

Kerrie Meyler
Jason Sandys
Greg Ramsey

Foreword by Wally Mead



Powered by

CLEARPointe

System Center 2012 R2 Configuration Manager

UNLEASHED

Supplement to
System Center
2012 Configuration
Manager (SCCM)
Unleashed

SAMS

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Kerrie Meyler

Jason Sandys

Greg Ramsey

with

Dan Andersen

Panu Saukko

Kenneth van Surksum

Michael Wiles

System Center 2012 R2 Configuration Manager

Supplement to System Center 2012
Configuration Manager (SCCM)

UNLEASHED



800 East 96th Street, Indianapolis, Indiana 46240 USA

System Center 2012 R2 Configuration Manager Unleashed

Copyright © 2015 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-672-33715-4

ISBN-10: 0-672-33715-0

Library of Congress Control Number: 2014943440

Printed in the United States of America

First Printing: September 2014

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Sams Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact international@pearsoned.com.

Editor-in-Chief

Greg Wiegand

Acquisitions Editor

Joan Murray

Development Editor

Keith Cline

Managing Editor

Kristy Hart

Senior Project Editor

Lori Lyons

Copy Editor

Keith Cline

Indexer

Erika Millen

Proofreader

Kathy Ruiz

Technical Editor

Steve Rachui

Editorial Assvistant

Cindy Teeters

Cover Designer

Mark Shirar

Compositor

Nonie Ratcliff

Contents at a Glance

Foreword	x
Introduction	1
Part I Overview	
1 People-Centric IT	5
2 What's Changed Since Configuration Manager 2012 RTM	19
Part II Deep Dive	
3 User Data and Profiles	61
4 New Application Deployment Types	77
5 On-Premise Cross-Platform Support	117
6 What's New in Operating System Deployment	147
Part III Journey to the Cloud	
7 Using the Intune Connector	199
8 Mobile Device Management in Configuration Manager 2012 R2	243
Part IV Appendixes	
A About Windows Intune	297
B Reference URLs	315
C Available Online	335
Index	337

Contents

Foreword	x
Introduction	1
Part I Overview	
1 People-Centric IT	5
Microsoft's People-Centric IT Philosophy	6
Enabling Users for People-Centric IT	7
Unifying Your Environment for People-Centric IT	8
Protecting Your Data in a People-Centric IT World	9
People-Centric IT and ConfigMgr 2012 R2 with Windows Intune	9
Enabling Users with ConfigMgr 2012 R2 and Windows Intune	10
Unifying Your Environment with ConfigMgr 2012 R2 and Windows Intune	12
Protecting Your Data with ConfigMgr 2012 R2 and Windows Intune	13
People-Centric IT and Windows Server 2012 R2	14
Enabling Users with Windows Server 2012 R2	14
Unifying Your Environment with Windows Server 2012 R2	16
Protecting Your Data with Windows Server 2012 R2	16
People-Centric IT and Microsoft Azure Active Directory	17
Summary	18
2 What's Changed Since Configuration Manager 2012 RTM	19
Administration Changes	19
Configuring Database Replication	20
Configuring Internet Proxy Server on Each Site System	24
Windows Intune Integration and Extensions for Windows Intune	25
Software Update Points	25
Certificate Profiles	27
Client Settings	27
Security	28
Distribution Points (DPs)	28
Automatic Client Upgrade	31
Network Access Accounts	32
PowerShell Support	32

Assets and Compliance	34
Collections	34
Compliance Settings	37
Software Library	38
Application Management	38
Software Updates	39
Operating System Deployment	41
Monitoring Changes	42
Alerts	43
Reporting	43
Distribution Status	43
Deployment Status	44
Client Operations	44
Other Improvements	44
Setup and Recovery	45
Client and Client Experience	48
Summary	58

Part II Deep Dive

3 User Data and Profiles	61
User Data and Profiles Overview	61
User Data and Profiles Prerequisites	62
Configuring User Data and Profiles	64
Using Folder Redirection	64
Using Offline Files	67
Using Roaming User Profiles	70
Roaming Profiles, Folder Redirection, and Offline Files in a Mash-Up	74
Deploying User Data and Profiles Configuration Items	75
Reporting User Data and Profiles Compliance	76
Summary	76
4 New Application Deployment Types	77
Application Overview	77
Definition of an Application	77
Defining Deployment Types	78
What's New for Applications Since ConfigMgr 2012 RTM	78
Support for Write Filters in Windows Embedded	79
Working with Virtual Applications	81
Creating a Microsoft Application Virtualization 5 Deployment Type	82

Using App-V Virtual Environments	83
Creating an App-V Virtual Environment	84
Deploying Applications to Mobile Devices	85
Creating Application Store Deployment Types	86
Sideloaded Applications	93
Using VPN Profiles in Your Applications	104
Deploying Software to OS X, Linux, and UNIX Platforms	105
Deploying Applications to Apple OS X Computers	105
Deploying Software to Linux and UNIX	108
Deploying Web Applications	111
Best Practices for Working with Applications	112
Best Practices for Installing Software	112
Best Practices for Working with Applications in Task Sequences	115
Summary	116
5 On-Premise Cross-Platform Support	117
Supported Platforms	117
Cross-Platform Agent Architecture	119
Cross-Platform Agent Communication	120
Client Agent Settings	120
Cross-Platform Settings	121
Linux/UNIX Requirements	121
OS X Requirements	121
Firewall Ports	125
Downloading Client Agents	126
Cross-Platform Agent Deployment	126
Deploying the Linux/UNIX Client	127
Deploying the OS X Client	129
Uninstalling or Reinstalling Linux/UNIX	132
Uninstalling OS X	134
Cross-Platform Agent Components	134
Settings Management	134
Software Inventory	135
Hardware Inventory	136
Client Agent Commands	143
Troubleshooting with Log Files	143
Linux/UNIX Log Files	143
Verbose Logs	144
OS X Log Files	144
Summary	145

6	What's New in Operating System Deployment	147
	The Alphabet Soup of Prerequisites	148
	Operating System Version Support	149
	Boot Images	151
	Windows Setup Support Change	155
	Deployment Control	160
	Deployment Monitoring	164
	New Task Types	166
	New Built-In Task Sequence Variables	175
	UEFI Support	176
	Virtual Hard Disks and Windows To Go	180
	Deploying to and Maintaining VHDs	180
	Deploying WTG Media	183
	Other Improvements	185
	Offline Servicing	185
	Driver Package Export and Import	186
	Unknown Computer Cleanup	187
	Prestaged Media	188
	Content Prestaging	189
	Task Sequence Size Ceiling	190
	Troubleshooting Hints and Tips	190
	Reviewing SMSTS.log	191
	Using SMSPXE.log	191
	SMSTSErrorDialogTimeout	192
	Power Scheme	193
	Pausing a Task Sequence	193
	Windows 8.1 Wireless Network Prompt	195
	Summary	196
Part III	Journey to the Cloud	
7	Using the Intune Connector	199
	Getting Started with the Intune Connector	199
	Synchronizing AD with Microsoft Azure AD	200
	Creating a Windows Intune Instance and Azure	
	AD Namespace	200
	Installing the Directory Synchronization Tool	204
	MDM Prerequisites	209
	Managing Windows 8.1 Devices	210
	Managing Windows Phone 8.x Devices	212
	Managing iOS Devices	215

