

Enterprise Mobility Suite

Managing BYOD and Company-Owned Devices



Yuri Diogenes
Jeff Gilbert

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

Enterprise Mobility Suite: Managing BYOD and Company-Owned Devices

Yuri Diogenes
Jeff Gilbert

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

Copyright © 2015 by Microsoft Corporation

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2014955635
ISBN: 978-0-7356-9840-6

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 Book Support at mspinput@microsoft.com. Please tell us what you think of this book at <http://www.microsoft.com/learning/booksurvey>.

Microsoft and the trademarks listed at <http://www.microsoft.com/en-us/legal/intellectualproperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Karen Szall

Developmental Editor: Karen Szall

Editorial Production: Box Twelve Communications

Technical Reviewer: Randall Galloway; Technical Review services provided by Content Master, a member of CM Group, Ltd.

Copyeditor: Box Twelve Communications

Indexer: Box Twelve Communications

Cover: Twist Creative • Seattle

Contents at a glance

	<i>Introduction</i>	<i>xiii</i>
CHAPTER 1	Enabling a mobile workforce	1
CHAPTER 2	Introducing the Enterprise Mobility Suite	17
CHAPTER 3	Hybrid identity	27
CHAPTER 4	Implementing hybrid identity	49
CHAPTER 5	Device management	75
CHAPTER 6	Implementing device management	95
CHAPTER 7	Data access and protection	127
CHAPTER 8	Implementing data protection	149
CHAPTER 9	Monitoring BYOD and company-owned devices	169
CHAPTER 10	Troubleshooting Enterprise Mobility Suite	187
	<i>Index</i>	<i>205</i>

This page intentionally left blank

Contents

Introduction

xiii

Chapter 1	Enabling a mobile workforce	1
	The shift towards mobility.....	1
	The challenges of enabling enterprise mobility	2
	What about BYOD?.....	4
	Understanding the challenges of BYOD	5
	Understanding the Microsoft Device Strategy Framework	7
	Designing a strategy to enable a mobile workforce.....	9
	Users	9
	Devices	10
	Apps	12
	Data	13
	Threat mitigation	14
Chapter 2	Introducing the Enterprise Mobility Suite	17
	Understanding the EMS solution.....	17
	Establishing a hybrid identity	18
	Managing mobile devices	20
	Protecting data	21
	EMS activation process	23
	Embracing a mobile workforce scenario.....	24

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

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

microsoft.com/learning/booksurvey

Chapter 3	Hybrid identity	27
	Cloud identity with Azure AD Premium	27
	Azure AD Premium advanced security reports and alerts	28
	Azure Multi-Factor Authentication	30
	User self-service from the Azure Access Panel	32
	Understanding directory integration	35
	Source of authority	36
	Directory synchronization	36
	Active Directory Federation Services	38
	Directory integration scenarios	39
	Directory sync	40
	Directory sync with password sync	40
	Directory sync with SSO	40
	Multiforest directory sync with SSO	41
	Directory synchronization tools	41
	Azure Active Directory Synchronization Tool	41
	Azure Active Directory Synchronization Services	43
	Azure AD Connect	45
Chapter 4	Implementing hybrid identity	49
	Scenario description	49
	Implementation goals	49
	Solution diagram	50
	Planning and designing the solution	51
	Microsoft Azure planning and design considerations	51
	On-premises planning and design considerations	53
	Single Sign-On components and considerations	54
	Implementing the hybrid identity solution	60
	Prepare the Azure AD service for directory integration	60
	Prepare the on-premises environment for directory integration	61
	Enable Single Sign-On	64
	Customize branding	70

Chapter 5	Device management	75
	Preparing for device enrollment	76
	Mobile Device Management authority	76
	Device management prerequisites	78
	Device enrollment profiles	80
	The Company Portal	80
	Customizing the Company Portal	81
	Custom company terms and conditions	83
	Deploying policies	83
	Configuration policies	84
	Compliance policies	88
	Conditional access policies	88
	Exchange ActiveSync policies	90
	Policy conflicts	90
	Managing inventory	91
	Computer inventory	91
	Mobile device inventory	91
	Performing full and selective wipes	92
	Selective device wipes	93
	Full device wipes	93
Chapter 6	Implementing device management	95
	Scenario description	95
	Implementation goals	96
	Solution diagram	96
	Planning and designing the solution	97
	Microsoft Intune service configuration considerations	97
	Policies	100
	Mobile Device Management enrollment considerations	102
	Implementing device management	105
	Prepare the Microsoft Intune service for device enrollment	105
	Satisfy external device enrollment dependencies	112

Enrolling devices	114
Enrolling iOS devices	114
Enrolling Android devices	117
Enrolling Windows devices	120
Chapter 7 Data access and protection	127
Leveraging on-premises resources	127
Windows Server Dynamic Access Control	128
Web Application Proxy	130
Protecting data at rest at the user device location using work folders	131
Azure RMS	135
How Azure RMS works	137
Choosing the right deployment topology	141
Azure RMS connector	143
Monitoring access to resources	145
Chapter 8 Implementing data protection	149
Scenario description	149
Implementation goals	149
Solution diagram	149
Planning and designing the solution	151
Leveraging Azure RMS	151
Preparing the environment	151
Implementing the solution	153
Configuring Azure RMS templates	153
Azure RMS connector	159

Chapter 9	Monitoring BYOD and company-owned devices	169
	Continuous monitoring and incident response	169
	Creating an incident response plan	170
	Leveraging EMS to monitor resources	171
	Azure AD monitoring capabilities	172
	Microsoft Intune monitoring capabilities	175
	Microsoft Azure RMS monitoring capabilities	179
	Leveraging EMS to respond to a security incident	180
	Scenario	181
Chapter 10	Troubleshooting Enterprise Mobility Suite	187
	Troubleshooting methodology	187
	Knowing where to find information	190
	Using troubleshooting tools	190
	Troubleshooting EMS cloud services	191
	Troubleshooting Azure AD Premium	191
	Troubleshooting Microsoft Intune	194
	Troubleshooting Azure Rights Management Services	199
	<i>Index</i>	205

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

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

microsoft.com/learning/booksurvey

This page intentionally left blank

Foreword

Of all the books you'll read about the Enterprise Mobility Suite, this one is probably the first. In my opinion, it is also the most comprehensive to date.

Enterprise Mobility Management—the thing that EMS so brilliantly supports and empowers—is one of today's defining trends, and it is the core area of focus for some of the most brilliant software architects and developers in the tech industry. The reason is obvious: No other technological development will have a greater impact on the way we live and work than our current device ubiquity.

From an IT perspective, the number of devices your users want to use, the volume of data they access, and protecting those corporate assets (and the end users themselves) are just a handful of the incredibly serious issues you must face every day. This reality is what makes EMS so exciting; it represents the intersection of great software architects with the IT teams working on the front lines of organizations all over the world. With this cloud-based technology, and by leveraging things like Machine Learning from the cloud, the feedback loop is faster than ever. Now you can enable your users in ways you never have been able to in the past.

In this book you'll see—in practical terms and examples—how to make these devices and the people using them dramatically more productive, more connected, and more secure. From the back end of your infrastructure (Microsoft Intune, Azure Active Directory Premium, Azure AD RMS) to the apps your end users interact with every day (Office 365), EMS is an incredibly sophisticated set of tools that dramatically simplify many previously intractable technical challenges.

The Enterprise Mobility Suite is where I believe a cloud-first, mobile-first perspective really takes shape. The speed of business, the constant movement of workers and data, and the need to keep innovating are all delivered with the entirely service-based solutions offered by the EMS. It's powerful, reliable, and offers you the cross-platform functionality that's required to help you successfully and optimistically bridge your organization's past and future.

Jeff and Yuri have spent an exhaustive amount of time with every corner of the Enterprise Mobility Suite, and this book will prepare you to use it to solve the unique challenges your organization is facing today—and to plan ahead for your organization's long-term success.

Brad

*Brad Anderson, Microsoft Corporate VP, Enterprise Client & Mobility,
@InTheCloudMSFT*

This page intentionally left blank

Introduction

This book provides you with an introduction to the Enterprise Mobility Suite (EMS). In it, you are put in the driver's seat through scenario-based content covering each of the independent technologies that make up EMS: Microsoft Azure AD Premium, Azure Rights Management Services (RMS), and Microsoft Intune. Throughout the chapters, we guide you through the process of implementing EMS to support Mobile Device Management (MDM) of both company-owned devices and personally-owned devices in your enterprise environment.

The scenarios described in this book are truly end-to-end. Starting with enabling hybrid identity, you will quickly learn how to secure corporate data access, protect your employees' personal information, manage iOS, Android, and Windows devices, and, finally, how to monitor and perform basic troubleshooting of all EMS components.

The target audience for this book is comprised of enterprise IT Pros who are either charged with implementing EMS for their organizations or just want to learn more about the technologies that are included in EMS. While it is not possible to cover every aspect and nuance of the technologies included in EMS in a single book, we have attempted to include the content we believe will provide you with the solid foundation you will need as you begin your own EMS implementation journey.

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 of our Microsoft colleagues who contributed by reviewing this book: Ben Hawken, Simon May, Robert Mazzoli, Sonia Wadhwa, Eddie Bowers, Keith Brintzenhofe, Marsha Shoemaker, Taylor Thomson, Ken Hoff, Gil Lapid Shafri, Debbie Furtado, and Stacey Ellingson. We would also like to thank the Microsoft MVPs who reviewed this book: Kent Agerlund, Kenny Buntinx, Peter Daalmans, John Marcum, Torsten Meringer, Stefan Schörling, and Steve Thompson.

Yuri Diogenes I would also like to thank my wife and daughters for their endless support and understanding; my great God for giving me strength and keep guiding my path; my friend and co-author Jeff Gilbert (without you this project would not have been possible—thanks); my great friends and former co-authors

Tom Shinder and Jim Harrison (you both keep inspiring me to write); my former managers Kathy Watanabe and Jason Whitmarsh for their support when I joined the team; 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 Gilbert I would also like to thank my wife and kids for their support in always lending a sympathetic ear to my excited technical ramblings—which I’m sure sounded like a foreign language to them. This book could not have been possible without the help of Yuri Diogenes, my co-author and the one who inspired me to join him on this journey. I’d also like to thank all those whom I work with at Microsoft and my friends in the systems management IT community who have always supported me and given focus to the work I do every day.

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!

Microsoft Virtual Academy

Build your knowledge of Microsoft technologies with free expert-led online training from Microsoft Virtual Academy (MVA). MVA offers a comprehensive library of videos, live events, and more to help you learn the latest technologies and prepare for certification exams. You’ll find what you need here:

<http://www.microsoftvirtualacademy.com>

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/EMSdevice/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>.

