

MDM Migration Guide



ninjaOne®

Reasons to upgrade include:

On-prem solution doesn't scale with your needs

You're using multiple tools to manage Android, Apple, and Windows devices

Lack of visibility into all mobile devices across the organization



Introduction

Congratulations! You've made the decision to migrate off your legacy mobile device management (MDM) solution. With effective MDM now a critical part of comprehensive endpoint management, if your legacy MDM solution is falling behind, it's time to migrate to a fully cloud-based MDM tool that delivers better visibility and control, additional functionality, and compatibility with both Android and Apple devices.

Upgrading your MDM tool is not a project to be undertaken lightly. It requires careful planning, thorough documentation, and a methodical approach to ensure minimal disruption to your organization's day-to-day operations and device management. This guide includes steps from assessing your environment, to planning

and preparation, from implementation to documentation. You'll learn how to ensure your devices are accounted for, the data on them is protected, and device and infrastructure downtime is minimal, so your end users can remain productive during and after the migration.

STEP 1

Assess your current MDM environment

The first step in any platform migration is assessment. By assessing the current state of your MDM environment, you're gaining an objective evaluation of the shortcomings of your current tool. In addition to helping determine your upgrade needs, you'll use this assessment report to compare against your post-migration report.



Step 1. Assess your current MDM environment *(continued)*

Inventory your existing managed devices so that you know the number and type of devices on your network. This is critical so that when your migration is complete, you can verify that all devices have been migrated and will continue to work as expected post-migration. Your detailed device inventory spreadsheet should include:

- Total number of devices
- Device type and platform – Android, iOS, iPadOS, or macOS
- Ownership status – e.g., company-owned or employee-owned (BYOD)
- Device enrollment types – e.g., supervised or unsupervised
- Any devices that may require special handling during the migration
- Current management method
- Age of devices in inventory. Migration is the perfect time to replace aging hardware. This is an assessment only you and your team can make.

In your assessment report, carefully document specific challenges present in your current device management method.

- How effective is the platform’s app management?
- How easy or difficult is it to set up device restrictions and security controls?
- What gaps are there related to visibility into and control of your mobile devices?
- Is the reporting on device performance and uptime sufficient for your team to effectively manage them?

Evaluate your migration requirements to ensure device enrollment, app deployment, policy setup and management are understood and planned appropriately. A migration is the perfect time to adopt Apple Business or School Manager if you’re not using it already. For your Android devices, be sure you have a plan for integrating Android Enterprise. Consider what cross-platform support looks like for your new MDM solution.

STEP 2

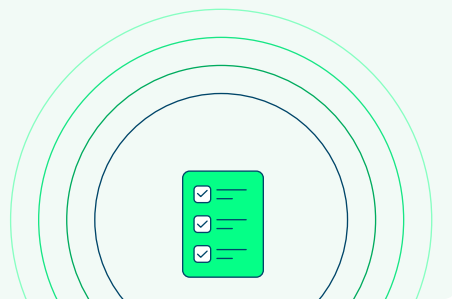
Preparing for migration

Now that you've finished your assessment, it's time to create your pre-migration checklist. This checklist will document the steps needed to complete your migration, keep you on track, and get the new solution operational with minimal disruption to end users.



Preparing for migration.

What should your checklist include?



Step 2. Preparing for migration *(continued)*

Your checklist should include:

- The device and user inventory created in Step 1
- Network and infrastructure considerations:
 - Accounting for device authentication and integration into Apple Business or School Manager or Android Enterprise
 - Device enrollment options and support for company-owned or BYOD devices
 - VPN settings, device restrictions, app management
 - Security controls
- Compliance and security requirement verification
- Backup and data preservation strategies
- Migration workflows, including testing and documentation of these workflows (more on that to come later)
- Technician training
- Communication plans for before, during, and after the migration
 - You'll need one set of communications for the techs performing the migration and another set of communications for end users
- Control group rollout
- Contingency plan in case one or more elements of the migration fail
- Goals and KPIs for the migration and the first 30 days after migration

STEP 3

Migration planning

At this point, you're ready to create your detailed migration strategy using the checklist you created in the previous step. It's a good idea to plan for a phased migration approach, with a small control group being migrated first, then prioritizing devices in a way that makes sense for your organization. This could mean you migrate less critical devices first so that you work out any complications in your process before turning your attention to the devices critical to your day-to-day operations.