Installing the Windows Intune Subscription and Connector	220
Creating the Intune Subscription	220
Adding the Windows Intune Connector Site System Role	231
Confirming the Installation of the Subscription and Connector Role	232
Removing or Overriding an Existing Intune Subscription	236
Receiving Feature Updates Using the Extensions for Windows Intune	238
Summary	241
8 Mobile Device Management in Configuration Manager 2012 R2	243
Understanding Mobile Device Management Challenges	244
Prerequisites of Mobile Device Management	246
Enrolling Mobile Devices	248
Enrolling Windows Phone 8 Devices	249
Enrolling Windows 8.1 Devices	251
Enrolling iOS Devices	252
Enrolling Android Devices	254
Inventorying Mobile Devices	254
Available Discovery and Inventory Data	255
Personal Versus Company-Owned Devices	259
Managing Mobile Device Settings	259
Configuration Items for Mobile Devices	260
Creating Custom Configuration Items for Mobile Devices	267
Remote Connection Profiles	267
Company Resource Access	271
Deploying Applications to Mobile Devices	281
Defining Application Information	282
Using the Company Portal	285
Retiring/Wiping Mobile Devices	288
Troubleshooting	290
Log Files on Site Server	291
Log File on iOS Devices	291
Log File on Windows Phone 8.x Devices	291
Log File on Android Devices	291
Troubleshooting Windows 8.1 OMA-DM Devices	293
Summary	293

Part IV Appendixes

A About Windows Intune	297
Introduction to Windows Intune	297
Intune Comes Into Focus	298
Microsoft Strategic Direction Announcement	299
Mobile Device Management Features	300
Device Management	301
Device Inventory	301
Policy Settings Management	303
Application Distribution and the Windows Intune Company Portal	303
Device Retirement and Remote Wipe	310
Windows Intune Licensing and Supported Architectures	311
Unified Architecture	311
Cloud-Only Architecture	312
The Windows Intune Connector and Subscription	314
B Reference URLs	315
General Resources	315
Microsoft's Configuration Manager Resources	322
Other Configuration Manager Resources	327
Blogs	331
Public Forums	332
Utilities	333
C Available Online	335
Setting SMSTSPreferredAdvertID	335
Creating an OfflineImageServicing Folder	335
Viewing the Current Drive Letter Set	336
Pausing a Task Sequence	336
Live Links	336
Index	337

Foreword

Wow, that didn't take long. Less than two years after System Center 2012 Configuration Manager was released, the Enterprise Client Management team (formerly known as the Configuration Manager product group) released two new versions of the popular software. Service Pack (SP) 1 for Configuration Manager 2012 was released just nine months after the RTM version was released. The service pack added a number of new features to the Configuration Manager 2012 product, such as pull distribution points, the ability to expand a stand-alone primary site into a hierarchy, real-time client actions, support for non-Windows-based clients, as well as the first integration with the cloud-based Windows Intune service for managing mobile devices.

Only nine months after the release of System Center 2012 Configuration Manager SP 1, System Center 2012 R2 Configuration Manager was released. The primary update to the R2 version of Configuration Manager is the updated support for managing mobile devices when integrated with Windows Intune, but many additional features were added as well. In addition to the updated features for mobile device management, a great addition is role-based administration for reports.

As with most of our products, this product has undergone thorough testing—not only by the product group, but also by Microsoft IT, by numerous Technology Adoption Program (TAP) customers testing the beta release in their production environments, by our MVPs (a number of who are authors on this book), and by thousands of open beta customers testing in lab environments. So, we're very confident in the quality of Configuration Manager 2012 R2 and the features that it will provide in your own environments. Thanks to all of you who helped test the beta release and provided feedback to help improve the quality of this and future versions of Configuration Manager.

I want to offer a huge welcome to those of you who are just entering into the Configuration Manager world; it is a great product. If you are still using an earlier version of Configuration Manager, I urge you to give this new version a look. I think you'll find it a great update to what you already have in place today. It is easy to move from Configuration Manager 2007 to the latest release of Configuration Manager 2012. For those who are currently running Configuration Manager 2012, but not the R2 version, you will want to perform your upgrade as soon as you can, as great features await you!

I know all the authors and contributors on this book, and knowing their professionalism and knowledge, I am confident that you will find this book a great value to you in the process of your learning and experiencing System Center 2012 R2 Configuration Manager. The best of luck to you all, and again, thanks for your loyalty and trust in us.

**Wally Mead, (former) Senior Program Manager
Enterprise Client Management Product Group
Microsoft Corporation
Now Principal Program Manager at Cireson**

About the Authors

Kerrie Meyler, System Center MVP, is the lead author of numerous System Center books in the Unleashed series, including *System Center 2012 Configuration Manager Unleashed (2012)*, *System Center Configuration Manager 2007 Unleashed (2009)*, *System Center 2012 Operations Manager Unleashed (2013)*, *System Center 2012 Orchestrator Unleashed (2013)*, and *System Center 2012 Service Manager Unleashed (2014)*. She is an independent consultant with more than 17 years of Information Technology experience. Kerrie was responsible for evangelizing SMS while a Sr. Technology Specialist (TSP) at Microsoft. She was a member of the Management Insiders Group and has presented on System Center technologies at TechEd and MMS.

Jason Sandys, Enterprise and Client Management MVP, is a Technology Evangelist and Principal Consultant for Catapult Systems LLC, with just under 20 years of experience in a wide range of technologies, environments, and industries. He has extensive knowledge about implementing and supporting all things SMS and Configuration Manager beginning with SMS 2.0. He is a coauthor for *System Center Configuration Manager 2012 Unleashed (2012)*, a contributing author to *System Center Configuration Manager 2007 Unleashed (2009)*, and is a frequent presenter at Microsoft TechEd and MMS, as well as various other events and user groups nationwide. Jason blogs at blog.configmgrftw.com and is active in the online support community.

Greg Ramsey, Enterprise and Client Management MVP, is the Enterprise Tools Strategist at Dell, Inc. He has a B.S. in Computer Sciences and Engineering from Ohio State University. Greg coauthored *System Center Configuration Manager 2012 Unleashed (2012)*, *Microsoft System Center 2012 Configuration Manager: Administration Cookbook (Packt, 2012)*, and *System Center Configuration Manager 2007 Unleashed (2009)*. Greg is a cofounder of the Ohio SMS Users Group and the Central Texas Systems Management User Group.

About the Contributors

Dan Andersen, MCSE, MCTS, MCTIP, is a Senior Technology Specialist (TSP) for Windows Intune at Microsoft, where he has worked since 2001. He, along with his team, provides cloud-only and ConfigMgr-integrated Intune technical solutions for large-scale enterprise customers and partner technical development. Dan has held various technical subject matter expert roles at Microsoft and previously was a Management TSP where he helped to architect System Center solutions around configuration and operations management. He was a member of the Management Insiders Group and continues to be a regular speaker at Microsoft conferences and local user group meetings.

Panu Saukko, Enterprise Client Management MVP and MCT, is a consultant and trainer at ProTrainIT and is based in Finland. With more than 20 years of experience working with Microsoft technologies, Panu has been a MVP since 2003. Panu has worked with SMS and Configuration Manager beginning with SMS 1.2 and has created training courseware for multiple Microsoft products over the years. He frequently speaks at different seminars.