This page intentionally left blank

Enabling a mobile workforce

The catchy phrase “work from anywhere” has evolved throughout the years and nowadays working from anywhere is the standard for many industries. However, as consumers started to use their own gadgets more and more to perform work-related tasks, “working anywhere and from any device” has become the new vision for many enterprises in a mobile-first, cloud-first world. This chapter explains why it is important for companies to develop an effective strategy for embracing a mobile workforce and also explains how the paradigm shift caused by the Bring Your Own Device (BYOD) trend impacts the overall strategy to securely adopt a mobile workforce.

The shift towards mobility

When companies started to understand the value of cloud computing—particularly as it related to how they could leverage its resources to be more agile and to reduce costs—they also discovered that users were already consuming cloud resources on their own devices. Cloud-based apps are intended to run on all types of portable devices. Also, cloud-based apps are usually programmed to run on several major operating systems, a strategy that drives rapid adoption from consumers. In this new era of Enterprise IT—also referred to by Gartner¹ as the “Third Era of Enterprise IT”—enterprise users not only demand agility, they demand a substantial increase in productivity.

While you might think that this concept is new, the fact is that this mobility phenomenon has been growing for at least the past seven years. A 2008 IDC study sponsored by Microsoft and performed by International Data Corporation (IDC) called *Mobility Solutions in Enterprise-Sized Businesses: Quantifying the Return on Investment*² revealed that the Return of Investment (ROI) with the use of mobility technologies pays off. So the question becomes, “What strategy should be implemented to support a mobile workforce and remain competitive in the marketplace?”

A 2014 survey³ published by IDG Enterprise Consumerization of IT in the Enterprise (CITE) suggests that the consumerization of IT maximizes the capabilities of mobility and

¹ For more information about the Third Era of Enterprise IT, visit <http://www.gartner.com/newsroom/id/2649419>.

² You can read the entire report at <http://aka.ms/MobileROI>.

³ You can read the entire survey at <http://www.idgenterprise.com/report/idg-enterprise-consumerization-of-it-in-the-enterprise-study-2014>.

empowers users. This survey documents several key findings. The following two key findings specifically address the trends for IT and mobile workforces; these key findings are the core foundation of this book:

- The proliferation of user-owned devices requires companies to adjust their policies and invest in Mobile Device Management (MDM) capabilities in order to maintain control over the devices while ensuring users can remain productive.
- Security is a key element to consider throughout the lifecycle of mobile devices.

These findings reinforce the fact that while CEOs are willing to enable users to be more productive by using their own mobile devices, the IT department must remain in control of those devices to ensure the company's data is protected.

The challenges of enabling enterprise mobility

To address the challenges that comes with enabling mobility in your company, you must understand the four elements of an enterprise mobility strategy (see Figure 1-1):

- Users
- Devices
- Apps
- Data

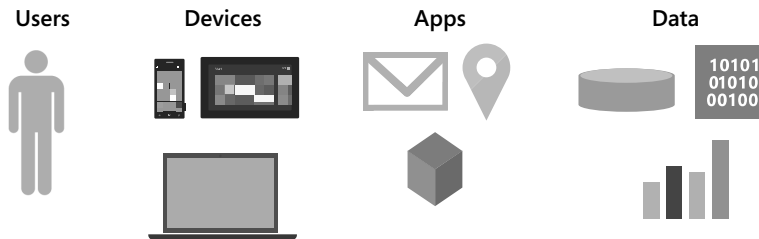


FIGURE 1-1 The four elements of an enterprise mobility strategy

When you embrace a mobile workforce, you not only must consider the user and the device he wants to use, you must consider how the apps that will be consumed will be affected by being on a mobile device. Even more importantly, you need to consider how to ensure that the company data remains secure. To effectively manage security of mobile devices, you should be sure to incorporate security into each of the four elements referenced in Figure 1-1. Focusing on each of the elements will help you to better address each challenge in a scenario-based approach. You want to ensure that your overall strategy is compliant with your business requirements while meeting the user's expectation about how she will perform at work using the device or devices of her choice.

Now that you know the elements, Figure 1-2 expands on the elements shown in Figure 1-1 and shows the three core scenarios that you will use throughout the entire book:

1. Enable users to choose their devices.
2. Unify the management of applications and devices
3. Protect corporate data.

By using this approach, you will be able to understand the challenges that must be addressed by your company before you embrace mobility.

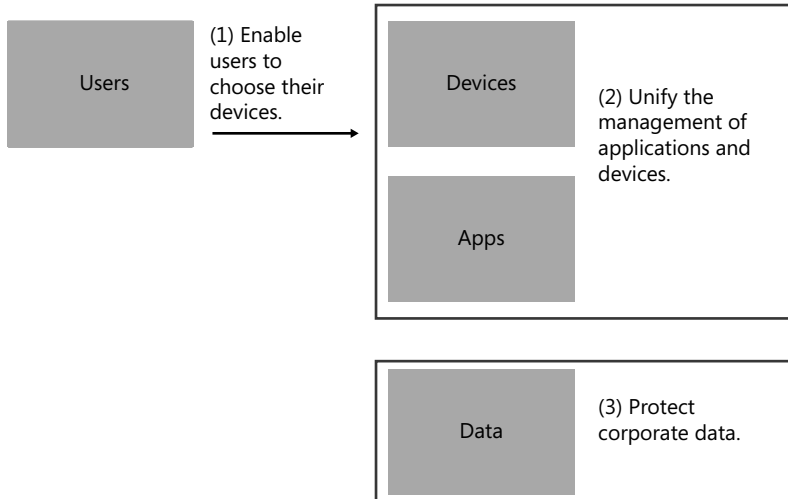


FIGURE 1-2 The three categories of challenges

As shown in Figure 1-2, the three core scenarios are bound to one or more of the elements shown in Figure 1-1. The following list explains the issues that must be addressed as part of your enterprise mobility strategy:

1. Enable users to choose their devices
 - Users want to use their own devices to access both their personal data and their work-related data/apps.
 - Users want access to these elements from anywhere.
 - While CEOs want to fulfill user requirements in order to enable users to be productive, they also want their IT department to be in control of how users access company data.
2. Unify the management of applications and devices
 - Users must have a common identity to access applications and company resources from any device and from anywhere.
 - IT must be able to manage, deploy, and maintain applications for all types of devices.

- IT must be able to manage company-owned devices as well as user-owned devices from a single location.
3. Protect corporate data
- Corporate data must be protected at all stages: while data is in the cloud, while data is at the company's datacenter, while data in the user's device, and while data is in transit between any (and all) of the aforementioned locations.
 - Corporate data must be isolated and protected from a user's personal data while also securing a user's privacy.
 - The IT department must be empowered to secure, classify, and protect the company's data while also maintaining regulatory compliance.

Throughout this book, these challenges will be used as examples for scenarios that explain how Enterprise Mobility Suite (EMS) can assist your company's efforts to enable a mobile workforce.

What about BYOD?

Your efforts to embrace a mobile workforce must include an effective strategy for handling the BYOD scenario. The BYOD scenario includes more than making your company "mobile ready;" it encompasses all the challenges and opportunities as well as the security risks of variations on the scenario. These variations will be explored in this chapter. Before you delve into the specific challenges involved with BYOD, think about why BYOD has become a "buzz-word" and why companies should proceed cautiously when adopting BYOD.

Real World The vendor-agnostic approach to BYOD

For the past two years, I've been delivering BYOD presentations that approach the topic from the architecture perspective and explain how to build a BYOD design with a vendor-agnostic approach. My first work on this field was released in April 2014 with the BYOD Design Considerations Guide (available at <http://aka.ms/BYODCG>), which features a collection of vendor-agnostic considerations regarding BYOD and how Microsoft technologies can help your company fulfill those requirements. The presentation that I delivered at TechEd North America 2014 was based on this paper; you can watch it at <http://aka.ms/byodtena14> and learn how to use a vendor-agnostic approach when developing your BYOD strategy.

To help IT professionals to think of BYOD as a problem domain that must have design considerations and choices aligned with company requirements, constraints, and vision, I also recorded a series of interviews (<http://ala.ms/byodseris>) for TechNet Radio. These materials can help you to plan, design and build your solution to address the BYOD challenges.

Yuri Diogenes

Senior Content Developer, CSI Enterprise Mobility Team, Microsoft Corporation

A November 2013 study by Gartner suggested that 20 percent of enterprise BYOD programs will fail before 2016. The study indicates programs will fail because of mobile device management measures that are too restrictive. This study shows that companies are moving towards the adoption of BYOD, but they are restricting access and thereby not necessarily realizing BYOD's full potential. Managing security is often a delicate balance. If your security policies aren't strict enough, you'll put corporate resources at risk. If your security policies are too strict, you might create an environment that becomes a tremendous challenge for the IT department to support, thereby adversely impacting your ROI. If your BYOD security produces a higher volume of help-desk calls from frustrated users, or, worse yet, if users are unable to perform their work, you might find that your organization needs to roll back to previous technology. As a result, BYOD becomes an enemy of the company. For this reason, you must ensure that your organization defines an effective BYOD strategy before BYOD is implemented or deployed.

In October 2014, a CheckPoint survey of 700 IT professionals showed mobile security incidents caused by BYOD had cost each organization more than \$250,000 US to remediate⁴. These costs are likely to increase as more organizations adopt BYOD as part of their enterprise mobility strategy—underscoring the importance of understanding the challenges of adopting BYOD.

Understanding the challenges of BYOD

Before you can understand the challenges introduced by BYOD, you must first understand your own business requirements, constraints, regulatory compliance needs, and users' needs and goals. Unfortunately, this planning phase is often completely overlooked and gaps are found when the next phase—designing the solution—is underway. The best way to mitigate risk is to be aware of how your own company operates. The assumption here is that your company already has a security policy in place. What if that security strategy does not address the security challenges that BYOD introduces to the environment? The same rationale can be applied to your current management infrastructure. What if the existing management platform does not allow users to bring their own devices or does not provide access to company resources?

The industry that your company works in also plays an important role in how BYOD should be adopted. With BYOD, the device contains both the user's personal data and the company-owned data. This results in unique challenges for each industry. For instance, in a school environment, BYOD can be very helpful; to improving user productivity; however, the challenges can be very unique, as you will see in this section of the book.

MORE INFO Read "BYOD Devices - A Deployment Guide for Education" for a better understanding of the design considerations applicable to the education industry at <http://www.microsoft.com/en-us/download/details.aspx?id=39681>.

⁴ For more information about the core findings of this survey, visit <http://www.infosecurity-magazine.com/news/byod-security-incident-costs/>.

