Mobile Device Management: Ensuring Functionality, Security, and Productivity

Author: William G. Wenzel, Ph.D.
# Table of Contents

- **Executive Summary**
- **An Overview of Mobile Device Management Technology**
- **Benefits of Mobile Device Management**
- **Challenges of Mobile Device Management and How to Overcome Them**
- **Mobile Device Management Use Cases by Industry**
- **Strategies for Successfully Integrating Mobile Device Management into Your Business**
- **The Future of Mobile Device Management**
- **Frequently Asked Questions About Mobile Device Management**
- **Conclusion**
- **References**
- **About U.S. Cellular®**
Executive Summary

This paper will give an overview of the Mobile Device Management (MDM) landscape and, where it is appropriate, inject a historical perspective about how the technology has evolved. This paper will also attempt to elaborate on how, in general, MDM solutions have been received by employees, managers, and executives. Then, the paper will dig deeper into the specific benefits and challenges associated with MDM. Examples from prioritized industries (e.g., Healthcare, Professional Services, Construction, Government Municipalities, Transportation, and Retail Services) will help bring the benefits to life and provide a context for the value of overcoming the challenges. Next, the paper will introduce a strategic approach for how to successfully integrate MDM solutions into businesses. All the while, the paper will attempt to focus on the industries and organizations that could benefit the most from MDM. Finally, the paper will briefly forecast the future of MDM and answer some frequently asked questions.
An Overview of Mobile Device Management Technology

Mobile Device Management (MDM) is a type of software that helps organizations monitor, manage, and secure corporate-owned and employee-owned mobile devices in the workplace. MDM solutions allow companies to securely transfer sensitive data by controlling aspects of device usage, such as permitted applications and outbound communications. The best MDM solutions are capable of working alongside any service provider and on multiple operating systems, including iOS, Mac OSX, Android™, and Windows. An example of MDM software is MaaS360 by IBM.

MDM involves:

1. Managing device policies, configurations, and patches, and supporting these devices as if they are desktop computers
2. Storing corporate information and data in a separate container on mobile devices, away from personal information via a secure Personal Information Manager (PIM)
3. Sharing and synchronizing content, applications, and data
4. Acting as a security gateway to applications and the network

Why do organizations need MDM solutions?

First, MDM is needed because of the increased use of mobile devices, such as Smartphones and Tablets, in the workplace. Companies have mostly moved away from BlackBerry® and are harnessing the power of a diverse array of mobile devices to tap the functionality and efficiency of fleet management technology, wireless forms, and wireless sensors, each of which is tied to the concept of the Internet of Things (IoT). IoT refers to all the connected devices in the world that help people achieve specific goals by monitoring the environment, collecting data, and autonomously collaborating with other devices to optimize human productivity. When this increased productivity occurs in the workplace, businesses make more money. Therefore, MDM helps businesses reap financial rewards.

Second, MDM is needed because of the booming Bring Your Own Device (BYOD) movement. BYOD refers to the phenomenon in which employees use their personally-owned mobile devices for work. This is a very common occurrence, since 90% of full-time American workers report having used their personal Smartphones for work purposes. Organizations can choose to fully empower employees to embrace this practice, completely discourage it, or strike some middle ground.
Companies have three options when crafting their BYOD strategy:\(^8\)

1. **Full BYOD Strategy** - Employees are required to use their own devices for work, and the employer offers a monthly stipend for business use.

2. **Hybrid BYOD Strategy** - Employers give employees the option of using corporate-owned devices, bringing their own, or choosing from a selection of pre-approved personally owned devices that are supported by the program. The company incentivizes the use of the pre-approved devices by offering a monthly stipend for business use and possibly negotiating with a wireless carrier to offer a group corporate rate.

3. **Corporate-owned Strategy with BYOD Policy** - The company owns all mobile devices that are used for business and enforces a strict policy about personally-owned devices to ensure data security in the workplace.

No matter which stance a business takes regarding BYOD, managers and executives must be aware that employees will routinely use their own mobile devices in the workplace, with or without organizational knowledge and oversight.\(^9\) Companies must attempt to maximize the functionality and productivity of these personally-owned mobile devices, while ensuring data security.