Kenneth van Surksun, MCT, is a trainer and System Center consultant at insight24, a company based in the Netherlands. With more than 10 years of experience, Kenneth has worked with SMS 1.2 and successive versions of the product and specializes in OS deployment. Kenneth was a contributing author to *System Center 2012 Configuration Manager Unleashed (2012)* and *System Center 2012 Service Manager Unleashed (2014)*, and coauthored *Mastering Windows 7 Deployment (Sybex, 2011)*. He blogs at <http://www.vansurksun.com> and is chief editor for several websites about virtualization and cloud computing, including <http://www.virtualization.info> and <http://www.cloudcomputing.info>.

Michael Wiles began working with SMS 1.1 as a Microsoft support engineer in 1997 and was a Senior Premier Field Engineer (PFE) from 2005 to 2012. As a PFE, Michael worked with several large customers and the Configuration Manager Product Group through the TAP program to affect changes within the product. He now works for Dell, Inc., as a Configuration Manager Senior Advisor, leading the infrastructure team in Dell Services and servicing as an escalation point of any and all Configuration Manager-related issues within Dell.

Dedication

*To Wally, Microsoft's guiding force for Configuration Manager
to the community for so many years.*

Acknowledgments

Writing a book is an all-encompassing and time-consuming project, and this book certainly meets that description. Configuration Manager is a massive topic, and this book benefited from the input of many individuals. The authors and contributors would like to offer their sincere appreciation to all those who helped with *System Center 2012 R2 Configuration Manager Unleashed*. This includes John Joyner and Bob Longo of ClearPointe Technologies for dedicating lab resources, Wally Mead, and Steve Rachui.

We would also like to thank our spouses and significant others for their patience and understanding during the many hours spent on this book.

Thanks also go to the staff at Pearson; in particular, to Joan Murray and Neil Rowe.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: consumer@samspublishing.com

Mail: Sams Publishing
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at informit.com/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

As Wally Mead says in his Foreword, things have certainly moved quickly since Microsoft's 2012 release of System Center 2012 Configuration Manager! *System Center 2012 Configuration Manager Unleashed* (Sams, 2012) was completed shortly after Microsoft released Configuration Manager (ConfigMgr) 2012 to production; the company then released a service pack and R2 within a mere 18 months.

The fast and furious pace of releases to ConfigMgr 2012 has prompted the authors to write this supplement to bring you up to date on what has changed since its initial release and the publication of *System Center 2012 Configuration Manager Unleashed*. By definition of a *supplement*, this work does not cover material in the previous book; it delivers more than 300 pages of material discussing what has changed with Configuration Manager 2012 Service Pack 1 and R2.

Configuration Manager 2012 is most noteworthy in its orientation toward the user, not the device. Applications can now be distributed to users, empowering them to use the devices and applications they need, while maintaining the corporate compliance and control your organization requires. This layer of abstraction lets Configuration Manager assist in enabling your users to be productive with a unified infrastructure that delivers and manages user experiences across corporate and consumer devices. The timing of Microsoft's orientation toward the user is most appropriate, as the past few years have seen the need for Information Technology (IT) departments to become increasingly people centric. The explosion in mobile devices has led to many of the enhancements in ConfigMgr 2012 Service Pack 1 and R2, including its integration with Microsoft Intune. Yet, while mobile device management and Intune may be what first comes to mind when thinking about what's new, it's not to say that these are the only updates to Configuration Manager 2012. Support for cross-platform devices and enhancements to user and data profiles, application management, and OSD are also in Microsoft's bag of goodies, along with a number of performance enhancements, usability enhancements, and other updates covered throughout this book:

- ▶ The consumerization of IT and onset of people-centric IT means that the world is changing for system and ConfigMgr administrators—whether we like it or not. Chapter 1 introduces this new paradigm and Microsoft's mantra of *any user, any device, anywhere*. With the releases of Windows 8.1, Windows Server 2012 R2, Windows Intune, and System Center 2012 R2, Microsoft is helping IT enable users to be productive no matter where they are or what device they are using. Chapter 2 highlights the many enhancements in Service Pack 1 and R2.

- ▶ The next several chapters can be considered a deep dive into user and data profiles (Chapter 3), changes in application management (Chapter 4), on-premise management and cross-platform support (Chapter 5), and what's new in OSD (Chapter 6).
- ▶ Chapter 7 and Chapter 8 take you on Microsoft's journey to the cloud with Configuration Manager and Windows Intune, discussing the Intune connector and mobile device management (MDM) in ConfigMgr 2012 R2. Given the ongoing plethora of mobile devices and nonstop enhancements to Windows Intune, the authors plan to document updates to MDM in as timely a manner as possible by publishing content on the InformIT page for this book.
- ▶ Appendixes include a Windows Intune primer, a listing of web URLs discussing Configuration Manager, and add-on value through online content of scripts and live links in this book.

Disclaimers and Fine Print

As always, there are several disclaimers. The information provided is probably outdated the moment the book goes to print. A particular challenge when discussing Configuration Manager has been writing about mobile device management and Windows Intune, which seem to have updates faster than they can be written about.

In addition, the moment Microsoft considers code development on any product complete, they begin working on a service pack or future release. As the authors continue to work with the product, it is likely yet another one or two wrinkles will be discovered! The authors and contributors of *System Center 2012 R2 Configuration Manager Unleashed* have made every attempt to present information that is accurate and current as known at the time. Updates and corrections will be provided on the InformIT website. Look in particular for updates on InformIT regarding new functionality in MDM and Intune at <http://www.informit.com/store/system-center-2012-r2-configuration-manager-unleashed-9780672337154>.

Thank you for purchasing *System Center 2012 R2 Configuration Manager Unleashed*. The authors hope it is worth your while.

This page intentionally left blank

APPENDIX A

About Windows Intune

By now, you may have heard the terms *consumerization of Information Technology (IT)* and *bring your own device* (BYOD, which is where devices are purchased by users and used at work) and understand that there are productivity benefits to supporting this new style of work. The IT department has to manage those devices, almost all of which are mobile devices, in a way that still meets IT security and compliance requirements. This appendix explains the genesis of Windows Intune, its history, licensing, and architecture for integrating with System Center 2012 R2 Configuration Manager to deliver a unified mobile device management solution.

Introduction to Windows Intune

Consumerization of IT makes it necessary to incorporate user and mobile device management as part of the IT experience, something with which Configuration Manager (ConfigMgr) and Systems Management Server (SMS) have historically struggled. Users have an unprecedented amount of consumer devices at home, which leads to higher expectations of technology usage at work. This increased pressure on IT to allow these devices to access corporate apps and data, and forced them to purchase multiple products to manage and secure them as ConfigMgr 2007/2012 lacked the functionality. However, it wasn't enough to add mobile device support in Configuration Manager (remember ConfigMgr already supported legacy devices such as Windows Mobile and Exchange ActiveSync devices with the Exchange connector). Microsoft also needed new agility to react quickly to industry trends and new mobile device features that enter the market. This is where Windows Intune comes in.