There are privacy elements that must be considered for both the individual and the corporation. For this reason, it is very important to involve your legal department when planning the BYOD adoption. Employees must be aware that when they enroll in the BYOD program, the devices that they use might be subject to discovery in litigation. The personal devices they use at work could be examined not only by the employer but by the other party in a lawsuit. Of course, this will vary according to country/region and state laws. As shown in Figure 1-3, the Human Resources (HR), legal, and IT departments should be used as input when you're creating an Enterprise Mobility Strategy.

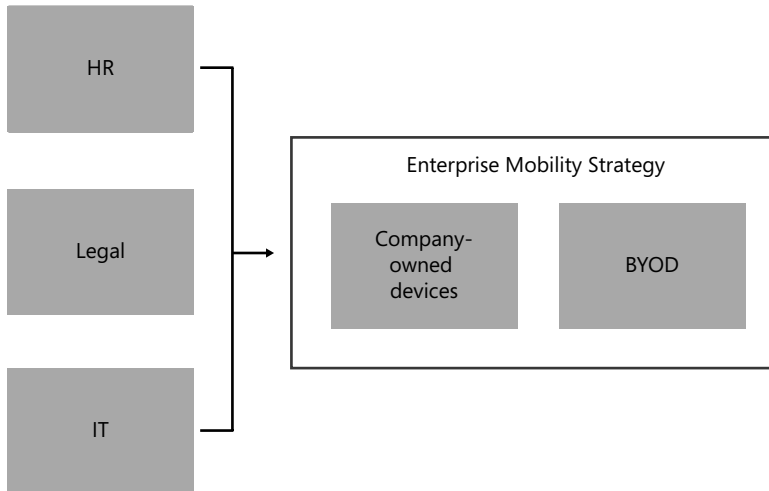


FIGURE 1-3 HR, Legal, and IT must review the enterprise mobility strategy

Awareness is an important aspect of BYOD. Employees need to be made aware of any legal risks involved in using their own devices for work-related tasks. For example, when employees travel internationally, their devices might be subject to search or seizure by border control agents. This affects not only the employee and his device but the company as well. Part of your self-assessment for BYOD adoption is making sure that the Legal and HR departments understand these scenarios. In this case, Legal should advise HR of the fact that an employee might forfeit certain rights to her personal device when using it for work. HR should also look for issues related to:

- Off-the-clock work for hourly employees and any potential compensation claims
- Local tax considerations
- Ownership of the telephone number (for a BYOD phone)

The responsibility for the loss of data on an employee-owned device can be proactively managed via policy. However, in a BYOD scenario it becomes more of a challenge. Deleting an employee's data from a personal device could have legal implications, so your organization should build a solid BYOD policy to protect itself. You should also be aware that some employees share their own devices with family members, and the shared use of employee-owned devices is one of the most pressing BYOD issues. This issue is very difficult to mitigate with policy. An employee sharing a BYOD device with his spouse invites the potential for serious issues, such as corporate data loss or security breaches.

Another BYOD scenario that must be addressed in partnership with HR and Legal is the situation whereby employees sell or recycle their own devices after those devices have been used to access company data. A common policy and technology strategy is to enable remote wiping of the device's data and require it as a condition of program participation.

IMPORTANT For policies to be effective, they must be well written, clearly communicated to employees, and enforced. Employees who are enrolling in a BYOD program must sign an agreement that holds them accountable for their actions.

The synergy among the HR, Legal and IT departments will help the company to better embrace enterprise mobility and address the challenges introduced by the BYOD scenario. In summary, the role of each department in this process is as follows:

- HR is responsible for developing policies for BYOD usage, selecting the people involved in setting those policies, as well as driving the training and compliance related to policies.
- Legal is responsible for identifying the information that can be accessed by specific individuals or groups and has input into policy development.
- IT implements the policies as directed by the HR and Legal departments, choosing the tools and technologies used to deliver the services, access resources, and protect data.

Understanding the Microsoft Device Strategy Framework

Figure 1-3 introduces the concept of two types of devices: company-owned device and user-owned device. However, there are variations in both ownership and management of the devices that make it necessary to expand the BYOD scenario to include the four core scenarios shown in Figure 1-4. These scenarios comprise the Microsoft Device Strategy Framework.

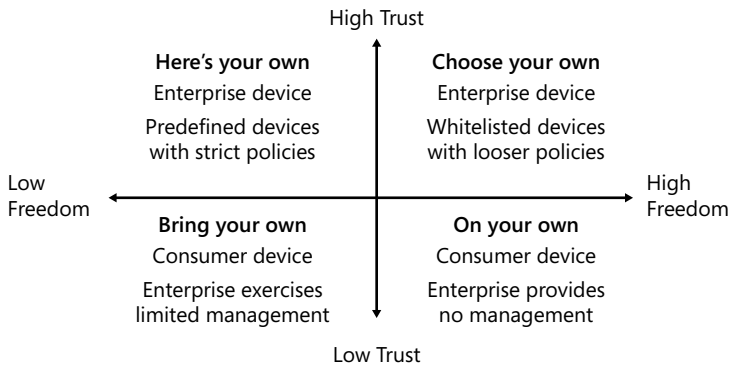


FIGURE 1-4 The Microsoft Device Strategy Framework

The scenarios shown in Figure 1-4 can be summarized as follows:

- **On your own** In this model, employees provide their own devices. There are no security policies in place, no organizational management of the device, and any device is acceptable. This is a very open approach, but it presents the highest security risk.
- **Bring your own device** This model includes two distinct variations on policy management:
 - Bring your own *unmanaged* device In this model, employees provide their own devices, but as part of the company policy, the company does not manage those devices. The employees are responsible for implementing and managing company policies on their devices. This is a flexible policy but it presents security risks; some businesses might not have the resources to manage these risks.
 - Bring your own *managed* device This is the most traditional format for BYOD. In this model, employees provide their own devices and the company enforces its policy to allow the devices to access company data. The device is fully managed by the company.
- **Choose your own device** (also called CYOD) In this model, the company provides a mobile device to employees so those employees can perform their jobs remotely. The company often allows employees to choose from a list of approved devices that are fully compatible with the company's apps and management infrastructure.
- **Here's your own device** In this model, the company has one device approved for the company's mobile platform and this device is provided to employees.

The landscape for enterprise mobility extends well beyond BYOD; you cannot assume enterprise mobility means BYOD only. There are many more elements that must be covered to completely embrace mobility and enable a mobile workforce. Each scenario has advantages and disadvantages that vary according to company requirements and goals.

MORE INFO For more information about the Microsoft Device Strategy Framework, see the blog post by the Enterprise Mobility Team at <http://blogs.technet.com/b/enterprise-mobility/archive/2014/10/08/looking-back-and-moving-forward-with-enterprise-mobility-suite-beyond-the-byod-scenario.aspx>.

Designing a strategy to enable a mobile workforce

This chapter has covered the factors that are driving enterprise mobility adoption and the core challenges you need to address when developing an enterprise mobility strategy. This section takes the elements shown in Figure 1-1 and explains how to use them to design an effective strategy to enable enterprise mobility.

Users

The first element is the user or employee. The user becomes a key element when companies start to move from a device-centric view to a user-centric view. Each user within your company has specific business needs; some have common business needs and some have unique business requirements. This part of the designing process is necessary to understand the user's profile. This is accomplished by defining *personas*. The following list provides examples of typical user profiles:

- **Executive** This persona expects the company to buy them whatever device they want to use as their primary device. An Executive isn't likely to be a BYOD user.
- **Mobile worker** This persona encompasses a large group of employees that are accustomed to using multiple devices.
- **Technical/field worker** This persona requires a robust device to perform their work. Usually, this type of user primarily accesses line of business (LOB) applications and email, and enters data into customer relationship management (CRM) tools.
- **Deskbound information worker** This persona uses a variety of devices and enrolls in the BYOD program. From taking notes in meetings on their own companion devices to potentially wanting to use their own machines while in the workplace, these users are likely to drive most of the BYOD adoptions in the company.
- **Remote information worker** This persona looks to optimize their workspace, blending personal priorities with company priorities. These users might be good candidates for the BYOD program.

Keep in mind that these are just some examples of user profiles for an enterprise. Different industries and business have different roles and requirements. It is important to identify the persona and comprehend the users' needs based on their roles. You will identify these roles as part of the company self-assessment, which should be done before you start designing the enterprise mobility strategy.

You also need to consider the persona distribution, which is based on two elements: autonomy and mobility. Figure 1-5 shows the rationale behind the persona distribution.

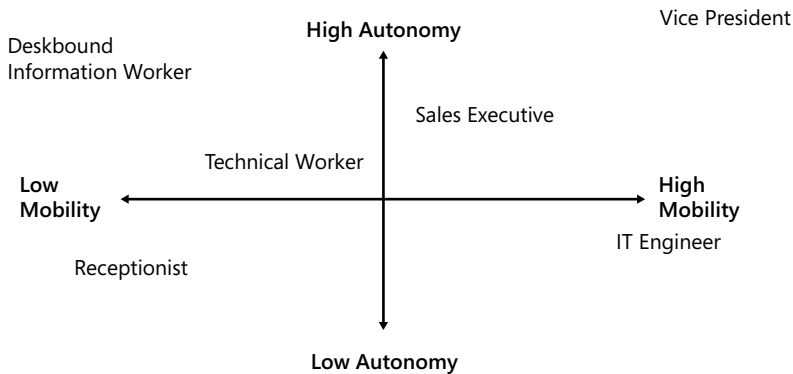


FIGURE 1-5 A persona distribution quadrant

This persona distribution relates to the user's work style and how the company can ensure that this user has what she needs to be productive. For example, some employees might always work at the same physical location (categorized as low mobility) while others might work at different branches, work from home, work from hotels, and so on (categorized as high mobility). The degree of autonomy is directly related to the balance between the freedom that the user needs to perform their business operations and the amount of restrictions added by the security policies.

Devices

Consider the type of devices that the company will allow. Access should be available from a broad set of device types, including managed devices, unmanaged devices, and consumer devices. Also, you should plan to include both Windows-based and non-Windows-based devices. Assuming your company will include a BYOD scenario, it is important to perform a survey of your employees to understand which devices they use and which operating systems they have installed on those devices.

When determining which devices will be supported by the company, carefully balance information security classification with the trustworthiness of the device and the point of connection. It is important to understand the device's capabilities and define how those devices will access corporate information. The required capabilities of each device might vary according to the company's security policy and business requirements. Figure 1-6 shows an example of some considerations regarding the device type and required capabilities. After you have defined the devices that will be supported, you need to define the required capabilities, such as data encryption, customization via policy, Mobile Device Management (MDM), and containerization.

