Microsoft

Enterprise Mobility with App Management, Office 365, and Threat Mitigation

Beyond BYOD

Yuri Diogenes
Jeff Gilbert
Robert Mazzoli

Foreword by Brad Anderson
Microsoft Corporate VP, Enterprise Client & Mobility

Microsoft

Enterprise Mobility with App Management, Office 365, and Threat Mitigation

Beyond BYOD

Yuri Diogenes
Jeff Gilbert
Robert Mazzoli

PUBLISHED BY
Microsoft Press
A division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2015951523
ISBN: 978-1-5093-0133-1

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Support at mspinput@microsoft.com. Please tell us what you think of this book at http://aka.ms/tellpress.

Acquisitions Editor: Karen Szall
Developmental Editor: Karen Szall
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Technical Reviewer: Mike Toot; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Copyeditor: Roger LeBlanc
Indexer: Maureen Johnson, MoJo's Indexing
Cover: Twist Creative • Seattle

Contents at a glance

Contents

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can improve our books and learning resources for you. To participate in a brief survey, please visit:

http://aka.ms/tellpress

Foreword

I speak with hundreds of IT Pros and CIOs every year, and each of them has the same priority: providing their users with an iconic work environment while securing and protecting company data. Doing this has become more difficult than ever thanks to the combination of more apps/data moving to the cloud and cyberattacks becoming more destructive. It is safe to say that the traditional perimeter that was used in the past to protect company data has evaporated; this means that organizations need to fundamentally rethink how they are securing and protecting company data. Microsoft has committed itself to being an ally to the IT professionals charged with protecting the assets of their companies.

It is no exaggeration to say that, at Microsoft, we are obsessed with enterprise security. Every software company struggles with the balance between making corporate data safe from attack but accessible to the appropriate parts of the workforce—and I believe Microsoft has struck the right balance.

Teams across the company have torn down the traditional barriers that existed between products and built end-to-end solutions that are not just interoperable, but built to protect data wherever it goes. This means protecting it at multiple layers throughout the organization: protecting it at the device and apps (with Microsoft Intune), protecting the file (with Azure RMS), and protecting identities (with Azure Active Directory Premium and Advanced Thread Analytics). These products all come together to form the Enterprise Mobility Suite (EMS).

This book is written by a trio of EMS experts, and it offers an insider's look at proven, real-world actions you can take to manage your enterprise mobility needs, enable your workforce to be productive (across devices and platforms) with an iconic work experience, and help you protect your organization's assets and your workforce's privacy.

As you read, I think you'll be consistently impressed by the ways you can leverage EMS's powerful ability to deliver an incredible work experience for your users that correctly balances between user empowerment and data protection. To do this, we have engineered EMS and Office 365 to be used together.

The value and power of what we've built is widely recognized by the IT industry —EMS has already outgrown its competitors and continues to regularly add more features and functionality. We are committed to continuing to build, refine, and deliver the tools you need to protect your organization and empower it to do more.

Brad Anderson, Microsoft Corporate VP, Enterprise Client & Mobility

@InTheCloudMSFT

Introduction

Enterprise mobility management is one of the fastest-growing areas in the Information Technology field, and having a solid understanding of the newest features and capabilities is an important part of configuring and managing mobile devices. This book continues forward from the information covered in *Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices* (Microsoft Press, 2015) and covers the fundamentals and capabilities of several Microsoft mobility management resources; the newest mobile application management features in Microsoft Intune, Microsoft Advanced Threat Analytics (ATA), and Mobile Device Management for Office 365 (MDM for Office 365). Throughout this book, we guide you through all the areas associated with planning, designing, and implementing these mobility management solutions.

Is this book for you? This book is for enterprise IT professionals who are responsible for implementing and managing mobility management technology as well as professionals charged with identifying and mitigating networking threats to on-premises networks. It is also meant to provide foundational expertise to IT professionals who aren't already familiar with these solutions or just want to learn more. We assume that the readers are familiar with the primary components of the Microsoft Enterprise Mobility Suite (EMS) and Office 365. It is also helpful to have basic knowledge about network-security principals and network-infrastructure components.

The scenarios described in this book are meant to be an end-to-end journey for each of the mobility management solution areas. They start with understanding overviews of each solution and then move on to implementing specific features and capabilities in the example organization. After completing the example scenarios, you'll have learned how to

- Manage and publish mobile applications, and deploy them to mobile devices and computers
- Deploy and configure the ATA Center and Gateway, including configuring reports to help identify suspicious activities
- Activate and configure MDM for Office 365, including enrolling and managing mobile devices

Acknowledgments

The authors would like to thank Karen Szall and the entire Microsoft Press team for their support in this project, Brad Anderson for writing the foreword of this book, and all the other Microsoft colleagues who contributed by reviewing this book: Gershon Levitz, Ophir Polotsky, Benny Lakunishok, Michael Dubinsky, Simon May, Sonia Wadhwa, Stacia Snapp, Owen Yen, Paul Mayfield, Joey Glocke, Rob Stack, and Karthika Raman. In addition:

Yuri I would like to thank my wife and daughters for their support and understanding, my great God for giving me strength and continuing to guide my path, my friends and co-authors Jeff Gilbert and Robert Mazzoli (you guys rock!), the Microsoft ATA Team in Israel for the endless support on this project, and last but not least, my parents for working hard to give me an education, which is the foundation that I use every day to keep moving forward in my career.

Jeff I would like to thank my wife, Chrissy, and kids, Nick, Haylee, Jackson, and Jillian for their love, patience, and unending support and encouragement throughout the long hours required to author content for a technical book of this depth. Also, thanks to my co-authors who kept me motivated to write and who I can count on every day for expert counsel and advice. Thanks also to the other Microsoft enterprise client management engineering team members who made themselves available for my never-ending stream of questions and clarifications.