IN THIS APPENDIX

- ▶ Introduction to Windows Intune
- ▶ Mobile Device Management Features
- ▶ Windows Intune Licensing and Supported Architectures
- ▶ The Windows Intune Connector and Subscription

Intune Comes Into Focus

What exactly is Intune? Windows Intune, billed as Microsoft's first cloud-based PC management solution, released to market in April 2011. In seeing that Configuration Manager was not penetrating the SMB (small medium business) market as well as it would have liked, Microsoft was interested in offering an alternative lightweight solution for customers. Data from that market segment showed customers were concerned with the amount of infrastructure needed to support ConfigMgr and the steep learning curve associated with the product. Their preference was PC management functionality delivered via the cloud. Through Intune and the licensing for Windows Client Software Assurance (SA), Microsoft offered SMB customers a current desktop experience (Windows 7) and the ability to manage their PCs from the cloud. This became the basis for the initial vision of Intune for customers:

- ▶ **Stay current:** Upgrade rights to Windows 7
- ▶ **Easy to use:** Cloud-based infrastructure and fast deployment
- ▶ **Smart parity:** Deliver core management features not duplicating ConfigMgr
- ▶ **Rapid release:** Deliver new features and updates every 6 months

After the product's second release in October 2011, Microsoft saw opportunities emerging for adoption by larger customer installations. While the SMB market adopted Intune well, other customer segments representing larger customers were just starting their evaluations. Intune had technical limitations that posed challenges for larger enterprise customers, as it leveraged Windows Live IDs for administrative accounts, which most customers viewed as a consumer-rated service rather than a corporate one. Intune also had scalability limitations governing the number of PCs that could be managed in a single Intune cloud instance. To expand the appeal and reach of the product, Microsoft decided in the third release to align Intune with Microsoft Online Services, the commercial offering including products such as Office 365 and Microsoft Dynamics. This changed the back-end account directory from Windows Live ID to Windows Azure Active Directory (formerly called Microsoft Online Directory Service). Azure Active Directory (AD) specifications and requirements for use with ConfigMgr and Intune are explored in depth in Chapter 7, "Using the Intune Connector."

In addition to the change to Azure AD, the third release of Windows Intune (June 2012) included the following features:

- ▶ **Antimalware:** Windows Intune Endpoint Protection based on Forefront Endpoint Protection 2010 and leveraging the same scan engine as System Center Endpoint Protection
- ▶ **Software updates:** Capable of delivering both operating system (OS) and third-party updates
- ▶ **Software distribution:** .MSI/.EXE based packages with content residing in Azure blob storage encrypted and compressed

- ▶ **Proactive monitoring:** Operating system and application monitoring leveraging System Center Operations Manager 2007 R2
- ▶ **Inventory:** Hardware and software inventory
- ▶ **Monitor and track licenses:** Upload or search for Microsoft Volume Licensing details and the ability to add third-party license information
- ▶ **Reporting:** Software updates, inventory, and license reports
- ▶ **Policy management:** Security policies to control configuration of the Intune agent and security configurations
- ▶ **End user self-service portal:** New user accounts available for self-service application provisioning and PC enrollment
- ▶ **Mobile device management and application delivery:** Supported applications delivery to Android and iOS devices and management of Microsoft Exchange ActiveSync policies

The final bullet, “Mobile device management and application delivery,” contained a very significant feature that at the time flew generally under the radar. Intune was the first Microsoft product that could now perform application deployment to modern smart-phone platforms. This was the beginning of an important shift of focus for the product.

Microsoft Strategic Direction Announcement

Following Intune’s third release, customers noticed its ability to deliver applications to Android and iOS devices, something not included within System Center 2012 Configuration Manager. This prompted customers to question the direction of both products and what Microsoft’s roadmap would be to support the next generation of “smart” devices: mobile phones and tablets. According to a recent IDC study, worldwide total unit shipments for smart connected devices, projected at 1.2B in 2012, would grow 16% to over 2B units in 2016.¹ After Intune’s third release, it was unclear to customers which solution to use for their overall management needs. Smaller customers would continue to expect a cloud-delivered solution, while larger enterprise customers wanted to leverage ConfigMgr.

Released to Microsoft’s Server and Cloud blog (<http://blogs.technet.com/b/server-cloud>) in September 2012, the company clarified its management vision by detailing some of the features in the fourth release of Intune (December 2012) and Service Pack (SP) 1 of System Center 2012 Configuration Manager, thus setting the direction for integration between the two products.

¹ IDC Press Release, “IDC Expects Smart Connected Device Shipments to Grow by 14% Annually Through 2016, Led by Tablets and Smartphones,” September 26, 2012

NOTE: STRATEGIC DIRECTION ANNOUNCEMENT

Microsoft is committed to a unified device management solution that combines cloud and on-premise capabilities, creating a premium offering that provides customers with scalability and infrastructure choice for their device management needs.

Unifying the management, security, and compliance of devices, a single infrastructure improves administrative efficiency and reduces the costs of tools and processes to support the organization. By delivering applications using a single application definition with multiple deployment types within ConfigMgr, it becomes easier to manage application lifecycles, and users become more productive as they have greater flexibility to use their choice of device. Microsoft has coined the phrase “Empowering People-centric IT.” Simply put, that meant enabling IT to focus on managing at the user level and delivering applications to users’ devices in a way that is optimized for each device and maximizes user productivity. IT can manage both corporate and personally owned devices with a unified infrastructure, now that all the devices can be seen and managed inside of ConfigMgr.

TIP: PEOPLE-CENTRIC IT

Microsoft now includes people-centric IT (PCIT) as part of their overall cloud OS vision. For more information on PCIT, see <http://www.microsoft.com/en-us/server-cloud/cloud-os/pcit.aspx> and download the PCIT whitepaper.

Mobile Device Management Features

With the December 2012 release of Windows Intune, the fourth release in less than 2 years, Microsoft shifted heavily into mobile device management. By integrating with Configuration Manager 2012 SP 1, organizations could now see mobile devices natively inside of the ConfigMgr console, and not just those devices discovered via the Exchange connector. The key features delivered in Configuration Manager are listed here, followed by an explanation of each feature:

- ▶ Device management
- ▶ Device inventory
- ▶ Policy settings management
- ▶ Application distribution
- ▶ Device retirement and remote wipe

For a detailed explanation of the use of the new features within ConfigMgr 2012 R2, see Chapter 8, “Mobile Device Management in Configuration Manager 2012 R2.”

Device Management

One of the exciting features supported within Intune is the ability to perform direct device management of modern smartphones such as Windows Phone 8 and iOS. This over-the-air enrollment and management process no longer requires the need to use Exchange ActiveSync policies to manage settings on the devices.

The December 2012 release of Intune and the January 2013 release of ConfigMgr 2012 SP 1 accomplished mobile device management by leveraging a management channel that exists within the mobile OS, versus deploying a management agent (app) to the device to perform all the management functions. Therefore Intune did not support Android devices, and only supported Windows 8 RT (RTM). The Android operating system platform did not include the functionality of an embedded management channel to deliver the functionality wanted by Microsoft. For Android policy and settings management, Microsoft still required the use of Exchange ActiveSync (EAS). Configuration Manager administrators could still see Android devices within the console, however it required using the Exchange connector and the Android device must have Exchange ActiveSync configured.

With the release of Configuration Manager 2012 R2, a new version of Windows Intune, and the Windows 8.1 client OS, there are new options available to manage mobile devices. Android 4.x devices and Windows 8.1 (both x86 and ARM) can now be managed directly using the Intune management channel. To manage Android 4.x devices, users would install the new company portal application available for free in the Google Play Store, and enroll their device into Intune with this application. Windows 8.1 builds on the mobile management capabilities first added to Windows 8 RT. Using the embedded MDM agent, based on the Open Mobile Alliance–Device Management (OMA–DM) protocol, Windows 8.1 Intel x86-based machines can now be managed as mobile devices even though they are running a full Windows 8.1 OS. This is critical for Microsoft to expose since many BYOD scenarios include new full OS 8.1 devices. Without this option, companies would have to install the traditional ConfigMgr agent to manage the device. iOS and Windows Phone 8.x also added new enhancements to improve management functionality.

