



MDM Migration Made Easy

7 Steps to Migrating
your Apple Devices
to Resolve MDM



Apple's Big Change for Device Management



In summer 2025, Apple announced a game-changing new capability: devices can now seamlessly migrate between Mobile Device Management (MDM) platforms without requiring a factory reset.

This breakthrough eliminates one of the most significant pain points in enterprise device management, saving IT teams countless hours and reducing disruption to employee productivity.

This ebook provides a comprehensive, step-by-step guide to help organizations easily complete the MDM migration process using Apple's new capability. Whether consolidating vendors to reduce operational complexity, upgrading systems, or moving away from a platform that no longer fits organizational needs, this guide offers practical insights and best practices to ensure a smooth and successful transition.

Key Terms



Before diving into Apple's groundbreaking update, let's establish a common understanding of the key terms and concepts you'll encounter throughout this guide.

Mobile Device Management (MDM)

A methodology and toolset used by IT departments to remotely configure devices, enforce security policies, deploy applications, and manage data.

Apple Business Manager (ABM)

Apple's free centralized portal used to manage your organization's devices and app licenses.

Automated Device Enrollment (ADE) - Previously called Device Enrollment Program (DEP)

The official method (via ABM) used to automatically enroll devices into an MDM the first time they are powered on.

Volume Purchase Program (VPP)

Now integrated into ABM, this is Apple's platform where Admins can acquire content like apps or books in volume and distribute them to devices in their organization.

Supervised Mode

A powerful management state that grants the MDM the highest level of control over the device, necessary for pushing out advanced security settings or restrictions, including blocking users from uninstalling the MDM from their device.

Tip: Refer back to this page if you need clarification on any acronym or term throughout the guide



The MDM Migration Game-Changer

Organizations that wanted to switch MDM platforms used to face a critical challenge: moving devices from one MDM to another required factory resetting every device, which was time-consuming, labor-intensive, and highly disruptive. Following Apple's 2025 announcement, this reality has fundamentally changed.

Before

Organizations wanting to migrate iOS devices from one MDM to another typically had to factory reset the devices, wiping them completely.

Without performing that wipe, devices wouldn't be fully managed or run in Supervised mode, which meant end users could uninstall them from their devices, and IT teams lost the highest level of control necessary for pushing out advanced security settings and restrictions.

The old reality: IT teams were often stuck with MDM vendors that no longer fit their needs, simply because the migration process was too costly and disruptive to undertake.

After

It is now possible for organizations to move from one MDM to another without wiping devices or losing data.

This means migrating between MDM platforms is now significantly less intrusive for end users and far easier for IT teams. Devices retain their configurations, data, and full management capabilities including Supervised mode throughout the transition.

The new reality: Organizations stuck with unsuitable MDM platforms can now transition to better-fit solutions without the traditional barriers that kept them locked in.

Why This Matters for Businesses

As organizations continue to expand their reliance on mobile devices, the ability to seamlessly migrate between MDM platforms without a factory reset represents a major advancement. With such a large portion of employees relying on iOS and iPadOS devices for daily work, this breakthrough simplifies IT workflows and enhances device management flexibility. For companies exploring new MDM software, Apple's update delivers a smoother migration process, minimizes disruption, and enables IT teams to implement best practices for secure, efficient management of their device fleet.

Device Eligibility for MDM Migration

To take advantage of seamless MDM migration, devices must meet specific operating system and enrollment requirements:

- Devices with iOS 26, iPadOS 26, or macOS 26.
- Owned devices enrolled via Automated Device Enrollment, (or Macs on macOS 26 enrolled with profile-based enrollment).
- If you enroll the device manually using Apple Configurator, it needs to be after the 30-day provisional period.

Migration Limitations

Currently, seamless MDM migration is not available in the following scenarios:

- Migrating to and from the device management service within Apple Business Essentials isn't currently supported.
- Device management service migration isn't available on Shared iPad.

Organizations using these configurations should monitor future OS updates for expanded compatibility.



Who Benefits Most from Apple's New MDM Migration Capability?

Apple's seamless MDM migration capability opens new possibilities for organizations to move to MDM platforms that better align with their needs. This is especially exciting news for anyone who falls into the following groups:

Organizations with Fragmented Device Management

IT teams managing device security across multiple MDM vendors—using one tool for Macs and iPhones, and a completely different tool for Windows devices—face significant challenges. This fragmentation forces IT staff to master redundant, labor-intensive consoles and increases the potential for security blind spots.

Teams Experiencing Complexity Fatigue

When the current MDM solution is overly complicated and difficult to use, it leads to slow administrative processes and low IT team morale.

Victims of Vendor Sprawl

Organizations relying on three or more separate vendors for core IT operations (MDM, Remote Monitoring and Management (RMM), Remote Support, Ticketing) waste significant time managing multiple contracts and siloed platforms.

