esper

MDM Compatibility Checklist

Scoring Analysis

Y/N	Question
☐	Are my devices company-owned and have multiple users?
☐	Do I need to lock my devices to a single application or kiosk mode?
☐	Do I have a fleet of mixed OS devices? (i.e. Android and iOS)
☐	Are my devices responsible for critical business operations?
☐	Do I need to update the content on my devices frequently — weekly or even daily?
☐	Do I need full remote control and access to my devices at any time?
☐	Do I need a way to quickly and easily update device configurations?
☐	Do I have a large device fleet or need to deploy new hardware at scale?
☐	Do I need immediate notifications if a device goes down, gets knocked offline, or falls out of policy?
☐	Do I need to customize the behavior or layout of an application or device interface as part of the initial setup?

Scoring Breakdown

0: You need basic MDM functionality

If you answered "no" to every question, it sounds like you have a very straightforward MDM use case. This is generally the type of situation MDM was made for — BYOD (bring your own device) or COPE (corporate owned, personally enabled) scenarios.

1-3: You need a specific type of MDM to manage your devices

If you answered "yes" to at least a few of the questions, then you have specific needs to simplify your device management strategy. Many MDMs offer this level of functionality, but this is where deeper analysis of each is required. You might be able to get 90-95% of what you need from a particular MDM solution, but that 5% could potentially leave you struggling at critical moments — especially as you scale.

4-7: Only certain MDMs can fit the bill

What you need from MDM is pretty specific. Maybe it's powerful remote control or a tried-and-tested kiosk mode. Or perhaps it's a repeatable, scalable solution for software delivery. Whatever it is, not just any MDM provider will cut it. It's time to look at the fine print of what each offers.

The good news is that you're getting into the space where Esper absolutely excels. Where other MDMs will leave you wishing for something more, Esper delivers. It's why we exist.

7+: You know what you need, and not just any MDM will cut it

If you answered "yes" to 70% or more of the questions, then we were made for each other. You probably already know that not just any MDM will offer the solution you need, but maybe you're not sure where to go from there. Well, you're in the right place, because Esper is the perfect next step for you.

We were designed for situations like yours. Most MDMs simply adopted the type of device management you need. But we were born in it. Molded by it.

01

Are my devices company-owned and have multiple users?

MDM software was originally designed to manage employee-owned devices on corporate networks for BYOD / CYOD (bring/carry your own device) or COPE (corporate owned / personally enabled) scenarios, which is what this question covers. In these situations, employees bring their own computing devices or company-provided laptops are open for personal use.

Today, devices are used for much more than just employee use. Modern businesses rely on corporate owned hardware for revenue-generating or mission-critical applications — like point of sale systems or remote patient monitoring, for example. These devices often use a 1:Many mapping instead of the 1:1 mapping of traditional COPE scenarios. Knowing the answer to this question will tell you where to start look MDM services.

If you answered yes to this question, then a BYOD or COPE solution is likely insufficient for your use case.

esper.io

02

Do I need to lock my devices to a single application or kiosk mode?

Many enterprise devices don't need a full suite of apps. In fact, these devices commonly only need access to a single application (or perhaps a very select few). For that, you need a way to lock the device to that app (or set of apps), with impenetrable restrictions in place to avoid device misuse and tampering.

That's where kiosk mode comes into play. Despite the name, this feature is for far more than just kiosks and should be used in any situation where a single application needs to be locked to the display. Think point of sale systems, in-vehicle navigation, self check-in kiosks, and more.

If you answered yes to this question, there's a strong possibility that you'll need more functionality than most MDM solutions have to offer.

03

Do I have a fleet of mixed OS devices? (i.e. Android and iOS)

If all of your devices run the same operating system, your MDM needs are slightly simpler. But if you have a device fleet with multiple OSes — Android and iOS, or even GMS Android and AOSP Android — then your MDM needs are dramatically more complex. For example, some MDM providers offer support for multiple OSes, but they're segmented, so it's like managing multiple device fleets. A provider that offers support for all of your devices from a single user interface can make your life much easier.

But going beyond that, think about your device fleet holistically and pick an MDM that aligns with your vision. If you want your Android and iOS devices to function identically, you'll need the right management partner to make that happen. Similarly, if you want to keep them grouped by OS, you'll need an MDM that supports that. Or, better yet, get you an MDM that can do both.

*If you answered yes to this question, your MDM provider should holistically support all the operating systems your devices run. You don't need to manage multiple device fleets because you need more than one OS — unless, of course, that's a strategic decision. But it should be **your** decision. Not theirs.*

04

Are my devices responsible for critical business operations?

Itf your devices are mission-critical — that is, any device that your business absolutely relies on — you need a device management solution designed for mission critical systems. Advanced management capabilities that allow you to fully control the device and optimize it specifically for your use case are crucial.

While almost all corporate owned devices can benefit from advanced management tools, not all devices will lead to business downtime in the event of a failure. If you're having a hard time deciding if your devices are truly mission critical, think about how your business would function with them — would operations come to a grinding halt? Would you simply shift to another way of doing things (for example, a cash only business)? We're talking about the difference between a fully automated ticketing system and one that's merely another means of getting a ticket that could easily be purchased from a traditional ticketing booth.