Adopting MDM technology is one of the best ways in which organizations can maximize the benefits and address the challenges of successfully integrating employee devices, as well as mobile devices in general, into the workplace. In the next section, we will explore some benefits of MDM in greater detail.
Benefits of Mobile Device Management

MDM is especially important for organizations that allow employees to use their own mobile devices for work. However, even companies that choose a corporate-owned strategy can benefit from these solutions.

There are four tiers of MDM, whereby each progressive step adds a new set of capabilities to the lower levels. Here is an overview of the features that are present at each tier:

<table>
<thead>
<tr>
<th>Tier</th>
<th>Features</th>
</tr>
</thead>
</table>
| 1. Basic Policy Management | a. Allows for full device wipes  
  b. Enforces password policies  
  e. Allows for role-based administration of different users  
  f. Includes a user self-service portal  
  g. Provides analytics |
| 2. Basic Device Management | a. Allows for full and partial device wipes  
  b. Deploys public and private applications  
  c. Keeps an inventory of hardware and applications  
  d. Provides basic management of iOS and Android™ systems  
  e. Supports Volume Purchase Programs of applications |
| 3. Advanced Device Management | a. Provides comprehensive iOS and Android™ management  
  b. Supports Mac OSX and Windows  
  c. Supports Windows Phones  
  d. Detects jailbroken devices, which are devices that have no software restrictions and allow users to access and modify operating system files |
| 4. Enterprise Mobility Management | a. Enables mobile application wrapping, or the layering of policies onto an app without changing the app (e.g., adding user authentication, preventing file sharing, limiting copy/paste)  
  b. Enables the use of a Software Development Kit (SDK) to create custom applications  
  c. Includes a secure Personal Information Manager (PIM), or container, to keep corporate and private data and applications separate  
  d. Allows for a secure web browser  
  e. Facilitates mobile content pushing, pulling, and syncing  
  f. Uses contextual awareness, such as location, to control access to certain features of mobile devices and to the network  
  g. Includes a Single Sign On (SSO) user authentication process across mobile and web applications |
These user-based MDM tiers are often related to the types and amounts of sensitive information employees need to access. Therefore, security posture is at the core of MDM. In a connected world, it has become increasingly important to protect sensitive data, while still allowing employees to access and share information. MDM helps keep this information safe, while allowing people to do their jobs. For example, MDMs allow organizations to enforce password protection, detect unsafe jailbroken devices, and remotely wipe data in case devices are lost or stolen. At more advanced stages, MDM can also ensure secure web browsing, enable app wrapping, and provide a seamless user authentication process.

PIM clients are another advanced feature of MDM that help with security. That is, these containers keep corporate and personal data separate. Employees use credentials to log in to the authenticated and encrypted area of their device to access certain information, as well as special applications. In some cases, a company could even restrict copy/paste, screenshots, browser activity, etc. in these containers. IT departments are able to backup, wipe, and restore only company data in the container, which helps organizations balance security of company data, while assuaging privacy concerns of employees about their personal information. Some data containers also allow administrators to push data and documents to them, which makes for a very functional environment in which employees can access the information they need to do their jobs most effectively.

This brings us to the important productivity benefits of MDM. By pushing and pulling important applications and content (e.g., documents and applications) to devices, organizations are able to empower their employees with the most up-to-date information and tools to get their jobs done. Secure gateways even allow for internal file sharing, collaboration, editing, and saving to shared folders, which enable effective teamwork among people in any location.

Summary of Benefits

1. Increased functionality of devices
2. Improved data security
3. Higher employee productivity
Challenges of Mobile Device Management and How to Overcome Them

Although there are important benefits of MDM, there are also some challenges.

There is usually a direct cost associated with setting up and maintaining MDM solutions. The cost typically increases as a company adds more advanced features. However, organizations must weigh this particular challenge against the benefits of adopting the technology.

Another challenge is that secure PIM containers might not be able to protect everything. For example, they might not be able to house enterprise applications, other third-party applications, or device browsers and email clients if the specific file types are not supported. This could limit the applications that an organization and its employees can use.

