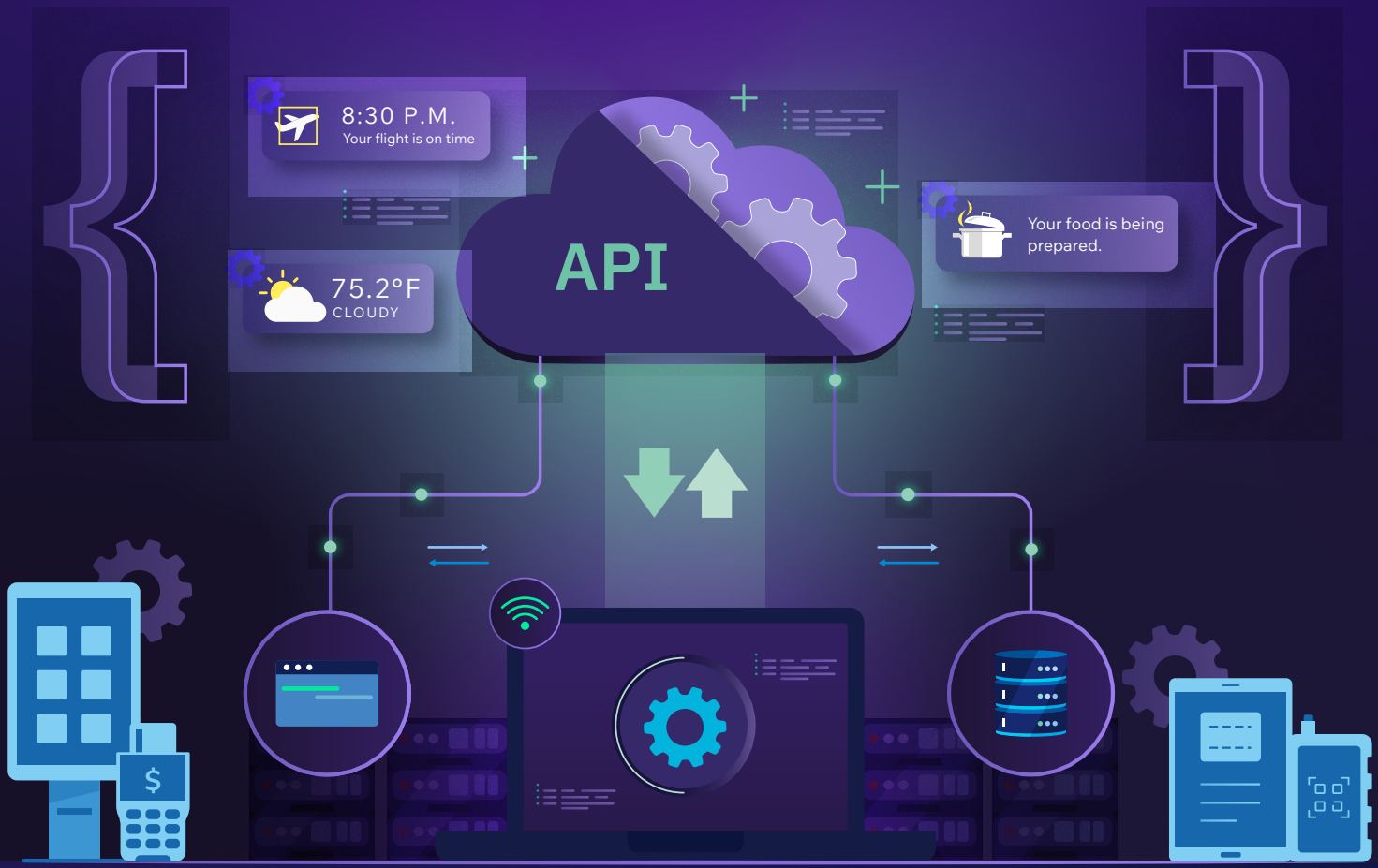
esper

# The MDM Migration Survival Guide:

## How To Avoid Risks and Unlock ROI with Confidence



# Table of Contents

# Who Should Read This Guide

## Everyone.
## Everyone should read this guide.
## Just Kidding.

We designed this guide to be a comprehensive companion for technical folks considering the switch from one MDM to another. While it aims to provide sound, thorough advice, it's not a technical manual, per se. Within its pages, you'll find a thoughtful walkthrough tailored to your specific goals. From assessing you current MDM, understanding associated risk with migration, and choosing the right platform to hardware considerations, preparation steps, and more, this guide covers it all.

---

Anyone interested in the subject will likely learn something new (or perhaps something they hadn't previously considered). Specifically, this guide is ideal for:

### IT Admins:

If keeping systems running smoothly, securely, and within budget is your bag, look no further. Think of it as a roadmap to help you successfully navigate MDM migration with minimal disruption and maximum efficiency.

### System Architects:

The stability of the infrastructure is on your back, and you need to ensure it's stable, secure, and adaptable. We get you. This guide dives into the complexities of MDM migration, offering insights and actionable steps into the strategic planning required for a smooth MDM migration.

### Technical Decision Makers:

For you, it's all about balancing innovation with risk management. This guide provides a structured framework to help you evaluate and implement a solution that fits your immediate needs and long-term goals.

### Devs:

Your role in MDM implementation, app support, security, and device functionality cannot be overstated. This guide offers detailed info on MDM considerations and testing, from provisioning to deployment.

### Fleet Managers:

Embedded in the day-to-day operations of device management, maintaining fleet functionality depends on you. This guide equips you with a holistic understanding of migration process, helping you keep devices secure, compliant, and performing smoothly through every stage.

**Grab your hard hat and lunch pail, friends — let's get to work.**

---

# Introduction

MDM (Mobile Device Management) migration is the process of transferring devices, policies, and configurations from one device management platform to another. While this sounds straightforward, it's a complex endeavor that requires strategic planning to minimize disruptions and maximize the benefits of a more capable system.

## Why Consider Migration?

Organizations may reach a point where their current MDM solution no longer meets their needs. Here are some of the most common reasons migration becomes a necessity:

### Solution mismatch:

Your operational or technical requirements don't align with the current platform. Perhaps it's missing key features, or you've outgrown its capabilities.

