SAMSUNG

White paper:

The beginner's guide to MDM

A practical guide to securing and managing mobile devices for small and medium-sized businesses

What is mobile device management, and why do you need it?

Whether you call it mobile device management (MDM), enterprise mobility management (EMM) or unified endpoint management (UEM), the goal is the same: Take control of mobile devices to deliver a manageable and secure environment that protects business data — no matter how large or small the organization. But how is that done, exactly?

This guide provides a 101 on the key benefits of MDM, outlining the planning steps you'll need to take and providing practical tips for an effective MDM deployment.

Let's start with mobile devices. Most MDM tools (we'll use the term "MDM" to encompass this range of products) focus on the two dominant mobile operating systems: Google Android and Apple iOS, almost always at the same time. That covers the overwhelming majority of smartphones and tablets in use by businesses today. Very few MDM products only support one operating system; these are the exception rather than the rule.

Some vendors are releasing products that cover laptops and desktops in addition to smartphones and tablets. These providers tend to prefer the term "UEM," which is relatively more complicated and often intended for larger enterprises. IT managers in small and medium-sized organizations will typically find that MDM products for mobile operating systems, which have comparatively simpler management models, fit better into their environments, filling a big gap in a platform-agnostic way.

IT managers in small and medium-sized organizations should be able to see the advantages of MDM tools right away, even for environments with fewer than 100 devices. But the cost to acquire and run yet another IT application is an equally obvious downside. Experience has shown that the benefits of saving time and reducing the burden of management are significant drivers for MDM adoption in organizations of all sizes, and these benefits far outweigh the costs.

However, there's another equally strong driver: Bring Your Own Device (BYOD) and Choose Your Own Device (CYOD) programs. As IT managers seek to balance the security and privacy requirements of the organization with the need to empower mobile staff by bringing information to their fingertips, BYOD/CYOD programs have become important in setting the "rules of the road." MDM tools are needed as reporting and enforcement arms when a BYOD/CYOD program dictates policy for device protection and configuration, such as requiring minimum length passcodes or software updates. As organizations of all sizes react to the requirement for mobile devices in the workplace, MDM is a key enabler in an effective BYOD/CYOD Program.

So what's MDM going to do for you? Most MDM tools cover four main IT requirements:

Deployment

The process of deploying mobile devices can always be faster. Once the device has been unboxed, it needs to be configured and delivered into the hands of end users as quickly and consistently as possible. Once a device has been linked to the MDM tool, a complete set of operating system configuration settings are downloaded, speeding initial installation and reducing the opportunity for human error.

Policies

Device settings such as password requirements, automatic updates, encryption, application blocklists and app store specifications can be controlled from a single management console, with changes automatically pushed out to all mobile devices managed. MDM policies are continuously evaluated, which means that once a device becomes managed remotely, any user changes to the configuration can be overridden by the MDM.

Reporting

Keeping track of devices — especially mobile ones — is a time-consuming challenge, even with just a handful of users. MDMs keep inventory of devices, note their last check-in date and can usually generate reports across an organization's entire user community, showing information such as operating system versions and patch compliance or policy status.

Security Tools

When a device is lost or stolen, IT managers want to contain the damage quickly. MDMs include the ability to remotely lock mobile devices, erase company data or even erase the contents of the entire device.

MDM options for small businesses

IT managers interested in MDM products will find an array of solutions available, all at different price points. In the end, though, the costs of MDM tools are always offset by the savings from automated tasks they enable.

The first option to consider is a dedicated MDM solution, which focuses on MDM as its only function. This is the part of the marketplace that is easiest to find. IT managers can select among a broad set of deployment options, including cloud-based subscription services that can be up and running in minutes, as well as traditional on-premises packages: appliances, virtual machines and server-based applications.

Small and medium-sized businesses looking for dedicated MDM should focus on cloud-based solutions first. With virtually zero initial capital expenses (CapEx) and a typical monthly operational expense (OpEx) in the range of $1 to $5 per device, cloud-based solutions combine minimal overhead — no servers, training, operating system licenses, backups, monitoring or maintenance — with reasonable ongoing costs.