Robert I would like to thank my daughter, Alyssa, for inspiring me to follow in her footsteps and become a published author; Barbara for being the love of my life and for all her patience and understanding; Bruna and Luciano for the use of their kitchen table and all the wonderful Italian meals that fueled my writing; my co-authors Jeff Gilbert and Yuri Diogenes for their ongoing friendship, guidance, and motivation; and "all" my parents (Constance, Claude, Henri, and Kathy) for a lifetime of love and support.

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

http://aka.ms/mspressfree

Check back often to see what is new!

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

http://aka.ms/EM2/errata

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

CHAPTER 1

Understanding Microsoft enterprise mobility solutions

Enterprise mobility management solutions aren't as simple anymore as connecting a few mobile devices to an email server or allowing some users to access company resources via a remote connection. Today's IT departments must support a much more robust and comprehensive user experience for modern employees. Users expect, and often even demand, application-feature and data-access parity between their mobile devices and the devices they use at the office. Add in the new challenges that IT departments face with managing cloud-computing services, user identity, applications, data security, and threat mitigation, and the enterprise mobility management landscape becomes much more complex and difficult to deploy and manage.

This chapter explains how Microsoft enterprise mobility solutions address these areas and covers the basics of enterprise mobility management. It also covers considerations for selecting and deploying these solutions, as well as introducing a sample enterprise mobility management scenario that will be used throughout this book.

Enterprise mobility management concepts

In enterprise IT management, companies are fully embracing the modern "work anywhere, from any device" vision. Trends like *bring your own device (BYOD)* and *mobile application management (MAM)* aren't just buzzwords or passing fads likely to fade out after a year or two. These concepts are part of the larger modern IT strategy supporting the consumerization of IT and the empowerment of users. Central to this strategy are cloud services, such as Microsoft Azure Active Directory and Microsoft Office 365. Leveraging the computing scale and ubiquity of access that these and other Software as a Service (SaaS) platforms provide to mobile devices and users requires planning and considering things from a different perspective than in the past.

Enterprise mobility management isn't just about connecting mobile devices to cloud services or resources. In fact, it's less about *devices* and more about *people*. Forward-looking organizations aim to empower employees and increase their productivity; the devices (mobile or not) they use are merely tools to help accomplish their work. This paradigm shift from a *device-centric* management structure to a *people-centric* management structure is significant. All the components that enable mobile productivity in an enterprise mobility management solution must have a people-centric architecture that aligns with enabling this vision. Finding the proper balance where employee empowerment and productivity meet the business needs of your organization is the crucial requirement for any enterprise mobility management solution.

With this vision in mind, be aware that a well-designed enterprise mobility management solution must address several key areas of the modern workplace, as shown in Figure 1-1.

- Users
- Devices
- Apps
- Data
- Protection

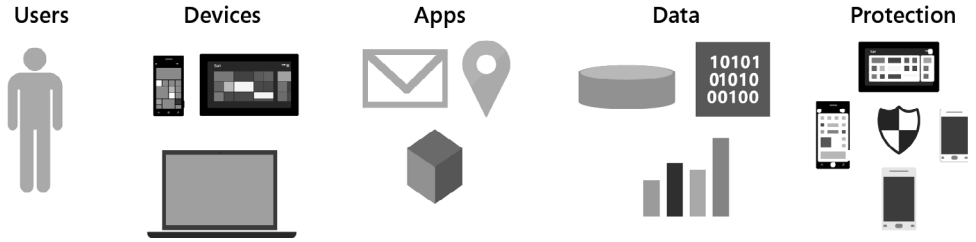

FIGURE 1-1 Elements of enterprise mobility management

> ***MORE INFO*** **For more information about why organizations should embrace enterprise mobility solutions, read Chapter 1 of *Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices* from Microsoft Press at *https://aka.ms/EMSdevice/details*.**

Users

The first and most important element of the enterprise mobility management solution is the user or employee. Without the employee, the IT infrastructure and management costs to enable enterprise mobility are expensive monuments to best intentions. The enterprise mobility solution must support effective ways to manage user accounts and make it easy for employees to access resources. If user identity is hard to manage by IT administrators, or if employees are required to take convoluted steps to gain access to devices or company resources, the enterprise mobility

management solution becomes an obstacle instead of an effective productivity management tool. As most experienced IT administrators have learned, workplace technology obstacles invite shortcuts, workarounds, and questionable data-protection practices.

Effectively managing user identity is critical to enabling cloud-based applications and data resources spanning multiple services or locations. Efficiently verifying that users are who they claim to be is essential to protecting resources and making the mobile experience feel like the traditional workplace experience. Keep in mind that employees with different types of roles and responsibilities, and even different geographic locations, often have unique requirements across all the areas of enterprise mobility management.

Devices

The rapid pace of technological advancement has changed the modern workplace from one of stationary workstations and company-issued devices to one containing a mix of all types of mobile computers and Internet-connected devices. This change is driving the BYOD trend across all markets, and industries and organizations must adapt to this new challenge. Using their personal mobile devices—such as smart phones, tablets, and laptops—employees are increasingly mixing their personal lives with their work responsibilities. As a result, IT departments are tasked with managing an ever-expanding collection of different mobile hardware, operating systems, and vendor-specific architectural requirements.

It's critical that organizations fully understand the capabilities and limitations of each type of device and how they will support each one. Only then can organizations define and configure the necessary enterprise mobility management features that support both the employee's needs and the organizations business requirements.