Device Inventory

Windows Intune supports gathering hardware inventory from the mobile device depending on mobile operating system support and settings defined within the ConfigMgr console. For devices that enrolled via Intune, Table A.1 identifies the attributes that are queried for and those devices that return the values.

TABLE A.1 Hardware Inventory Attributes from ConfigMgr R2 and Intune

Hardware Inventory Class	WP8	Windows 8.1	iOS	Android (Using the Company Portal App)
Name	✓	✓	✓	—
Unique Device ID	✓	✓	✓	—
Serial Number	—	—	✓	✓
Email Address	✓	✓	✓	—

Hardware Inventory Class	WPS	Windows 8.1	iOS	Android (Using the Company Portal App)
Operating System Type	✓	✓	—	✓
Operating System Version	✓	✓	✓	✓
Build Version	—	✓	—	—
Service Pack Major Version	—	✓	—	—
Service Pack Minor Version	—	✓	—	—
Operating System Language	✓	—	—	—
Total Storage Space	—	✓	✓	✓
Free Storage Space	—	✓	✓	✓
International Mobile Equipment Identity or IMEI (IMEI)	—	—	✓	✓
Mobile Equipment Identifier (MEID)	—	—	✓	—
Manufacturer	✓	✓	—	✓
Model	✓	✓	✓	✓
Phone Number	—	—	✓	✓
Subscriber Carrier	—	—	✓	✓
Cellular Technology	—	—	✓	✓
Wi-Fi MAC	—	✓	✓	✓

NOTE: HARDWARE INVENTORY

Review <http://technet.microsoft.com/en-us/library/dn469411.aspx> for the latest hardware inventory list from Microsoft. Also note that hardware inventory is controlled through the Client Settings node in the Administration pane of the ConfigMgr console. Not all hardware classes are enabled for mobile devices; you may need to review the settings if you are not receiving the inventory information you expect.

For those devices managed using EAS, the attributes are first returned to Exchange, and then they are placed into the ConfigMgr database if the ConfigMgr Exchange connector is configured. Without installing the Exchange connector role in ConfigMgr, the information only resides within Exchange. Mobile devices that are managed using Windows Intune and EAS would have duplicate information returned to ConfigMgr. In those instances, ConfigMgr merges the two data records together into the device object.

Prior to ConfigMgr 2012 R2, mobile device software inventory was limited to the line-of-business (LOB) applications that were installed on the devices. ConfigMgr could then be used to query and report the users and devices that installed various LOB applications. Windows Intune did not support querying for all the installed software in the

ConfigMgr 2012 SP 1 release. Microsoft added support for full software device inventory in ConfigMgr 2012 R2 by adding a device setting that defines whether the device is company or personal owned. Any mobile device that the ConfigMgr administrator defined as “company-owned” reports full software inventory to the extent that the device platform supports it. Currently, only iOS and Android support a full software inventory, which is returned during the hardware inventory cycle timeframe.

Policy Settings Management

Microsoft’s vision of “people-centric IT” and unifying all device management inside of ConfigMgr is extremely attractive for organizations. A benefit of this approach is seen within mobile device policy settings. ConfigMgr administrators use similar skills and tasks for creating mobile device policies as for creating PC compliance items and baselines. Table A.2 enumerates the mobile device settings provided for unified device management in ConfigMgr 2012 R2.

TIP: COMBINING POLICY SOURCES

Users often configure the ActiveSync client to receive email. In the case where an EAS and ConfigMgr 2012 R2 mobile device policy overlap, the most restrictive policy is enforced.

Expect ConfigMgr to release mobile device features as rapidly as possible, as seen with the February 2014 release of new iOS 7 security and data-retention policies, the new Exchange email profile configuration capability, and the May 2014 Windows Phone 8.1 policies. For the latest policy and feature support list, review <http://technet.microsoft.com/en-us/library/dn376523.aspx>. To support the release of MDM features without requiring large architecture changes and system upgrades, Configuration Manager R2 includes a new node under Cloud Services called Extensions for Windows Intune. Chapter 7 includes additional information on how to receive and enable new MDM feature updates.

Application Distribution and the Windows Intune Company Portal

Windows Intune application distribution for mobile devices is a user-friendly approach to self-service provisioning. In ConfigMgr 2012 R2, Windows Intune added additional application delivery options, building on the SP 1 features, which now support the following:

- ▶ Internal LOB apps written by the company.
- ▶ External public store applications. Also call deep links, these are shortcuts to applications that reside in the public marketplaces of the device platform, such as the Windows Phone Store or Apple App Store.
- ▶ Web links for users to access web-based applications.
- ▶ Device-targeted application “push” deployments.

TABLE A.2 ConfigMgr R2 Unified Device Management Policy Settings

Device Setting Group	Settings	Values	Windows Phone 8.x	Windows 8.1 Enrolled via Intune	iOS	Android (Using the Company Portal App)
Browser	Default browser	Allowed /Prohibited	Windows Phone 8.1 only	—	✓	—
Browser	Autofill	Allowed /Prohibited	—	✓	✓	—
Browser	Plug-ins	Allowed /Prohibited	—	✓	—	—
Browser	Active scripting	Allowed /Prohibited	—	✓	✓	—
Browser	Pop-ups	Allowed /Prohibited	—	✓	✓	—
Browser	Fraud warning	Allowed /Prohibited	—	✓	✓	—
Browser	Cookies	Allowed /Prohibited	—	—	✓	—
Cloud	Encrypted backup	Allowed /Prohibited	—	—	✓	—
Cloud	Document synchronization	Allowed /Prohibited	—	—	✓	—
Cloud	Photo synchronization	Allowed /Prohibited	—	—	✓	—
Cloud	Cloud backup	Allowed /Prohibited	—	—	✓	—
Cloud	Settings synchronization	Allowed /Prohibited	Windows Phone 8.1 only	✓ (GET only)	—	—
Cloud	Credentials synchronization	Allowed /Prohibited	—	✓ (GET only)	—	—
Cloud	Synchronization over metered connection	Allowed /Prohibited	—	✓ (GET only)	—	—
Cloud	Microsoft Account	Enabled /Disabled	Windows Phone 8.1 only	—	—	—
Content Rating	Adult content in media store	Allowed /Prohibited	—	—	✓	—
Content Rating	Ratings region	Country of choice	—	—	✓	—

Device Setting Group	Settings	Values	Windows Phone 8.x	Windows 8.1 Enrolled via Intune	iOS	Android (Using the Company Portal App)
Content Rating	Movie rating	Rating	—	—	✓	—
Content Rating	TV show rating	Rating	—	—	✓	—
Content Rating	App rating	Rating	—	—	✓	—
Device	Voice dialing	Allowed /Prohibited	—	—	✓	—
Device	Voice assistant	Allowed /Prohibited	—	—	✓	—
Device	Voice assistant while locked	Allowed /Prohibited	—	—	✓	—
Device	Screen capture	Enabled /Disabled	Windows Phone 8.1 only	—	✓	—
Device	Video conferencing	Enabled /Disabled	—	—	✓	—
Device	Add game center friends	Allowed /Prohibited	—	—	✓	—
Device	Multiplayer gaming	Allowed /Prohibited	—	—	✓	—
Device	Personal wallet software while locked	Allowed /Prohibited	—	—	✓	—
Device	Diagnostic data submission	Enabled /Disabled	Windows Phone 8.1 only	✓	✓	—
Device	Geolocation	Enabled /Disabled	Windows Phone 8.1 only	—	—	—
Device	Copy and Paste	Enabled /Disabled	Windows Phone 8.1 only	—	—	—
Encryption	File encryption on mobile device	On/Off	✓	✓ (GET only)	—	✓, for Android 4
Internet Explorer	Go to intranet site for single word entry	Allowed /Prohibited	—	✓	—	—
Internet Explorer	Always send Do Not Track header	Allowed /Prohibited	—	✓	—	—



