Making Everything Easier!™

ManageEngine Special Edition

Managing and Securing Mobile Devices

FOR DUMMIES®

A Wiley Brand

Learn to:

- Manage a diverse mobile environment
- Address mobile security concerns
- Integrate user-owned and company-owned devices

Brought to you by ManageEngine

Brian Underdahl

About ManageEngine

More than 120,000 companies around the world — including three of every five Fortune 500 companies — trust ManageEngine products to manage their networks, data centers, business applications, IT services, and security. More than 300,000 administrators optimize their IT using the free editions of ManageEngine products.

For more information about ManageEngine products, visit **www.manageengine.com.**

Managing and Securing Mobile Devices

FOR DUMMIES®

A Wiley Brand

ManageEngine Special Edition

by Brian Underdahl

FOR DUMMIES®

A Wiley Brand

Managing and Securing Mobile Devices For Dummies®, ManageEngine Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-34985-3 (pbk); ISBN 978-1-119-34984-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Executive Editor: Katie Mohr

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Magesh Elangovan

Table of Contents

Introduction

Organizations are rapidly embracing a move to mobile devices to serve the communication and computing needs of their people. These devices enable greater mobility, faster responses, and higher productivity. At the same time, mobile devices present new challenges in areas such as compatibility, security, access, and device management. Rapidly evolving mobile environments demand that organizations have the ability to adapt and adjust quickly to remain competitive while ensuring the security of their assets and the data they store.

About This Book

Managing and Securing Mobile Devices For Dummies, ManageEngine Special Edition, introduces you to the challenges and options of meeting the increasingly complex world of mobile devices. You'll see how you can manage a mobile environment that includes many different types of devices. You'll be introduced to some important security concerns that are unique to mobile devices. You'll also see how you can manage both user-owned and corporate-owned devices successfully.

In short, this book shows you how to successfully survive in an increasingly mobile world.

Icons Used in This Book

This book uses the following icons to call your attention to information that you may find helpful in particular ways.

The information in paragraphs marked by the Remember icon is important and therefore repeated for emphasis.

Sometimes I need to introduce a bit of technical information in order to more fully explain a particular topic. You can think of the text marked with this icon as your chance to pick up a bit of jargon you can use to impress your boss in the next staff meeting.

The Tip icon indicates extra-helpful information.

Where to Go from Here

Hey, it's your book, so dive in anywhere. No, seriously. You can thumb through the book anywhere you like, skipping around here and there. Or, you can read it straight through from front to back if you prefer. Either way, when you're finished, you can keep it handy and refer back to it at any time you want.

Chapter 1

Understanding the Move to Mobility

In This Chapter

- Looking at mobile technology advances
- Gaining confidence in your devices
- Making sure you have the right apps
- Managing and securing mobile environments

The enterprise workforce is rapidly becoming more mobile as devices such as smartphones and tablets enable workers to be productive no matter where they might be. This chapter takes a look at the factors influencing this shift, discusses how you can increase your comfort level with this move, shows you how having the right apps is important, and touches upon the tasks of managing and securing your mobile devices.

Seeing the Advances in Mobile Technology

Anyone who has shopped for a smartphone recently knows that the manufacturers are in an arms race to

see who can add the most power and new features to their devices. Gigabytes of memory, better displays, and more powerful processors make each generation of these devices even more capable. Likewise, the technology in mobile devices such as tablets has also been rapidly advancing.

More capable mobile devices have enabled users to take their computing power with them, thus decreasing the use of workstations and even laptops.

Mobile devices such as smartphones and tablets often serve slightly different needs. While both can provide email access and enable users to view documents, users often prefer the larger screen of a tablet for editing documents, filling in forms, or accessing web meetings.

Establishing Confidence in Mobile Devices

As device manufacturers have begun to realize the importance of mobile devices to the enterprise, they've been focusing more of their efforts on the needs of the enterprise. This increased focus has resulted in better security, better apps, and higher productivity.