Apps

Apps are the centerpiece of most business requirements and the portal for information access for modern organizations. Though managing different device types creates new administration challenges, managing a mixture of commercial and customized line-of-business (LOB) apps can be equally challenging. Employees need access to all their productivity tools from all their devices, including email, data storage services, and role-specific tools. These services can be either locally hosted in on-premises networks or hosted in the cloud.

How to properly install and manage these apps depends on several factors. Different apps have different installation requirements, can require individual adjustments to function properly on different devices, and often have varying levels of risk associated with keeping information secure. Misjudging or improperly managing any of these areas can lead to exposing sensitive company data or employee personal information. IT departments must take care to fully understand which apps will be supported and how they will be managed to help protect company data. Mobile application management will be covered in more depth in Chapter 2, "Introducing mobile application management with Microsoft Intune," and Chapter 3, "Implementing MAM."

Data

Working from a mobile device from any location really means accessing data from anywhere. Operating hand in hand with identity management, apps, and the architecture of mobile devices, data must be consumed securely and easily for users to be productive and to keep them from finding alternative access routes to information. Understanding how data is stored on devices and how data is protected in transit is critical when planning and configuring enterprise mobility management features and policies.

Depending on your business needs and user requirements, your organization might require multiple layers of data protection, ways to classify information according to sensitivity, methods for data encryption, and integrated ways to manage access control. Different enterprise mobility management solutions offer varying levels of control for each of these areas and offer different levels of reporting and monitoring in the case of breaches.

Protection

Protecting mobile devices and company data from threats is just as important as securing data access. No matter how carefully planned security is, all levels of mobile device security are potentially vulnerable to a wide variety of malicious activity. These vulnerabilities include threats to company data, personal information, and even user identity.

Depending on the enterprise mobility management solution, preventing risk and protecting mobile devices from these threats can be included as tightly integrated features or standalone services. Understanding how these solutions address potential gaps in threat mitigation is extremely important to effectively protecting mobile devices that are coming from the cloud or located on-premises. Threat protection and mitigation will be covered in more depth in Chapter 4, "Introducing Microsoft Advanced Threat Analytics," and Chapter 5, "Implementing Microsoft Advanced Threat Analytics."

Microsoft enterprise mobility solutions

Microsoft has aggressively pursued a strategy of "mobile first, cloud first" in their enterprise mobility management vision. This vision is centered on helping organizations enable their users to be productive on the devices they prefer, while protecting company resources. Central to this vision is the concept of *balance*—balancing the financial and data-security needs of the company with the productivity and privacy needs of users. Finding an appropriate balance often means splitting authority between the company and users, and keeping added management complexity to a minimum to ensure satisfaction and compliance.

Instead of piecing together parts of existing on-premises products and attempting to update and rebrand them as cloud services, Microsoft chose to design an enterprise mobility management solution from the ground up and leverage the powerful features of its proven cloud services, such as Azure and Office 365.

Microsoft Enterprise Mobility Suite

The Enterprise Mobility Suite (EMS), shown in Figure 1-2, is a comprehensive set of cloud services and on-premises technologies designed to extend user identities to the cloud, manage mobile devices and apps, increase user productivity through native support for Microsoft Office apps and support for thousands of SaaS applications, and protect files accessed and stored on managed devices.

EMS comprises the following products:

- Microsoft Azure Active Directory Premium
- Microsoft Intune
- Microsoft Azure Rights Management
- Microsoft Advanced Threat Analytics

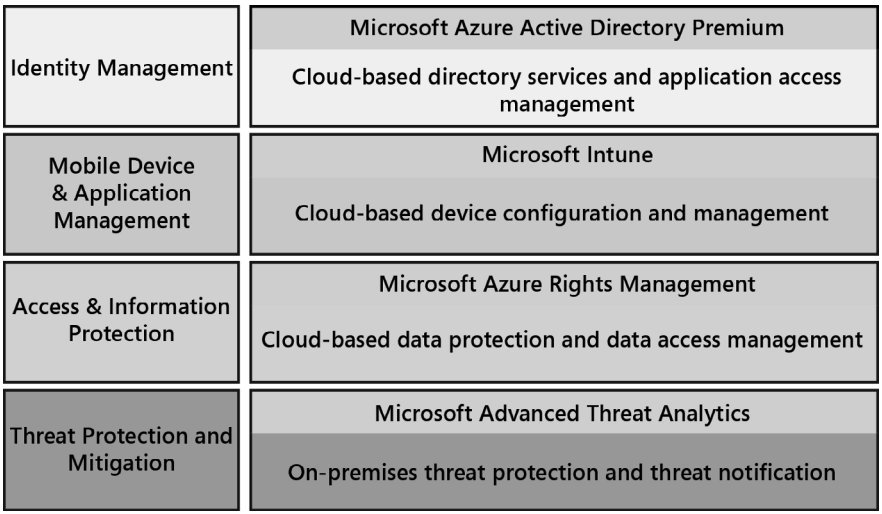

FIGURE 1-2 Enterprise Mobility Suite products

IMPORTANT **This book doesn't cover all the products included in EMS in depth. Instead, it focuses on several key features and capabilities of some EMS services, such as mobile application management (without device-enrollment requirements) and threat protection using Advanced Threat Analytics. It also covers the enterprise mobility management features of Microsoft Device Management (MDM) for Office 365 that aren't included in EMS. You can learn more about the products included in EMS in the first book in this series, *Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices (https://aka.ms/EMSdevice/details)*.**

Azure Active Directory Premium

Azure Active Directory (Azure AD) Premium is a Microsoft cloud-based service that provides comprehensive user identity and application access management capabilities. Built on the rich set of directory-service features of Azure AD that is included in all Microsoft Azure subscriptions, the Azure AD Premium subscription includes additional capabilities for enterprise-level identity management. One of the most popular features of Azure AD Premium is its integrated single sign-on (SSO) support for thousands of popular Software as a Service (SaaS) apps. This means that instead of users having to use multiple sets of user names and passwords to access apps such as Salesforce, Concur, or Workday, they can use a single user name and password for a consistent experience across every app and device.