PIM containers could also change an employee’s normal workflow, forcing users to access information in new ways and causing them to have to learn new processes to do the same job. Companies might consider only using secure data containers on the highest-risk devices or on the devices of employees who have access to the most sensitive information.

A recent study revealed that MDM solutions can potentially compromise employee privacy by tracking data, revealing real-time location, browsing history, and personal information, including login information and general interests. In addition, MDM software can remotely wipe personal data stored on employees’ devices. These issues concern employees, so companies should choose an MDM solution and pick settings that ensure data security but do not compromise employee privacy.

Summary of Challenges

1. Cost
2. Limitations of PIMs
3. Employee concerns about privacy
In this section, we dig deeper into the specific benefits associated with Mobile Device Management technology by providing examples from several industries (e.g., Healthcare, Professional Services, Construction, Government Municipalities, Transportation, and Retail Services).

**Healthcare**

In a healthcare setting, security concerns are more serious than in a lot of other industries. This is because Health Insurance Portability and Accountability Act (HIPAA) laws, enforced by the U.S. Department of Health and Human Services’ Office for Civil Rights, require maintaining strict control over personal health information.

Lehigh Valley Health Network is one of America’s premier healthcare organizations. They are employing a fleet of mobile devices to treat a large number of patients and stay on the forefront of modern healthcare practices. They realized that the use of mobile devices would allow caregivers to make accurate assessments, track their work, and collaborate with other departments. At the same time, the hospital wanted to ensure security of sensitive patient data. The hospital seized the opportunity to leverage mobile technology and deployed an MDM solution to manage their fleet of devices and ensure security.

As a result, the hospital has been able to greatly enhance patient care. For example, the Home Care department uses mobile devices for nurses who work in patients’ homes. The Division of Education is looking into using devices for training new employees. Hospital staff members are using devices with an interpreter service to communicate with patients who don’t speak English. The hospital is even giving mobile devices to high risk pregnancy patients to track their health throughout the duration of their pregnancies. Taking full advantage of the new technology, the hospital uses a Volume Purchase Program (VPP) to manage more than 2,000 application licenses that are distributed to their mobile fleet.14

**Professional Services**

Burr & Forman LLP, a century old, full-service law firm with offices in Alabama, Florida, Georgia, Mississippi, and Tennessee, needed to manage the transition from BlackBerry® to a variety of mobile devices. They chose a hybrid BYOD strategy that involved a mix of corporate-owned and personally-owned devices. The company wanted to ensure productivity and uptime, provide a great end-user experience, support multiple mobile applications, and control and manage devices that accessed the network. The company also wanted to maintain control over devices when employees used them for work purposes outside of the office. To achieve their goals, they implemented a strict BYOD policy and MDM solution.

As a result, the company is deploying and managing a variety of mobile apps that help their employees be more productive wherever and whenever they are working. They are also ensuring that sensitive data is kept secure.15

**Construction**

Arrow International (NZ), a construction company in New Zealand with 10 offices and a strong regional presence, recently began deploying mobile apps to reduce paperwork and save money. These new apps allow project/site managers to more easily capture and distribute information about construction sites. Because the company was going mobile and relying heavily on applications to collect and share sensitive data, they needed a solution that would simplify the management of Smartphones and Tablets in the field, while enhancing security. To achieve this goal, the company began using cloud-based MDM software that enabled them to swiftly distribute the new apps to every device.
As a result, the MDM software protects the company’s intellectual property by detecting and remediating malware threats. In addition, the company is saving substantial time and money related to mobile administration. Previously, it had to have a staff engineer focus solely on mobile devices. Now, the employee is freed up to focus on other areas that will add value to the business. Project/site managers also experience less downtime, because they do not have to send their mobile devices to the office for updates. Overall, the company expects their return on investment to be in the tens of thousands.16

Government Municipalities

The City of South Bend, Indiana sought innovative ways to serve its residents, without spending too much money. They decided to empower their workforce to be more mobile by giving them quick and secure access to email, city maps, and record keeping procedures for better communication in the field. A specific program that they wanted to streamline was their Vacant and Abandoned Properties initiative, which required the evaluation of 1,000 vacant and abandoned homes for rehabilitation or demolition. To efficiently evaluate these properties, employees required accurate record keeping tools and constant communication with colleagues.