### Scalability and new use cases:

As your organization grows, so does your device fleet. Adding new device types or scaling operations may expose limitations in your current MDM.

### Vendor lock-in:

If your MDM was bundled with hardware, you might feel stuck with a limited solution. Moving to a more versatile provider can unlock flexibility and efficiency.

### Compliance needs:

Regulatory requirements are evolving, and not all MDM solutions are equipped to handle the stringent demands of highly regulated industries like healthcare or finance.

### Future-proofing:

Upgrading to a modern MDM ensures you're prepared for emerging technologies and can maintain competitive advantages.

A successful migration is about more than just switching platforms — it's an opportunity to enhance security, streamline operations, and better align device management with organizational goals.

## Risks of Poor Migration

Once you've decided that migration is the right choice for you, it's not necessarily wise to jump right into the "search and evaluate" stage. To avoid potential setbacks, it's important to understand the risks associated with a poor or improper migration.

### Operational disruptions:

Mishandling an MDM migration can interrupt business-critical operations. The scale of that disruption ranges from minor inconvenience to total system failure, neither of which is ideal (though one is clearly worse than the other).

### Security vulnerabilities:

Security is a critical component of any device fleet, requiring constant vigilance to stay ahead of the latest threats. When migration is rushed or configurations aren't meticulously managed, it can lead to misconfiguration, outdated security policies, or insecure access points. These gaps open the door to new vulnerabilities, exposing devices and data to potential risks.

**Compliance failure:**
Maintaining compliance across your device fleet is essential, especially in regulated industries. During a poorly managed MDM migration, critical compliance settings or policies may be overlooked, or data could be mishandled, resulting in breaches of industry standards. This may incur costly fines and can compromise your organization's reputation and trustworthiness.

**User friction:**
A suboptimal MDM migration can create difficulties for IT managers, end users, customers, and others who rely on the devices. Frustrating user experience from misconfigured devices, missing apps, or inconsistent device settings disrupts workflows, impacts productivity, erodes user trust, and increases support demands.

The risks go far beyond this simple list, but you get the gist. Successfully migrating an entire fleet to a different MDM is a meticulous process, and rushing, improper handling, and skipping steps all put your device fleet and business at risk.

---

## Migration Options

Once you've decided on migration (and committed to doing it the right way), you have a few options for approaching the process. Each has its own pros and cons, and there is some overlap among them.

### Total Flip

The most straightforward approach is to move directly from one MDM to another as quickly and seamlessly as possible. And for smaller device fleets, that might work. Although the process still requires detailed planning and precise execution, switching in one fell swoop is possible.

However, this is usually less practical for larger device fleets. The bigger and more dynamic the fleet, the more challenging a quick migration becomes, which is where the next two options come into play.

### Gradual Migration

For large, complex device fleets, gradual migration is typically a better approach. This method involves onboarding a second MDM and running it alongside your existing provider, allowing for a smooth, extended transition. The migration can be broken down by device type, location, or other logical groupings to best fit the organization's needs.

In this case, the adage "It's a marathon, not a sprint" applies. Gradual migration may take months—or even years—to fully execute, depending on the fleet's size and complexity.

### Running Dual MDMs

While likely the least appealing option to many, running two MDMs can sometimes be necessary. This approach is situational but useful when managing distinct types of devices with different needs. For example, if you have a fleet of COPE (Corporate Owned, Personally Enabled) laptops, smartphones, or tablets for employee use and a fleet of customer-facing digital kiosks, in-store point of sale systems, or digital signage. These different use cases might require separate MDM providers for optimal management.

Choosing to migrate to a new MDM is a major decision that demands thorough preparation and strategic planning. Understanding the potential reasons, risks, and methods involved in migration helps lay a strong foundation for a successful transition. Whether your goal is to improve security, ensure compliance, or simply scale with ease, each decision you make in this process will impact the efficiency and stability of your entire device fleet.

With the groundwork now laid, it's time to dive into the essential first step of the journey: assessing the current MDM. In the next chapter, we'll guide you through evaluating your current setup, identifying gaps and needs, and determining how well it aligns with your goals for the future. This assessment will set a clear path forward, helping you make the most informed choices for a seamless migration.

# Chapter 1:

# Assessing the Current MDM Environment

Alright, let's kick things off with a little MDM reality check. Migrating to a new MDM solution isn't exactly what we'd call "easy," but with the right game plan, it doesn't have to be a nightmare either. Think of it like moving to a new house — before you start packing boxes, you need to know what you're keeping and what's going to the donation bin.

## Device Inventory and Types: Know Your Subjects

First things first, take a roll call on your hardware. What devices are currently under top priority? Are we talking smartphones, tablets, rugged handhelds, point of sale systems, digital kiosks, or a mix-and-match grab bag of some kind? Knowing the types of device offerings in your fleet is crucial, as different platforms and operating systems might have unique requirements for enrollment, management, and security.

This is also a good time to consider your cross-platform needs. Are you all in on one platform, or do you use different platforms for different needs? If you're juggling iOS, Android, Windows, and who knows what else, keep all that in mind as you assess your fleet and MDM needs.

---

## Current MDM Capabilities: What's Working, What's Not

Next, dig into your current MDM setup. What features do you use and love? What causes headaches or holds you back? Understanding an existing MDM's strengths and weaknesses will help you identify must-have features and potential dealbreakers in a new solution. More than anything, knowing what features and functionality you absolutely can't live without is critical here. Similarly, that punch list of "nice to have" features will come in clutch as you explore all the offerings out there in the world.

The goal here is to create a "current state assessment" of your MDM, highlighting what's working and what's causing friction. This way, when it's time to evaluate new providers, you have a clear roadmap of must-haves and nice-to-haves.

---

## Deep Fleet Evaluation: Future-Proofing Your MDM

This is also a good time to take a hard look at your fleet at the hardware level and consider the future. This will help you conceptualize how your hardware will evolve over the next few years and plan your MDM strategy around those changes.