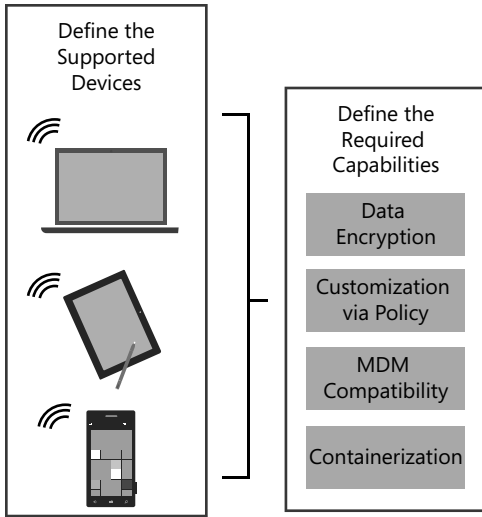


FIGURE 1-6 An example of device type selection based on required capabilities

It's important for the IT department to understand if the devices that will be supported by the company have these capabilities. Once the device type is established, you need to define the access level that the device will have based on pre-established variables. User, device, location, and data can be used as variables to define the user's experience when accessing corporate data. One variable, for example, can be the device's location. Your company policy might allow full network access only for devices that are located on-premises. When the device is located on-premises, it will have one set of policies applied to it; if it is coming from the cloud, it will have a more restrictive policy. *It is important to balance security with usability.* You don't want to enforce so much restriction that there is a negative effect on the user's productivity. If you find the right balance, you will increase productivity. Figure 1-7 shows an example of some of these variables.

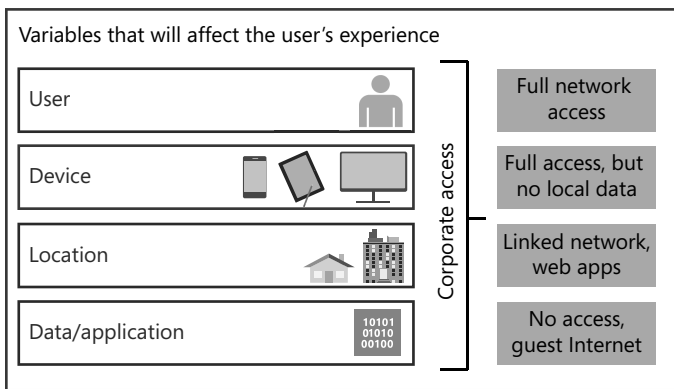


FIGURE 1-7 Examples of variables that will affect the user's experience while accessing corporate data

Using the diagram in Figure 1-7 as model, a sample policy can be defined as follows: if the device type is a Windows 8.1 phone and the device is located on-premises and it is trying to access an LOB application and the user has privileges to access that application, then the device should have full network access. Notice that each piece of the definition is connected to the next piece with “and,” which makes each part of the definition a test. By creating this test, all answers to these questions must be true in order to grant full network access. These tests can vary. For example, your company might choose to use “or” instead of “and,” which means only one requirement must be true to allow the device full access to the target resource.

Now that you have defined the key capabilities that are required by each device and the variables that will influence the user’s experience according to the device’s current state, the next important point to cover for the device is the supportability. If your company operates as a service provider, you could use a Service Level Agreement (SLA) to ensure that your users are aware of what to expect when they open an incident report with IT. An enterprise mobility strategy must include a plan to support the user’s device and also set the boundaries of this support. The fact is that not all devices will be treated equally and this will impact the supportability boundaries. This should be very clear not only to the IT team but to the user as well. By knowing what to expect from support, you mitigate the possibility of user frustration when that user opens an incident report and her device has limited support.

Apps

Although the industry tends to put more emphasis on devices, apps are the main gateway to information access. If your company doesn’t have mobile apps, embracing a mobile workforce won’t be very productive. As part of your design considerations, you must understand the current LOB applications that are used by your employees, how these apps will behave on the different operating systems that you are about to support, as well as the user’s skill level on each device that is approved by IT. When developing a strategy for apps, you must:

- Define which apps will be available for the users to consume using their devices
- Validate if those apps need any type of adjustment to correctly run on different platforms
- Perform a threat assessment on each app that will be available for mobile users and verify if there is any flaw that can lead to a security risk
- Mitigate potential flaws by fixing the root cause of the problem or adding counter-measures that can reduce the risk
- Verify how these apps will be available for user’s consumption from those different devices
- Enumerate the options that are feasible for your business to make those apps available (for example, deployment via web portal, access via remote app, access via VPN, and so on)

During this exercise, you will identify different gaps and each gap should be documented in detail. The output of this design consideration for apps might induce you to upgrade your server infrastructure to support this new model or adopt cloud-based apps for your mobile users.

Data

Remember, the CEO wants to enable users to be productive from anywhere, using the device of their choice, while keeping company data secure. The key to a successful enterprise mobility adoption is to allow users to consume company resources without compromising the data. The considerations regarding data protection should include:

- A security envelope to protect the data
- Safety net policies that control access and reporting
- An additional level of authentication, such as multifactor authentication
- Business-driven policies for data protection
- A classification of data according to sensitivity and business impact
- Access control to data based on identity and role
- Data encryption

You should understand how data can be protected on different platforms. Also, you should understand each platform's capabilities so those capabilities can be leveraged to protect data. Some mobile platforms will use the principle of least privilege to protect and isolate data, such as the Windows Phone security model and its use of AppContainer as a secured isolation boundary.

MORE INFO To better understand the Windows Phone 8.1 security model, read the white paper at <http://www.microsoft.com/en-us/download/details.aspx?id=42509>.

While IT has full control over the data stored at the company's data center, the same level of assurance can be a challenge with unmanaged BYOD devices. How data will be stored in users' devices can directly impact how you choose to address data access and protection for enterprise mobility. Data encryption must be considered, and devices must allow IT to control when data encryption is enabled and for which types of data. Companies must review their policies and regulations to understand which types of data are allowed to leave the data-center and be at rest in remote devices' storage.

Protecting the data is not enough; you must monitor how this data has been accessed so you can take measures to mitigate potential breaches. Part of your enterprise mobility strategy includes data governance. Choosing the right management platform to monitor your data access and take actions based on what you are able to find via reporting capabilities should be a very important decision point to your company. With the assumption that users can access

data from anywhere, you must be vigilant to potential patterns that can help your company understand that an attack is in place.

Threat mitigation

After evaluating each element of your enterprise mobility strategy, you can now perform a threat modelling exercise to understand the interactions between each component and identify threats that might occur during those interactions that require mitigation. Using the core elements of Figure 1-1, you can determine who should be allowed to access the data. The first goal during threat mitigation is to reduce the attack surface by disallowing direct access to some of those elements. Figure 1-8 shows an example of the core elements of an enterprise mobility strategy. In the Before scenario, each element has direct access to the data. In the After scenario, direct access is limited to Apps only.

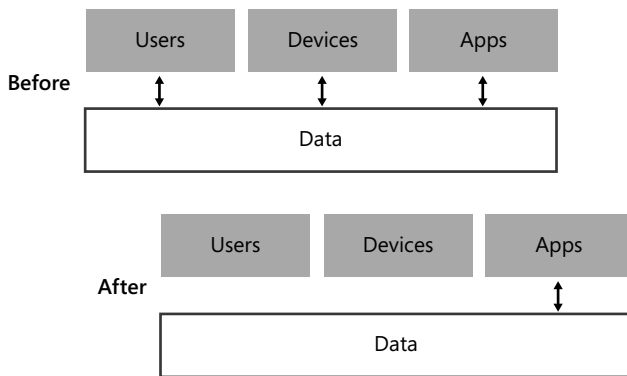


FIGURE 1-8 Reducing the attack surface by limiting direct access to the data

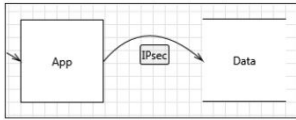
Another step of the threat mitigation process is to understand the risks on each interaction between these components. In Figure 1-8, for example, what risks are present when these apps have direct access to the data? You might conclude that the following actions must be performed:

- For apps to have access to data, the communication channel must be encrypted
- All mobile apps should be developed using a security development lifecycle
- Data at rest on the application server must be encrypted

To assist you through the process of understanding the risks of each interaction, you can leverage the Microsoft Threat Modeling Tool. Although this tool was created for another purpose, the rationale behind threat modeling is the same for interactions between the components of this model. Once you build the diagram and the data flows through the components, you can generate a report that will highlight the potential threats that must be mitigated. Figure 1-9 shows an example of this report.

MORE INFO You can download the Microsoft Threat Modeling Tool at <http://www.microsoft.com/en-us/download/details.aspx?id=42518>.

Interaction: IPsec



1. Spoofing of Destination Data Store Data [State: Not Started] [Priority: High]
Category: Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.
Description: Data may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Data. Consider using a standard authentication mechanism to identify the destination data store.
Justification: <no mitigation provided>
2. Lower Trusted Subject Updates Logs [State: Not Started] [Priority: High]
Category: Repudiation threats involve an adversary denying that something happened.
Description: If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. Only allow trusted code to log.
Justification: <no mitigation provided>
3. Data Logs from an Unknown Source [State: Not Started] [Priority: High]
Category: Repudiation threats involve an adversary denying that something happened.
Description: Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.
Justification: <no mitigation provided>

FIGURE 1-9 A report generated using the Microsoft Threat Modeling Tool

This report also categorizes the threats according to priorities, which can also help you understand which threats should be addressed first. When you finish this designing process for enterprise mobility, you should have:

- A full understanding of how your company will benefit from the adoption of enterprise mobility
- A vendor-agnostic design of your enterprise mobility solution
- A threat mitigation report with core points that must be addressed during the implementation
- A list of requirements that must be met by the vendor

This page intentionally left blank

Index

Symbols

- 2008 IDC (International Data Corporation) study, 1
- 2014 IDG Enterprise CITE (Consumerization of IT in the Enterprise) study, 1–2

A

access, data

- Azure RMS, 135–147
 - choosing right deployment topology, 141–143
 - how Azure RMS works, 137–140
 - monitoring access to resources, 145–147
 - RMS connector, 143–145
- leveraging on-premises resources, 127–135
 - Web Application Proxy, 130–131
 - Windows Server Dynamic Access Control, 128–129
 - Work Folders, 131–135

access levels (devices), 11

access management benefits, hybrid identity implementation, 58–59

Activate button, turning on directory synchronization, 37

activation

- Azure RMS Tool, 152
- directory synchronization in Azure AD, 61
- EMS, 23–24

Active Directory Federation Services. *See* AD FS

activity logs, Azure AD Premium, 30

Add A New Rights Policy Template dialog box, 154

adding public domains, 60–61

Add Software wizard, 113

AD FS (Active Directory Federation Services)

directory integration, 38–39

Farm page (Azure AD Connect Wizard), 65–66

planning/designing hybrid identity solution, 55–56

sign-in page

- customized branding, 71–73
- planning/designing hybrid identity solution, 56

Admin Console, Policy workspace, 84

Advanced Encryption Standard (AES), 135

AES (Advanced Encryption Standard), 135

A Host records, 55

alerts

Azure AD Premium, 28–30

Microsoft Intune monitoring capabilities, 175–176

Allow A Server To Utilize The Connector page (Azure RMS Connector Administrator Tool), 162

analysis of data, troubleshooting EMS, 189

Android devices

- configuration policies, 86–87
- deploying email profile configuration policies, 109
- enrollment, 117–120

anomalous activity reports, Azure AD Premium, 29–30

APN certificate signing request file, 103

APNs (Apple Push Notification service) certificates, 78, 103

AppContainer, Windows Phone security model, 13

Apple Configurator, 86

Apple Push Certificates Portal, 103

Apple Push Notification service (APNs) certificates, 78, 103

Application log, Event Viewer, 203

applications (apps)