When a cloud-based solution isn't acceptable, IT managers can opt for MDM solutions that run on-premises. These local appliance, virtual machine or application-style MDMs usually have monthly per-user costs 25 to 50 percent lower than equivalent cloud-based solutions — although the subscription savings are usually not enough to offset the one-time CapEx and other nonsubscription OpEx costs associated with running a server or application in their own infrastructure (such as backups, hardware costs, data center charges, application management and monitoring tasks).

Dedicated MDM solutions aren't the only option. For example, many of the endpoint security suite (antimalware, URL filtering, content management, etc.) vendors are shifting their products to take a larger role in managing endpoints, adding MDM features as a secondary function. Although these product suites have strong roots in the Windows security world, they are adding Android and iOS capabilities as part of product migration toward UEM. IT managers may discover that their standard antivirus tool has turned into a full-fledged desktop and mobility management product.

At the end of the year, though, it's not so much about the cost of the MDM tool but the savings that it delivers. IT managers looking at tight budgets should consider more than the CapEx and OpEx outflows. MDM is a time-saver and risk-reducer, and time saved and risk eliminated is money saved. MDM tools are strong force multipliers for IT managers. By creating policies in a central console and letting MDM enforce compliance, IT managers get a strong handle on security and mobile management without having to think about touching every device individually.

Trying to quantify the savings of MDM versus the costs requires a lot of assumptions, making a straightforward, by-the-numbers comparison nearly impossible. However, some comparisons are easy to see: If MDM can cut out one 30-minute help desk visit a year, it'll have paid for itself for that user. And if better control of security configurations helps to prevent a data breach, MDM will be one of the wisest investments your business can make.

MDM can make Herculean tasks such as updating settings on devices both simple and fast, enabling what might not have been possible before. MDM solutions save money through:

Faster device setup and configuration

Reducing help desk costs by locking down configurations and ensuring that devices are properly updated

Improving inventory control and the ability to respond to compliance audits by providing information on all mobile devices and their configurations in a single portal

Mitigating security risks by controlling security policy, preinstalling Wi-Fi and mobile data configurations, configuring virtual private network (VPN) clients, and offering remote wipe and lock capabilities in case of device theft or loss

Getting started with MDM

By now you should be convinced that MDM is something worth investigating. Now, let's walk through the steps for getting started with MDM.

First and most importantly, make sure that everyone knows you're going to be using an "agile" methodology for this project. That means working with mobile device users from the beginning to understand the impact of MDM on their day-to-day work, collaborating and updating your plan as you learn more about how MDM works in your environment, and being willing to shift direction in response to feedback and problems.

Your next step is to set the scope of MDM: Which devices and users are going to be part of the initial deployment? You can expand the scope later, but it's critical to draw a circle around a set of devices and users (or applications, such as kiosks powered by mobile devices) and say, "This is our initial focus." The reason is simple: MDM tools are flexible. If you don't have the end state in mind as you progress, it's easy to get distracted by flashy features that don't lead you down the right path. Remember, you can always turn something on later once you're more confident with the MDM's behavior and side effects.