Continued

# Assessing the Current MDM Environment

Every device has a shelf life, and those lifespans need to be accounted for. This is where you'll evaluate your fleet based on performance, security updates, and expected end-of-life (EOL) timelines. Devices nearing EOL might be better candidates for replacement rather than migration, so this step can help streamline your future hardware roadmap and minimize complications during the MDM switch. Chapter three will explore the hardware refresh cycle in more detail (but please don't skip one and two!).

As you assess, also keep in mind any new hardware or device types on the horizon. If you're planning to add rugged tablets, digital kiosks, or IoT sensors, make sure these will be compatible with the new MDM. Forward-thinking is key here — you don't want to be in a position where you've chosen an MDM that doesn't support the devices that are critical to your future operations.

---

## Stakeholder Requirements: Keeping Everyone Happy

MDM migrations aren't just an IT project — they impact the entire organization. Talk to IT admins, end-users, security teams, and even the C-suite to gather their requirements and concerns. This will help you choose a solution that meets everyone's needs and avoids unpleasant surprises down the road.
For example:

- *IT Teams may need improved automation, better security controls, or lower maintenance overhead.*
- *Operations might look for increased visibility into device status or simplified compliance reporting.*
- *End Users want seamless, frustration-free experiences with minimal disruption.*

Just make sure to keep the bigger picture in mind here. You'll likely have more success if you loop in essential stakeholders earlier in the process.

---

**Remember, a successful MDM migration starts with a thorough assessment of your current environment.**

**By taking the time to understand your devices, capabilities, future plans, and stakeholder needs, you'll be well on your way to choosing a new MDM solution that's a perfect fit.**

# Chapter 2: Choosing the Right MDM

Alright, let's dive into the nitty-gritty of picking the best MDM solution for your organization. We're going to get a little technical here, but we'll keep it pretty high-level — informative without being overwhelming. So grab your favorite caffeinated beverage and settle in — or non-caffeinated, if that's your thing. No judgment here.

Choosing the right MDM for your enterprise is no small task — it's about balancing technical requirements, operational goals, and future scalability. For many organizations, it might make sense to leverage trusted partners who bring expertise and industry insight to the table.

## Technical Requirements: The Backbone of Your MDM

Let's kick things off with some tech talk. The foundation on which your MDM house is built is within your existing systems, so it makes sense to start there. We're talking seamless integration with your directory services, identity providers, and other management tools. Nobody wants an unwieldy Frankenstein's monster of a tech stack, right?

As you start to evaluate MDM solutions, ask yourself:

- How well does this MDM work with our existing tech stack?
- Does it integrate with the apps and systems we use daily?

It might not hurt to take a detailed inventory of all the tools and services you rely on — go deep in the stack because it's all too easy to forget or overlook one! If you're uncertain about specific requirements, consider consulting with a technical or implementation partner. They can help assess your IT landscape and provide recommendations tailored to your needs. But with the right resources and a clear roadmap, this is a step your IT team can handle confidently.

## Cross-Platform Capabilities: The MDM Juggling Act

Remember the good ol' days when managing a fleet meant handling one device type or OS? Well, not anymore. Today's enterprises juggle iOS, Android, Linux, Windows, and everything in between, so your MDM needs to be a master juggler.

And that goes without even mentioning scalability. If your organization is looking to grow (as we hope it is!), your MDM needs to keep up without breaking a sweat. Remember, the goal here is to simplify and streamline — not make more work for your IT team.

Continued

# Choosing the Right MDM

The best approach here is to think about cross-platform support and scalability from the top down. If you're constantly switching between Apple devices with ABM (Apple Business Manager) and Android hardware with or without GMS (Google Mobile Services), an MDM equipped to comfortably support both is critical. Keeping the future state of your device fleet in mind will also make life easier for you. If your fleet spans highly diverse devices or includes legacy systems, a partner can validate compatibility and guide you on platform-specific setups like ABM enrollment or Samsung Knox.

When evaluating MDMs, here are a few considerations:

- Does it handle cross-platform configurations seamlessly?
- Can it enforce policies uniformly across different operating systems?
- Can I manage my entire fleet from a single pane of glass?
- What does our device fleet look like for the next year? Or the next five?

A little extra work on the front end will save you a lot of headaches in the long run — especially when it comes to cross-platform capabilities and scalability.

## Security and Compliance: The MDM Fort Knox

Let's be clear here: Security and compliance are at the core of everything you do. This is a top priority for businesses of all sizes — from SMBs to the biggest enterprises. That's why you need your MDM to be a fortress of protection.

When it comes to security, granular control over security policies is critical. This includes everything from device encryption and app management to remote wiping capabilities and password enforcement. Your MDM should reliably enable all of this while being flexible enough to meet the security needs of your entire fleet.

That goes without mentioning compliance, which is a whole 'nother can of worms. If your organization operates in a regulated industry (healthcare, finance), compliance is a hard requirement. The ideal MDM makes it easy to not only enforce compliance standards but also generate reports quickly and easily. Bonus points if it can also automate these reports — you just became the compliance officer's new best friend.

Continued

# Choosing the Right MDM

## Deployment and Automation: The MDM Autopilot

Who's ready to spend hours manually configuring devices?! Not you, that's who. Because you're reading this guide, you already understand that streamlined deployment tools are your secret weapons for efficiency. We're talking about saving your IT teams tons of time and frustration.

How, you ask? With the power of repeatable, automated deployments. Imagine it: you set up your desired device state once, then push it to any device or number of devices whenever you want. Suddenly, days worth of manual kitting is done in hours.

Automated, templatized provisioning options make deployments dead simple, regardless of the org size. An SMB with a handful of devices? No problem. An enterprise working with a 3PL partner to push out 10,000 new devices? Piece of cake.

But we can take this one step further: What if you could do all of this with zero human interaction (well, aside from taking the device out of the box and turning it on)? Yeah, it's possible. Touchless deployments aren't just a pipe dream — they're the future. So make sure to get an MDM that doesn't live in the past.

Bam — suddenly, your IT team can focus on more strategic initiatives (and maybe even take a coffee break).

## Support: The MDM Lifeline

No one wants to think about something going wrong, but let's be honest here: things go wrong. No matter how reliable your MDM is, you'll hit a snag now and then. Robust support is a critical component of getting the right MDM. Look for a vendor with a thorough knowledge base, dedicated enterprise support staff, and 24/7 assistance. Keep in mind that the level of support you want may require a different pricing tier, but if a crisis hits, you won't have to wait for an email reply.