Budget-Conscious Organizations

Organizations spending significant amounts due to complex licensing tiers and the maintenance of multiple, unoptimized contracts—where functionality often overlaps—end up paying twice for the same features.

7 Steps to Migrating MDMs

The M.I.G.R.A.T.E. Framework

To simplify the MDM migration process, we've created a structured, seven-step framework that organizations can follow to ensure a smooth transition.

Map out existing devices and configurations

Integrate new MDM with ABM

Generate equivalent profiles, apps, files in new MDM

Reassign devices to new MDM in ABM

Assign enrollment profiles & tags

Track enrollment progress

Ensure migration has been successful

Note: This process is based primarily on Resolve MDM, but the general approach will be similar for other MDM platforms.

Best Practices for a Successful Migration

Before diving into each step of the M.I.G.R.A.T.E. framework, it's important to keep a few best practices in mind to ensure a smooth and successful migration. These tips will help organizations avoid common pitfalls, stay on schedule, and maintain a positive experience for both IT teams and end users throughout the transition.

1

Phase the Approach

Follow a phased migration plan, starting with a small group of less critical devices first.

2

Set Appropriate Deadlines

If volume purchased (VPP) apps are part of the deployment, note that you have 30 days to complete the migration. Set deadlines accordingly. [Learn more](#)

3

Communicate With End-Users

Put together a guide for end users, and a plan for communicating to them in advance on what is changing and what actions are needed on their end.



01

Map Out Existing Devices and Configurations

Before you get started, it's important to make a record of all of your current inventory, their operating systems, and configurations such as:

- Configuration Profiles (Passcode, Wi-Fi, VPN)
- Encryption settings and certificates
- Managed applications (VPP apps) and their specific settings
- Grouping or tagging strategies

This list helps you compare features, recreate the environment exactly, and determine if devices meet the right criteria to be migrated.