Device Setting Group	Settings	Values	Windows Phone 8.x	Windows 8.1 Enrolled via Intune	iOS	Android (Using the Company Portal App)
Internet Explorer	Intranet security zone	Allowed /Prohibited	—	✓	—	—
Internet Explorer	Security level for Internet zone	High, Medium-high, Medium	—	✓ (GET only)	—	—
Internet Explorer	Security level for intranet zone	High, Medium-high, Medium, Medium-low, Low	—	✓ (GET only)	—	—
Internet Explorer	Security level for trusted sites zone	High, Medium-high, Medium, Medium-low, Low	—	✓ (GET only)	—	—
Internet Explorer	Security level for restricted sites zone	High	—	✓ (GET only)	—	—
Internet Explorer	Namespace exists for browser security zone	Sites	—	✓	—	—
Password	Require password settings on mobile devices	Required	✓	—	✓	✓, for Android 4
Password	Password complexity	PIN, Strong	✓	✓	✓	—
Password	Idle time before mobile device is locked (minutes)	1 minute – 12 hours	✓	✓	✓	✓, for Android 4
Password	Minimum password length (characters)	4–18	✓	✓	✓	✓, for Android 4
Password	Number of passwords remembered	0–50	✓	✓	✓	✓, for Android 4
Password	Password expiration in days	1–365	✓	✓	✓	✓, for Android 4

Device Setting Group	Settings	Values	Windows Phone 8.x	Windows 8.1 Enrolled via Intune	iOS	Android (Using the Company Portal App)
Password	Number of failed logon attempts before device is wiped	0–100	✓	✓	✓	✓, for Android 4
Password	Password quality	Low security biometric, Required, At least numeric, At least alphabetic, Alphanumeric with symbols	—	—	—	✓, for Android 4
Roaming	Allow voice roaming	Allowed /Prohibited	—	—	✓	—
Roaming	Allow data roaming	Allowed /Prohibited	—	✓	✓	—
Security	Removable storage	Allowed /Prohibited	✓	—	—	—
Security	Camera	Allowed /Prohibited	Windows Phone 8.1 only	—	✓	✓, for Android 4.1
Security	Bluetooth	Allowed /Prohibited	Windows Phone 8.1 only	✓ (GET only)	—	—
Security	Allow app installation	Allowed /Prohibited	—	—	✓	—
Security	Near field communication (NFC)	Enabled /Disabled	Windows Phone 8.1 only	—	—	—
Store	Application store	Allowed /Prohibited	Windows Phone 8.1 only	—	✓	—
Store	Force application store password	Enabled /Disabled	—	—	✓, this setting applies to iTunes only	—
Store	In-app purchases	Allowed /Prohibited	—	—	✓	—



Device Setting Group	Settings	Values	Windows Phone 8.x	Windows 8.1 Enrolled via Intune	iOS	Android (Using the Company Portal App)
System Security	User to accept untrusted TLS certificates	Allowed /Prohibited	—	—	✓	—
System Security	User access control	Always notify, Notify app changes, Notify app changes (do not dim desktop), Never notify	—	✓	—	—
System Security	Network firewall	Required	—	✓ (GET only)	—	—
System Security	Updates	Automatic updates is required	—	✓	—	—
System Security	Virus protection	Required	—	✓ (GET only)	—	—
System Security	Virus protection signatures are up-to-date	Required	—	✓ (GET only)	—	—
System Security	SmartScreen	Enabled /Disabled	—	✓	—	—
System Security	Lock screen control center	Enabled /Disabled	—	—	✓ (iOS 7)	—
System Security	Lock screen notification view	Enabled /Disabled	—	—	✓ (iOS 7)	—
System Security	Lock screen today view	Enabled /Disabled	—	—	✓ (iOS 7)	—
System Security	Fingerprint for unlocking	Allowed /Prohibited	—	—	✓ (iOS 7)	—
Data Protection	Open managed documents in other unmanaged apps	Allowed /Prohibited	—	—	✓ (iOS 7)	—
Data Protection	Open unmanaged documents in other managed apps	Allowed /Prohibited	—	—	✓ (iOS 7)	—

Device Setting Group	Settings	Values	Windows Phone 8.x	Windows 8.1 Enrolled via Intune	iOS	Android (Using the Company Portal App)
Windows Server Work Folders	Work folders URL	URL	—	✓	—	—
Email Management	Custom Email account	Enabled /Disabled	Windows Phone 8.1 only	—	✓ (iOS 7)	—
Wireless Communication	Wi-Fi Tethering	Enabled /Disabled	Windows Phone 8.1 only	—	—	—
Wireless Communication	Offload data to Wi-Fi when possible	Enabled /Disabled	Windows Phone 8.1 only	—	—	—
Wireless Communication	Wi-Fi hotspot reporting	Enabled /Disabled	Windows Phone 8.1 only	—	—	—
Wireless Communication	Wireless network connection	Enabled /Disabled	Windows Phone 8.1 only	—	—	—



To install the available self-service applications, users leverage a company portal application on their mobile device. In ConfigMgr 2012 R2, Microsoft shows their commitment to a consistent user experience by releasing updated company portal applications for Windows Phone 8 and Windows 8.1, along with new company portal applications for iOS and Android that bring parity to functionality and appearance. However, the company portal is used for more than just application delivery; it is designed to allow a user to have control over their devices and is tailored to each device platform. In addition to accessing applications that were published to that user, the company portal is used to enroll iOS and Android devices, and even control aspects of other devices linked to that user account. The exact functionality in the Company Portal depends on the device platform. Table A.3 lists company portal features.

TABLE A.3 Company Portal Features

Action Taken	Windows 8.1	Windows Phone 8.x	iOS	Android
Enroll local device	—	—	✓	✓
Rename devices	✓	✓	✓	✓
Retire local device	✓	✓	✓	✓
Wipe other devices remotely	✓	✓	✓	✓
Install company line of business apps	✓	✓	—	✓
Install deep-linked apps from Public Stores	✓	✓	✓	✓
Install or launch web-based application links	✓	✓	✓	✓

NOTE: SIDELADING IOS APPLICATIONS

Apple currently restricts Microsoft from using a public store app, such as the Windows Intune company portal, to sideload LOB applications. Users must open their Safari browser and access the Windows Intune web portal on their device to view and install a company’s LOB apps. In addition, iOS LOB applications requiring administrator approval are currently not supported using the Intune web portal.

Device Retirement and Remote Wipe

Windows Intune provides two distinct functions for a mobile device that is either lost/stolen or at end-of-life for management. Mobile devices can be retired from management, breaking the management channel where the device no longer receives management policies. Both administrators and users have the ability to perform this action, which could also be considered a “selective wipe” procedure, as it removes company applications, data, and management policies. Mobile devices can also be remotely wiped; for those devices that support that command, it is a factory reset of the device.