## ROI and TCO: The MDM Moneymaker

Finally — and perhaps most critically — there's ROI (return on investment) and TCO (total cost of ownership). These might not be the first things on your mind when evaluating MDM providers, but this is the sort of long-term thinking that impacts the bottom line.

Continued

# Choosing the Right MDM

It's not just about the cost per device. You need to consider long-term expenses like maintenance, support, and upgrades. In other words, don't just look at the initial or upfront price tag — look closely at the overall financial impact. Do your homework and crunch those numbers!

- Factor in all costs: licensing, support, hardware integration, and ongoing maintenance.
- Compare time and resource savings against the cost of the platform.

Partners can help you find hidden savings through trade-in programs, bundled services, or bulk licensing discounts. They also reduce IT overhead by offering managed services, which could lower operational costs.

---

Choosing the right MDM takes careful consideration of your organization's unique needs and goals. But with the right approach, you can find an MDM solution that enhances your workforce, protects your data, and streamlines operations. With the right MDM, you're not just managing devices — you're supercharging the entire organization to work better, faster, and more securely.

Oooh, I just got chills!

---

### Continued Reading: The MDM Evaluation Toolkit

Choosing the right MDM is no small task, but the **Ultimate MDM Evaluation Toolkit** makes it manageable. From detailed comparison templates to must-ask vendor questions, this toolkit helps you cut through the noise and evaluate platforms with confidence. Stop second-guessing and start making informed decisions—your perfect MDM is just a few steps away.

**Download Now**

# Chapter 3: The Hardware Refresh Cycle

Let's be real: hardware doesn't live forever. Devices that once ran like the wind start to feel more like they're slogging through quicksand, and security updates eventually dry up. Neither of these scenarios is ideal for delivering exceptional device experiences for customers or employees, which ultimately leads to decreased productivity, decreased revenue, or worse — both.

That's why a well-planned hardware refresh cycle is a game-changer for organizations managing large fleets. In this chapter, we'll explore how to evaluate device lifespans, strategically plan refreshes, and optimize costs — all while keeping environmental impact in mind. Because, yes, even devices deserve a thoughtful send-off.

## Device Lifespans: The Ticking Clock

Before you plan a hardware refresh, you need to know when it's time to retire a device. Many factors go into making that call, so let's break it down.

### Performance and EOL/Manufacturer Support

Devices don't normally just fail overnight. Instead, all the metrics that matter — performance, battery life, etc. — gradually degrade. You know what we're talking about: apps take forever to open, battery life is half of what it used to be, and the device generally feels like a snail on a treadmill. Good telemetry data can give you a heads-up when devices are becoming more of a hindrance than a help. That, and you'll be hearing complaints. If you hear enough people talk about how a device is being sluggish or buggy, it's your cue to tune in and listen.

That's not the only consideration here — there's also manufacturer support. Most manufacturers put an EOL (End of Life) date for how long they plan to support the device with software updates and service. Once a device hits its EOL, it's like a ticking time bomb for security risks — no more security patches, no more OS updates, no more support. I'm sure you already see why that's a problem.

In case we need to say it explicitly, security updates are non-negotiable in today's world. Insecure devices are a liability to your network and company data — full stop. Knowing your hardware's EOL date lets you plan ahead and prepare for this kind of change.

---

## Planning Refresh Cycles: The Art of Timing

With your devices' EOL dates in mind and lifespans evaluated, it's time to map out a refresh strategy. This is your roadmap that balances operational efficiency, cost management, security, and future-proofing.

Continued

# The Hardware Refresh Cycle

## The Staggered Refresh

Imagine replacing every device in your fleet at once — chaos. Not only is that a logistical nightmare, but the costs stack quickly—especially for large fleets. That's why a staggered refresh is often the best approach. You'll spread updates and device replacements over time, which helps better manage costs and avoid situations where large numbers of devices become obsolete at the same time. This way, you ensure that part of your fleet is always running the latest hardware.

## Align Refreshes with MDM Migration

Here's where things start to get strategic. If you're already planning (or even considering) an MDM migration, it only makes good sense to align your hardware refreshes with it. This will not only make it easier to switch MDM providers but also simplify onboarding new hardware.

This affords another beneficial opportunity, too: working with your incoming MDM's partner network. Many device management providers have a robust network of reliable OEMs/ODMs, distributors, and solution providers that can supercharge the migration process. This can include deep discounts on hardware, bulk onboarding, streamlined provisioning, and more. Plus, you guarantee compatibility between the new MDM and your upgraded hardware. Win-win.

Solution providers can manage staggered refreshes for you, coordinating timelines with your MDM migration for maximum efficiency.

3PLs handle bulk provisioning, device enrollment, and policy configuration, ensuring that new devices are MDM-ready from day one.

They can even streamline remote flips, enabling seamless transitions to the new MDM platform without manual intervention.

Partner support doesn't just save time — it enhances ROI by reducing IT overhead and ensuring refresh cycles are optimized for long-term scalability.

## Hardware Flipping

Before we move into cost optimization (well, along those same lines), there's a potential solution beyond simply refreshing your hardware: flipping. With the right hardware, you can install a new operating system that breathes new life into existing devices. As you might expect, planning this sort of thing is pretty complex — What kind of hardware are you looking to flip? What OS do you plan on moving to? Will you build and maintain the new OS in-house or hire a third party to manage the load?

All of these (and many more) are considerations for flipping, and it's not the right choice for everyone. But in some situations, it's a great solution.

Continued

# The Hardware Refresh Cycle

## Cost Optimization and ROI: The Money Talk

Real talk: Buying new hardware is expensive. There's no way around it. But how costly it is depends on your strategy. Let's talk about dollars and sense.

### Considering TCO (Total Cost of Ownership)

When it comes to new hardware, you buy it, and you're done, right? Ha! Don't we wish. It's easy to focus on the upfront cost of a new device, but that's just the first piece of the puzzle. You have to consider the initial cost, ongoing maintenance, and eventual disposal costs — that's the TCO (Total Cost of Ownership). Think of TCO like budgeting for a road trip — you have to consider gas, food, and lodging, not just the price of the car.

