator can see in Intune. Scope tags are created and then assigned to administrators, and then objects in Intune. Administrators can only see objects with matching scope tags. For example, if I create an accounting scope tag and assign it to all accounting related objects they cannot be seen by an administrator who doesn't have the accounting scope tag assigned to them.	Role Based Access, RBAC
Diagnostic Settings	Intune supports sending logs to Azure Monitor for storage and advanced reporting. Diagnostic settings is where administrators configure integration between Intune and Azure Monitor.	
Terms and Conditions	An Intune feature that presents users enrolling devices with the Terms and Conditions for enrolling devices and accessing company resources.	