NOTE: RETIRING AND REMOTE WIPING DEVICES

In ConfigMgr 2012 R2, support for selective wipe and full factory resets vary by mobile device platform. There could also be longer time delays between when the administrator issues a wipe command and when it the device receives it. Refer to Chapter 8 for additional information, and ensure proper testing of the device platforms your organization plans to support.

Windows Intune Licensing and Supported Architectures

In addition to new mobile device features, the December 2012 release of Windows Intune changed the licensing model for the product, moving from a device-based license to a per-user model. The per-user licensing change aligned Windows Intune with other Microsoft Online Commercial Services that also leveraged per-user licensing, such as Office 365. For Windows Intune, a user license allows an organization to manage up to five devices. In addition to per-user licensing, the full Windows Intune SKU also includes the rights to System Center 2012 Configuration Manager R2 and System Center Endpoint Protection. For organizations that have already licensed Configuration Manager 2012 R2, options are available to license only Windows Intune, reducing organizational costs for the software.

With the unified device management and licensing options, organizations now have a wide variety of devices that can be managed by the unified device management solution. They can choose to deploy Configuration Manager to manage devices such as Macs, Windows Embedded, Windows PCs, and integrate with Windows Intune for their mobile device support. In addition, organizations could also deploy a cloud-only Windows Intune solution to solve their one-off PC management needs.

This book focuses solely on Configuration Manager R2, but it is important to take a moment to discuss the supported architecture environments for Windows Intune, discussed in the following sections

Unified Architecture

Unified device management (UDM) is the term used to describe an environment where Windows Intune and ConfigMgr are integrated together. *Hybrid cloud model* is another way to describe the UDM architecture because it leverages both on-premise and cloud components seamlessly. In this configuration, all device management is performed through the ConfigMgr administrator console. Achieving this interoperability requires both the on-premise Active Directory and a cloud Azure AD are synchronized together, in addition to having Configuration Manager R2 and Windows Intune licensed, deployed, and connected together. Therefore, customers need to plan to deploy the following technologies within their environment if they don't have this in place for other Microsoft cloud services:

- ▶ **Active Directory Synchronization (DirSync):** Used to synchronize user and security group objects and attributes from the on-premise AD to Azure AD
- ▶ **Active Directory Federation Services (ADFS):** Used as an authentication mechanism to reduce the user password complexity

Figure A.1 illustrates the key components used to support this solution. ADFS is not required for this solution; however, Microsoft highly recommends it as ADFS is used for other services such as the new Workplace Join feature and true single sign-on (SSO).

When installing the UDM configuration, ConfigMgr administrators install the Windows Intune connector site role within the CAS (or the single primary site), and define one of the primary sites as the location where devices are to be created. Only one Windows Intune connector per hierarchy is supported. Currently, the total number of mobile devices supported within the unified architecture is 100,000, based on the total supported number of devices that can be in a primary site. Therefore, if the ConfigMgr administrator dedicates a primary site to mobile devices and uses the Enterprise edition of Microsoft SQL Server for the site database, it can scale to the maximum supported limit.

Cloud-Only Architecture

Cloud-only architecture is the term used to describe an environment where only Windows Intune is deployed. Another name for this is the *Windows Intune stand-alone solution*. Outside of the removal of Configuration Manager 2012 R2, the major difference in the cloud-only solution is the number of devices supported and the limitations inside the product itself (as in fewer features). However, it is important to understand the future direction of the cloud-only solution. In a January 29, 2014 blog announcement (<http://blogs.technet.com/b/server-cloud/archive/2014/01/29/new-enhancements-to-windows-intune.aspx>), Microsoft reaffirmed its commitment to providing customers choice in management solutions by announcing new mobile device capabilities would be built in to the cloud-only architecture with a goal of striving for parity between solutions.

In this configuration, administrators might deploy Intune to manage PCs, mobile devices, or both. Even though Microsoft is striving for parity between both solutions, it is incorrect to assume that new Intune features work in both solutions. When System Center 2012 R2 Configuration Manager was released, nearly all the new capabilities initially required ConfigMgr 2012 R2. With the February 2014 update, Android management is now supported in both configurations, and Microsoft added new choices for policy settings. Integration with the local on-premise AD via DirSync is not required, unless an organization is interested in integrating with their on-premise Exchange environment. In that case, DirSync is a required component to install the Windows Intune Exchange connector.

Figure A.2 illustrates the key components used to support this solution. Related to PC management, the cloud-only solution supports fewer clients than ConfigMgr 2012 R2. Windows 8.x, Windows 7, Vista, and XP SP 3 are supported; missing, however, is support for OS X, Windows To Go, Windows Embedded, and Windows Server management. A customer that requires management of those devices would look to ConfigMgr.

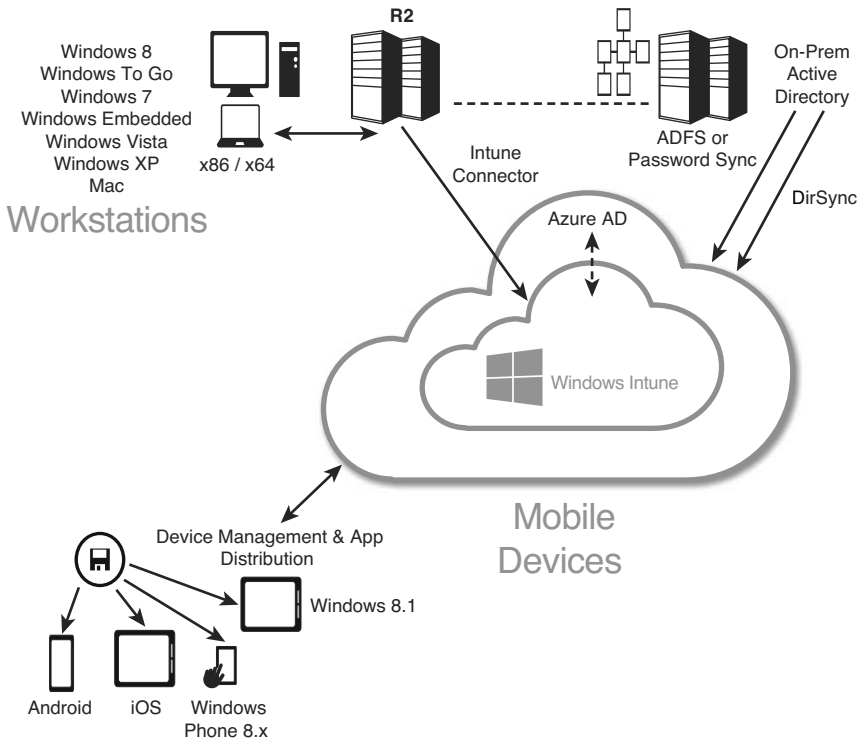


FIGURE A.1 UDM components.