Step 3. Migration planning *(continued)*

For the control group rollout, identify a group of power users or use your internal IT team. You'll run the migration on their devices only, validate that the new MDM solution performs well, works as expected, and users retain access to any and all services. Correct any errors in the migration with this group before moving on to full migration planning and implementation.

Communication with and training for technicians who will be involved in the migration is vital. Plan who will be trained on which aspects of the migration and communicate this to all the techs involved. Include a subject matter expert or point of contact for the various stages of the migration. In a larger organization, this could be a different person for each stage or group of devices being migrated with a single top-level point of contact for each of these tiered contacts to coordinate communications. In smaller organizations, a single point of contact for status updates may be sufficient. Note: Your communications and training plans will be unique to your situation.

Also include a communication plan for end users. Your communication plan should include:

- Expected start and completion dates

- Tip: If possible, plan your migration during a low-activity period to minimize disruptions.

- What end users need to do to prepare
- What end users can expect for each phase
- Device enrollment options for end users
- How mobile device access may change with the new solution
- Who to contact with questions or problems during the migration

In your planning, include time at the beginning for a system backup to ensure you don't lose any data should a problem arise during the migration. Include rollback and contingency planning as well, so that you can restore your system to its previous state if needed. Keep in mind, you will need to un-enroll your devices and re-enroll them if, during the migration, you experience a system failure or other problem that requires a system restore.

Plan time for testing the new solution on representative groups of devices as the migration proceeds. If you roll out the new solution in phases, test at the end of each phase and address any issues that surface before moving to the next phase.

STEP 4

Installation and device configurations

1. Once you've installed the new MDM, set up the configurations in the new MDM platform to match your current/previous MDM or to match what you want your new full state to be.
2. Migrate your control group to the new platform. Ensure the end state for the control group is as expected. Correct problems with the process that you discover during this control group migration.
3. Migrate your full set of users.



STEP 5

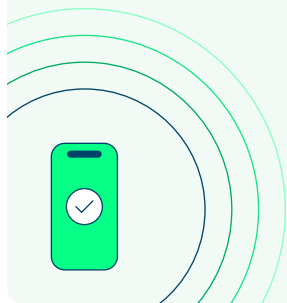
Device unenrollment/ enrollment

Because mobile devices can only be enrolled in one MDM solution at a time, you'll need to unenroll your devices from the previous solution first and then enroll them on the new MDM solution. As with testing and migration, this should be done for your control group first so that if you encounter any issues, they don't affect your entire fleet of mobile devices.



Device enrollment options:

- Automated enrollment
- User-initiated enrollment



Step 5. Device unenrollment/enrollment *(continued)*

Once you've unenrolled your devices from the old solution and your new MDM solution has been installed, it's time to enroll your network's mobile devices onto the new platform.

There are a number of options to complete device enrollment.

- **Automated enrollment:** On Apple devices this is done via Automated Device Enrollment with Apple Business or School Manager. On Android, you can use zero-touch or vendor-managed platforms like Knox Mobile Enrollment, Stagenow, etc.
- **User-initiated enrollment:** Allow employees to easily register their device by scanning a QR code or side loading a mobile configuration file.

Once you've enrolled your devices onto the new solution, you'll want to ensure that critical policy and configuration management settings have been migrated accurately. This ensures security policies continue in force uninterrupted, and app licenses and distribution settings are preserved and carried over to the new MDM solution.

Now that you've installed the new MDM solution, enrolled all your devices, tested to make sure the new solution is performing as expected, and unenrolled the devices from the old solution, it's time to uninstall the old MDM solution. Once you've done that, the technical steps of your migration are complete.