One area where device manufacturers have worked to improve their devices has been in biometric security. For example, it's much harder to bypass enterprise security controls on a mobile device that uses a fingerprint or iris scan in place of unreliable passwords. Passwords can be lost, stolen, or even guessed, but it's nearly impossible to fool a

fingerprint reader or an iris scanner. In fact, Microsoft Windows Hello's facial recognition system was even shown to be able to tell the difference between identical twins.

Finding an App for Every Organizational Task

Another factor in the popularity of mobile devices has been the growth of apps. Unlike the large application programs typically found on workstations and laptops — and loaded with features most users will never use — apps are small, focused, and easy to use.

Apps are available for many different industrial and business tasks. In fact, mobile device app stores contain thousands of apps to suit different needs. In addition, because apps are small and focused, developing a specialized app to suit a unique need is generally a fairly easy and inexpensive task.

Different mobile devices use different operating systems. Apps that run on one OS can't be used on a different type of device without some special adaptation. For example, Apple uses different operating systems on its phones (iOS) and desktops (macOS), so you need different app versions on each of them. iOS apps don't run on any flavor of Android or Windows, and the same applies in reverse.

Considering Management and Security

The rapid growth of mobile technology and devices has created some new concerns for the enterprise. Unlike the traditional workstation that typically resided within your physical workspace, mobile devices can be used from a wide variety of locations, thus making controlling access to corporate resources and securing apps a far more complicated task.

You can't, for example, have a mobile workforce if all the resources they need are locked up inside your office. At the same time, you can't throw open the doors and allow people to come and go as they please, taking whatever they want with no control.

Unfortunately, the broad range of mobile devices that are in use means that managing and securing those devices can be complicated. As I mention earlier, different types of devices use different operating systems and therefore different controls are needed to accommodate the spectrum of devices.

As later chapters show, ManageEngine has developed a solution called Mobile Device Manager Plus to help you address the complex task of managing and securing diverse mobile devices.

Chapter 2

Managing Mobile Devices

In This Chapter

- Understanding the realities
- Creating your guidelines

The move to mobile devices brings many changes to the management cycle. This chapter introduces a number of factors you'll need to consider and also discusses some guidelines you can use to make certain that you've covered all the bases with your management plans.

Defining the Inevitable in Mobile Environments

In order to effectively manage your mobile devices, you need to be able to define and understand the entire landscape. By first seeing the inevitable set of issues involved in the typical mobile environment, you won't be faced with unexpected surprises later.

Enterprise-owned devices

These days, most mobile environments are comprised of a mix of enterprise-owned and user-owned (or BYOD — *bring-your-own-device*) devices. From a management perspective, enterprise-owned devices entail some considerations that BYOD largely avoids. These include the cost of:

- Liability
- Maintenance
- Upgrades

Depending upon the particular types of devices your enterprise owns, you may also have some multiplatform considerations as mentioned in Chapter 1. For example, although Windows 10-based devices use a common operating system, the same is not true of Android or Apple devices. As a result, you may need to license different versions of apps depending upon whether a user has an Apple, Android, or Windows tablet or a smartphone.

You can reduce some of the difficulties involved in multiplatform environments by applying a management solution that supports a broad range of platforms. For example, ManageEngine Mobile Device Manager Plus supports iOS versions 4.0 and later (iPhone, iPad, and iPod touch), Android versions 2.2 and later (smartphones and tablets), and Windows Phone 8 and later, as well as Samsung SAFE and Knox.

Common management problems

In addition to the unique management challenges posed by enterprise-owned devices, you need to deal with a number of scenarios such as:

- **BYOD (bring-your-own-device):** Devices owned by the worker
- **COPE (corporate-owned, personally enabled):** Devices owned by the corporation and assigned to the worker
- **CYOD (choose-your-own-device):** Devices owned by the corporation, where the worker can choose the specific device
- **COSU (corporate-owned, single-use):** Devices intended for a single, specific purpose such as digital signage, ticket printing, point of sale, or inventory management

Although each of these situations is slightly different, you're likely to encounter some common themes. For example, users may feel a sense of ownership that gives them the right to install whatever apps they prefer. Unfortunately, when users install apps that you haven't approved, you face additional security concerns. These can include viruses, key loggers, or other malware intended to steal or corrupt corporate data.

