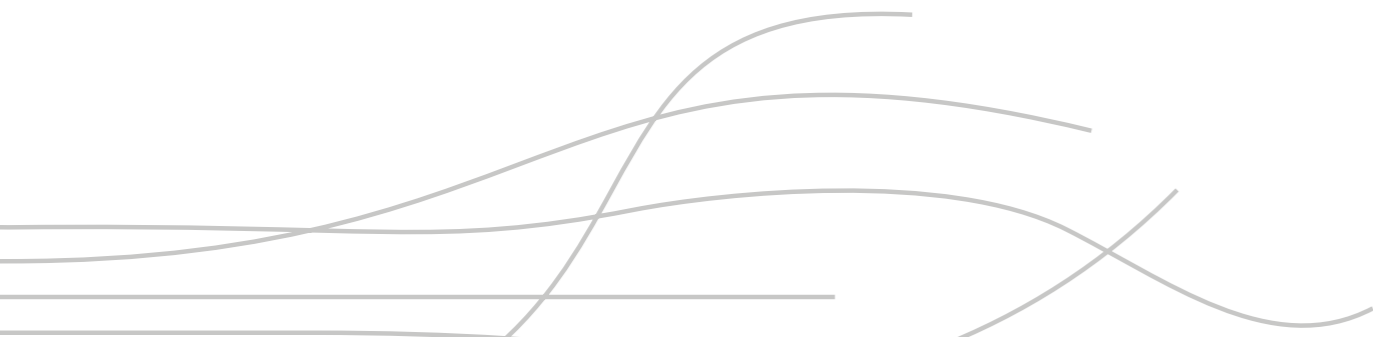




IBM Security Thought Leadership White Paper

# 11 best practices for mobile device management (MDM)

*How to manage and protect mobile devices in the enterprise*



## Staying afloat with the mobile tide

Our devices have become so ingrained in our lives—both personal and at work—that it's almost impossible to envision a time when they weren't at our disposal. Today's businesses and their employees rely on their devices for such a large number and wide assortment of use cases that the importance of effectively managing them has never been greater.

Modern IT and security leaders are faced with the challenge of provisioning, managing and securing mobile devices in their corporate environments. Now with smartphones, tablets, PCs and Macs in the workplace, IT needs a single platform that's capable of managing all devices—no matter what kind.

Although it may sound complex, the approach you can take to manage these devices is relatively simple. Just follow these 11 steps and you'll be on your way to effectively managing mobile in the enterprise.

## 11 best practices for MDM

1. Check yourself before you wreck yourself
2. You don't have to go it alone
3. Try before you buy
4. Knowledge is power
5. Going from big picture to nitty gritty
6. Automate, report and remediate
7. Lock. It. Down.
8. Only the right apps
9. Policies: The spice of life
10. "You used how much data?!"
11. Plays well with others



# 1

## Check yourself before you wreck yourself

Before you begin thinking of the various ways you're going to manage your devices, you first need to understand what types of devices are in your environment. Here are some questions all IT professionals should ask in their initial assessment:

- **What kinds of devices am I managing?**
  - Apple iOS or macOS? Google Android? Microsoft Windows?
- **How many devices are in my environment?**
  - Where do I go for a definitive number?
- **What use cases do I have in place for my devices?**
  - What specific applications (apps) do I need for specific tasks?
- **What are my devices connecting to internally?**
  - Microsoft Exchange ActiveSync? Microsoft Active Directory? Google Apps? EWS? IBM® Notes® Traveler?

Only when you've answered these questions can you begin planning the next steps for your MDM implementation.

# 2

## You don't have to go it alone


Before you actually take the initial steps on your mobile journey, what's ahead can seem daunting. You're pressured to make sure that all devices are accounted for and running properly—but you aren't sure how you're going to keep track of it all.

Make sure to evaluate an MDM tool that has a strong partner network that you can rely upon to execute your strategy—or that has the framework in place to support you before you begin your rollout.

A strong MDM provider will have resellers, managed service providers (MSPs), carriers and other types of partners you can work with hand-in-hand to assess your goals and make sure that your steps for getting there are executed properly.

If your IT team will be rolling up its sleeves and doing the management on its own, make sure you work with a vendor that includes complementary pre- and post-sales support—and that has your back from start to finish.