STEP 6

User experience and communications

We mentioned in the migration planning step to ensure you have a communication plan for end users. If your end users understand what to expect, they'll take the migration in stride. For those who will enroll their mobile devices themselves, you should provide a self-service enrollment guide that outlines the steps they will need to follow and includes a technical contact on the migration team who can answer any questions the end user may have during and after self-enrollment.

If your IT team is performing the mobile device enrollments, you should provide a guide showing them what screens they will see, any buttons they may need to press to complete the migration, and how they'll know the migration is complete. The exact steps will vary depending on each organization's processes. But this gives a general idea of what to communicate to end users.



STEP 7

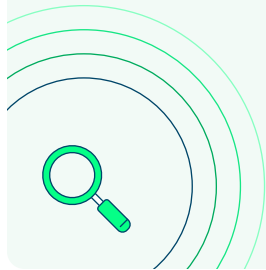
Post-migration optimization and reporting

You can breathe a sigh of relief! Your MDM migration is complete. The software is updated, your Android and Apple devices have been unenrolled from the old solution and enrolled in the new solution. Now, you'll need to fine tune the new MDM tool and document migration process wins and lessons learned. Ongoing performance monitoring is important to ensure your new MDM solution continues to provide the visibility, control, and device management you need.



Post-migration optimization and reporting

Learn more about performance monitoring.



Step 7: Post-migration optimization and reporting *(continued)*

Part of the fine tuning includes ensuring that the new MDM configuration matches the previous configuration as closely as possible. If configurations between the old and new MDM platforms are significantly different, the user experience might look different to the end user and cause confusion. Intentional changes should be documented by the migration team so the end users know what to expect. For example, if an app changed during migration, document the change and instruct the users to use the new app.

Additionally, you should compare your pre-migration assessment with your post-migration

report to ensure you have addressed all the concerns highlighted before beginning the migration. Listen to your end users to ensure their apps are functioning as expected post-migration. If you hear, “I can’t find X app” or “I can’t do XYZ anymore after the migration,” your team should listen to the feedback and determine if the change in behavior is due to a configuration difference between the two MDMs. If so, these changes should be investigated and remediated as needed. If not, work with the end user to help them understand the new functionality.

Final thoughts

By following the steps outlined in this guide, you can plan and execute a successful MDM solution migration. Yes, it's a big undertaking but with careful attention to detail you will succeed.

- **Preparation is critical:** Thorough planning and testing before the migration significantly reduces risks and unexpected downtime.
- **Communication:** Regular communication with technicians, users, and stakeholders ensures user buy-in and smooth transitions.
- **Security and compliance:** Uphold data security and adhere to compliance requirements throughout the migration process.
- **Process documentation:** Detailed documentation enables data-driven decision-making throughout all phases and sets a baseline for future upgrades or migrations.
- **Continuous improvement:** Use lessons learned and stakeholder feedback to iteratively improve processes.

NinjaOne MDM

Mobile devices drive efficiency by enabling employees to work anytime and anywhere. However, ineffective mobile device management can lead to technician and user frustration. For end users, the inability to access applications and resources required to support specific workflows or delays in resolving technical issues can impact their productivity. For technicians, an inefficient or ineffective MDM solution can lead to more trouble tickets, increase the organization's attack surface, and take the IT team away from strategic business projects.

NinjaOne MDM helps MSPs and IT teams reduce cost and complexity by enabling management of Android and Apple mobile devices alongside their Windows, Mac, Linux, VMs and networking devices, all within the intuitive NinjaOne platform.

[Learn more](#)

About NinjaOne

NinjaOne, the automated endpoint management platform, delivers visibility, security, and control over all endpoints for more than 30,000 customers in 130+ countries.

The cloud-native NinjaOne platform simplifies endpoint management, patching, and visibility for environments at any scale. It is proven to increase productivity, reduce security risk, and lower costs.

NinjaOne is obsessed with customer success and provides free and unlimited onboarding, training, and support.

[Try NinjaOne free](#)

ninjaOne[®]