In addition, increasing the number and variety of mobile devices presents a greater challenge in your efforts to control access to enterprise resources. You need a management solution that automatically works across a multitude of devices and provides the necessary security protocols so that unauthorized users can't gain access to your corporate systems.

Remember that many of your workers are already bringing their own devices to work, whether you sanction that practice or not. This reality means that even if you'd prefer to deal with an environment where you have complete control over all mobile devices, a realistic plan must include BYOD.

End-user app usage

End-users expect to be able to use their favorite apps on their devices, especially if they own their devices personally. If you allow BYOD, you need a mobile device management solution that includes:

- Containerization of corporate data
- Separate profile strategies for employee-owned devices
- Access denial to corporate resources
- Effective management of different types of devices
- Confidence that the owner's personal data is untouched

A mobile device management solution that includes these features enables people to use their personal apps but acts as a firewall between those apps and your corporate resources. Users can play Pokémon Go without corrupting your systems.

Considering Ways to Control and Monitor Mobile Endpoints

Given the complexity you're likely to face in your mobile device environment, it's important for you to

establish some guidelines as you look for the best solution for your organization. Here are some points to consider:

- **Managing device diversity:** Although you could try to limit users to certain devices, in reality, you'll need a solution that supports many different types of devices. Remember that today's hot device could easily become tomorrow's Blackberry. The mobile device world is evolving at such a rapid pace that you simply can't afford to be stuck with proprietary, obsolete systems that won't meet users' future needs.
- **Deploying over-the-air configurations:** Another important consideration as you plan your system is ease of registering and configuring mobile devices that will be used in your environment. You need a system that enables users to perform these tasks remotely.

You can also use your over-the-air configurations system to deploy necessary updates without user intervention. These automatic updates can help you maintain system security because you don't need to rely upon users to apply those updates in a timely manner.

- **Controlling compliance:** Depending on your industry, you may have a number of compliance requirements such as retaining copies of all messages for a specified period of time. Even if you don't have regulatory requirements to comply with, you may have certain corporate policies that you want to enforce. Your mobile device management solution should take into account all requirements, whether they are regulations or corporate policies.

- **Maintaining access controls:** Finally, you need to establish guidelines regarding controlling access to enterprise resources. For example, certain information such as employee records almost certainly should be restricted so that only authorized personnel can access it.

  You may also need a policy that specifies exactly who is allowed to access corporate resources using mobile devices. Make sure that your mobile management solution is flexible enough that making changes to these access rights is both simple and fast.

Chapter 3

Understanding Mobile Security

In This Chapter

- Understanding mobile device security
- Looking at the threats to apps

As your organization adopts an ever more mobile device-oriented work environment, it becomes vital that you understand the security issues that are involved so that you can act to protect your resources. This chapter looks at the two major elements of mobile security: the devices, and the apps they run.

Looking at Device Security

The move to mobile devices has brought about big changes in device security. In the past, the IT department could count upon a pretty stable environment where end-users typically worked on-premises using equipment and applications vetted by and controlled by IT. These days, users are more likely to have mobile devices that they expect to be able to use anywhere.

These changes have brought a new set of challenges that you need to deal with.

Device loss or theft

As the name implies, mobile devices are small and portable. Users carry them along, and unfortunately, often lose them.

But even when users are careful, mobile devices have another characteristic that makes them an attractive target for theft — they tend to be expensive. A thief can easily pocket a high-end smartphone or hide a tablet, and probably won't have much trouble quickly selling it.