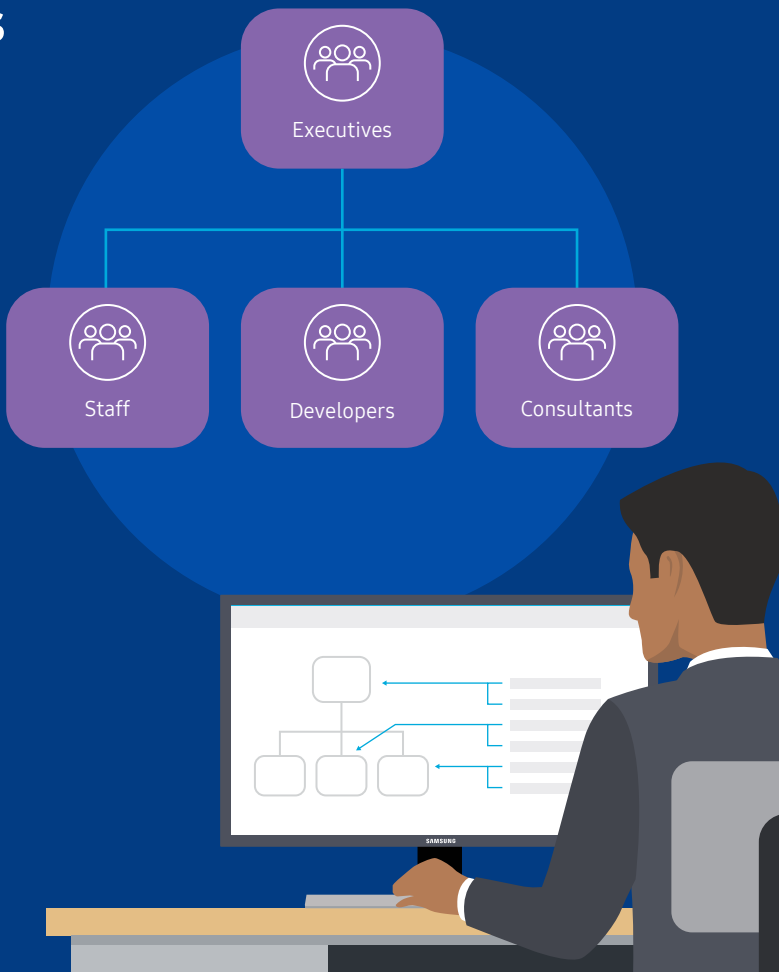
With the scope clearly in mind, now is the time to tackle the MDM console. All products are a little different, but there's some commonality: Most MDM products divide users and devices into groups, and then apply policies to the groups. Reporting is also often summarized by groups as well. So start with groups, policies and operations — a little at a time.

Step 1: Start With Groups

Many MDM tools have the ability to link to your corporate Microsoft Windows Active Directory (AD), which gives them knowledge of your group structure and the ability to authenticate users against the directory. While this sounds like a big plus, it can be complicated, especially if you are starting with a cloud-based product. The user experience is usually better when you have AD linked to your MDM, but it may be simpler to begin without AD integration at first.

This means that you'll have to create groups manually. Remember that groups are used to help apply MDM policies (and to drive reporting), so you'll want to think about how different people — and different devices — will have different security and MDM policies and set up your groups accordingly. Meanwhile, keep an eye to how you're going to maintain these groups — eventually, hopefully, with the help of your corporate directory tools such as AD. Having multiple groups that take exactly the same policy all the time won't hurt anything, and may make it easier to understand what is happening in the MDM tools. In other words, you can have as many groups as you need, even if some of them seem the same from an MDM point of view.

For example, if you have staff, executives, consultants and developers in your AD, start with these same groups in the MDM. Your job will be easier if you decide to link your MDM to your AD.



However, especially at the beginning, your MDM path will be filled with exceptions: Some users will be early adopters of new versions of software applications or operating systems, or may have different security policies because of special job requirements. Rather than handle those devices individually, set up groups that indicate these special status situations. This makes it easier to swap devices in and out or give multiple users the same policy. For example, if you have an "Executives" group, add an "Executives-EarlyAdopters" group for Executives who will be the first to get software updates.