- challenges of enabling enterprise mobility, 2–4
- data access and protection diagram, 150
- design strategies for mobile workforces, 12–13
- solution diagram for hybrid identity, 51

- Application Settings, Mobile Device Security Policy, 100
 - application usage reports, 30, 174
 - apps (applications)
 - challenges of enabling enterprise mobility, 2–4
 - data access and protection diagram, 150
 - design strategies for mobile workforces, 12–13
 - solution diagram for hybrid identity, 51
 - Apps section, Company Portal, 81
 - Assign Custom Rights page, creating custom templates, 156–157
 - auditing conditional expressions, 129
 - autonomy (persona distribution), 10
 - Azure Access Panel, 32–35
 - accessing SaaS applications, 32–33
 - group management, 33–34
 - password management, 34–35
 - Azure Active Directory Synchronization Services (Azure AD Sync), 43–45
 - Azure Active Directory Sync Services Wizard, 43
 - Azure AD (Microsoft Azure Active Directory), 27
 - directory integration, 35–47
 - AD FS, 38–39
 - directory synchronization, 36–38
 - scenarios, 39–41
 - source of authority, 36
 - synchronization tools, 41–47
 - disabling user access, 184
 - monitoring capabilities, 172–174
 - preparing service for directory integration, 60–61
 - Azure AD App and Attribute Filtering (optional feature, Azure AD Sync), 44
 - Azure AD Connect Wizard, 45–47
 - enabling SSO (Single Sign-On), 64–70
 - Getting Started page, 46
 - planning/designing hybrid identity solution, 57–58
 - troubleshooting Azure AD Premium, 191–192
 - Azure AD Premium*
 - Azure Access Panel, 32–35
 - self-service group management, 33–34
 - self-service password management, 34–35
 - user access, SaaS (Software-as-a-Service) applications, 32–33
 - Azure Multi-Factor Authentication, 30–32
 - cloud identity, 27–28
 - security reports and alerts, 28–30
 - troubleshooting EMS, 191–194
 - Azure AD Sync (Azure Active Directory Synchronization Services), 43–45
 - Azure AD Sync Scheduler task (Task Scheduler Library), 69
 - Azure Management Portal
 - activation of Azure RMS Tool, 152
 - creating custom templates, 154–156
 - Azure Multi-Factor Authentication, 30–32
 - Azure Rights Management Administration Tool, installation, 151
 - Azure Rights Management Services. *See* Azure RMS; RMS
 - Azure RMS (Azure Rights Management Services), 135–147
 - configuring templates, 153–159
 - connector, 159–168
 - data protection, 135–147
 - choosing right deployment topology, 141–143
 - how Azure RMS works, 137–140
 - monitoring access to resources, 145–147
 - RMS connector, 143–145
 - templates, 135
 - integrating DAC feature, 133–134
 - integration with Work Folders, 166–168
 - leveraging for data protection, 151
 - monitoring capabilities, 179–180
 - troubleshooting EMS, 199–203
 - Azure RMS connector webpage, 162
- ## B
- BitLocker technology, 134
 - branding
 - adding company branding, Microsoft Azure Management Portal, 70–71
 - AD FS sign-in page, 71–73
 - customizing Company Portal, 98
 - Bring Your Own Device (BYOD) devices
 - monitoring
 - continuous monitoring and incident response, 169–170
 - incidence response plans, 170–171
 - leveraging EMS to monitor resources, 171–180
 - leveraging EMS to respond to a security incident, 180–186
 - scenarios, 4–7
 - challenges, 5–7

- Microsoft Device Strategy Framework, 7–9
- Bring Your Own Key (BYOK) capability, Azure RMS, 135, 142
- built-in capabilities, data protection, 134–135
- BYOD (Bring Your Own Device) devices
 - monitoring
 - continuous monitoring and incident response, 169–170
 - incidence response plans, 170–171
 - leveraging EMS to monitor resources, 171–180
 - leveraging EMS to respond to a security incident, 180–186
 - scenarios, 4–7
 - challenges, 5–7
 - Microsoft Device Strategy Framework, 7–9
- BYOD Design Considerations Guide, 4
- BYOK (Bring Your Own Key) capability, Azure RMS, 135, 142

C

- central access policies, 128–129
- Certificate Compliance Reports (Microsoft Intune), 177
- certificates
 - APNs (Apple Push Notification service), 78, 103
 - CLCs (Client Licensor Certificates), 140
 - code-signing (Symantec), 78
 - publicly trusted X509 v3 SSL, 56
 - security, 56–57
 - SLCs (Server Licensor Certificates), 140
- challenges
 - BYOD (Bring Your Own Devices) scenarios, 5–7
 - enabling mobile workforces, 2–4
- check compliance option, Company Portal app, 196
- CheckPoint survey (2014), 5
- choose your own device (CYOD) scenario, 8
- CITE (Consumerization of IT in the Enterprise), 2014 study, 1–2
- claims-aware FCI, 128
- CLCs (Client Licensor Certificates), 140
- client access validation, 166
- Client Licensor Certificates (CLCs), 140
- client-side RMS, troubleshooting, 199–201
- closure documentation, troubleshooting EMS, 190
- cloud identity, Azure AD Premium, 27–28
- Cloud Policy Settings, Mobile Device Security Policy, 100
- cloud services
 - data access and protection diagram, 150
 - disabling user access, 184
 - solution diagram for hybrid identity, 51
 - troubleshooting EMS, 191
- cloud topology, Azure RMS, 141
- cmdlets
 - Connect-AadrmService, 200
 - GenConnectorConfig, 163
 - Get-AadrmConfiguration, 200
 - Get-AADRMTemplate, 200
 - Get-AADRMTemplateProperty, 201
 - Import-Module AADRM, 200
 - Set-AdfsGlobalWebContent, 72
 - Set-AdfsWebTheme, 72
 - Update-WebApplicationProxyDeviceRegistration, 131
- CNAME records, 56
- code-signing certificates (Symantec), 78
- code-signing Company Portal, 104
- company-owned devices, monitoring
 - continuous monitoring and incident response, 169–170
 - incidence response plans, 170–171
 - leveraging EMS to monitor resources, 171–180
 - leveraging EMS to respond to a security incident, 180–186
- Company Portal
 - check compliance option, 196
 - Company Portal app, 80–81
 - customizing, 81–82
 - company terms and conditions, 83
 - preparing Microsoft Intune for enrollment, 106–107
 - usage terms and conditions, 108
 - Microsoft Intune service configuration, 98–99
- Complete Action dialog box, 118
- compliance policies, 88
 - Microsoft Intune service enrollment, 109–110
 - planning/designing device management solution, 101–102
- computer inventory management, 91
- Computer Inventory Reports, Microsoft Intune, 91
- computers
 - configuration policies, 87

- enrollment, 123–125
- Conditional Access Control, 129
- Conditional Access For Exchange Online Policy, 102
- conditional access policies, 88–90
 - Microsoft Intune service enrollment, 110–112
 - planning/designing device management solution, 102
- conditional expressions
 - auditing, 129
 - permissions and, 129
- Confidential template (Azure RMS), 154
- Confidential View Only template (Azure RMS), 153
- Configuration Manager, 77
- configuration policies, 84–87
 - Android devices, 86–87
 - common mobile device settings, 85–86
 - computers, 87
 - iOS devices, 86
 - Microsoft Intune service enrollment, 109
 - planning/designing device management solution, 100–101
 - Windows devices, 86
- configuring
 - Azure RMS templates, 153–159
 - applying custom templates to a document, 157–159
 - custom templates, 154–156
 - compliance policies, 88
 - conditional access policies, 88–89
 - configuration policies, 84–87
 - Exchange ActiveSync policies, 90–91
 - file classification, 163–165
 - File Server to use Azure RMS, 163
 - Mobile Device Security Policy, 85
 - name resolution, 63–64
 - synchronization filtering, 68–69
 - users/groups for synchronization, 62–63
 - Windows DNS name resolution, 79
- conflicts, policies, 90–91
- Connect-AadrmService cmdlet, 200
- connector (Azure RMS)
 - planning/designing data protection solution, 159–168
 - configuring file classification, 163–165
 - configuring File Server, 163
 - integration of Azure RMS with Work Folders, 166–168
 - validating client access, 166

- troubleshooting, 201–203
- Consumerization of IT in the Enterprise (CITE), 2014
 - study, 1–2
- contact information, customizing Company Portal, 98
- Contact IT section, Company Portal, 81
- containerization (required capability), 10
- continuous monitoring of devices, 169–170
- corporate network
 - data access and protection diagram, 150
 - solution diagram for hybrid identity, 50
- CSS (Customer Service and Support), 142
- Customer Service and Support (CSS), 142
- Customization section, Company Portal, 82
- customization via policy (required capability), 10
- customizing
 - branding, 70–73
 - adding company branding, Microsoft Azure Management Portal, 70–71
 - AD FS sign-in page, 71–73
 - Company Portal, 81–82
 - Microsoft Intune service configuration, 98–99
 - preparing Microsoft Intune for enrollment, 106–107
 - usage terms and conditions, 108
- custom templates (Azure RMS)
 - applying to a document, 157–159
 - configuring, 154–156
- CYOD (choose your own device) scenario, 8

D

- DAC (Dynamic Access Control)
 - integrating with AD RMS, 133–134
 - leveraging for data protection, 128–129
- data analysis, troubleshooting EMS, 189
- data collection, troubleshooting EMS, 189
- data encryption, 10, 13
- data governance, 13
- data protection
 - Azure RMS, 135–147
 - choosing right deployment topology, 141–143
 - how Azure RMS works, 137–140
 - monitoring access to resources, 145–147
 - RMS connector, 143–145
 - challenges of enabling enterprise mobility, 2–4
 - design strategies for mobile workforces, 13–14