Depending upon the type of mobile device and how secure your network is, thieves may find that the access to your corporate resources they may obtain is worth far more than the cost of the device. It's vital that users report any loss or theft of a device as soon as possible so that you can immediately deny access from that device to your network.

All recently produced smartphones have the capability of being locked or wiped remotely. Make sure that this capability is enabled (often it is turned off by default) on all your devices and that you have a record of information such as passwords, serial numbers, or International Mobile Equipment Identity (IMEI) numbers that you will need in order to initiate a remote lock or wipe.

Jail-breaking and rooting

Mobile device operating systems generally include controls that prevent users from installing apps from any

source except an official app store. Apps found in an official app store are vetted by the store in an effort to weed out any that contain malware.

In order to circumvent these controls, users sometimes *jail-break* or *root* their devices. This procedure modifies the device to allow any app to be installed, no matter the source. This modification essentially removes the app protection from the device and can present a major security threat to your corporate resources.

You need a strong policy against jail-breaking or rooting of any mobile device that's allowed to access your network. But often a policy is not enough. You need to make sure that your mobile device management solution can detect modified devices and prevent them from gaining access to your network.

Open network access — a losing game

Mobile users need to access corporate resources on the go. In order to gain this access, their mobile devices must connect to your network.

The easiest way of allowing mobile users to access your network would be to simply make your network open so that making a connection is quick and easy. Unfortunately, such open access means that anyone can easily access your network and therefore browse any corporate resources he or she cares to. Obviously, you can't afford to let anyone come in and take whatever that person wants.

You need effective network access controls that can allow authorized people in, while at the same time keeping out unauthorized users. At the very least, you need a system that employs authentication such as a username and password.

Many of the more capable recent smartphone models include biometric methods such as iris/retina scans or fingerprint readers to authenticate users. Because these biometric methods are far more secure than old-fashioned passwords, you may find it worthwhile to update to newer devices that include biometrics.

Because passwords are generally considered a rather poor means of security, many experts recommend using two-step authentication, such as a one-time passcode sent as a text message to the device.

Considering App Security Threats

In addition to device security issues, you need to be aware of the threats posed by the apps that run on those devices. Here's a quick look at some of the threats:

- **Hacking** is most often associated with making unauthorized modifications. When applied to mobile devices, these modifications can include such things as jail-breaking or rooting, as mentioned earlier in this chapter, or modifications to apps so that they don't function as the developer intended.
- **Phishing** is a term used to describe social engineering techniques intended to get users to provide private information. In terms of mobile app security, this information is typically a username and password. Once this information is obtained,

an attacker may be able to access your network and steal corporate resources.

- **Malware** is software that does damage or steals information. A common type of malware on mobile devices is software that records information such as account numbers, usernames, or passwords, and then later sends that information to the malware developer via the data connection.
- **Unauthorized file transfers** can steal one of your most valuable resources: your corporate information. You need effective access controls to prevent users from accessing information they aren't authorized to see. For example, many organizations require that mobile devices use biometric or two-step authentication.
- **Distributed denial of service (DDoS)** is a technique used to flood a web server with so much traffic that legitimate traffic can't get through. Often this type of attack is initiated by malware the user doesn't even know exists on his or her device. Strong mobile device authentication may help prevent this type of attack from your mobile workforce.
- **Man-in-the-middle** refers to someone listening in as data passes between two devices. This type of attack enables someone to steal your information as it crosses the Internet.

The best defense against having corporate data stolen somewhere between your network and your mobile devices is to use end-to-end data encryption.

- **Ransomware** is a particularly insidious type of malware that encrypts your data and offers to release the data only if you pay a ransom. Generally, the person demanding the ransom insists on payment in some form of non-traceable electronic currency such as Bitcoin. This type of malware usually arrives as an email attachment or as the result of visiting an infected website. Remote device wiping may help you fight this threat.