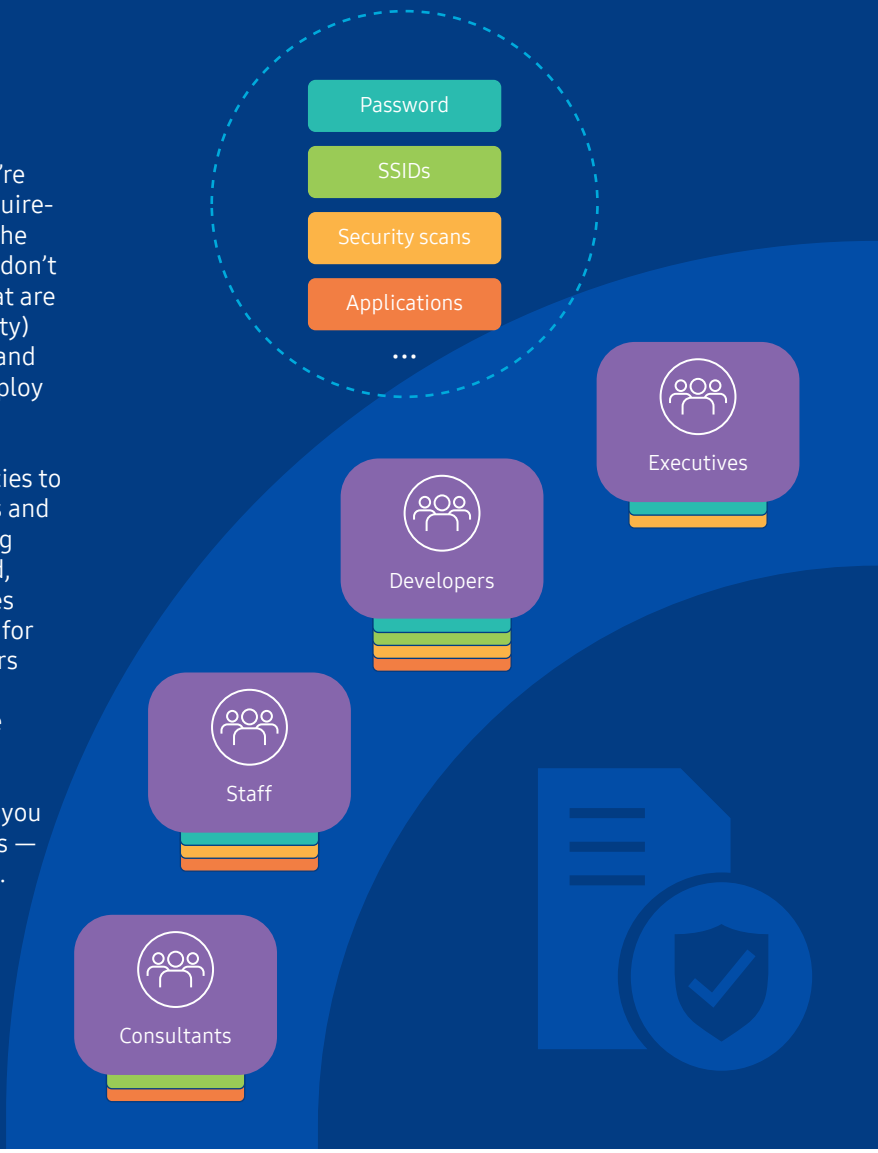
These are just some ideas on how to set up groups. Regardless of your choice, it's best practice to start with a small number of groups — five or six at most. Don't go overboard. The key is to step back for a few moments to think about how you want to set up your groups, but don't try and get it all done before moving forward. Everything else in the MDM will revolve around groups: policy assignment, reporting, software management and inventory. If you have your groups cleanly defined from the start, you'll save a lot of time as you expand the scope of MDM across the business — and achieve this clean set of groups as you gain experience.

Step 2: Policies

Policies are the core of the MDM. Policies (or whatever they're called in your MDM) define the settings and compliance requirements for devices. Policy definitions can be overwhelming the first time you log in, with literally hundreds of settings, but don't worry about understanding them all. Pick a few settings that are easy to test (such as minimum passcode length or complexity) and lay out a few sample policies. As with groups, don't try and do all your policies at the beginning. Put in three or four, deploy them, then adjust and grow based on experience.

Better MDM products will allow you to assign multiple policies to a single group, so you should be able to make small policies and layer them on top of each other. Don't try and get everything into a single policy (unless your MDM requires that). Instead, break things into chunks, keeping in mind that some policies may be applied to many groups — password requirements, for example, or preloading corporate Wi-Fi service set identifiers (SSIDs) — and other policies may be very specific to some groups, such as allowing or blocking specific features of the mobile platform.

As you're deciding on initial policies, look back to the scope you defined at the beginning. Many settings in the MDM policies — even most of them — will be irrelevant to your organization. Keep in mind your end goal and the scope of the initial deployment as you set up policies. Settings that look interesting, but are out of scope, shouldn't be part of your policies. And don't let policy analysis slow you down from getting the first devices enrolled.



Step 3: Enroll Devices and Dive In

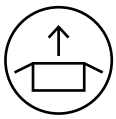
Now is the time to start enrolling devices, adding them to groups and pushing policies. Obviously the first device will take time and you may need to change some policy elements almost immediately. But once you get over first-day problems, get a good number of devices into the system and start to look at operations, explore other areas. You'll want to dig into reporting and see if the compliance and inventory reports meet your needs, and whether you need to change your grouping strategy. This is also a time to test out some of the more intrusive features, such as remotely locking devices, wiping data, enabling SIM lock, doing a remote factory reset and setting up device tracking.