- implementation
 - Azure RMS connector, 159–168
 - configuring Azure RMS templates, 153–159
 - goals, 149–150
 - planning/designing solution, 151–153
- leveraging on-premises resources, 127–135
 - Web Application Proxy, 130–131
 - Windows Server Dynamic Access Control, 128–129
 - Work Folders, 131–135
- understanding EMS solution, 21–23
- Deactivate button, turning off directory synchronization, 37
- default AD FS sign-in page, 56
- default Device Enrollment Policy, 80
- default enrollment profile, Microsoft Intune service, 106
- defense-in-depth strategy, data protection, 127
- deployment
 - Mobile Device Security Policy, 108
 - policies (device management), 83–91
 - compliance policies, 88
 - conditional access policies, 88–90
 - configuration policies, 84–88
 - Exchange ActiveSync policies, 90
 - policy conflicts, 90–91
 - topology (RMS), 141–143
- design
 - data protection solution, 151–153
 - leveraging Azure RMS, 151
 - preparing the environment, 151–153
 - device management solution, 97–105
 - Microsoft Intune service configuration, 97–99
 - Mobile Device Management enrollment, 102–105
 - policies, 100–102
 - enabling mobile workforces, 9–15
 - apps, 12–13
 - data protection, 13–14
 - devices, 10–12
 - threat mitigation, 14–15
 - users, 9–10
 - hybrid identity solution, 51
 - Microsoft Azure Access Panel, 52–53
 - Microsoft Azure Management Portal, 51–52
 - on-premises environment, 53–54
 - SSO (Single Sign-On) components, 54–60
- deskbound information worker (user profile), 9
- Detected Software Reports (Microsoft Intune), 176
- detection
 - security incidents, 181–183
 - security phase, 170
- Device Capability Settings, Mobile Device Security Policy, 100
- Device Enrollment dialog box, 115
- Device History Reports (Microsoft Intune), 177
- Device Registration Service, 131
- devices
 - access levels, 11
 - challenges of enabling enterprise mobility, 2–4
 - data access and protection diagram, 150
 - design strategies for mobile workforces, 10–12
 - management, 75
 - enrollment, 76–83, 114–125
 - external device enrollment dependencies, 112–114
 - full and selective wipes, 92–93
 - implementation goals, 96
 - inventory management, 91–92
 - planning/designing solution for implementation, 97–105
 - policy deployment, 83–91
 - preparing Microsoft Intune service for enrollment, 105–112
 - solution diagram, 96–97
 - Managed By Exchange ActiveSync, 89
 - Managed By Microsoft Intune And Exchange ActiveSync, 89
 - Managed By Microsoft Intune, 89
 - monitoring
 - continuous monitoring and incident response, 169–170
 - incidence response plans, 170–171
 - leveraging EMS to monitor resources, 171–180
 - leveraging EMS to respond to a security incident, 180–186
 - registration, 131
 - required capabilities, 10
 - solution diagram for hybrid identity, 50
- dialog boxes
 - Add A New Rights Policy Template, 154
 - Complete Action, 118
 - Device Enrollment, 115
 - Manage Mobile Devices, 76
 - Microsoft Intune report export, 178
 - Retire Device confirmation, 93

- Select Containers (Synchronization Service Manager), 69
- Set Up Service To Service Connector, 111
- Upload The APNs Certificate, 112
- View Policy Issues, 88
- Warning, 116
- directory integration, 35–47
 - AD FS, 38–39
 - directory synchronization, 36–38
 - preparing Azure AD service for, 60–61
 - preparing on-premises environment for, 61–64
 - scenarios, 39–41
 - directory sync, 40
 - directory sync with password sync, 40
 - directory sync with SSO, 40
 - multiforest directory sync with SSO, 41
 - source of authority, 36
 - synchronization tools, 41–47
 - Azure AD Connect, 45–47
 - Azure AD Sync, 43–45
 - DirSync, 41–43
- directory sync scenario (directory integration), 40
- directory synchronization, 36–38
 - activating in Azure AD, 61
 - forcing action and verifying success, 69–70
- directory sync with password sync scenario (directory integration), 40
- directory sync with SSO scenario (directory integration), 40
- DirSync, 41–43
- DirSync Welcome page, 41–42
- disabling user access, 184
- DNS CNAME records, 104
- DNS name resolution, configuring, 79
- domain synchronization, Microsoft Azure Management Portal, 60
- Dynamic Access Control (DAC)
 - integrating with AD RMS, 133–134
 - leveraging for data protection, 128–129

E

- Email Policy Settings, Mobile Device Security Policy, 100
- email profile configuration policies
 - Microsoft Intune service enrollment, 109
 - settings, 101–102

- EMS (Enterprise Mobility Suite)
 - activation process, 23–24
 - embracing mobile workforce scenario, 24–26
 - leveraging response to security incidents, 180–186
 - detection, 181–183
 - prevention, 181
 - reaction, 183–186
 - leveraging to monitor resources, 171–180
 - Azure AD monitoring capabilities, 172–174
 - Microsoft Azure RMS monitoring capabilities, 179–180
 - Microsoft Intune monitoring capabilities, 175–179
 - troubleshooting
 - Azure AD Premium, 191–194
 - Azure RMS, 199–203
 - cloud services, 191
 - methodology, 187–190
 - Microsoft Intune, 194–198
 - tools, 190
 - where to find information, 190
 - understanding EMS solution, 17–23
 - data protection, 21–23
 - hybrid identity, 18–19
 - MDM (Mobile Device Management), 20–21
- enabling
 - mobile workforces, 1
 - BYOD (Bring Your Own Devices) scenarios, 4–7
 - challenges, 2–4
 - design strategies, 9–15
 - shift towards mobility, 1–2
 - SSO (Single Sign-On), 64–70
 - configuring synchronization filtering, 68–69
 - forcing directory synchronization and verifying success, 69–70
- encryption of data, 13
- End-User License Agreement page (Rights Management Connector Setup Wizard), 160
- enrollment, devices, 76–83, 114–125
 - Android devices, 117–120
 - Company Portal, 80–82
 - custom company terms and conditions, 83
 - device management prerequisites, 78–79
 - external device enrollment dependencies, 112–114
 - iOS devices, 114–117
 - Microsoft Intune, 105–112
 - compliance policies, 109–110

- conditional access policies, 110–112
- creating default enrollment profile, 106
- customizing Company Portal, 106–107
- customizing usage terms and conditions, 108
- deploying email profile configuration policies, 109
- deploying Mobile Device Security Policy, 108
- service configuration, 98
- setting MDM authority, 105–106
- Mobile Device Management, 102–105
 - iOS devices, 103
 - name resolution, 104–105
 - Windows Phone 8.0, 104
- Mobile Device Management authority, 76–77
- profiles, 80
- Windows devices, 120–125
- Enterprise IT, enabling mobile workforces
 - BYOD (Bring Your Own Devices) scenarios, 4–7
 - challenges, 2–4
 - design strategies, 9–15
 - shift towards mobility, 1–2
- Enterprise Mobility Suite. *See* EMS
- environment preparation, data protection solution, 151–153
- Event Viewer, Application log, 203
- Exchange ActiveSync policies, 90, 135
- Exchange Hybrid Deployment (optional feature, Azure AD Sync), 44
- Exchange Online, conditional access policies, 89
- Exchange on-premises, conditional access policies, 89–90
- executive (user profile), 9
- external device enrollment dependencies, 112–114

F

- factory reset option, Company Portal, 93
- FCI (File Classification Infrastructure), 128
- Federal Information Processing Standards (FIPS)-compliant Hardware Security Modules (HSMs), 135
- Fiddler, 190
- fields, Azure RMS log files, 180
- field worker (user profile), 9
- file classification
 - configuring, 163–165
 - File Classification Infrastructure (FCI), 128

- File Classification Infrastructure (FCI), 128
- File Server, configuring to use Azure RMS, 163
- File Server Resource Manager (FSRM)
 - configuring file management tasks, 164–165
 - downloading GetConnectorConfig.ps1 tool, 163
 - enabling, 159
- FIM (Forefront Identity Manager), 27, 68
- Forefront Identity Manager (FIM), 27, 68
- formats, PFILE, 140
- FSRM (File Server Resource Manager)
 - configuring file management tasks, 164–165
 - downloading GetConnectorConfig.ps1 tool, 163
 - enabling, 159
- full device wipes, 92–93

G

- Gartner study (2013), 5
- GenConnectorConfig cmdlet, 163
- generic files, data protection, 136
- Get-AadrmConfiguration cmdlet, 200
- Get-AADRMTemplate cmdlet, 200
- Get-AADRMTemplateProperty cmdlet, 201
- Get Started With Rights Management Quick Start page, creating custom templates, 154
- Getting Started page (Azure AD Connect Wizard), 46
- gMSA (Group Managed Service Account), 66
- goals
 - data protection, 149–150
 - device management implementation, 96
 - hybrid identity implementation, 49–50
- governance (data), 13
- Group Managed Service Account (gMSA), 66
- groups
 - activity logs, 30
 - configuring for synchronization, 62–63
 - self-service management, 33–34
- Groups Activity report (Azure AD), 174

H

- HR (Human Resources), creating enterprise mobility strategy, 6–7
- Human Resources (HR), creating enterprise mobility strategy, 6–7
- hybrid identity, 27

- Azure Access Panel, user self-services, 32–35
 - accessing SaaS applications, 32–33
 - self-service group management, 33–34
 - self-service password management, 34–35
- Azure AD Premium
 - cloud identity, 27–28
 - security reports and alerts, 28–30
- Azure Multi-Factor Authentication, 30–32
- device management, 96
- directory integration, 35–47
 - AD FS, 38–39
 - directory synchronization, 36–38
 - scenarios, 39–41
 - source of authority, 36
 - synchronization tools, 41–47
- implementation
 - customized branding, 70–73
 - enabling SSO (Single Sign-On), 64–70
 - goals, 49–50
 - identity and access management benefits, 58–59
 - planning and designing solution, 51
 - preparing Azure AD service for directory integration, 60–61
 - preparing on-premises environment for directory integration, 61–64
 - solution diagram, 50–51
 - understanding EMS solution, 18–19
- hybrid topology, Azure RMS, 141

I

- IDC (International Data Corporation), 2008 study, 1
- identity management benefits, hybrid identity implementation, 58–59
- identity synchronization, 37
- implementation
 - data protection
 - Azure RMS connector, 159–168
 - configuring Azure RMS templates, 153–159
 - goals, 149–150
 - planning/designing solution, 151–153
 - device management, 95
 - enrollment, 114–125
 - external device enrollment dependencies, 112–114
 - goals, 96