As a result of using an MDM solution, the city doubled their inspectors’ productivity in the field and reduced their workforce by 40%. The city has also been able to increase its government transparency with their citizens by creating a digital paper trail for the project and more quickly collecting feedback from residents about how the program is affecting their communities. The city has experienced so much success that it is exploring options for putting more mobile devices in the hands of local police and engineering departments within the government.17

Transportation

Garuda Indonesia, a national airline, sought to provide its pilots with an “electronic flight bag” to replace paper aircraft manuals in the cockpit. The traditional printed manuals often weighed more than 66 pounds and required pilots to transport them in rolling suitcases from flight to flight. To find the necessary information they needed to perform required safety checks and calculate performance metrics, pilots had to painstakingly search through the stacks of paper documentation.

To save this time and effort, the airline created an electronic Performance Calculation app and electronic Viewer for their aircrafts. These apps provide all the data and calculations that pilots need to help ensure the safety of flights. To manage the deployment of the new apps and update content in real time, the airline adopted MDM software that would meet their immediate needs and could be scaled to support growth of their mobile push.

As a result of deploying the MDM software, the airline increased pilot productivity over previous processes by 50% and operations staff productivity by 30%. Pilots can now find the information they need and perform calculations in 5 minutes that used to take 10-50 minutes. In addition, the airline was able to meet all the necessary regulatory requirements for mobile device management and reduce its implementation time and costs.18

Retail Services

Luxottica Group, a luxury and sports eyewear company with 7,000 retail stores around the world, wanted to enable their sales associates to use mobile devices in their LensCrafters, Sunglass Hut, Oakley, Pearle Vision, Sears Optical, and Target Optical stores. The goal was to improve customer engagement and increase security. The company chose a cloud-based MDM solution that would provide security and mobile content management for any kind of device. Then, they deployed more than 7,000 Tablets that sales associates could use to locate, sell, and ship products to customers at the touch of a button.

As a result, mobile content management empowered the organization to distribute apps and push content to employees. Sales associates are able to take advantage of these applications and allow customers to “try on” different styles of eyewear and post photos of the potential purchases via social media. This provides a more streamlined, engaging, and interactive branded experience for their customers. Finally, store managers are able to access new training content in real time to better train their employees.19
Strategies for Successfully Integrating Mobile Device Management into Your Business

Business decision makers should look for MDM software that...

1. Works on multiple operating systems and devices.
2. Has the ability to increase productivity and employee satisfaction.
3. Enhances security and compliance.
4. Enables mobile application management and security.
5. Allows managers to distribute, edit, and share content securely.
6. Prevents malware threats.

Business decision makers should also strive to...

7. Use MDM software that allows them to place business data in a secure container on employee devices but does not impede usability of the devices.8
8. Keep personal information private.10
9. Communicate with employees and include them in decisions that could affect their personal devices and data.20
10. Ensure staff understands ownership of information on each mobile device that is used for work and understands under what conditions data might be remotely wiped.21, 22
11. Consult legal about getting express written consent about wiping any data on employee-owned devices and set policies in advance of an incident.23
12. Decide what amount of mobile device management their company needs, whether that is basic policy management, basic device management, advanced device management, or enterprise mobility management.11
13. Understand that there could be ways for some smaller organizations, or those with minimal security concerns, to operate without an MDM solution. However, even these organizations should still adopt a device policy.11
The Future of Mobile Device Management

Enterprise Mobility Management (EMM) has already begun to take over for MDM, and this trend will continue into the near future. EMM is an all-encompassing term that includes devices, data, applications, security, overall management of device functionality and security, and enhancing employee productivity through the use of mobile.