Why are we talking about TCO? Because a piece of hardware with a more affordable price tag up front may seem like a good deal, but if you can't keep it running or it becomes obsolete quickly, it actually costs more in the long run (womp womp). On the opposite side of that coin, a more expensive device might seem like a poor investment on the front side, but if it offers several years of reliable service, it more than pays for itself.

---

### Maximizing ROI of Existing Hardware

Speaking of TCO, you should focus on squeezing every bit of value out of your existing hardware, dramatically improving TCO and ROI (Return on Investment). That might mean repurposing older devices to less resource-intensive tasks, like using old tablets for digital signage. It might also mean OS flipping, as we discussed earlier in this chapter.

Either way, the key is to find creative ways to extend the life of your hardware, maximizing ROI without compromising performance or security. It's like turning yesterday's leftovers into a delicious new meal!

Alternatively, many manufacturers offer trade-in programs that allow you to offset the cost of new devices by sending in your still-working hardware. Plus, this ensures responsible recycling of old hardware. Win-win.

Continued

# The Hardware Refresh Cycle

## Disposal and Environmental Impact: The Green Guardian

Speaking of responsible recycling, let's quickly touch on the environmental aspect of hardware management. It's not the most glamorous thing to consider, but neglecting it has consequences that might surprise you.

### Secure Disposal and Environmental Sustainability

Tossing old hardware in the trash isn't just environmentally irresponsible — it could also put your data at risk. Before saying goodbye to any device, you'll want to securely wipe all data. IT teams should have thorough documentation that covers best practices here, but at the very least, you should factory reset the device. You'll also want to work with certified e-waste disposal partners that follow industry standards for data destruction.

E-waste is a serious problem, but your organization can make a dramatic difference. Practicing environmentally friendly disposal options like recycling programs or refurb-and-donate initiatives go a long way in cutting back on the amount of e-waste generated, but also carry the added benefit of helping but devices in the hands of folks who might not otherwise have access to them!

Many companies already have sustainability goals, and your hardware refresh cycle is a perfect opportunity to contribute to those efforts.

---

**Refreshing hardware may not be the most thrilling part of your job, but it's critical to keeping your organization running smoothly and securely. By evaluating device lifespans, planning strategic refreshes, optimizing costs, and considering environmental impact, you'll manage your fleet more effectively and make a positive impact.**

**That's something we can all get behind.**

# Chapter 4: Preparing for Migration

Okay, we're making progress! You've evaluated your current MDM environment, chosen your new solution, and maybe even started dreaming about a world with fewer headaches. But before you jump headfirst into the migration itself, there's one more crucial step: preparation. Think of this phase as stretching before a marathon — skip it, and you're setting yourself up for a painful experience.

In this chapter, we'll unpack how to assess your incumbent MDM, set a realistic timeline, provide the necessary training, and mitigate risks. Ready? Let's get warmed up.

## Assessing the Incumbent MDM: What's the Situation?

Before you start packing your bags and moving to a new MDM, you need to know exactly what you're working with. Your incumbent MDM holds all the keys to your current device configuration, so it's critical to assess it thoroughly.

### Getting the Source Code and OTA Access

Start by confirming that you have access to all the configuration files, settings, and over-the-air (OTA) update capabilities managed by your current MDM. If you don't, now's the time to negotiate with your current provider. Some providers are more cooperative than others when you're leaving, so it's smart to anticipate any roadblocks and address them early.

Why does this matter? Because your new MDM will require this data to ensure a smooth transition. Without it, you might be stuck rebuilding policies and configurations from scratch — not fun.

### Data Backup

Backing up your data is non-negotiable — it's your safety net in case anything goes wrong during migration. Make sure to securely back up all device settings, configurations, and important data before making any changes. And don't forget about sensitive compliance-related data — losing that could land you in hot water.

💡 **Pro tip:** Test your backups before you start the migration. A backup that doesn't actually restore when you need it is as useful as an umbrella is a hailstorm.

Continued

# Preparing for Migration

## Setting a Timeline: Avoid the Rush Job

A successful migration isn't about speed — it's about doing it right. Setting a realistic timeline ensures you're not rushing critical steps, which can lead to mistakes, downtime, or angry stakeholders.

### Device Prioritization

Not all devices are created equal, and some are more critical to business operations than others. Start by categorizing your devices based on priority. For example:

- **Mission-critical devices** like point of sale systems and digital kiosks
- **Non-critical devices** like test devices and lesser used hardware

From there, you'll need to consider the best approach for which set of devices to start with. Each approach has its own pros and cons.

---

### Start with Non-Critical Devices

This safer and more common approach involves migrating less essential devices first, allowing you to test and refine your process.

| Pros: | Cons: |
| --- | --- |
| • Provides a low-stakes testing ground to identify and resolve issues.<br>• Reduces risk of major operational disruptions.<br>• Builds confidence and stakeholder trust through early successes. | • Delays migration of mission-critical devices that might benefit most from the new MDM.<br>• Requires patience, as operational impact comes later in the process. |

---

### Start with Mission-Critical Devices

This approach prioritizes high-value, operationally critical devices that are essential to daily workflows.

| Pros: | Cons: |
| --- | --- |
| • Immediate benefits for devices that impact business operations most.<br>• Resolves pressing issues with outdated or underperforming management systems. | • Higher stakes; any issues could disrupt critical operations.<br>• Limited room for error, as there's no opportunity to test the process first. |

Continued

# Preparing for Migration

## The Balanced Approach

A hybrid strategy can often provide the best of both worlds. Begin with a small subset of non-critical devices to test the migration, then tackle mission-critical devices in phases. This approach minimizes risk while delivering value where it's needed most.

## Stakeholder Communication

Migration isn't just an IT initiative — it's an organizational effort that touches nearly every department. Clear and consistent communication with stakeholders ensures alignment, minimizes surprises, and keeps everyone confident in the migration plan. Here's how to approach communication with key stakeholder groups:

### CTO/CIOs and Executive Leadership

Your CTO, CIO, or even the CEO will want to understand the strategic rationale for the migration. Frame updates in terms of organizational benefits:

- **Why it matters:** Highlight how the new MDM supports growth, security, and operational efficiency.
- **What's happening:** Provide high-level timelines and reassurance that risks are being mitigated.
- **How it aligns with business goals:** Tie the migration to broader strategic objectives, like scalability or digital transformation.