- planning/designing solution, 97–105
- preparing Microsoft Intune service for enrollment, 105–112
- solution diagram, 96–97
- hybrid identity
 - customized branding, 70–73
 - enabling SSO (Single Sign-On), 64–70
 - goals, 49–50
 - identity and access management benefits, 58–59
 - planning and designing solution, 51
 - preparing Azure AD service for directory integration, 60–61
 - preparing on-premises environment for directory integration, 61–64
 - solution diagram, 50–51
- Import-Module AADRM cmdlet, 200
- incidence response plans, monitoring devices, 169–171
- Installation Of Microsoft Rights Management Connector Completed page (Rights Management Connector Setup Wizard), 160–161
- Installing Microsoft Rights Management Connector page (Rights Management Connector Setup Wizard), 160–161
- integrated applications, Azure AD Premium, 30
- International Data Corporation (IDC), 2008 study, 1
- inventory management, 91–92
- iOS devices
 - configuration policies, 86
 - deploying email profile configuration policies, 109
 - device management prerequisites, 78
 - diagnostic information dialog box, 198
 - enrollment, 114–117
 - external device enrollment dependencies, 112–113
 - Mobile Device Management enrollment considerations, 103
- Irregular Sign In Activity report (Azure AD), 173
- IT department, enterprise mobility strategy, 6–7

K

- Kerberos authentication support, 128
- Key Management Service (KMS), 135
- KMS (Key Management Service), 135

L

- legal department, enterprise mobility strategy, 6–7
- License Installation Reports (Microsoft Intune), 177
- License Purchase Reports (Microsoft Intune), 177
- limitations, DirSync, 42
- line of business (LOB) apps, 78
- LOB (line of business) apps, 78
- logs, Azure RMS, 179–180

M

- Managed By Exchange ActiveSync devices, 89
- Managed By Microsoft Intune And Exchange ActiveSync devices, 89
- Managed By Microsoft Intune devices, 89
- management of devices, 75, 95
 - enrollment, 76–83, 114–125
 - external device enrollment dependencies, 112–114
 - full and selective wipes, 92–93
 - implementation goals, 96
 - inventory management, 91–92
 - planning/designing solution for implementation, 97–105
 - policy deployment, 83–91
 - preparing Microsoft Intune service for enrollment, 105–112
 - solution diagram, 96–97
- Manage Mobile Devices dialog box, 76
- MDM authority (Mobile Device Management authority)
 - Microsoft Intune service configuration, 97
 - preparing Microsoft Intune service for enrollment, 105–106
- MDM (Mobile Device Management), 10
 - device enrollment, 76–77, 102–105
 - iOS devices, 103
 - name resolution, 104–105
 - Windows Phone 8.0, 104
 - as part of the solution to device management, 97
 - understanding EMS solution, 20–21
 - MDM authority
 - Microsoft Intune service configuration, 97
 - preparing Microsoft Intune service for enrollment, 105–106
- methodology, troubleshooting EMS, 187–190
- MFA (multi-factor authentication), 30–31
- Microsoft Azure Access Panel, planning hybrid identity solution, 52–53
- Microsoft Azure Active Directory. *See* Azure AD
- Microsoft Azure Management Portal
 - customized branding, 70–71
 - domain synchronization, 60
 - planning hybrid identity solution, 51–52
- Microsoft Azure RMS Connector Administrator Tool, 161
- Microsoft Connectivity Analyzer tool, 192–193
- Microsoft Customer Service and Support (CSS), 142
- Microsoft Device Strategy Framework, 7–9
- Microsoft Intune
 - device management, 75
 - enrollment, 76–83
 - full and selective device wipes, 92–93
 - inventory management, 91–92
 - policy deployment, 83–91
 - monitoring capabilities, 175–179
 - alerts, 175–176
 - reports, 176–179
 - preparing service for enrollment, 105–112
 - compliance policies, 109–110
 - conditional access policies, 110–112
 - creating default enrollment profile, 106
 - customizing Company Portal, 106–107
 - customizing usage terms and conditions, 108
 - deploying email profile configuration policies, 109
 - deploying Mobile Device Security Policy, 108
 - setting MDM authority, 105–106
 - service configuration, 97–99
 - Company Portal customization, 98–99
 - device enrollment profiles, 98
 - Mobile Device Management authority, 97
 - terms and conditions, 99
 - troubleshooting EMS, 194–198
- Microsoft Intune Center, 87
- Microsoft Intune Company Portal URLs, customizing Company Portal, 82
- Microsoft Intune Online Connector for Online Exchange, 111–112
- Microsoft Intune report export dialog box, 178
- Microsoft Intune Setup Wizard, 124–125
- Microsoft Online Services Directory Synchronization tool. *See* DirSync
- Microsoft Rights Management Connector Setup Wizard, 159–160

- Microsoft RMS Administrator Credentials page (Microsoft Rights Management Connector Setup Wizard), 160
- Microsoft Threat Modeling Tool, 14
- mobile device inventory management, 91–92
- Mobile Device Inventory Reports (Microsoft Intune), 177
- Mobile Device Management authority (MDM authority)
 - Microsoft Intune service configuration, 97
 - preparing Microsoft Intune service for enrollment, 105–106
- Mobile Device Management (MDM), 10
 - device enrollment, 76–77, 102–105
 - iOS devices, 103
 - name resolution, 104–105
 - Windows Phone 8.0, 104
 - as part of the solution to device management, 97
 - understanding EMS solution, 20–21
 - MDM authority
 - Microsoft Intune service configuration, 97
 - preparing Microsoft Intune service for enrollment, 105–106
- Mobile Device Security Policy
 - configuring, 85
 - deployment, 108
 - settings, 100
- mobile worker (user profile), 9
- mobile workforces
 - embracing enterprise mobility scenarios, 24–26
 - enabling, 1
 - BYOD (Bring Your Own Devices) scenarios, 4–7
 - challenges, 2–4
 - design strategies, 9–15
 - shift towards mobility, 1–2
- monitoring
 - access to resources, 145–147
 - devices
 - continuous monitoring and incident response, 169–170
 - incidence response plans, 170–171
 - leveraging EMS to monitor resources, 171–180
 - leveraging EMS to respond to a security incident, 180–186
- Multi-Factor Authentication app, 31
- multi-factor authentication (MFA), 30–31
- multiforest directory sync with SSO scenario (directory integration), 41

MyDevices section, Company Portal, 81

N

- name resolution
 - configuring, 63–64, 79
 - Windows devices, 104–105
- Network Monitor, 190
- New Sync Share Wizard, 167–168
- Noncompliance Apps Reports (Microsoft Intune), 177

O

- OMA-URI (Open Mobile Alliance Uniform Resource Identifier) policies, Windows devices, 87
- Online Connector for Online Exchange (Microsoft Intune), 111–112
- on-premises environment
 - directory integration with Azure AD, 35–47
 - AD FS, 38–39
 - integration scenarios, 39–41
 - source of authority, 36
 - synchronization tools, 41–47
 - leveraging resources for data protection, 127–135
 - Web Application Proxy, 130–131
 - Windows Server Dynamic Access Control, 128
 - Work Folders, 131–135
 - planning/designing hybrid identity solution, 53–60
 - Microsoft Azure Access Panel, 52–53
 - Microsoft Azure Management Portal, 51–52
 - on-premises environment, 53–54
 - SSO (Single Sign-On) components, 54–60
 - preparing for directory integration, 61–64
 - publishing apps, 130–131
 - syncing AD with Azure AD to enable SSO, 39
- Open Mobile Alliance Uniform Resource Identifier (OMA-URI) policies, Windows devices, 87
- Optional Features page, Microsoft Azure Active Directory Sync Services Wizard, 44
- organization units (OUs), configuring users/groups for synchronization, 62–63
- OUs (organization units), configuring users/groups for synchronization, 62–63

P

- Password Reset Activity report (Azure AD), 174
- password reset registration activity logs/reports, 30, 174
- Password Synchronization (optional feature, Azure AD Sync), 44
- Password Write-Back (optional feature, Azure AD Sync), 44
- passwords
 - password sync, 40
 - reset activity log, 30
 - self-service management, 34–35
- perimeter network
 - data access and protection diagram, 150
 - solution diagram for hybrid identity, 50
- permissions, conditional expressions and, 129
- persona distribution, 10–11
- PFILE format, 140
- pfile (protected file) encapsulation, 136
- PhoneFactor, 31
- planning
 - data protection solution, 151–153
 - leveraging Azure RMS, 151
 - preparing the environment, 151–153
 - device management solution, 97–105
 - Microsoft Intune service configuration, 97–99
 - Mobile Device Management enrollment, 102–105
 - policies, 100–102
 - hybrid identity solution, 51
 - Microsoft Azure Access Panel, 52–53
 - Microsoft Azure Management Portal, 51–52
 - on-premises environment, 53–54
 - SSO (Single Sign-On) components, 54–60
- plan of action, troubleshooting EMS, 189
- PL (Publishing License), 140
- policies
 - creating Enterprise Mobility Strategy, 6–7
 - deployment (device management), 83–91
 - compliance policies, 88
 - conditional access policies, 88–90
 - configuration policies, 84–88
 - Exchange ActiveSync policies, 90
 - policy conflicts, 90–91
 - Mobile Device Security Policy, 108
 - planning/designing device management solution, 100–102
 - compliance policies, 101–102
 - conditional access policies, 102
 - configuration policies, 100–101
- Policy workspace, Admin Console, 84
- Prerequisites, device management, 78–79
- prevention
 - security incidents, 181
 - security phase, 170
- profiles
 - device enrollment, 80, 98
 - users, 9
- protected file (pfile) encapsulation, 136
- protection of data
 - Azure RMS, 135–147
 - choosing right deployment topology, 141–143
 - how Azure RMS works, 137–140
 - monitoring access to resources, 145–147
 - RMS connector, 143–145
 - challenges of enabling enterprise mobility, 2–4
 - design strategies for mobile workforces, 13–14
 - implementation
 - Azure RMS connector, 159–168
 - configuring Azure RMS templates, 153–159
 - goals, 149–150
 - planning/designing solution, 151–153
 - leveraging on-premises resources, 127–135
 - Web Application Proxy, 130–131
 - Windows Server Dynamic Access Control, 128–129
 - Work Folders, 131–135
 - understanding EMS solution, 21–23
- PTXT extensions, 136
- public domains, 60–62
- publicly trusted X509 v3 SSL certificates, 56
- Publishing License (PL), 140
- publishing on-premises apps, 130–131