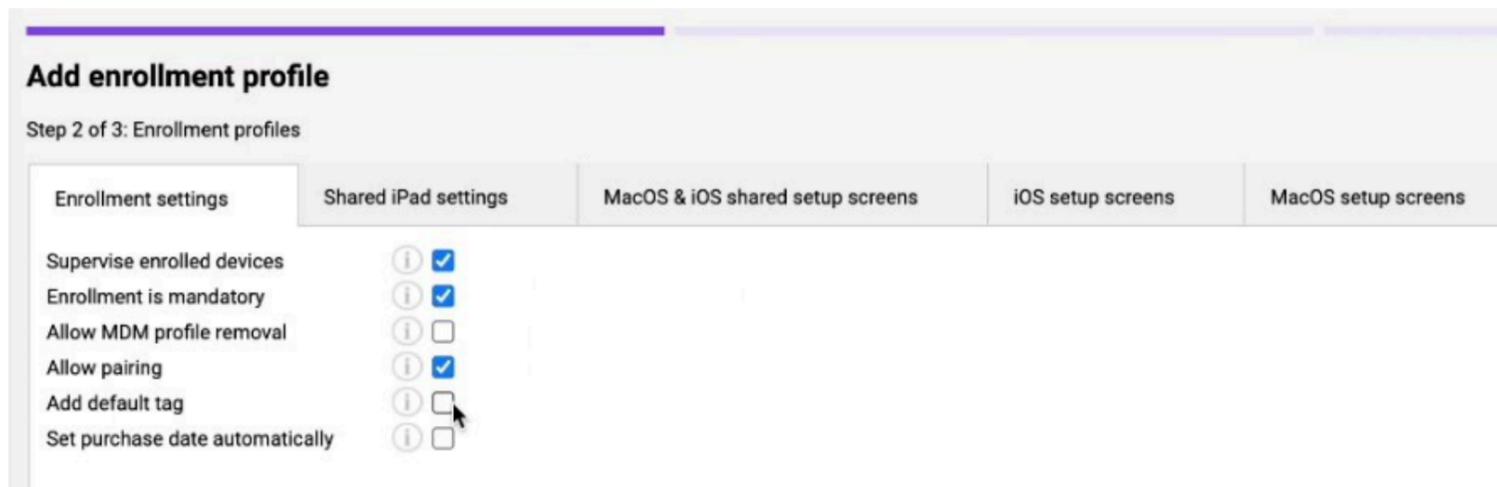
02

Integrate Resolve MDM and ABM

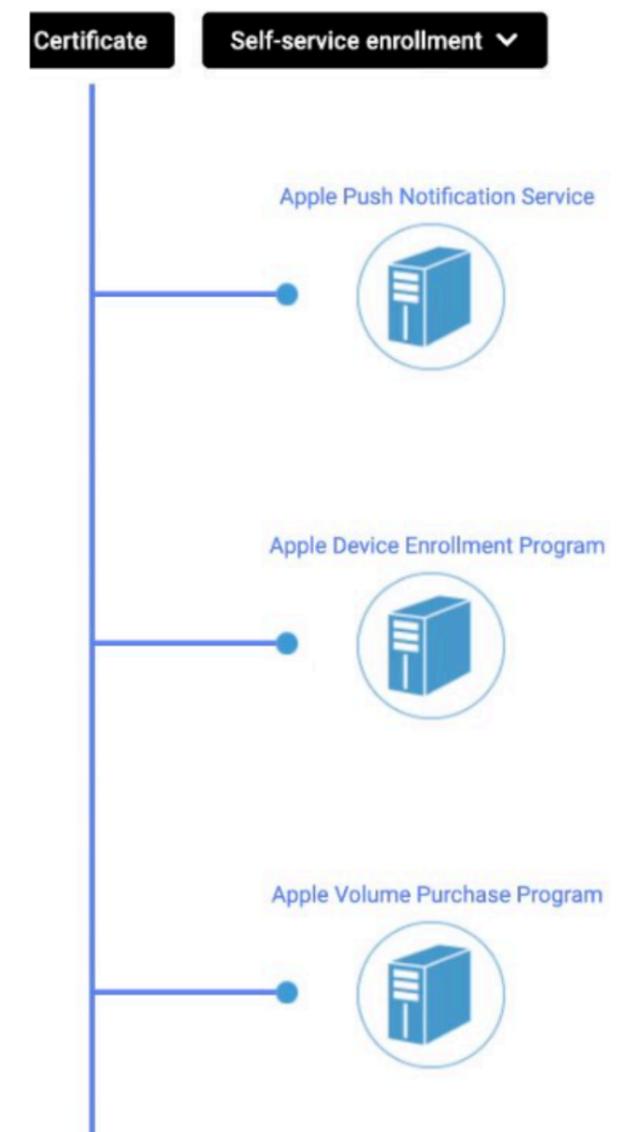
Before you move a single device, you'll need to build and authorize the Resolve MDM environment. In most cases, this will include doing the following three things:

- Set up [Apple Push Notification Service](#) (APNs).
- Connect [Automated Device Enrollment](#) (ADE) with Resolve MDM and build an Enrollment Profile.
- Configure [Apple VPP](#) to manage app licenses.

These can all be done from the Infrastructure Diagram in Resolve MDM.



Tip: When building the Enrollment Profile, selecting the "Add default tag" will automatically add a "dep" tag to all devices using this enrollment profile. This will make it so you can more easily group your devices or assign Business Profiles.



The Infrastructure Diagram

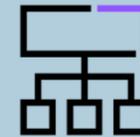
Resolve MDM 101

Understanding a new MDM's framework and terminology can often be one of the most daunting steps in a migration. To make it easier, here's a quick guide to the building blocks of Resolve MDM.



Enrollment Profiles

Specifies settings that apply when a device is first turned on, like if it will be managed in Supervised mode, whether the MDM can be removed, and the Setup screen experience will be. Enrollment Profiles are part of ADE and set up in the Apple DEP page (visible once ADE is set up).



Configuration Profiles

All device settings and configurations (such as WiFi or passcode settings, restrictions and application blocklists, and policies around system updates) are centrally managed in the Configurations Profile page.



Applications

App Store, VPP, Google Play, Managed Google Play, in-house, and custom apps across all operating systems are managed in the Applications page. This is also where you'd add and manage custom scripts and packages.



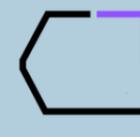
Certificates

Any PEM and DER encoded certificates and certificates in #PKCS12 file format in the Files and Certificates tab.



Business Policies

While items like Configuration Profiles, Applications and Files and Certificates can be deployed directly to selected devices in their respective pages, applying them with a Business Policy is recommended for more advanced automation and tracking. Business Policies act as a "blueprint" that bundles these items, with options for adding dependencies and a centralized place for tracking deployment progress. Devices are assigned to Business Policies using Tags.



Tags

The primary way define the scope (or target devices) for a Business Policy. Some Tags can be added automatically (like the "dep" tag), but you can also create and add custom tags in the overall Devices Page or in an individual Device page.

03

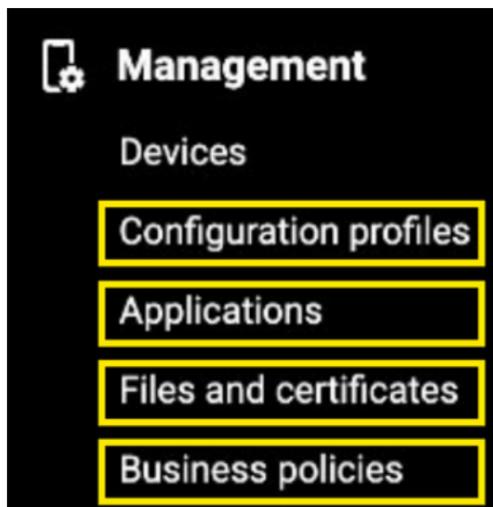
Generate Equivalent Profiles, Apps, Files

Every MDM uses different terminology and has different ways of accomplishing the same things. Familiarizing yourself with your new MDM's framework is critical in a successful migration.