In addition to the features in the Azure AD Free and Basic subscriptions, the Premium subscription includes the following:

- Self-service group management that users can use to create and manage customized user groups
- Advanced security reports and alerts based on machine-learning that organizations can use to monitor and protect access to cloud applications
- Multi-factor authentication (MFA) that supports configuring user verification steps in addition to a single user name/password authentication process
- Microsoft Identity Manager (MIM) support option you can use if you need to configure additional on-premises hybrid identity services
- Password reset with write back for user self-service password management with on-premises directory services
- Azure AD Connect Health to monitor on-premises identity infrastructure and synchronization services available through Azure AD Connect

Microsoft Intune

Microsoft Intune is another Microsoft cloud-based service that provides mobile device management (MDM), mobile application management (MAM), and Windows PC management capabilities. Supporting Android, iOS, and Windows-based devices, Microsoft Intune also can be used as a standalone cloud service or connected to an existing on-premises Microsoft System Center Configuration Manager 2012 R2 or later deployment. Additionally, Microsoft Intune provides the infrastructure support for enterprise mobility management features included with Office 365.

Microsoft Intune supports a comprehensive mix of MDM and MAM capabilities, including

- Simplified device enrollment for Android, iOS, and Windows devices
- Mobile device management through configuration and compliance policies
- Device access profiles for managing access to virtual private networks, wireless networks, email servers, and certificate-controlled resources

- Conditional access to Microsoft Exchange Server or Exchange Online–based email accounts
- Mobile application deployment, installation, and management
- Mobile device lock, remote PIN reset, complete device factory reset, or selective wipe of company data while leaving personal data intact

Azure Rights Management

Azure Rights Management (Azure RMS) is a cloud-based service that helps you protect your organization's sensitive information from unauthorized access and controls how this information is used or shared. Using encryption, identity, and authorization policies to secure files and email, Azure RMS applies policies and permissions directly to files and email messages, independent of where they are located. Permissions follow files and email messages inside or outside your organization, networks, file servers, and applications. This behavior enables users to access company data no matter what device they use or how the data is shared.

Microsoft Advanced Threat Analytics

Cyberattacks and Internet-based threats have grown more and more sophisticated and continue to increase in frequency and severity. Organizations realize now more than ever that they need to be proactive in their efforts to protect corporate data, user identities, employee and customer personal information, and their online reputation. Advanced Threat Analytics (ATA) identifies suspicious activities and abnormal behavior in on-premises networks, helps detect malicious attacks, and provides alerts for security risks. ATA is covered in more depth in Chapters 4 and 5.

Mobile Device Management for Office 365

The Office 365 business productivity suite is a group of cloud-based services and software subscriptions designed to increase productivity and lower licensing costs for organizations of all sizes. Office 365 and EMS are complementary suites of services and share many of the same architectural services. By sharing a common cloud-based infrastructure, both suites offer identity management provided by Azure AD, mobile device and application management capabilities provided by Microsoft Intune, and access and information protection enabled by Azure RMS. Microsoft ATA is an on-premises service and is included with EMS, but it isn't currently included with Office 365 subscriptions. Table 1-1 shows the relationships of these services.

Mobile Device Management for Office 365 (MDM for Office 365) is the group of mobility device management features included as a part of most Office 365 subscription plans. MDM for Office capabilities are enabled by Microsoft Intune and mobile device management features are tightly integrated with Office 365 services like Exchange Online and SharePoint Online. Instead of using the Microsoft Intune management portal, MDM for Office 365 management is built into the Office 365 admin console. Details about MDM for Office 365 will be covered in more depth in Chapter 6, "Introducing Mobile Device Management for Office 365," and Chapter 7, "Implementing Mobile Device Management for Office 365."

TABLE 1-1 Enterprise Mobility Suite and Office 365 products and services

	Enterprise Mobility Suite	Office 365
Identity management	Azure AD Premium ■ Single sign-on for SaaS apps ■ Advanced multifactor authentication ■ Microsoft Identity Management (MIM)	Identity management enabled by Azure AD ■ Basic single sign-on for Office 365 ■ Basic multifactor authentication for Office 365
Mobile device and app management	Microsoft Intune ■ MDM and MAM support ■ Advanced device and app policies ■ System Center integration	MDM for Office 365 enabled by Microsoft Intune ■ Basic device settings management ■ Selective wipe/device reset ■ Built into Office 365 Management Console
Access and data protection	Azure RMS ■ Protection for content in Office apps (on-premises or Office 365) and Windows Server files ■ Email notifications for shared documents	RMS protection enabled by Azure RMS ■ Protection for content in Office apps (on-premises or Office 365) ■ Access to RMS Software Development Kit (SDK)
Threat protection	Advanced Threat Analytics ■ Detects abnormal user behavior ■ Detects malicious attacks ■ Identifies known risks	Advanced Threat Analytics ■ Detects abnormal user behavior ■ Detects malicious attacks ■ Identifies known risks

Selecting the best solution for your organization

Determining the enterprise mobility management solution that best fits the needs of your organization can be difficult. As you've seen from the brief overview of the capabilities of the Enterprise Mobility Suite and MDM for Office 365, differences exist between the features and capabilities for each suite (and component services). Choosing one over the other before thoroughly understanding the differences and matching each to the specific needs of your organization will likely result in wasted time, wasted money, and user dissatisfaction and frustration.