Q

- quickconfig command (WinRM), 192–193

R

- reaction
 - security incidents, 183–186
 - security phase, 170

- Reactivate button, turning on directory synchronization, 38
- Ready To Install Microsoft Rights Management Connector page (Microsoft Rights Management Connector Setup Wizard), 160
- registration, devices, 131
- Registry Editor, 158
- remote information worker (user profile), 9
- reports
 - Azure AD Premium, 173, 182-183
 - Microsoft Intune monitoring, 176-179
- Require Device Encryption policy, Exchange ActiveSync Mailbox Policies users, 135
- Retire Device confirmation dialog box, 93
- Return of Investment (ROI), 1
- Review Options page (Azure AD Connect Wizard), 67
- Rights Management Services. *See* Azure RMS; RMS
- Rights Management Sharing App, 140
- rights-protected documents, 139-140
- risk mitigation
 - design strategies for mobile workforces, 14-15
 - understanding EMS solution, 22-23
- RMS (Azure Rights Management Services), 135-147
 - configuring templates, 153-159
 - connector, 159-168, 201-203
 - data protection, 135-147
 - choosing right deployment topology, 141-143
 - how Azure RMS works, 137-140
 - monitoring access to resources, 145-147
 - RMS connector, 143-145
 - templates, 135
 - integrating DAC feature, 133-134
 - integration with Work Folders, 166-168
 - leveraging for data protection, 151
 - monitoring capabilities, 179-180
 - troubleshooting EMS, 199-203
- ROI (Return of Investment), 1
- running reports, Azure AD Premium Reports, 28

S

- SaaS (Software-as-a-Service) applications, user access, 32-33
- scenarios, directory integration, 39-41
 - directory sync, 40
 - directory sync with password sync, 40

- directory sync with SSO, 40
- multiforest directory sync with SSO, 41
- SCEP (System Center 2012 Configuration Manager and Endpoint Protection), 77
- scope of integration, planning/designing hybrid identity solution, 54
- security
 - certificates, 56-57
 - data protection
 - Azure RMS, 135-147
 - Azure RMS connector, 159-168
 - configuring Azure RMS templates, 153-159
 - goals, 149-150
 - leveraging on-premises resources, 127-135
 - planning/designing solution, 151-153
 - leveraging EMS response, 180-186
 - detection, 181-183
 - prevention, 181
 - reaction, 183-186
 - monitoring devices
 - continuous monitoring and incident response, 169-170
 - incidence response plans, 170-171
 - leveraging EMS to monitor resources, 171-180
 - leveraging EMS to respond to a security incident, 180-186
 - reports, Azure AD Premium, 28-30
- security identifiers (SIDs), 129
- Select Containers dialog box (Synchronization Service Manager), 69
- selective wipes, 92-93
- Select Users And Groups page, creating custom templates, 155
- Select Your Solution page (Azure AD Connect Wizard), 65
- self-service features, Azure Access Panel, 32-35
 - group management, 33-34
 - password management, 34-35
 - SaaS applications, 32-33
- Server Licensor Certificates (SLCs), 140
- service configuration, Microsoft Intune, 97-99
 - Company Portal customization, 98-99
 - device enrollment profiles, 98
 - Mobile Device Management authority, 97
 - terms and conditions, 99
- Service Level Agreements (SLAs), 12
- service-to-service connector, Microsoft Intune, 89

- Set-AdfsGlobalWebContent cmdlet, 72
- Set-AdfsWebTheme cmdlet, 72
- settings, Mobile Device Security Policy, 85, 100
- Set Up Service To Service Connector dialog box, 111
- shift towards mobile workforces, 1–2
- sideloading, 78
- SIDs (security identifiers), 129
- sign-in behaviors, anomalous activity reports, 29
- Sign Ins After Multiple Failures report (Azure AD), 182
- Sign Ins From IP addresses With Suspicious Activity report (Azure AD), 173
- Sign Ins From Multiple Geographies report (Azure AD), 183
- Sign Ins From Possibly Infected Devices report (Azure AD), 173
- Single Sign-On (SSO), 33
 - adding organization's public domain, 39
 - enabling, 64–70
 - configuring synchronization filtering, 68–69
 - forcing directory synchronization and verifying success, 69–70
 - planning/designing hybrid identity solution, 54–60
 - AD FS, 55
 - AD FS sign-in page, 56
 - Azure AD Connect, 57–58
 - security certificates, 56–57
 - Web Application Proxy, 55–56
- SLAs (Service Level Agreements), 12
- SLCs (Server Licensor Certificates), 140
- Software-as-a-Service (SaaS) applications, user access, 32–33
- solution diagram
 - hybrid identity implementation, 50–51
 - device management implementation, 96–97
- source of authority, directory integration, 36
- Specify Domain For Federation page (Azure AD Connect Wizard), 67
- Specify Federation Server Credentials page (Azure AD Connect Wizard), 66
- Specify Federation Service Account page (Azure AD Connect Wizard), 66
- SSO (Single Sign-On), 33
 - adding organization's public domain, 39
 - enabling, 64–70
 - configuring synchronization filtering, 68–69
 - forcing directory synchronization and verifying success, 69–70
 - planning/designing hybrid identity solution, 54–60

- AD FS, 55
 - AD FS sign-in page, 56
 - Azure AD Connect, 57–58
 - security certificates, 56–57
 - Web Application Proxy, 55–56
- strategies, design strategies for mobile workforces, 9–15
 - apps, 12–13
 - data protection, 13–14
 - devices, 10–12
 - threat mitigation, 14–15
 - users, 9–10
- supportability (devices), 12
- support contact information, customizing Company Portal, 98
- Symantec, code-signing certificates, 78
- synchronization
 - configuring filtering, 68–69
 - configuration policies, 101
 - directory integration, 36–38
 - Azure AD Connect, 45–47
 - Azure AD Sync, 43–45
 - DirSync, 41–43
- Synchronization Service Manager, 69
- System Center 2012 Configuration Manager and Endpoint Protection (SCEP), 77
- System Center Configuration Manager 2012, 77

T

- Task Scheduler Library, Azure AD Sync Scheduler task, 69
- technical worker (user profile), 9
- Template Distribution Web Service, 200
- templates, configuring, 153–159
- tenant key topology, Azure RMS, 141
- terms and conditions
 - customizing Company Portal, 83–84, 108
 - Microsoft Intune service configuration, 99
- Terms and Conditions Reports
 - Company Portal, 83
 - Microsoft Intune, 177
- Third Era of Enterprise IT, 1
- threat mitigation
 - design strategies for mobile workforces, 14–15
 - understanding EMS solution, 22–23
- Threat Modeling Tool, 14

tools

- directory synchronization, 41–47
 - Azure AD Connect, 45–47
 - Azure AD Sync, 43–45
 - DirSync, 41–43

troubleshooting EMS, 190

troubleshooting EMS

Azure AD Premium, 191–194

Azure RMS, 199–203

cloud services, 191

methodology, 187–190

Microsoft Intune, 194–198

tools, 190

where to find information, 190

two-factor authentication, 30–31

U

Update Reports (Microsoft Intune), 176

Update-WebApplicationProxyDeviceRegistration
cmdlet, 131

Upload The APNs Certificate dialog box, 112

UPNs (User Principal Names), 39

- planning/designing hybrid identity solution, 53–54
- suffixes, 54, 62

usage terms and conditions, customizing Company
Portal, 108

user access

disabling, 184

SaaS (Software-as-a-Service) applications, 32–33

user-owned devices, 7–8

User Principal Names (UPNs), 39

- planning/designing hybrid identity solution, 53–54
- suffixes, 54, 62

user profiles, 9

users

- Azure Access Panel self-services, 32–35
- challenges of enabling enterprise mobility, 2–4
- configuring for synchronization, 62–63
- data access and protection diagram, 150
- design strategies for mobile workforces, 9–10
- solution diagram for hybrid identity, 50

Users With Anomalous Sign In Activity report (Azure
AD), 174, 182

V

validation

client access, 166

results, troubleshooting EMS, 189

vendor-agnostic approach to BYOD, 4

verifying public domains, 60–61

viewing Azure AD Premium reports, 28

View Policy Issues dialog box, 88

VLSC (Volume Licensing Service Center), 78

Volume Licensing Service Center (VLSC), 78

W

Warning dialog box, 116

Web Application Proxy

leveraging for data protection, 130–131

planning/designing hybrid identity solution, 55–56

Welcome page

Azure AD Sync, 43

DirSync, 41–42

Windows 8.1 computers, enrollment, 123–125

Windows devices

configuration policies, 86

deploying email profile configuration policies, 109

device management prerequisites, 79

enrollment, 120–125

external device enrollment dependencies, 113

name resolution, 104–105

Windows Phone 8.0

device management prerequisites, 79

enrollment, 120–121

external device enrollment dependencies, 113–114

Mobile Device Management enrollment

considerations, 104

Windows Phone 8.0, enrollment, 121–123

Windows Phone OMA-URI (Open Mobile Alliance

Uniform Resource Identifier) policies, 87

Windows Phone Open Mobile Alliance Uniform

Resource Identifier (OMA-URI) policies, 87

Windows Phone security model, AppContainer, 13

Windows Remote Management (WinRM) functionality,
191

Windows Server Dynamic Access Control, 128–129

WinRM (Windows Remote Management) functionality,
191

wiping compromised devices, 186

wizards

- Add Software wizard, 113

- Azure AD Connect Wizard, 46, 57

 - enabling SSO (Single Sign-On), 64–70

 - Getting Started page, 46

 - planning/designing hybrid identity solution,
57–58

 - troubleshooting Azure AD Premium, 191–192

- Azure Active Directory Sync Services Wizard, 43

- Microsoft Intune Setup Wizard, 124–125

- Microsoft Rights Management Connector Setup
Wizard, 159–160

- New Sync Share Wizard, 167–168

Work Folders

- data protection at user device location, 131–135

- integration with Azure RMS, 166–168

WS-Management protocol, 192

X

X509 v3 SSL certificates, 56

Y

Your Template Has Been Added Quick Start page,
creating custom templates, 155

This page intentionally left blank

About the authors



YURI DIOGENES is a Senior Content Developer on Microsoft's CSI Enterprise Mobility Team and has more than 20 years of experience in the IT field. He holds a Master of Science degree in Cybersecurity Intelligence and Forensics Investigation (Utica College) and has been working for Microsoft for the past nine years, including five years as a Senior Support Escalation Engineer on the CSS Forefront Edge Team. Yuri also holds an MBA and several industry certifications, including MCSE, MCTS, CISSP, E|CEH, E|CSA, Security+, Cloud Essentials Certified, Mobility+, Network+, Cloud+, and CASP. You can follow Yuri on Twitter *@yuridiogenes* or read his articles on his personal blog at *<http://aka.ms/yuridio>*.



JEFF GILBERT is a Senior Solutions Content Developer for the Cloud & Enterprise Division at Microsoft. From his office outside Boston, he authors cross-product solutions to IT business problems involving enterprise client management technologies, including Microsoft System Center Configuration Manager, Microsoft Intune, and Microsoft Desktop Optimization Pack (MDOP) products. In addition to local user groups, Jeff has been a speaker on enterprise client management and MDOP technologies at several conferences over the years, including the Microsoft Management Summit (MMS) and TechEd. Previous to this role, 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 2.0/SMS 2003 administrator with the US Army. You can follow Jeff on Twitter *@jeffgilb*.