A mobile success service program shouldn't be looked at as an added bonus; it should be an expectation. Make sure your MDM solution has a variety of service packages to choose from that will help you maximize the return on your investment. Make sure you're working with people who've been there before, who understand what you're looking to achieve, and can help get you there.



# 3

## Try before you buy

No matter what, it should be easy to get started with your MDM solution. Make sure yours offers free access to a full-production (not “lite” or limited) portal where you can begin enrolling devices and testing features in minutes. For added convenience, make sure the portal has a cloud delivery model, so you can get started right from your favorite browser.

After you’ve created your account and have access to the portal, device enrollment should be a straightforward process. Make sure it’s simple to:

- **Get your first device enrolled**
  - Whether it’s an Apple iPhone or iPad, an Android, or a Windows 10 tablet, you should be able to get it set up and configured quickly.
- **Configure and publish your initial set of policies**
  - Do your devices need to be passcode protected? Do you want cameras disabled? Is Wi-Fi connectivity important? Customization options should be extensive.
- **Push out some apps**
  - Going back to your use cases, which apps are integral to your environment? Start with these first.



As you begin to familiarize yourself with the portal and begin taking specific actions, ensure that you’re also closing the loop with the device(s) you’re testing.

- Was the enrollment process quick, easy and seamless?
- Are the policies you configured and pushed out going into effect?
- Is it easy to find, access and use the mobile apps that were pushed down to devices?

# 4

## Knowledge is power

Whether you already have some experience or are getting set up with MDM for the first time, the learning process should be quick, intuitive and engaging. Since every solution is configured differently, the process can sometimes be a bit confusing as you go from one solution to the next. It's best to conduct due diligence to determine what educational resources are at your disposal. When reviewing a solution's technical support capabilities, you should ask yourself:

- **What kind of support do I have?**
  - At a minimum, the solution should have a dedicated help desk number or an online chat feature that will enable you to speak with a support representative immediately.
- **Is there an owner's manual?**
  - Portal guides and documentation on how to make the most of your experience are key to a successful rollout.
- **Are there how-to videos if I don't have time to read an owner's manual?**
  - Whether you're a visual learner or have a very busy schedule, video tutorials may be the easiest way to get step-by-step guidance you need, and should be included in your solution's offering.

You should never feel like you've been left in the dark, and there should be plenty of areas where you can go to achieve MDM enlightenment. Ask questions—get answers. It should never be more difficult than that.

# 5

## Going from big picture to nitty gritty

The enterprise is riddled with different endpoints—everything from smartphones, tablets and laptops, to wearables and Internet of Things (IoT) devices. Let's not forget various integrations for email, user directories and secure access to documents. No matter what you need to keep track of, your MDM solution should be accessed through a single pane of glass where you can see endpoints, end users and everything in between.

Here are three best practices to consider in selecting your MDM solution, crafted around the bare necessities:

- Be sure your reporting and inventory tool consolidates all of your enrolled devices and associated information into easy-to-follow reports. You will come to rely on your daily updates, so these should be generated automatically without manual input.
- Beyond the advantages of instant accessibility afforded by cloud MDM, there should be no hardware to buy, install or maintain—and no associated fees. The platform should be automatically updated with new features at your disposal.
- The ability to search for anything and everything with ease is key to a cloud-based solution. You should be able to access your devices, integrations, reports, apps and secure documents all with the simple click of a mouse.

# 6

## Automate, report and remediate

Protecting corporate data is one of the highest priorities for modern IT and security leaders—and, no surprise, also one of the biggest challenges. Your MDM solution should have robust security capabilities that are easy to use.

With sensitive data on both corporate and employee devices, you should be able to know and control what is accessed. Reporting tools must provide in-depth information about device inventory, security risks and compliance. Here are some things to consider when it comes to reports:

- Devices can report their locations over a period of time, so you can see where they've been.
- If a device is out of compliance with your corporate policies, reports and alerts can be generated and immediately sent to the IT staff.
- Remediation should be swift and automatic for violations including device lock, selective wipe or appropriate corporate actions by the human resources department. All these can be viewed with a simple report that can be exported for your enterprise records.

# 7

## Lock. It. Down.

With the rise of bring-your-own-device (BYOD) initiatives, organizations run the risk of exposing their corporate information on employee-owned, personal devices. However, your MDM solution should offer some form of enterprise data containment. The idea is to separate work from play, so your IT team has more control of what the user has access to—and, more specifically, who has access to the data on that device. Your MDM solution should be able to set up specific guidelines for accessing secure data, and it should take actions in case of a potential breach such as lost or theft of a device.