Keep updates concise and impact-focused. Leadership doesn't need the nitty-gritty but should feel confident in the plan and its outcomes.

### IT Teams

For IT stakeholders, transparency and detail are key. They're the ones configuring, troubleshooting, and ensuring the migration runs smoothly. Provide:

- **Regular updates:** Share progress reports, key milestones, and any potential roadblocks.
- **Technical details:** Ensure the team is clear on their roles and responsibilities during the migration.
- **Resources:** Equip them with guides, tools, and training to address issues as they arise.

### Operations and Compliance Teams

These teams are often overlooked in migration communication, but they play a critical role in maintaining workflows and regulatory alignment. Address their specific concerns

Continued

# Preparing for Migration

- **Impact on daily operations:** Clarify how the migration will affect productivity and timelines.
- **Compliance assurance:** Provide reassurance that regulatory standards will be maintained throughout the process.

## End Users

End users are the ones who interact with devices daily, so keeping them informed and comfortable with changes is crucial. Focus on:

- **What's changing:** Explain how the migration affects their devices, workflows, or access.
- **When it's happening:** Provide clear timelines and advance notice to minimize disruption.
- **What they need to do:** Offer simple, actionable instructions for any required actions (like re-enrolling devices).
- **Where to go for help:** Include helpdesk contact info or FAQs to address questions quickly.

## Vendors and Partners

If you're working with external vendors or partners (e.g., hardware suppliers or managed services providers), ensure they're looped in early.

Share:

- **Key timelines:** Ensure partners understand when and how they'll be involved.
- **Dependencies:** Clarify any resources or support you'll need from them to keep the migration on track.

## Pro Tips for Communication Success

**Tailor Your Messaging:** Speak to each group's specific concerns — execs care about strategy, IT about details, and users about their daily impact.

**Use Multiple Channels:** Emails, dashboards, and live check-ins can all help ensure information is clear and accessible.

**Be Transparent:** Communicate any delays or hiccups early. If stakeholders feel informed, they are more likely to stay supportive.

**Celebrate Milestones:** Migration is a long process. Recognizing progress boosts morale and keeps everyone engaged.

Continued

# Preparing for Migration

Effective communication turns migration from a potential stress point into an opportunity for collaboration. By keeping stakeholders informed and engaged, you build trust and ensure the migration stays on track.

## Training and Support: Equipping the Team

Even the best MDM won't run itself (but with the right automation tools, it might feel like it 😉). Proper training ensures your IT team and end users are ready to hit the ground running post-migration.

### IT and User Training

Start with IT teams. They're the ones who will configure, manage, and troubleshoot the new MDM, so they need to know it inside and out. Schedule hands-on training sessions and make sure they have access to documentation, tutorials, and support resources.

Next, don't forget about end users. It's unlikely they'll need a deep dive into the technical details, but they do need to understand how the migration will affect their devices. Offer simple guides or quick training sessions to help them navigate any changes.

## Helpdesk Capacity and Scaling

Let's be real: migration usually means an increase in support tickets, at least temporarily. Make sure your helpdesk team is ready for the influx by scaling capacity if necessary. This might mean temporarily reallocating staff, adding a dedicated migration support line, or extending support hours during the rollout.

At the very least, let support staff know to expect extra load over the course of the migration and after.

## Risk Mitigation: Expect the Best, Plan for the Worst

Every migration comes with risks, whether it's the possibility of data loss, device bricking, or downtime. The key to a successful transition lies in identifying potential pitfalls early and having a robust plan to address them. For enterprises managing large fleets, the stakes are even higher — but that's where a mix of proactive planning and external expertise can make all the difference.

### Identify Potential Risks

Some of the most common migration risks include:

- **Data Loss:** Backups are your best defense here, but double-check that everything is accounted for before you start migrating.

Continued

# Preparing for Migration

- **Device Bricking:** Firmware updates can sometimes go awry, leaving devices unusable. Test updates on a small batch of devices before scaling up.
- **Downtime:** Even a brief interruption can be costly. Plan for worst-case scenarios and ensure critical devices have fallback options.

For organizations with complex environments, a partner or consultant associated with your incoming MDM can help conduct a pre-migration risk assessment. Their experience in managing similar transitions allows them to pinpoint hidden vulnerabilities that might otherwise go unnoticed.

## Establish a Rollback Plan

Let's say something does go wrong — what's your plan? A rollback plan is your insurance policy. If a deployment fails or devices start acting up, you need a way to revert to the previous MDM configuration quickly. Test your rollback process in advance so you're not scrambling if you need to use it.

> 💡**Pro tip:** Document your rollback steps clearly, and make sure everyone on the IT team knows the process. A well-coordinated rollback is far less stressful than a chaotic one.

Preparing for migration is like building a solid foundation for a house. Get it right, and the rest of the process becomes much smoother. With a thorough assessment, a realistic timeline, proper training, and a solid risk mitigation plan, you'll be ready to tackle the migration head-on.

# Chapter 5: Migration at Scale

Congratulations! The planning is done, the stakeholders are informed, and the IT team is caffeinated — it's time to put your migration plan into action. But before you dive in, remember: a systematic approach wins the race. A smooth MDM migration isn't about speed — it's about precision, testing, and constant iteration.

In this chapter, we'll explore how to prototype your migration, manage the overlap between old and new MDMs, roll out changes in phases, and continuously monitor and optimize as you go. Ready to flip the switch? Let's do this.

## Prototyping the Flip: Test, Tweak, Repeat

Prototyping is your safety net, trial run, and best chance to work out the kinks before going all-in. Think of it like a dress rehearsal for a big performance — you want everything to go smoothly when it's showtime.

### Device Variety and Processes

Start by selecting a diverse subset of devices for your prototype. Include different OS platforms (iOS/Android), device types (tablets, point of sale systems, kiosks), and user groups. Why? Because a prototype that only works for one device type or one use case does you no favors in the long run. Or the short run, for that matter.