Think hard about this one. If you need a device to accept money from customers (like a credit card terminal), that device is critical to your business. Even if one hour, or an entire day, of downtime is something you're prepared for, you wouldn't want to go a week without it — and more importantly, neither would your customers.

If you answered yes to this question, you need to be vigilant in your search for MDM software. Mission critical devices need a management system that understands that criticality.

05

Do I need to update the content on my devices frequently — weekly, or even daily?

Many legacy dedicated devices are largely set-and-forget, with content and features locked in at the factory. This philosophy was thoroughly disrupted by innovative consumer brands like Nest, Peloton, and Tesla (yep: a car is a dedicated device!) — but in the enterprise, updateable dedicated devices are a recent phenomenon. If you need to update the devices in your fleet, you should consider the type of updates your devices require, as well as the frequency of said updates. For example, do you need to update your custom application on a weekly basis? Or are you updating content like images, videos, and webpages across a range of devices on a daily basis? Do you have an AI model that requires frequent updates?

The type and frequency of content updates can be a tremendous burden if you're using the wrong delivery system. For simple file updates, you may be able to leverage a third-party tool that works for cross-device sync, but if you need something more dynamic — like updates that roll out in stages across multiple devices in a variety of locations — then you'll need to focus closely on your management partner.

If you answered yes to this question, you'll need to take a hard look at your exact use case and determine what sort of content and at what frequency you want to update. Some MDM providers may allow for easy file sharing across devices, but app or OS updates can present bigger challenges. Document everything you need and ask the important questions as you vet MDM services.

06

Do I need full remote control and access to my devices at any time?

As reliant as we are on technology, we also know that it can break at any moment. And when that happens, your strategy to deal with it is important. Do you have techs on site at every location? Do you use phone support to walk employees through troubleshooting? Endless email chains? Or would you prefer full remote access and control of any devices from anywhere in the world?

Troubleshooting and debugging are critical components of device management. But don't just think about your needs today — think about your needs as you scale. Right now, you may only have a handful of devices in two or three local locations. But as you expand, the ability to access any of your devices from anywhere in the world becomes much more important.

If you answered yes to this question, you'll want a full suite of remote access and debugging tools. While there are third-party tools available to enable remote access on many devices, finding an MDM provider that bakes this functionality in will save you time and money.

07

Do I need a way to quickly and easily update device configurations?

Just because you need a device to work a certain way today, doesn't mean it'll always be that way. What if another device goes down, and you need to repurpose one quickly? Or if company policies change and you need to update your edge devices as a result? There are a lot more hypotheticals where those came from, but you get the idea.

A quick, streamlined way to update device settings, policies, and overall configurations is an absolute must in the modern enterprise. Big bonus points if you can do this across device groups instead of one at at time, too.

If you answered yes to this question, the way your MDM handles device provisioning, grouping, settings, and policies is of paramount importance. Ask questions and dig into the details of available features that support your uses.

08

Do I have a large device fleet or need to deploy new hardware at scale?

Deploying new devices takes time — lots of time. Depending on your exact use case and the types of devices you currently use, deploying new hardware can be a multi-year process that requires a team of people. And if you have a large number of devices to deploy as you scale, this problem grows exponentially.

Automatic deployment tools can help ease the burden in a truly measurable way. By creating templatized provisioning profiles that can be applied to any number of devices at one time, the deployment process can literally go from hours (or days) to minutes. Adding new hardware (or repurposing existing hardware) becomes a no brainer instead of a head scratcher.

If you answered yes to this question, a management tool designed for rapid deployment using automation will allow your organization to scale rapidly and move with agility.

09

Do I need immediate notifications if a device goes down, gets knocked offline, or falls out of policy?

Do you know what every device in your fleet is doing right now — or do you at least have a way to easily find out? We're talking about everything from battery level to Wi-Fi connection status to current location (and beyond). If you don't have access to this kind of information, you're making life harder on yourself than it needs to be.

If you do have that kind of access, is your device fleet self-monitoring with customizable alerts and notifications if specific criteria is met? For example, if a device drops offline? Or moves outside of a geofenced area? Automation at every level makes constant monitoring a thing of the past.

If you answered yes to this question, an MDM solution with robust location, monitoring, and telemetry capabilities is critical. Just knowing where a device is or its connection status isn't enough. The right MDM will enable you to proactively monitor vital system stats and react before issues turn into big problems.

10

Do I need to customize the behavior or layout of an application or device interface as part of the initial setup?

As part of your provisioning process, do you have to manually set up a custom device layout or install a specific set of applications? How does that process scale as you add more and more devices? If you only have a few devices right now, it may not seem like a problem. But think about what happens if you then need to complete this process for 100 devices. Suddenly that 30-minute provisioning process becomes several days' worth of work.

With touchless provisioning, however, this process can largely be automated. By creating a single blueprint that defines how a specific device should be set up, you can easily apply custom setups, installed applications, and more in a matter of minutes. Not only that, but with the right management partner, the entire process can happen automatically when the device comes out of the box — no previous setup required.

If you answered yes to this question, you need truly advanced and unique functionality. As you scale, custom setups become more and more trouble to effectively apply to a large number of devices. Finding a tool that allows for automated provisioning saves time, money, and headache.