Here's where the agile strategy will pay off. As you go through these three simple steps, you're going to make mistakes, learn from them and adapt your deployment. Create some groups, but not all of them. Create a few policies, but don't try and cover everything. Then deploy some devices to see how it all works together. You may have to go back to the drawing board, but by using agile methodology, you'll have a minimum to throw out and will shorten your overall timeline.

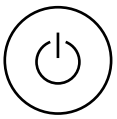
Zero-touch deployment for small and medium-sized businesses

If you've made it this far, you should be convinced that MDM is a great investment for businesses of all sizes, and you may have already started deploying MDM. But there's an even bigger time-saver available — zero-touch.

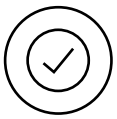
The Holy Grail of IT managers for device setup is zero-touch, often illustrated as a Post-it note with three steps on it:



1. Take device out of box



2. Turn on power



3. There is no step three

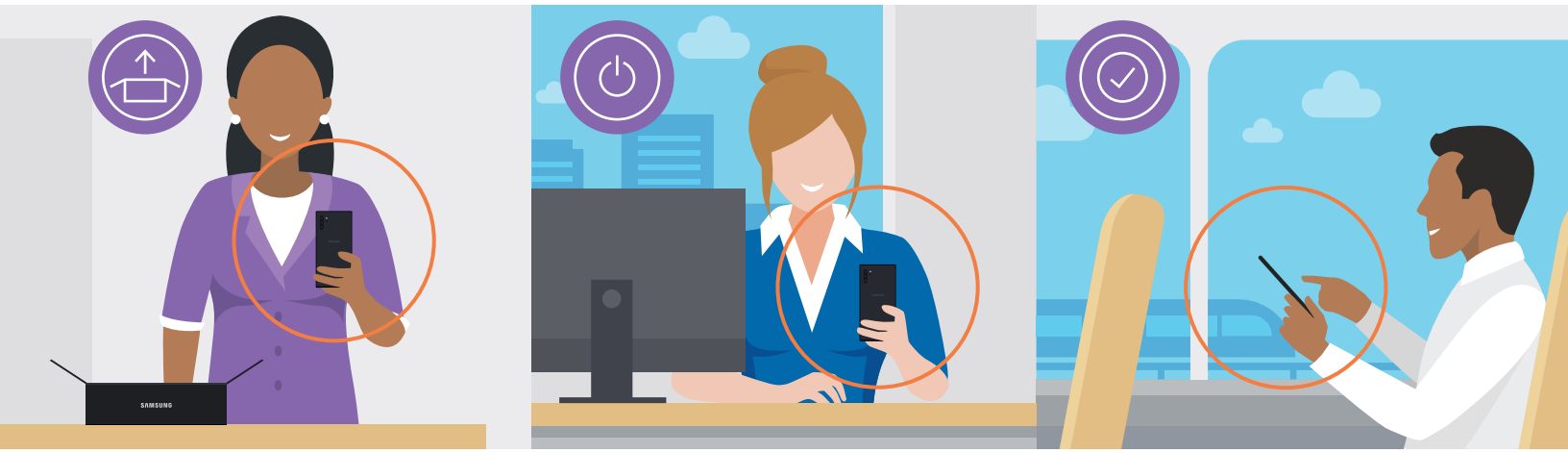
The idea is that the user doesn't have to do anything at all to get themselves a fully functioning mobile (or laptop) device. As you might imagine, full zero-touch is difficult to accomplish and may require resources and a time commitment out of reach of a small or medium-sized business IT manager.

However, you can still get partial zero-touch in the mobile world. With zero-touch MDM enrollment programs, device vendors, device resellers and MDM product vendors all work together to create an ecosystem that shortens and simplifies the enrollment process. These all work using a similar model: Resellers upload serial numbers of devices to a central portal, linking them to a specific organization that bought the device. The organization's IT manager uses the same central portal to register their MDM servers, and to assign each purchased device to a server. When the smartphone, tablet or laptop powers up the first time, it contacts the portal, identifies itself and downloads enough information to enroll in the organizational MDM service.