It's important to know that the old MDM's configurations are not automatically transferred, and will need to be rebuilt in your new MDM.

Using the inventory created in Step 1 as your guide and bearings, you'll need to:

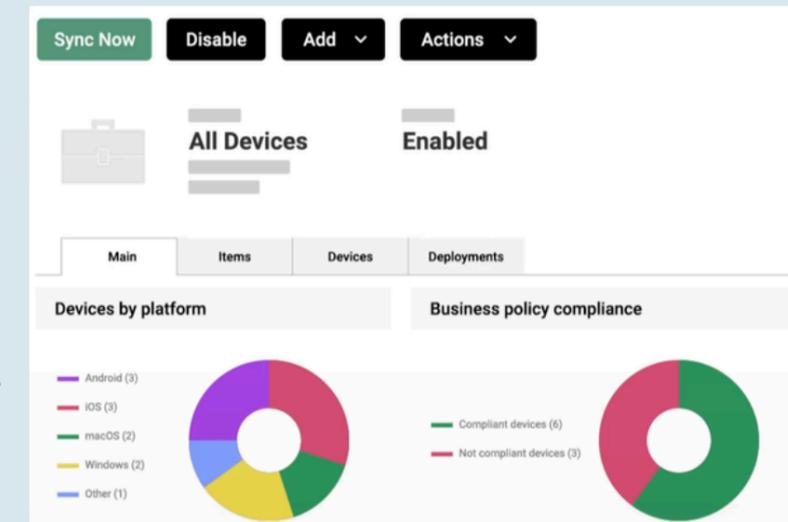
1. [Recreate all configuration profiles](#) for iOS, iPadOS, and macOS, as well as any additional [Enrollment Profiles](#) and [Certificates](#).
2. [Add applications](#) to be installed and configure their managed settings.
3. Bundle these into [Business Policies](#) and assign those policies with tags.



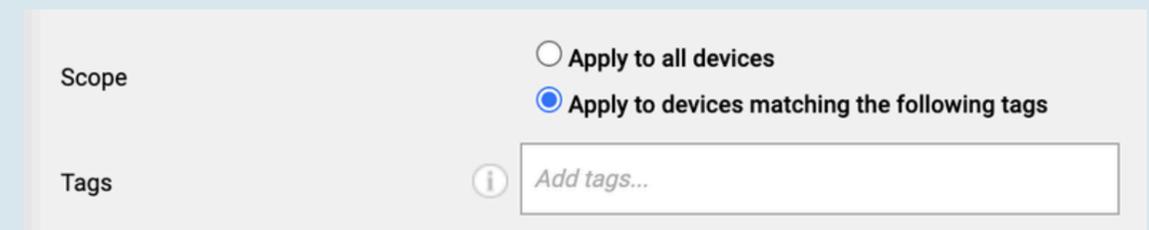
Note: Applications deployed through your current MDM solution will not be automatically uninstalled for Macs. We recommend removing them with your old MDM.

What are Business Policies?

Instead of adding individual applications or configuration policies to devices one-by-one, we recommend bundling these into a Business Policy (or multiple Business Policies).



Not only do Business Policies offer advanced capabilities around tracking progress and setting dependencies, they're also the best way to ensure that all these configurations and applications **are applied to your devices as soon as they're enrolled.**



Business Policies can either be assigned to all devices, or to groups of devices using **tags**. You can create the tags now, and then assign them to devices later in the migration process, or even use automatic tags like the "dep" tag.

After creating the Business Policy, **make sure that the Status is set to "Enabled"** to ensure it will be applied to your devices as soon as they are enrolled.