In this section, you'll cover key enterprise mobility management planning and design considerations you'll need to define to choose the best Microsoft solution for your organization. Additionally, you'll compare the features and capabilities of the Enterprise Mobility Suite, Microsoft Intune (standalone deployment), and MDM for Office 365.

Planning and designing a solution

The first step in determining what enterprise mobility management solution best meets the needs of your organization is defining your requirements. These requirements aren't just a list of mobility management capabilities you think your organization needs—they must meet the actual business and productivity needs of your organization and users. You'll need to review the functional and service capabilities of each solution to answer questions in the following areas:

- Business needs, including device ownership, device platform, application, and user requirements
- Mobility management location needs, including geographic network requirements
- Mobile device management life-cycle requirements, including device enrollment, configuration, security, management, and monitoring
- Software as a Service (SaaS) connectivity requirements

Defining your business needs

To get started, you must understand your current and future business needs and how they fit with your organization's business strategy. If you don't take a long-term approach with your mobility management planning, chances are that your solution won't be scalable as your organization changes and grows. Although each organization will have different business requirements, a good place to start is to leverage best practices from other organizations in your industry. Because more and more organizations are embracing mobility management solutions with each passing day, it's likely that mobility management resources are available to help you with this planning. If your organization is regulated by governmental agencies or need to meet industry-specific compliance standards, you should review the applicable standards for your organization for any mobility management requirements or guidance.

Next, it's time to match the business requirements you've defined to the specifics of mobile device management:

- **Device ownership** Who will own the mobile device? The employee, the company, or a mix of both options?
- **Device platform** Which mobile device operating systems need to be supported? Just one or a mix of several?
- **Applications** Which mobile applications or SaaS apps need to be supported? Are the applications supported on the required device platforms? How will the applications be deployed?
- **Users** Will different groups of users have different mobility needs? Will users need mobile access to the same resources accessible from on-premises workstations?
- **Compliance** How will compliance requirements affect mobile applications? Are management policies in place for mobile devices? Does your organization already have a BYOD policy in place, or will you need to create one?

Defining your location needs

Location can affect the administrative model of your mobility management solution. Some solutions support only a cloud-based service model, while others support a hybrid cloud/on-premises administrative model, where cloud-based services are connected to on-premises solutions. Depending on your network infrastructure and the geographic location of your company offices, having the flexibility to connect to existing device management solutions and use a central point of administration can significantly reduce costs and administrative overhead.

Modern mobile devices almost always include Global Positioning System (GPS) features by default. These features enable mobile applications to leverage geolocation capabilities. Some organizations might have business scenarios in which disabling location services on mobile devices is a requirement. For example, a company might have employees working in areas where applications that use location services cannot be used because of the sensitive nature of the work. IT departments would need to disable location services on devices that have access to these areas.

Answer the following questions about your location requirements:

- **Administrative model** Which administrative model best meets your current and future infrastructure needs, centralized or distributed?
- **Location services** Does your organization need the ability to disable location services on mobile devices?

Defining your mobile device life-cycle requirements

Managing mobile devices, both company-owned and user-owned devices, encompasses several important life-cycle management decisions. You need to define how your organization will manage devices in the each of the areas shown in Figure 1-3, making sure that each aligns with your overall MDM strategy, business needs, and other network management and support policies.

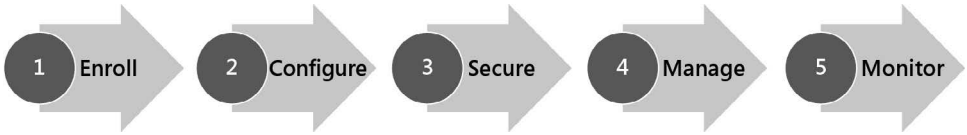

FIGURE 1-3 Mobile device management life-cycle stages

ENROLL

Mobile device management starts with enrollment, and it must be simple, easy, and reliable. If device enrollment is complicated, difficult, or unreliable, users will be resistant to following the process or slow to enroll their mobile devices for management. Typically, devices are registered with a mobility management solution either by a user self-enrollment or an administrator-managed bulk-enrollment process.

In the self-enrollment process, users enroll devices by accessing an enrollment or management portal. This is a manual process, and organizations need to provide users with clear enrollment guidance to avoid creating additional support cases. In most cases, IT will require users to enroll their devices if they want to access corporate resources from their mobile device. For example, most users want to immediately configure access to their work email account from their mobile device, and policies can be configured to automatically provision user devices to access corporate email when they enroll the device.

Answer the following questions about your device-enrollment needs:

- Will mobile devices be enrolled by administrators, by users, or by both?
- Does your organization need to bulk-enroll devices?
- How many devices will each user typically use and need to enroll?
- What are the connectivity requirements for users to self-enroll devices?
- What are the enrollment requirements for each device operating system your organization needs to support?
- Do you require special policies for device-enrollment failures?
- Will IT and users both need to unenroll devices?
- If a device is selectively wiped, should it automatically be unenrolled from management?

CONFIGURE

The configuration and compliance policies in the mobility management solution must align with the business requirements for your organization. Typically, a mobile device is automatically assigned these policies and permissions when the device is enrolled, and administrators can associate these policies with groups of either devices or users.

Answer the following questions:

- Which internal and external applications and services will be deployed, managed, and accessed by mobile devices?
- What mobile device security and access configurations do you need to enforce?
- Do you need to deploy apps and agents automatically and manually?
- Do you need separate levels for device-management permissions for IT roles and positions?
- Will your organization require digital certificates to authenticate mobile devices to company resources?
- How will mobile devices connect to the Internet when connected to the company network?