Chapter 4

Considering BYOD and Corporate-Owned Practices

In This Chapter

- Living with BYOD
- Getting the best from corporate-owned devices

As you adopt an ever more mobile environment, it's important that you understand and initiate a set of best practices for both bring-your-own-device (BYOD) and corporate-owned devices. By establishing these guidelines and making sure that everyone in your organization understands them, you'll be far more successful in seeing those practices accepted by your users. This chapter discusses what you need to consider as you establish your corporate practices for mobile devices.

Making BYOD Work

Organizations often find that people work best when they're allowed to choose their tools. BYOD lets people use their own devices to access corporate resources occasionally, most of the time, or completely.

Employees are likely bringing their own devices to work whether you have a formal BYOD policy or not. By establishing guidelines for BYOD, you're taking control of the situation.

People need to have access to your corporate resources such as applications, data, and other files when they're using their own devices. But you need to balance the need for access against the security, privacy, and compliance risks presented by allowing people to use their own devices.

Consider, for example, how your corporate data could be compromised if users decided to save copies of those files to their personal Dropbox accounts. Or imagine the havoc that would ensue if a user connected to your corporate systems with a device infected with a virus or other malware.

To protect your enterprise resources and provide easy, full-featured access to authorized users, you need a BYOD program that's device independent. One way to achieve device independence is to use a solution that virtualizes the desktop environment as well as hosted apps. With this approach, users can access your systems with their preferred devices, but you maintain security and access control.

Using session virtualization also makes it easier for you to implement a single sign-on, not only to your network but also to the apps and file shares that users need. A single sign-on is vital to ease of use, especially on mobile devices that typically rely upon on-screen keyboards for entering usernames and passwords.

Your BYOD system should also implement a virtual firewall between the personal apps and data on a user's device and your corporate apps and data (this process is also referred to as *app-sandboxing* or *containerization*). Essentially, you want to keep the two environments completely isolated from each other so that you maintain the user's privacy and ensure the security of your enterprise data. Your data should never be accessible on a device that isn't properly logged in to your systems. You need to ensure that users can't copy data and store it on their devices or in their private cloud data storage.

Your BYOD policy should also clearly state that although users maintain ownership of their personal devices, all data used in the course of their employment is explicitly owned by the corporation. A statement of this type can prove invaluable if a key employee leaves to join a competitor.

Your BYOD policy should clearly state who will pay for network access using things such as cellular data plans, public Wi-Fi, or a user's home broadband connection.

Managing Corporate-Owned Devices

You almost certainly have a number of corporate-owned devices in addition to user-owned BYOD. Both corporate-owned and BYOD devices require careful management.

As I mention in Chapter 2, you may have several different levels of ownership and use for corporate-owned devices. These may include the following:

- Standard mobile devices configured and distributed to users by the organization
- Choose-your-own-device (CYOD)
- Corporate-owned, personally enabled (COPE)
- Corporate-owned, single-use (COSU)

Regardless of the specifics, corporate owned devices represent a level of capital expenditure you don't have with BYOD.

All mobile devices, regardless of ownership, should have the same types of access controls mentioned in the preceding section for BYOD. If a device is lost or stolen, it doesn't matter who owns that device — you still need effective access controls so that unauthorized users can't compromise your corporate data. With corporate-owned devices, it's vital that you enable all remote locking and wiping options on the device.

Organizations often keep using their corporate-owned devices even when those devices become functionally obsolete. Remember that device manufacturers tend to stop supporting older devices after new generations are released, and the result can be that the devices don't receive important security updates. Be aware of the need to budget for device replacements on a much shorter cycle than you'd likely experience with other

equipment such as desktop workstations and laptops. Unfortunately, you won't find much of a resale market for older generation mobile devices.

Implementing and enforcing policies to protect corporate data may be easier with corporate-owned devices. For example, you may be able to disable printing or saving data to local storage, such as a portable USB drive. Depending on the type of device, you may also consider implementing measures to prevent users from booting the device from a source such as a USB key so that users can't bypass your security features.