EMM combines MDM, Mobile Application Management (MAM), and Mobile Information Management (MIM). Mobile Content Management (MCM) is also part of this multi-faceted approach. Breaking the functions down in these ways allows organizations to be more flexible and adaptable in a world where an increasing number of the devices that are used for work are owned by employees. This new way of operating relinquishes some control over devices themselves, which is often too challenging to achieve in the rapidly evolving BYOD context, and puts the controls on applications, information, and content instead.

In addition to the shift toward EMM, it is likely that we will see advances in the user experience of PIM containers. One of the challenges related to these containers is that they usually force employees to change their normal workflow and learn new mobile environments. More seamless integration of these containers will eventually benefit end users.

There will also likely be changes in the way IT manages devices. For example, they might utilize new technology, such as Smartwatches, to receive security alerts in real time and immediately access and review information about possible breaches on Smartglasses. At the same time, there will need to be advances in security for these types of wearable devices.

Finally, MDM will probably begin to incorporate artificial intelligence, which will automatically learn from the past and adapt to help mobile devices perform more effectively and efficiently, while ensuring better data security.
How difficult is it to incorporate an MDM solution?

It is not very difficult if you communicate well with your employees about your new device management policy. You should attempt to make the policy and implementation process as simple as possible to maximize the chance that employees will follow new protocols.

Will MDM solutions compromise my employees' privacy?

Your best MDM option for minimizing privacy concerns is a solution, such as MaaS360, that places business data on your employees’ phones into a secure container. This containerization keeps business data secure and separate from private data. You should always be careful to explicitly outline what data is shared between the employee and the company, and what is private employee information.

Who can I turn to for additional advice on MDM solutions?

You can start with your IT personnel, as well as your internet and cellular service providers. You should also consult legal counsel about compliance issues and drafting employee agreements.
To help decision makers understand the topic of mobile device management, this paper dug into the context of why MDM is needed. Chiefly, MDM is needed because of the increasing diversity of devices present in the workplace and the variety of security threats that attackers use to compromise sensitive data.

The paper also illuminated the benefits and challenges of adopting MDM solutions. The benefits include increased functionality of devices, improved data security, and higher employee productivity. Challenges include direct monetary costs, certain limitations of PIM containers, and employees’ concerns about privacy. To maximize the benefits of MDM and overcome the challenges to adoption, companies must choose the appropriate level of device management that is right for their organization. Depending on their needs, organizations can implement basic policy management, basic device management, advanced device management, or enterprise mobility management. The paper also highlighted the features and benefits of MDM software with example use cases in numerous industries, including healthcare, professional services, construction, government municipalities, transportation, and retail services.

To help decision makers approach the process of implementing an MDM solution, this paper offered strategic pointers. The most important thing for managers and executives to keep in mind is to be as transparent as possible with employees and involve them in the implementation process. Armed with all of this new information, plus future directions of MDM and a few FAQs, you can be more confident that you will make the right decisions for your company about deploying an MDM solution to ensure your organization takes full advantage of the benefits and overcomes the challenges of adopting MDM.
References

17. Airwatch by VMware Case Studies. City of South Bend reduces IT costs by $5,000 a year with AirWatch-managed devices. Available: air-watch.com/downloads/resources/20150612_AirWatch_Case_Study_SouthBend_digital.pdf

Disclaimer: This white paper is provided for informational purposes only. Although this white paper is intended to provide accurate information with regard to the subject matter covered, the authors and their organizations accept no responsibility for errors and omissions. This white paper is provided “as is” with no warranties whatsoever including any warranty of merchantability or fitness for any particular purpose.
References


U.S. Cellular® offers a broad suite of solutions for your business. Finding the right technology solutions for your business can be complicated and you want to make sure you invest wisely. Let our Business Concierge Services Team help. We’ll listen to your needs, explain your options and deliver a solution that’s right for your business. You’ll get everything you need. Nothing you don’t. And you can be confident in your investment.

With a network that works coast to coast and in the Middle of Anywhere, offering the latest Smartphones, Tablets, and technology—U.S. Cellular has everything your business needs to stay connected and thrive.

Call today for a free, informational consultation: 1-866-616-5587 or go to uscellular.com/business to learn more.