When considering secure containment, ask yourself:

- **What should I do if a device is lost or stolen? How can I protect my organization's data?**
  - Your MDM solution should be able to remotely locate, lock and wipe a device. Some solutions offer a “selective wipe,” which will affect only the data and settings you've pushed down to the device, leaving the personal information intact.
- **How can I lock down my corporate data?**
  - Locking down data is simple. In most cases, you can set up enterprise data security through a policy and apply it to the user and/or the device. Security can include passcode protection for the MDM app and time-based restrictions for when users can access their corporate data, including email and documents.

# 8

## Only the right apps

With the advent of a custom home screen, your organization can dictate what apps will appear on your corporate devices and limit users from non-essential apps. Android and iOS devices can enable a device “kiosk,” where users can see only enterprise-approved apps, and nothing else. Limiting access to apps means there is less of a chance of a user breaking corporate policy; the result is to make it easier to manage the device. Also, when there aren’t any games or non-enterprise approved apps on the device, users will be more productive.



# 9

## Policies: The spice of life

When mapping out your MDM strategy, it’s wise to keep in mind what kind of device policies you’re going to need. An MDM solution should offer a customizable policy that can be built upon previous iterations—not to mention accommodate an unlimited number of policies. This way, you can have fully customized policies set for the specific needs of your enterprise at a moment’s notice. As an added bonus, your MDM should offer cloud-sourced benchmarking capabilities that allow you to compare your configurations to those of your peers with the same company size or in the same industry.

- **Why are multiple policies recommended?**
  - Policies can be applied to an individual user/device, a defined group or everyone in the enterprise. Multiple policies can also be used if and/or when a device is out of compliance and security measures must be taken.
- **What should I look for in a policy?**
  - You should be able to easily change detailed aspects of the device’s behavior to match your organization’s needs. You also should be able to set up profiles for Wi-Fi, email and virtual private network (VPN) capabilities.

# 10

## “You used how much data?!”

All too often, a major pain point with company-owned devices is cellular data usage. With the rise of streaming video and music services, data usage can grow out of control pretty quickly, and you’ll be stuck with the bill. Your MDM solution should be able to integrate with all of the major carriers in your region.

Your organization has the ability to set up data limits to alert users and staff when they are going close to, or over, their monthly allotment. Along with these alerts, there are automatic actions that can be taken against users if the need should arise. It’s best to have a conversation with your wireless carrier about what can be done to limit users from going overboard with their data use.

- Learn how your carrier can help curb data overages.
- Your MDM solution should be able to integrate with your carrier.
- Data usage reports should be a part of your solution’s offering.

# 11

## Plays well with others

Your MDM solution should be able to integrate with mobile device manufacturer solutions, such as Android work profiles, Samsung Knox, Apple’s Device Enrollment Program (DEP) and Apple’s Volume Purchase Program (VPP). These integrations will be key ingredients to your MDM success because they can make overall management easier and save you time, money and stress.







## About IBM MaaS360 with Watson

Thousands of organizations of all sizes across all industries trust IBM MaaS360® with Watson™ as the foundation for their digital transformation with endpoint and mobile. The industry's first and only cognitive unified endpoint management (UEM) platform, MaaS360 delivers augmented intelligence (AI), contextual analytics, and strong security controls across users, devices, apps and content to support endpoint and mobile deployments. Delivered from a best-in-class IBM Cloud on a mature, trusted platform, MaaS360 helps to manage a wide variety of devices for multiple users from a single console, and to provide integration with solutions from Apple, Google, Microsoft and other suppliers of management tools. IBM works hand-in-hand with these suppliers not only to provide integration but also to ensure that integration can occur as soon as new tools or updates to existing tools are available.

### For more information

To learn more about MaaS360, and to start a no-cost 30-day trial, visit: [ibm.com/maas360-trial](https://ibm.com/maas360-trial)

## About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 30 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.





Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: [ibm.com/financing](http://ibm.com/financing)

## IBM MaaS360



© Copyright IBM Corporation 2018

IBM Security  
New Orchard Road  
Armonk, NY 10504

Produced in the United States of America  
January 2018

IBM, the IBM logo, ibm.com, MaaS360, Watson, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.