During this phase, test every critical process:

- Device enrollment and configuration
- Policy enforcement
- Application distribution and updates
- Security protocols

If something doesn't work during prototyping, celebrate — it's better to find out now than during a full rollout. Trust us.

---

### Feedback

Your prototype isn't complete until you've gathered and acted on feedback. Talk to end users, IT admins, and anyone else involved. What worked? What didn't? What could be smoother? Use their input to refine your process, ensuring the larger rollout goes off without a hitch.

---

## MDM Overlap: Embracing the Temporary Chaos

During your migration, you'll likely have devices running on both the old and new MDMs. And while that might feel like juggling chainsaws, it's actually a good thing — it gives you flexibility and reduces risk.

Continued

# Migration at Scale

## Accept That Dual Management Is a Short-Term Probability

Dual management is like having one foot in the past and one in the future. It's not ideal, but it allows you to transition gradually, minimizing disruptions. Embrace it as a necessary part of the process rather than a headache to avoid.

The key to successful overlap is avoiding conflicts between the two systems. Define clear boundaries:

- Assign specific devices or user groups to each MDM.
- Disable overlapping policies that could clash (e.g., security protocols or app restrictions).

Decide how long you'll run dual MDMs and set a clear timeline. This will keep the process moving forward while giving you enough time to resolve any unexpected issues. A defined end date will ensure you're not stuck in dual-management limbo forever.

---

## Phased Rollouts: Slow and Steady Wins the Race

Once you refine your prototype and have a handle on the dual-management setup, it's time to start rolling out the new MDM. But don't do it all at once. Phased rollouts are the way to go.

Break your rollout into clearly defined, manageable stages.

For example:


Start with a single department or location


Gradually expand to more devices and teams


Save the most complex setups for last

This approach gives you time to monitor each stage, fix issues as they arise, and build confidence in the new system.

---

## Monitoring the Migration Process: Keep an Eye on Everything

Monitoring is the backbone of a successful migration. As you roll out your new MDM, constant oversight ensures the process stays on track, you catch potential issues early, and can make adjustments quickly. This isn't a "set it and forget it" moment — it's an opportunity to keep your migration secure, stable, and seamless.

To effectively monitor the migration, focus on these key areas:

Continued

# Migration at Scale

## System Health

Keep a close eye on the overall health of your fleet. Are devices staying online and functional? Are configurations correctly applied? Use a centralized dashboard to track:

- Device status (online/offline, functional issues)
- Configuration success rates (e.g., apps installed, security policies applied)
- Device enrollment metrics

Regularly reviewing these metrics helps you identify patterns and potential problem areas before they escalate.

## Security Monitoring

Migration often creates temporary gaps that bad actors might try to exploit, so security monitoring should be top of mind. Watch for:

- Devices that fail to comply with your security policies (e.g., encryption, password requirements)
- Unauthorized access attempts or unusual login activity
- Data transfer issues, such as incomplete encryption during the process

Proactively addressing these gaps ensures that your devices stay protected throughout the migration.

## Error Tracking and Troubleshooting

Even with the best planning, errors happen — it's part of the process. The key is spotting them quickly and having a response plan. Common errors to monitor include:

- **Failed enrollments:** Devices that don't register with the new MDM
- **App installation issues:** Missing or incorrect apps on migrated devices
- **Configuration issues:** Improper configuration execution on migrated devices
- **Connectivity problems:** Devices dropping off the network or failing to sync with the MDM

By assigning resources accordingly, you can address the most pressing problems first while keeping the migration on schedule.

Continued

# Migration at Scale

## Pro Tips for Effective Monitoring

To streamline your monitoring efforts and ensure a smooth migration, keep these best practices in mind:

- **Centralized visibility:** Use a unified dashboard that aggregates all key metrics so your IT team doesn't have to switch between tools
- **Automation tools:** Deploy monitoring tools that automatically flag compliance or enrollment issues, saving your team time
- **Checkpoints:** Set predefined checkpoints at various stages of the migration to review progress and identify adjustments

Focusing on system health, security, and troubleshooting ensures your migration stays on track. With proactive monitoring, your IT team will have the visibility and tools needed to address issues quickly, keeping disruptions to a minimum while building confidence in the new MDM.

---

## Post-Migration Testing and Optimization: The Home Stretch

The migration may be complete, but your job isn't done. Post-migration testing and optimization ensure everything is running as smoothly as possible.

- **Compliance Checks and Enforcement:** Verify that all devices comply with organizational and regulatory standards. This includes security policies, access controls, and data protection measures. Automation tools can make this process faster and more reliable.
- **Drift Management:** Device drift happens when settings and configurations start to deviate from their desired state. Regularly audit your fleet to catch drift early and enforce consistency.
- **User Experience Feedback:** Don't forget about your users! Check in with employees to see how the migration has impacted their workflows. Is the new system intuitive? Are there any frustrations? Addressing these concerns early can boost adoption and satisfaction.
- **Fine-Tuning:** With feedback and data in hand, make final adjustments to your MDM setup. This might include tweaking policies, optimizing app deployment strategies, or refining your monitoring processes.

---

**Migration at scale isn't for the faint of heart, but with careful planning, thoughtful execution, and constant iteration, you'll**