SECURE

Although usage of mobile devices can increase employee productivity, it also can increase security threats that you'll need to mitigate to protect your company's data and maintain user privacy. Defining your organization's data-protection requirements for mobile devices is an important planning step to address this concern. You should plan for mobile-device encryption (for both in-transit and at-rest data), data segregation, and device hardening. Each of these high-level areas build on other protection-related design considerations that need to be defined.

Each mobile-device operating system you plan to support can also control and protect devices using different methods and different levels of granularity. For example, if one operating system has more options for hardening the device than another, you need to define a common set of hardening options to protect each type of device. These hardening options can include defining custom compliance policies for device passwords, sign-in attempts, and encryption settings.

Maintaining user privacy and properly classifying data stored on devices is equally important. Your organization might already have privacy standards and policies in place for workstation computers, and these should extend to mobile devices. This is especially important when conducting device hardware, software, and file inventories. A clearly defined, transparent privacy policy outlining what, when, and how data is collected from mobile devices will ensure that users are comfortable about what information is shared with the organization. This policy should also establish clear boundaries regarding what is considered company data and how it will be protected.

> ***MORE INFO*** **For more information about privacy and compliance, visit the Microsoft Intune Trust Center at *http://www.microsoft.com/server-cloud/products/intune-trust-center/faq.aspx*.**

Defining who and which devices will have access to company data will also need to align with your organization's standards and policies. This access is controlled by establishing authentication and authorization policies in the mobility management solution. To control access for resources, the solution must verify that users are who they claim to be (authentication) and determine whether they should have access to the resource (authorization). Once these steps are completed, the solution must validate both the level of access the user will have for the resource and that the device accessing the resource complies with company policies.

No matter how carefully these security principles are configured, you need to plan for potential security incidents. If your organization is just getting started with mobility management, make sure that any existing security incident-response policies and requirements apply to mobile devices and that the mobility management solution supports meeting these requirements. Especially in larger organizations, mobility management responsibilities might be assigned to a department or personnel not normally accustomed to responding to security incidents. It's a good idea to involve your organization's security team early in the mobility management planning and design process to prevent this from occurring.

When defining your security requirements, answer the following questions:

- How will data be protected on devices at rest and in transit?
- Will your organization need data encryption for devices and data within applications?
- Will you need the ability to erase company data from devices, while preserving personal data on devices?
- What level of device-hardening settings do you need?
- How will you communicate the organization's privacy policy to mobile-device users?
- Where will mobile-device data be stored? Only on the device or also in the cloud? How is privacy managed in these locations?
- Do you need to classify data on mobile devices? Does the classification travel with the data or apply only to data on the device?
- How will you authenticate users? Will you need multi-factor authentication features?
- Does your organization use an on-premises Public Key Infrastructure (PKI) to issue certificates? How will this apply to mobile devices?
- Will you need to control access to mobile apps? Does access need to have different levels of control?
- How will lost mobile-device incidents be handled? If the device is compromised, what policies will ensure that malicious activity doesn't spread to other devices or the larger network?
- How will you be notified of security incidents? Proactively or in real time?

MANAGE

As you've just seen, mobility management security integrates with virtually every facet of an organization's technology infrastructure. Managing mobile devices is a topic that's just as broad and comprehensive. Mobile device management typically involves several administrative and management areas, such as configuring devices, managing applications, configuring access to networks and resources, and monitoring and reporting. In most mobility management solutions, configuration policies are used to define general organizational settings for devices and compliance policies enforce requirements for resource access. Additionally, conditional access policies can define access to specific services, such as email or file-sharing resources.

To simplify and standardize enforcement of these policies, many mobile management solutions use profiles to push settings for networks and services to mobile devices. For example, by setting up and deploying email profiles, IT departments can automatically configure mobile devices with the appropriate email server connection information. This arrangement helps users connect to the correct email server without having to remember specific connection details. Profiles can typically be configured for virtual private network (VPN) and Wi-Fi network access and certificate management.

Answer the following questions when defining your MDM management requirements:

- Do you need specific policies applied to groups of users, groups of devices, or groups of device operating systems?
- Will you need to apply separate policies based on whether devices are company or user owned?
- Will you need customized policies for network access? Email access?
- Do policies need to be exported to third-party security devices?
- Do you need a customized company portal for users to install apps?
- How will policies be used to manage access to on-premises or cloud-based resources?

MONITOR

Capturing and monitoring event and status information from mobile devices is vital to ensuring that users and devices comply with your organization's policies and standards. This is especially important for organizations that must comply with government or industry-specific requirements and guidelines. Reporting also can assist with inventory management and provide detailed information about installed software, hardware capabilities, and licensing compliance. Remember the importance of user privacy discussed earlier, particularly for user-owned mobile devices. Your mobility management solution shouldn't monitor, capture, report, or share any personal activity or information without the consent of your users. You need to be able to answer the following monitoring questions:

- What kind of reports will you need for mobile devices?
- Will reports need to be shared or accessed remotely?
- Are there specific issues or problems you will need to identify?
- Do you need customized or on-demand reports?
- After a device is unenrolled, should legacy information be archived or maintained?

Defining your SaaS requirements

Understanding how your mobile management solution will integrate with current or future cloud services is vital as more organizations leverage the scalability and power of cloud-based computing. This has a large impact on managing user identity and directory services. Connecting and synchronizing your on-premises directories with a cloud service is the driving force to uniting users, mobile devices, mobile apps, and mobile device management. Additionally, configuring and managing connections to third-party SaaS apps can be difficult and time-consuming if those tasks are not handled correctly and the connections are not properly maintained.