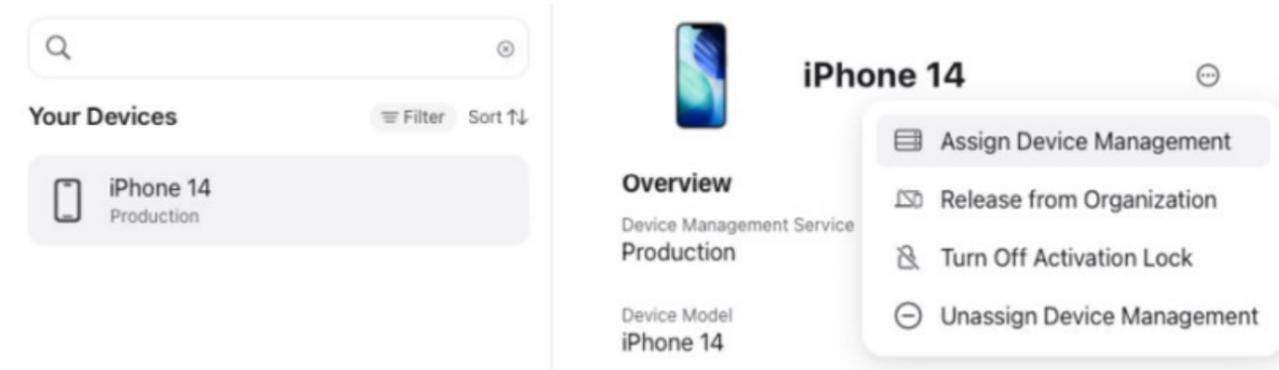
04

Reassign Devices to new MDM in ABM

Now that we've laid the groundwork in our new MDM, we're ready to migrate! Thanks to the new Apple update, this is now the easiest part of the process. Here's what you need to do:

1. In ABM/ASM, navigate to Devices and select the target devices.
2. Use the "Assign Device Management" option.
3. Select the Resolve MDM server from the Device Management Service drop-down list.
4. Set the Enrollment Deadline:
 - **Set a Deadline:** This triggers the persistent "Enrollment Required" notification sequence on the user's device.
 - **No Deadline:** The user will not receive a notification and must initiate enrollment manually from the device's Settings app.

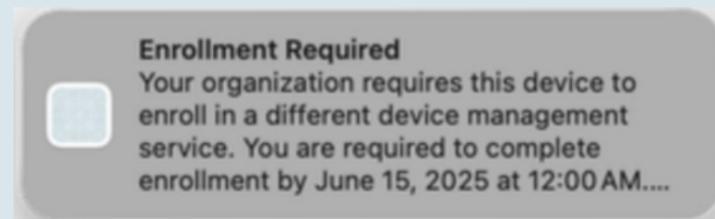
At this point the end user will receive a notification on their device informing them about the update and prompting them to complete enrollment.



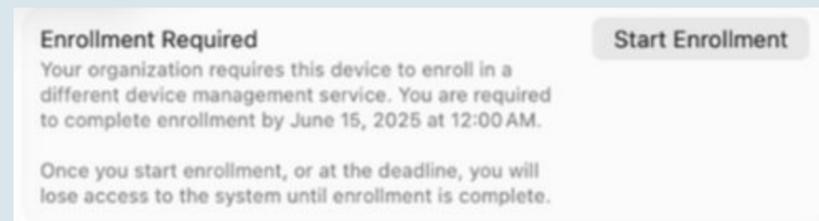
End User View

The process for end users is fairly straightforward. If the user doesn't initiate enrollment before the admin set enrollment deadline, an enforced migration occurs, which results in a non-dismissible and full-screen prompt that must be completed by the user before using the device. Make sure that you've communicated with them in advance to help make this process smoother.