For Android-based devices, Google has a zero-touch program (part of Android for Enterprise) as well. Android Zero-Touch Enrollment links a network of resellers, a zero-touch service operated by Google, and cooperating MDM developers together. Once you've set up your organization with Google's zero-touch service, Android devices are loaded into Google's portal by the reseller. When these devices are first powered on, they will discover your organizational MDM server and can immediately start enrollment, shortening the MDM enrollment process for new Android devices.

Individual hardware vendors also offer more tailored solutions. For example, Samsung's Knox Suite includes Knox Mobile Enrollment (KME), which can be used as part of a zero-touch deployment.

KME is a free tool that delivers zero-touch bulk enrollment out of the box for Samsung smartphones and tablets. Samsung devices registered with KME by participating resellers automatically initiate MDM setup the moment they're powered up and connect to a network. IT managers can even prepopulate user credentials to fully automate enrollment, letting end users skip setup wizards and get to work faster. KME can be configured to persist across factory resets or deinstallation of the MDM agent so that KME automatically reinitiates enrollment the next time the device connects to a network.



Measuring the success of MDM

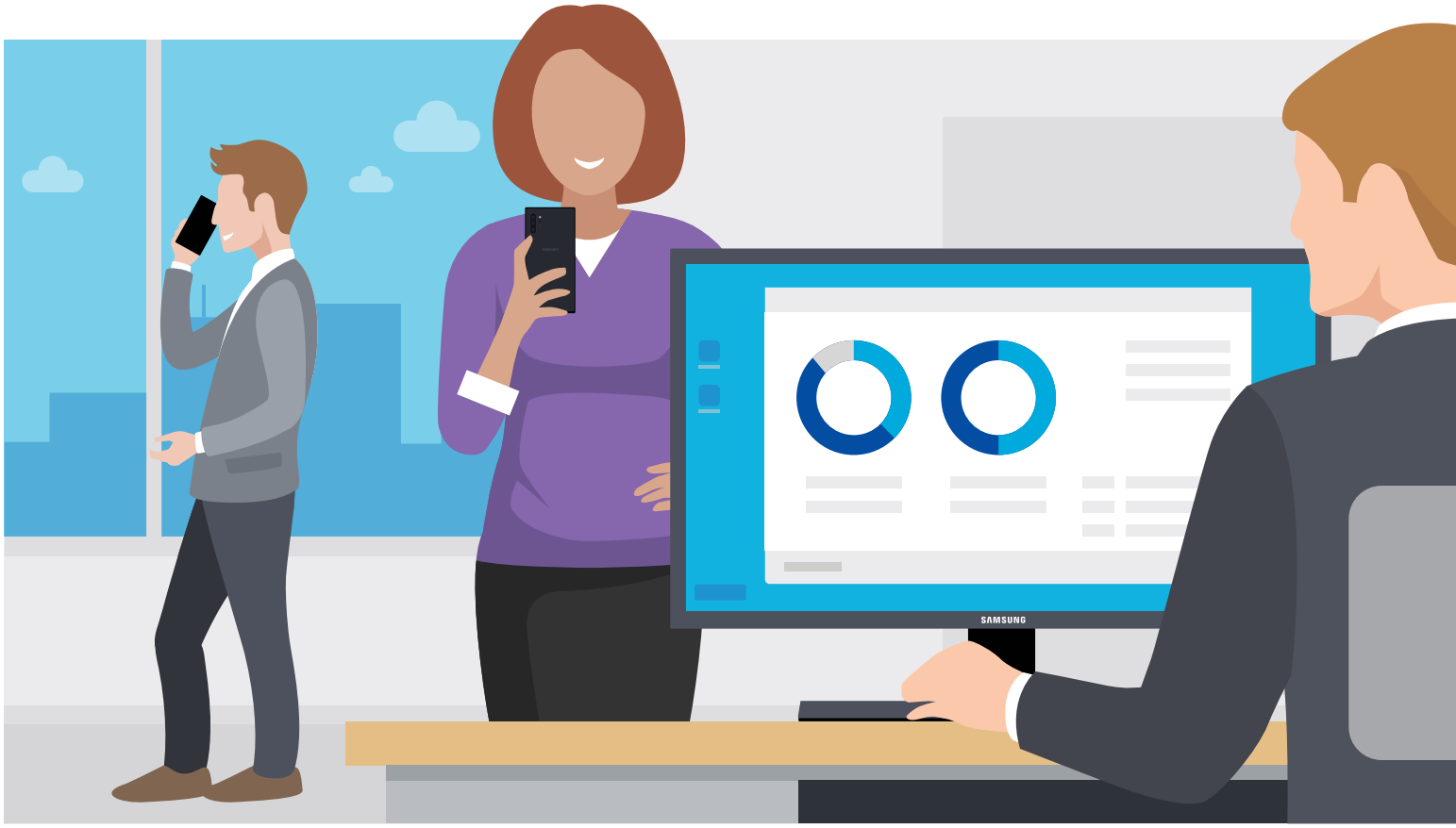
Another advanced MDM topic, but one every IT manager should look at, is measuring success of their MDM program. There's no question that MDMs come with ongoing operational expenses. They may be inexpensive, but even "free" has costs. IT managers should define metrics to show that MDM OpEx is a good investment — that MDMs don't cost money but save money.