If your organization maintains a pool of mobile devices that can be checked out and shared by multiple users, it's important that user authentication is handled at the server level, not at the device level. If you authenticate users at the server, it won't matter which device a user is using to access your systems. Any device that has the proper access protocols installed can be used by any authorized user.

Mobile devices are typically used in environments where they need to access your network using consumer-grade access methods such as Wi-Fi, cellular data, or the user's home Internet connection. These types of connections are inherently insecure, leading to possible compromise of corporate data. You need to make sure that the mobile device management solution you choose incorporates secure encryption methods to protect your data.

For example, a VPN connection is encrypted over the entire path between the mobile device and your network, so even if someone were to manage to listen in to the connection, the encrypted data would be meaningless to that person.

Chapter 5

Ten Things You Need to Know

In This Chapter

- Ten important things to remember

In this chapter, I've compiled a list of ten things that are important for you to consider as you choose your mobile device management (MDM) solution.

Understanding Business Needs and Security Standards

The nature of your industry, such as defense, healthcare, IT, retail, law, and so on, presents varying security requirements. You need to be aware of the standards that apply in your case.

Knowing What's in Store While Embracing Mobility

Understanding mobility, along with its pros and cons, will help you as you transition to a mobile workforce and will also enable you to avoid many potential problems.

Understanding App Management and Security

Managing mobility in organizations involves numerous device and app risks. Make sure that you understand the possible preventions and remediation available through a comprehensive mobile device management solution.

Deploying a Good MDM Solution

In mobile device management, no single solution is one-size-fits-all. An MDM solution, such as ManageEngine Mobile Device Manager Plus, is customizable to match an individual organization's requirements. Many industries such as healthcare, retail, IT, and so on can use MDM to their advantage. Ask your vendor to help you establish and adopt effective day-to-day MDM practices.

Segmenting Your Organization Based on Level of Trust

Segments can be hierarchical or department-wise. Remember that top-level employees need higher encryption but more flexibility. On the other hand, the Sales/CRM department may find that single-app locked (kiosk) devices fulfill all its needs.

Setting Policies and Restrictions for Devices and Apps

You want a solution that enables you to push policies and restrictions to devices. You need to be able to

blacklist unauthorized apps (especially on corporate-owned devices). You need to disable data distribution by preventing local printing or data storage so that you protect corporate data behind a firewall.

Identifying Non-Compliant Devices

You need a system that can detect malware, app risks, network attacks, and more, while quarantining devices so that threats cannot spread. Make sure that your solution enables you to device-lock or remote-wipe non-compliant devices while also barring them from your organization's network.

Creating Awareness among Users

Develop an end-user license agreement (EULA) or general acceptance agreement, educating the users on the need for security while also making users feel comfortable in the MDM setup.

Auditing Regularly for Compliance

Run regular audits so that you can prove compliance. Push secure apps and enable patching and updates for devices and apps.

28

Embracing New Technology, with a Bit of Caution

Survey and study in depth any new device enhancements or app technologies so that your people have what they need to be effective, but avoid simply grabbing the newest thing just to be cool. Remember that you want an effective return on your investment. Make sure the bugs are out before spending your money.

Be successful — and secure — in a mobile world

Rapidly evolving mobile environments demand the ability to adapt and adjust quickly. This book introduces the challenges and possibilities of the increasingly complex world of mobile devices.

- ***Move forward with mobile* — *achieve faster response times and higher productivity***
- ***Address the challenges* — *find solutions to compatibility, access, and device management***
- ***Adapt and stay safe* — *remain competitive while ensuring the security of your data***

Open the book and find:

- **Creating device management guidelines**
- **Overcoming mobile security threats**
- **Making the most of BYOD and corporate-owned devices**

Go to Dummies.com®
for more!

Brian Underdahl is a well-known author and technologist who enjoys making complicated topics easy for ordinary people to understand.

FOR DUMMIES®
A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-34985-3
Not for resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.