When defining your SaaS requirements, answer the following questions:

- Are business-critical SaaS applications available?
- How will your existing on-premises user and device accounts connect?

- Do passwords need to be synchronized with Azure AD?
- Will you implement single sign-on for your organization?
- What existing SaaS platforms do you currently use? Do they support specific mobility management solutions and features?
- How is user and device authentication handled? How are identity-related threats and anomalies addressed?

MORE INFO **For more information about planning and designing a mobile device management solution, see the "Mobile Device Management Design Considerations Guide" at *http://aka.ms/mdmdcg*. This guide covers many of the areas in this section in greater depth. You can also view a Channel 9 TechNet Radio presentation on design considerations for MDM by Yuri Diogenes and Robert Mazzoli at *https://channel9.msdn.com/Shows/TechNet+Radio/TNR1610*.**

Comparing Microsoft mobility management solutions

Now that you've defined the mobility management requirements that meet the needs of your organization, you're ready to compare the requirements and features of Microsoft's enterprise mobility management services. You'll cover the main features and capabilities of the Enterprise Mobility Suite, Microsoft Intune, and MDM for Office 365 side by side so that you can easily compare them. However, because these are all cloud-based services and continuously updated, make sure you verify the most current features and capabilities of these services when you're ready to deploy a service.

Prerequisites

Make sure your organization and infrastructure meet the requirements of each mobility management solution:

ENTERPRISE MOBILITY SUITE

The main requirements for EMS depend on the individual requirements for each of the component services. EMS-specific requirements focus only on activation and licensing. The basic steps to activate EMS are as follows:

1. Sign up for EMS.
2. Activate a licensing plan.
3. Activate access.
4. Assign user licenses.
5. Deploy Azure AD, Microsoft Intune, Azure RMS, and Advanced Threat Analytics.

MORE INFO **For more information about deploying EMS, see the Enterprise Mobility Suite Activation Guide at *http://aka.ms/EMSGetStarted*.**

MICROSOFT INTUNE

Microsoft Intune is a cloud-based service, and there isn't a requirement to have any on-premises network infrastructure. Microsoft Intune uses the public Internet to communicate directly with devices and cloud-based users. If you do have an on-premises network infrastructure, Microsoft Intune will use your network to communicate with on-premises devices in your subscription. Although you are not required to use a dedicated server, options are available that use on-premises infrastructure components like Microsoft Exchange and Windows Server Active Directory tools. The basic requirements are

- **Mobile device platforms** Versions of Android 4 and later, iOS 7.1 and later, Windows Phone 8 and later
- **Computer platforms** Windows Vista and later versions (excluding Home editions)
- **Network ports** TCP 80 and 443

MORE INFO **For more in-depth Microsoft Intune requirements, see "What to know before setting up Microsoft Intune" at *https://technet.microsoft.com/library/dn646966.aspx*.**

MDM FOR OFFICE 365

MDM for Office 365 is simply a set of mobility management capabilities and requires only an Office 365 subscription. MDM for Office 365 requires

- An Office 365 commercial subscription (Business, Enterprise, EDU, or Government plan)
- Android 4 and later, iOS 7.1 and later, and Windows Phone 8.1 and later mobile devices

Features and capabilities comparison

Because the mobility management features in EMS are provided by Microsoft Intune, you really just need to compare the features and capabilities of Microsoft Intune and MDM for Office 365. The other component services of EMS don't provide mobility management–specific capabilities, though they do support mobility management–related capabilities.

Because many organizations use the basic mobility management features offered by Exchange ActiveSync, its features are included in Table 1-2 for a fuller comparison of features.

TABLE 1-2 Comparison of mobility management features for Exchange ActiveSync, MDM for Office 365, and Microsoft Intune

Category	Feature	Exchange ActiveSync	MDM for Office 365	Microsoft Intune
Device configurations	Inventory mobile devices that access corporate applications	x	x	x
	Remote factory reset (full device wipe)	x	x	x
	Mobile device configuration settings (PIN length, PIN required, lock time, and similar)	x	x	x
	Self-service password reset	x	x	x
Basic mobile device and app management	Provides reporting on devices that do not meet IT policy		x	x
	Group-based policies and reporting (the ability to use groups for targeted device configuration)		x	x
	Root and jailbreak detection		x	x
	Remove Office 365 app data from mobile devices while leaving personal data and apps intact (selective wipe)		x	x
	Prevent access to corporate email and documents based upon device enrollment and compliance policies		x	x
Premium mobile device and app management	Self-service company portal for users to enroll their own devices and install corporate apps			x
	App deployment (Android, iOS, Windows Phone, Windows 10)			x
	Deploy certificates, VPN profiles (including app-specific profiles), email profiles, and Wi-Fi profiles			x
	Prevent the cut, copy, paste, and save as operations from being used on data from corporate apps to share the data for use with personal apps (mobile application management)			x
	Secure content viewing via managed browser, PDF viewer, Imager viewer, and AV player apps for Intune			x
	Remote device lock via self-service company portal and via admin console			x
PC management	Client PC management (for example, Windows 8.1, inventory, antimalware, patch, policies, and similar)			x
	PC software management			x

MORE INFO **For more information about planning and designing a mobile device management solution, see the "Mobile Device Management Design Considerations Guide" at *http://aka.ms/mdmdcg*. This guide covers many of the areas in this section in greater depth. You can also view a Channel 9 TechNet Radio presentation on design considerations for MDM by Yuri Diogenes and Robert Mazzoli at *https://channel9.msdn.com/Shows/TechNet+Radio/TNR1610*.**

Enterprise mobility management scenario

To help you understand of how each enterprise mobility management product will be used as part of the overall solution, the following scenario will be used throughout this book. Each implementation chapter will reference the scenario and implement one or more of the listed requirements. At the end of this book, you'll have the solution fully implemented, and it will meet all the requirements of the fictitious company shown in Figure 1-4.