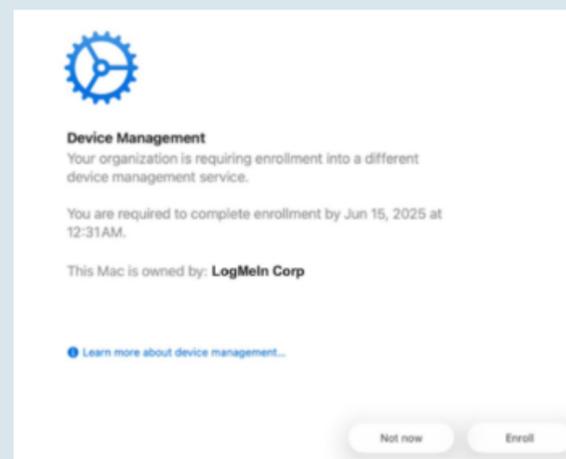
For Macs



1. Click on the **Enrollment Required** notification.



2. Select **Start Enrollment** on the **Enrollment Required** prompt

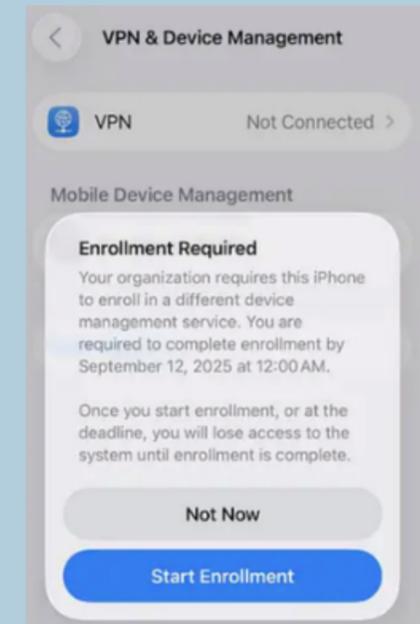


3. On the **Device Management** screen, select **Enroll**.

4. They may then be required to enter their username and password to complete the process

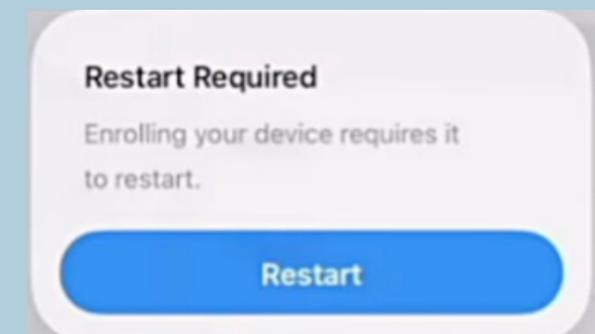
For iPhones and iPads

1. Click on the view **Enrollment Required** notification



2. Click **"Start Enrollment"**

3. Click **Restart** to restart the device

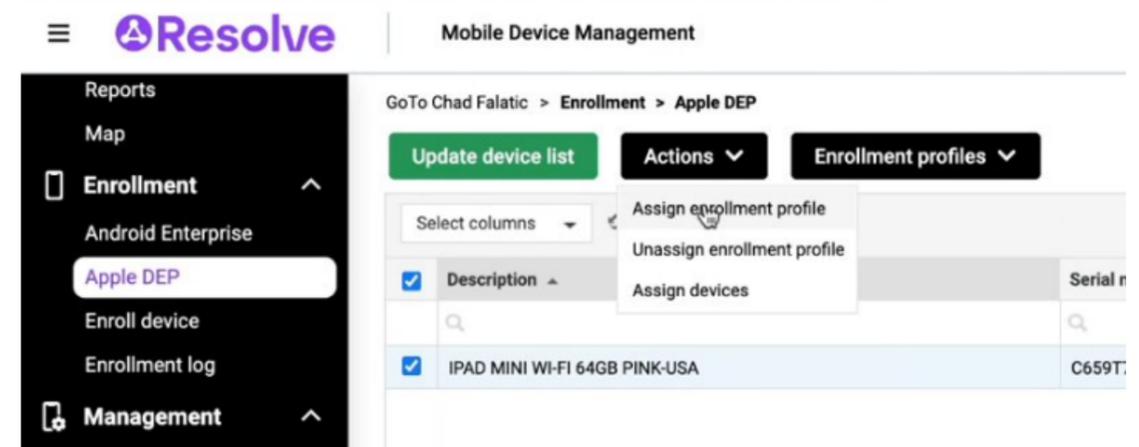


05

Assign Enrollment Profiles & Tags

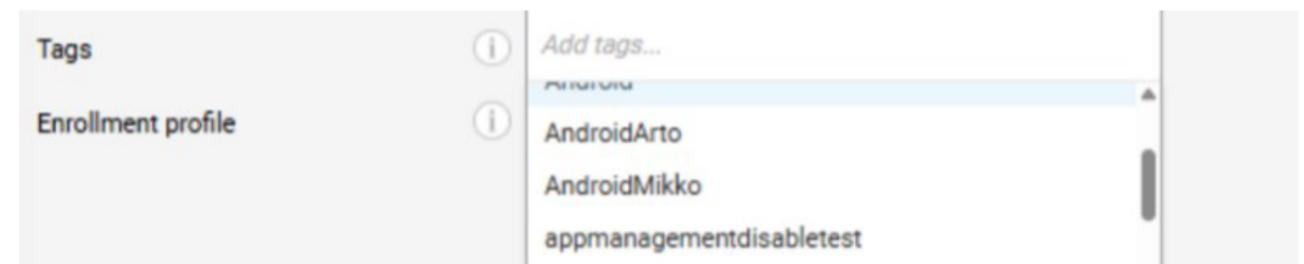
To confirm the devices have migrated successfully, navigate back to Resolve and in the Apple DEP tab in Resolve, click “Update Device List”. You should now see all devices you have migrated.

Now that the migration has been initiated, you can assign enrollment profiles and tags to your devices in order to ensure they have all the necessary configurations and applications from the moment they're enrolled. This helps reduce any downtime and make the process as seamless as possible.



If an Enrollment Profile was set to default, it will be applied automatically. If they were set to Manual, you would now assign the Enrollment Profile.

When assigning the Profile, you can also designate any tags you'd like to apply to the device(s). These will be used to designate which Business Policy to apply to the device. If you checked the “add default tag” box when creating the enrollment profile, the “dep” tag will already be added automatically.