Continued

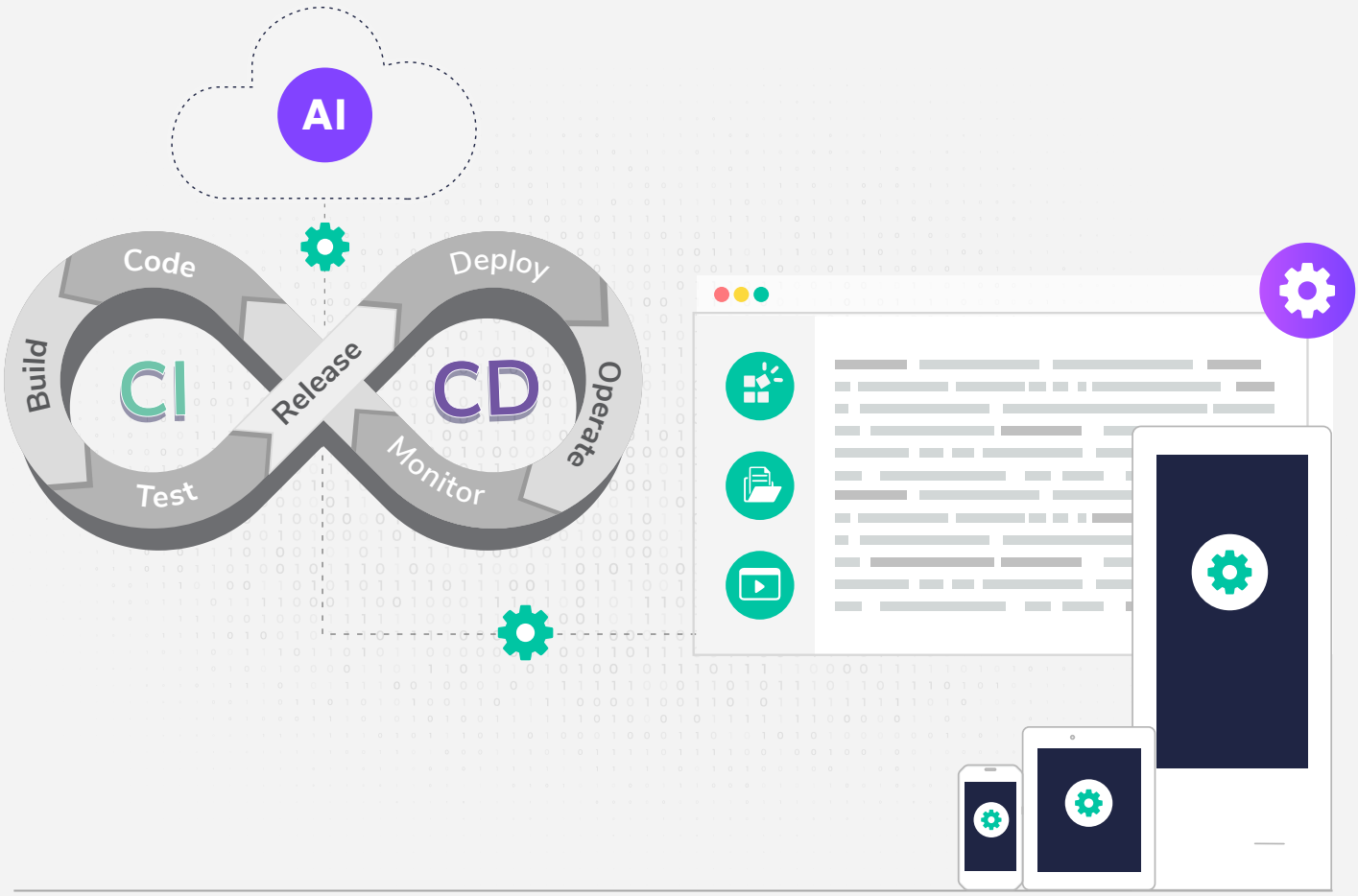
# Migration at Scale

come out the other side with a better managed, more secure, and future-ready fleet.

### Continued Reading: The Beginner's Guide to DevOps for Devices

DevOps isn't just for software anymore—it's transforming how organizations manage their device fleets. **The Beginner's Guide to DevOps for Devices** breaks down the basics, showing you how to streamline deployments, automate updates, and scale operations with ease. Whether you're just getting started or refining your strategy, this guide is your first step toward smarter, faster device management.

Download Now



# Conclusion

MDM migration is no small feat. It's a journey that requires careful planning, thoughtful execution, and ongoing optimization. But when done right, it's more than just a technical transition—it's a golden opportunity to transform how your organization manages its devices, drives efficiency, and prepares for the future.

This guide has walked you through every step of the migration process, from evaluating your current MDM to choosing the right solution, planning a seamless migration, and optimizing your hardware refresh cycles. Along the way, we've highlighted the importance of proactive risk mitigation, strategic rollout planning, and stakeholder communication. Whether you're self-serving or leaning on the expertise of a trusted partner, the roadmap is now in your hands.

---

## The Why Behind the Work

At its core, MDM migration isn't about switching platforms for the sake of change — it's about aligning your technology with your organization's goals. It's about ensuring your device fleet operates securely, efficiently, and at scale, enabling your teams to focus on innovation rather than troubleshooting.

For enterprises managing thousands of devices, the stakes are high. Poorly executed migrations can result in downtime, security vulnerabilities, and compliance risks. But with the right preparation and support, you can sidestep these challenges and activate your fleet's full potential.

---

## The Value of a Strategic Partner

While this guide provides the tools and insights you need to self-serve your migration, never underestimate the value of collaboration. Partners and solution providers bring specialized expertise to streamline the process, mitigate risks, and optimize outcomes. Whether it's managing staggered refresh cycles, ensuring compliance, or providing post-migration support, the right partner amplifies your success and saves your team time and effort.

---

## Looking Ahead

The journey doesn't end with the migration. Once your new MDM is in place, it becomes a foundation for ongoing growth and innovation. With the right tools, you can:

- Keep your fleet compliant and secure, even as regulations evolve
- Scale effortlessly as your organization grows
- Adopt new technologies, from IoT devices to emerging platforms, without skipping a beat
- Your new MDM isn't just a solution — it's a strategic asset that empowers your organization to thrive in an increasingly complex and connected world

## Your Next Step

You've got the knowledge, the tools, and the roadmap. Now it's time to take the next step. Whether you're just beginning to assess your current MDM or preparing for a full-scale migration, remember: this process is an investment in your organization's future. Approach it with purpose, collaborate when needed, and don't shy away from asking for help.

At Esper, we're here to support you every step of the way — whether that's through our platform, our partners, or simply our expertise. Over the years, we've seen and assisted on many migrations, handling everything from simple, straightforward flips to incredibly complex, multi-stage conversions. Regardless of where you are in your migration journey, we've got your back.

Let's make it happen.

### Ready to get started?

Get in touch for personalized information about MDM migration.

### To learn more about Esper MDM, visit us at

esper.io/mobile-device-management