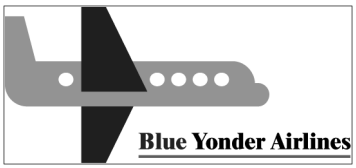

FIGURE 1-4 Fictitious company's logo that will be used in this book

Blue Yonder Airlines recently completed some acquisitions and is expanding its business to different regions of the country. As result of these acquisitions, the company added several new branch offices around the country. Many of these branch offices are small (fewer than 50 employees) and don't have dedicated IT personnel on site, with some mobile devices currently being managed by an MDM solution the company will migrate away from and move to Microsoft Intune. The Blue Yonder Airlines IT department needs an easy solution to manage devices and applications to enable employees to be productive while physically located at the branch office and while out visiting customers. These acquisitions have also brought new challenges for application management because the scope of what needs to be managed has expanded to include new line-of-business and publicly available applications. To make things more difficult, some of the remote offices and remote users are bound by noncompete agreements for the next year and there are legal questions about how to incorporate these offices into the existing IT infrastructure.

Access to on-premises resources will likely increase, and Blue Yonder Airlines also wants to enhance its on-premises and cloud-based data-protection capabilities. After a meeting between the CEO and the CSO, it was agreed that part of this investment must also include ways to detect abnormal user behavior and malicious attacks, and to automatically identity known security

issues and risks. Blue Yonder Airlines currently uses the Microsoft Enterprise Mobility Suite for its existing offices and has the following infrastructure components deployed:

- Windows Server Active Directory running on-premises and Azure Active Directory Premium in the cloud, with hundreds of users authenticating daily.
- Microsoft Intune subscription with security policies configured to manage existing BYOD scenario. All employees have devices enrolled, and there isn't an on-premises device management system deployed.
- Azure Rights Management Services (RMS) is configured for data access and protection.
- Exchange Server 2013 with users accessing their mailbox via Outlook client, native email clients included on mobile devices (using Exchange ActiveSync), and Outlook Web App (OWA).

Blue Yonder Airlines' goals for this project are to enhance its current Enterprise Mobility Suite deployment to ensure that data is more protected, applications can be more closely managed, and the new branch offices are included in the overall enterprise mobility management infrastructure. Blue Yonder Airlines established the following requirements in order to consider this project successful:

- Require remote office employees to have managed access to company resources and services from their personal mobile and corporate work devices, including remote offices bound by restrictive noncompete agreements
- Enable IT to enforce security, encryption, email, and device policy settings for remote offices using MDM for Office 365
- Monitor on-premises resources, and identify abnormal behavior in the network
- Prevent attacks to exploit known vulnerabilities for the resources located on-premises
- Detect security issues and risks, and alert administrators to them.
- Reduce false-positive alerts to avoid unnecessary red flags and distraction from real issues.
- Make full use of the Microsoft Intune mobile application management and data-protection capabilities mentioned earlier, and use it beyond basic app deployment.
- Define and implement a mobile-application strategy to support mobile device application deployment to all employee devices, regardless of whether they are managed by Microsoft Intune or not.
- Monitor app usage, and ensure the company complies with licensing agreements as the company grows through acquisitions.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

About the authors

YURI DIOGENES is a Senior Content Developer on the CSI Enterprise Mobility Team, focusing on BYOD and Azure Security Center. Previously, Yuri has worked as a writer for the Windows Security Team and as a Support Escalation Engineer for the CSS Forefront Team, also at Microsoft. He has a Master of Science degree in Cybersecurity Intelligence and Forensics from UTICA College and an MBA from FGF in Brazil, and he holds several industry certifications. He is co-author of *Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices* (Microsoft Press, 2015), *Microsoft Forefront Threat Management Gateway (TMG) Administrator's Companion* (Microsoft Press, 2010), and three other *Forefront* titles from Microsoft Press.

JEFF GILBERT is a Senior Content Publishing Manager on the Enterprise Mobility Team at Microsoft. He manages the documentation teams supporting Microsoft System Center Configuration Manager and Microsoft Intune. Prior to returning to management, he was responsible for authoring cross-product solutions to IT business problems involving enterprise client-management technologies, including Microsoft System Center Configuration Manager, Microsoft Intune, and MDOP. Previously, Jeff was the content publishing manager for MDOP and a senior technical writing lead for the Configuration Manager 2007 documentation team. Before joining Microsoft, Jeff was an SMS administrator with the US Army. Jeff is a regular speaker on enterprise client management and MDOP technologies at conferences including the Microsoft Management Summit (MMS), TechEd, IT\Dev Connections, and the Minnesota Management Summit (MMS).

ROBERT MAZZOLI is a Senior Content Developer with Microsoft on the Enterprise Mobility team, working on developing enterprise mobility solutions using the Microsoft Enterprise Mobility Suite and MDM for Office 365. Robert joined the Enterprise Mobility team in 2014 and has been a speaker on enterprise mobility solutions and mobile device management at several conferences, including Ignite 2015 and the 2015 Microsoft MVP Summit. Previously, Robert was a Senior Content Developer for Microsoft Exchange Server and Exchange Online in Office 365, specializing in Exchange hybrid deployments and managing the Exchange Server Deployment Assistant. Before joining Microsoft, Robert owned an information technology consulting business and served as an officer in the United States Navy.