06

Track Enrollment Progress

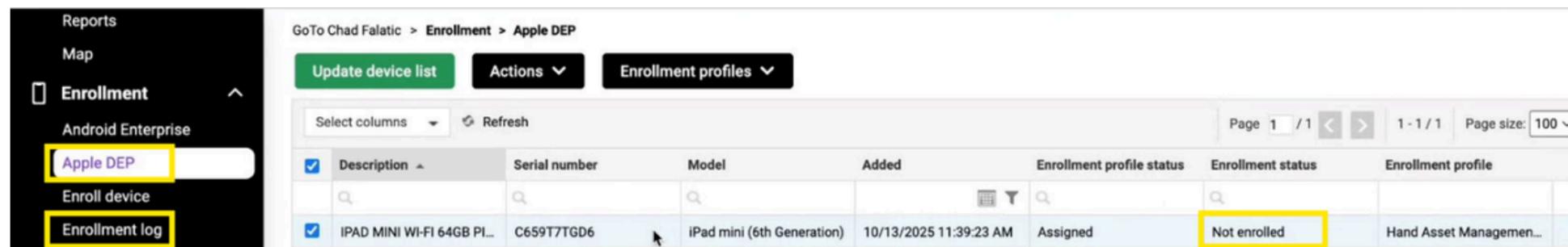
Now, all that's left to do is wait for your end users to complete the migration steps.

Remember that if you are using Volume Purchased (VPP) apps, once you've set up VPP on your new MDM, you have 30 days to migrate devices before your old MDM loses access to the VPP licenses and cannot manage or revoke assigned apps anymore. This means that the apps may stop working, since they will no longer register as having a license. This may even happen before 30 days if the app developer performs a license check.

For this reason, it is **very important** that you have communicated to your end users what action is needed from them, especially if you did not set a deadline, and that you carefully monitor progress.

You can track progress in Resolve MDM in 2 places:

- Enrollment > Enrollment log. Check the Status column.
- Enrollment > Apple DEP. Check the Enrollment status column.



The screenshot shows the 'Enrollment > Apple DEP' page in the Resolve MDM interface. The left sidebar has 'Enrollment' selected, with 'Apple DEP' and 'Enrollment log' highlighted. The main content area shows a table with columns: Description, Serial number, Model, Added, Enrollment profile status, Enrollment status, and Enrollment profile. A single device is listed with the status 'Not enrolled' highlighted in yellow.

Description	Serial number	Model	Added	Enrollment profile status	Enrollment status	Enrollment profile
IPAD MINI WI-FI 64GB PL...	C659T7TGD6	iPad mini (6th Generation)	10/13/2025 11:39:23 AM	Assigned	Not enrolled	Hand Asset Managemen...

07

Ensure everything has migrated successfully

Once your end users complete the enrollment steps, your devices should be successfully enrolled.

If you created, enabled and assigned Business Policies, all Configuration Profiles, Applications and Certificates should be deployed automatically once the user completes enrollment.

You can track the status of the Business Policy deployment from the Business Policy Page.

	Product name	Marketing name	Software version	User	Last reported	Ownership	Lease/warranty end date	Tags	Management type
<input type="checkbox"/>	Apple iPad14,1 M...	Apple iPad mini 6...	iOS 26.0	Falatic Chad	9/24/2025 8:34:1...	Purchased			Supervised
<input type="checkbox"/>	Apple iPhone14,4...	Apple iPhone 13 ...	iOS 26.0.1	Falatic Chad	10/21/2025 1:34:...	Leased		personal lockdown	Supervised
<input type="checkbox"/>	Apple MacBookP...		macOS 26.0.1	Falatic Chad	10/21/2025 2:36:...	Purchased		Android Tablets, ...	Client + MDM
<input type="checkbox"/>	Google Pixel 2	Google Pixel 2	Android 11	Falatic Chad	3/22/2024 2:46:0...	Purchased		Android Tablets, ...	Fully managed
<input type="checkbox"/>	Microsoft Corpor...		Windows 10 Ente...	Falatic Chad	10/1/2025 9:30:4...	Purchased		Android Tablets, ...	Client + MDM
<input type="checkbox"/>	samsung SM-X800	samsung Galaxy ...	Android 14	Falatic Chad	5/22/2025 11:53:...	Purchased		Device owner, Ou...	Fully managed
<input type="checkbox"/>	samsung SM-X800	samsung Galaxy ...	Android 14	Falatic Chad	11/13/2024 2:04:...	Purchased		Outlook Users	Work profile

Note: You can deploy individual Configuration Profiles, Applications and Certificates to individual devices from this page at any time.

Confirm all applications and profiles have been applied successfully, and all migrated devices are showing up. It may help to refer back to your documentation from Step 1 for this.

If everything looks good, then congratulations! You've just mastered the MDM migration. If this was phase 1 of the rollout, you can now move on to migrating the next round of devices. But first, take a moment to pat yourself on the back. The hardest part is over!