Start by looking at help desk costs. This is where MDM provides huge savings, because help desk teams dramatically reduce the time spent manually managing mobile devices as users bring them in, or dealing with configuration and update issues over the phone. A simple comparison of helpdesk tickets before and after MDM is installed will always show savings in deployment, support and even in redeployment.

Be fair in your metrics by also factoring in the cost of the MDM solution and the IT group time spent managing the solution. Any CapEx and OpEx for your MDM solution have to be accounted for when considering the overall benefits.

Equally important at this stage is to measure user satisfaction with their mobile devices. MDM starts by providing a better user experience, preloading applications and configurations so that users are ready to go and have less self-management to do. When MDM lets the organization easily configure and update devices without direct user contact, the result is always happier users. It's not that they don't like your help desk, it's just that they don't want to spend work time solving IT problems instead of getting their jobs done.

Finally, there are softer metrics that can help show the benefits of an MDM program. Small and medium-sized businesses that fall under some regulatory compliance regime, such as HIPAA or the SEC's broker and investment advisor guidelines, can help speed audits and self-certify compliance when MDM tools are in place. At the same time, being in compliance, having security patches installed, and devices securely configured will reduce the risk of a data breach. It's hard to measure something that doesn't happen, like the costs avoided by not having a data breach, but savvy IT managers should use the reporting and compliance tools from their MDM to show that they are doing a good job at keeping devices as secure as they can.



Implementing MDM from Samsung

While Samsung is well known as a premium smartphone and tablet manufacturer, it has also led the way in building advanced device management capabilities for the Android platform. Samsung's Knox Suite provides IT managers a complete set of tools to secure, deploy and manage mobile devices for businesses of every size.

We've already discussed KME, a free service that delivers bulk enrollment and fast, seamless deployment of Samsung devices into organizational MDM tools. KME takes over the moment a device is powered on, ensuring mobile devices remain enrolled and protected by MDM even after a factory reset.

Knox Suite also includes Knox Manage, Samsung's own cloud-based MDM solution. Using Knox Manage's intuitive web-based console, IT managers can remotely manage a fleet of Android, iOS and Windows 10 devices. Knox Manage delivers all the core controls IT managers need from an MDM product, including managing apps, content and device features such as connectivity. Building on Samsung's security and Android expertise, Knox Manage can also control high-security features within Android Enterprise — such as multiple profiles — and it's optimized for Samsung, giving IT managers the most comprehensive controls for Samsung Galaxy devices. As a full-featured MDM solution, Knox Manage also includes real-time device location monitoring, remote access for troubleshooting and remote lock and wipe capabilities.

IT managers who need tight control of software updates on mobile devices can utilize Enterprise Firmware Over-the-Air (E-FOTA), another component of Knox Suite. Every IT manager has horror stories about unplanned software updates interrupting critical applications. E-FOTA helps avoid the downtime that results from untested updates, instead giving IT managers complete control of OS and firmware updates, with scheduled updates, control by user groups and — when a critical security threat emerges — the ability to force mandatory updates without user interaction.

Samsung's mobile management and security solutions:

Knox Suite

Knox Manage

Knox E-FOTA

Knox Mobile Enrollment

Sign up for a free trial of Samsung's Knox Manage.