Simplifying Device Management Is Now Easier Than Ever

MDM Migrations are no small feat, but thanks to Apple's update to ABM, they've gotten all the more easier. And now that you've learned the M.I.G.R.A.T.E framework, you are well equipped to take the first step towards a simplified, more cost effective MDM experience.

If you've been feeling stuck with your fragmented, expensive or overly complicated MDM, now is the perfect time to simplify your life by switching to Resolve.

LogMeIn
Resolve



LogMeIn

Resolve

Easy, all-in-one IT management and support solution helping IT teams do more with less.

Powerful MDM

Manage Android, Apple, and Windows devices efficiently from a single intuitive console, powered by Miradore

Unified Endpoint Management

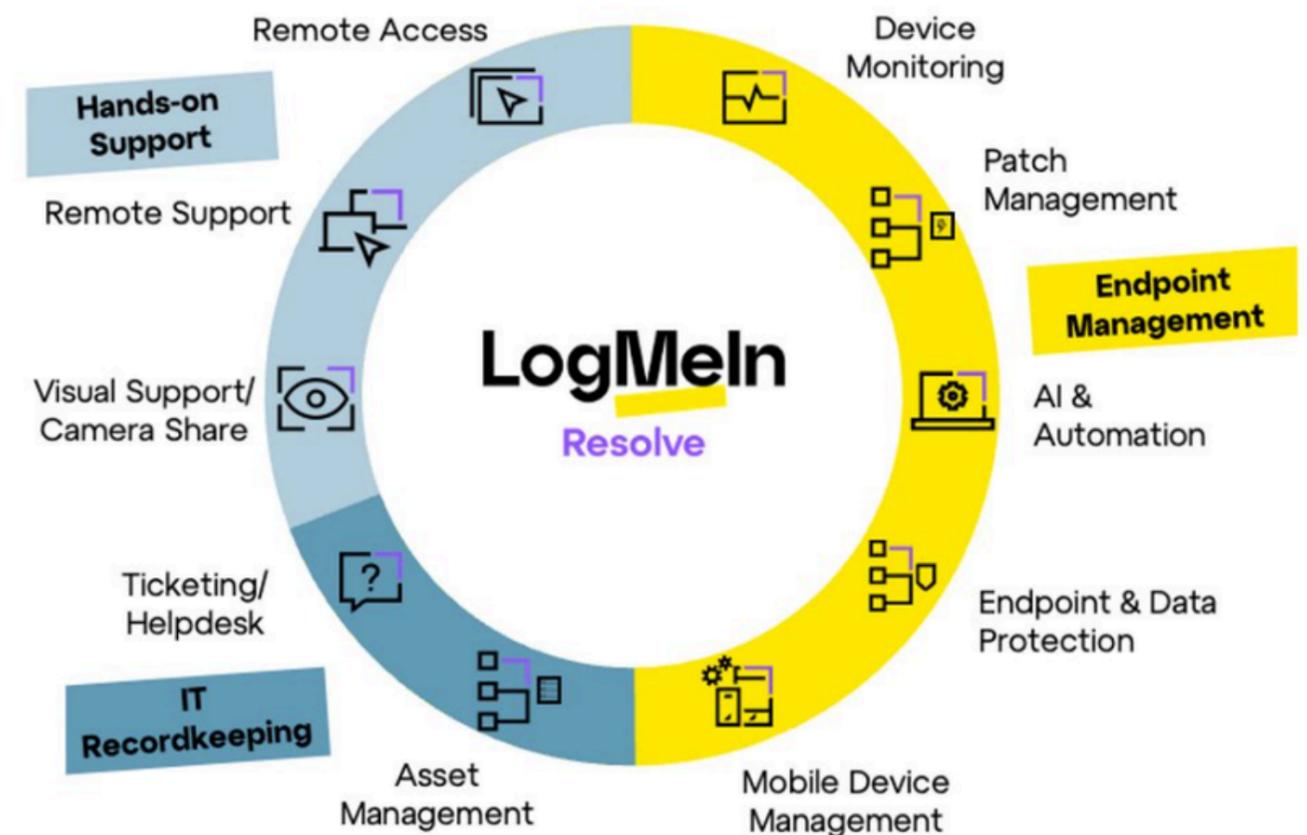
Protect, manage, and remotely access mobile devices and desktops with monitoring, patching, and automation

All-in-one IT

Go beyond device management with integrated ticketing, asset management, data protection, knowledge management, and more—in one, easy solution.

Simplified workflows

Save time with a single login and unified interface for every admin task – from provisioning to billing.





Ready to modernize your MDM strategy?

LogMeIn Resolve provides a powerful, intuitive platform to take full advantage of Apple's new capabilities.

[Get a demo](#)