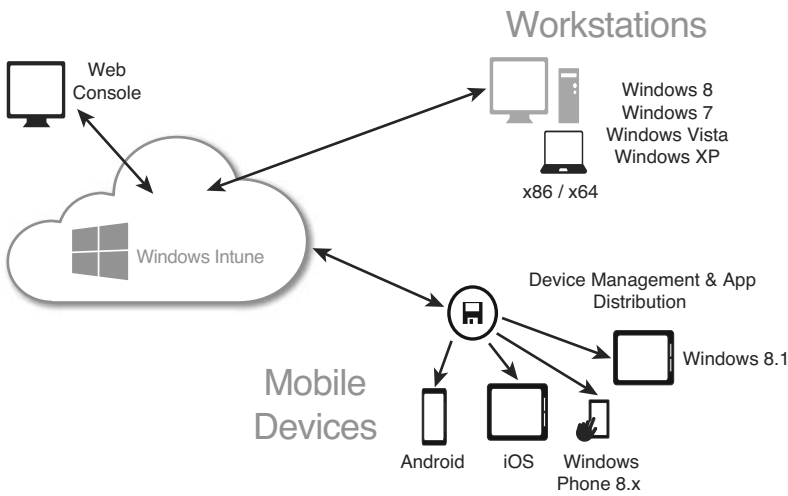


FIGURE A.2 Cloud-only components.

Refer to <http://www.windowsintune.com> for additional information about Windows Intune for cloud PC management.

The Windows Intune Connector and Subscription

Until this point, there have been references to a connector within Configuration Manager to integrate with Windows Intune, without fully explaining what this is. The Windows Intune connector is a ConfigMgr site system role that uses Secure Sockets Layer (SSL) port 443 to communicate to the Windows Intune cloud service. A Windows Intune subscription is created within ConfigMgr to define the mobile platforms ConfigMgr supports and the Microsoft Online Services cloud tenant to which to connect.

The subscription allows the organization to specify the mobile device configuration settings for the Windows Intune service. It is defined before the Intune connector is installed and contains the following items:

- ▶ **Windows Intune Organizational ID:** This is the actual Windows Intune service the organization must license (separately) and Azure AD namespace that defines the service in the format of *.onmicrosoft.com. The ConfigMgr administrator needs the service available to configure the remainder of the Intune subscription.
- ▶ **Setting the Management Authority:** This defines the way the organization manages mobile devices, either using ConfigMgr or Intune cloud-only. An organization can only choose a single authority method.
- ▶ **ConfigMgr User Collection:** This collection defines the users within the organization that can enroll mobile devices.
- ▶ **Company Portal Information:** Details on the color scheme and general information listed in the company portals.
- ▶ **Primary Site Code:** The ConfigMgr site code into which the Intune connector site system role is installed.
- ▶ **Mobile Device Platforms Provisioning:** Defines which mobile platforms users can enroll into the environment along with configurations necessary to support each mobile device.

After the subscription has been configured, the Windows Intune connector site system role is installed, and the connection to Intune is complete. On a set schedule, the connector site system role pushes device settings and deploys applications to the Windows Intune service, enables new users to be able to enroll their mobile devices, and pulls new data about existing managed mobile devices and stores it within the database.

Chapter 7 includes detailed information on installing and using the connector.

Index

Numbers

0x80004005 error code, 172
0x8007000E error code, 190
0x80072ee2 error code, 176
1E, 332

A

accounts, Network Access, 32

Active Directory

ADFS (Active Directory Federation Services), 203

Azure AD, 17-18, 199-200

DirSync

Directory Synchronization Tool, installing, 204-208

DirSync Configuration Wizard, 204-208

installing, 204-208

overview, 312

integrating, 13

overview, 318

rights management services, 16

synchronizing with Microsoft Azure AD, 200

Azure AD namespace, creating, 200-204

Directory Synchronization Tool, installing, 204-208

Windows Intune instance, creating, 200-204

Active Directory Federation Services (ADFS), 203, 312

Active Directory Synchronization (DirSync), 312

- AD. See Active Directory
- Adaptiva Software, 331
- Add Site System Roles Wizard, 233-234
- ADFS (Active Directory Federation Services), 203, 312
- ADK (Automated Deployment Kit), 148, 319
- administration changes (ConfigMgr 2012 R2)
 - automatic client upgrade, 31
 - certificate profiles, 27
 - client settings, 27-28
 - database replication configuration, 20
 - configuring interval for replication data summary, 23
 - managing replication alerts, 23-24
 - modifying SQL Server replication configuration, 20-21
 - scheduling transfer of site data across replication links, 21-22
 - support for distributed views, 22
 - DPs (distribution points), 28-31
 - cloud-based DPs, 28
 - pull DPs, 28-31
 - Internet proxy server configuration, 24
 - Network Access accounts, 32
 - PowerShell support, 32-34
 - security, 28
 - software update points, 25-27
 - multiple software update points, 26
 - specifying internal WSUS server as synchronization source, 26-27
 - in untrusted forests, 26-27
 - Windows Intune integration and extensions, 25
- AdminStudio, 331
- ADRs (automatic deployment rules), 40-41
- Agerlund, Kent, 328
- alerts, 43
- Always On, Always Connected, 51-52
- Android devices
 - configuration items, 261
 - enrolling, 254
 - log files, 292
 - mobile device management, 248
 - retiring/wiping mobile devices, 289
 - sideloading applications, 103
- Apple App Store deployment type, creating, 90-91
- Apple Developer License, 101
- Apple devices. See iOS device management
- Apple OS X computers. See OS X support
- application compatibility, 319
- application deployment
 - to Apple OS X computers, 105-107
 - application deployment type, 111
 - best practices, 112-115
 - applications in task sequences, 115
 - software installation, 112-115
 - definition of application, 77-78
 - DTs (deployment types), 78
 - to Linux and UNIX computers, 108-109
 - to mobile devices, 85-86, 281-286
 - Apple App Store deployment type, 90-91
 - with company portal, 285-288
 - defining application information, 282-284
 - Google Play Store deployment type, 92-93
 - sideloading applications, 93-103
 - Windows Phone Store deployment type, 89-90
 - Windows Store deployment type, 86-89
 - new features, 78-79
 - overview, 77

- sideloading applications, 93-94
 - for Android devices, 103
 - for Apple iPhone, iPod, and iPad devices, 101-103
 - certificate profiles, 96-97
 - domain-joined machines, 95
 - for Windows and Windows RT devices, 94-95
 - Windows modern applications, 97-99
 - for Windows Phone devices, 99-101
- virtual applications, 81-82
 - App-V 5 deployment type, 82-83
 - App-V virtual environments, 83-85
- VPN profiles, 104
- web applications, 111
- Windows Intune, 309-310
- write filter support, 79-81
- application deployment type, 111
- Application Management, 38-39
 - App-V virtual environments, 39
 - overview, 38
 - Windows sideloading keys, 39
- applications
 - definition of, 77-78
 - deployment. *See* application deployment
 - sideloading, 93-94
 - for Android devices, 103
 - for Apple iPhone, iPod, and iPad devices, 101-103
 - certificate profiles, 96-97
 - domain-joined machines, 95
 - VPN profiles, 104
 - for Windows and Windows RT devices, 94-95
 - Windows modern applications, 97-99
 - for Windows Phone devices, 99-101
- targeting, 13
- App-V 5 deployment type, creating, 82-83
- App-V virtual environments
 - creating, 83-85
 - overview, 39
- .appx file format, 101
- architecture
 - cross-platform agent architecture, 119-120
 - Windows Intune
 - cloud-only architecture, 313-314
 - unified architecture, 311-313
- asset inventory. *See* inventory
- Assets and Compliance (ConfigMgr), 34
 - client notification, 36-37
 - collections, 34
 - company resource access, 37-38
 - compliance settings, 37
 - maintenance windows for software updates, 35
 - Reassign Site option, 36
 - Remote Connection Profiles, 37
 - Resultant Client Settings, 34-35
 - user data and profiles, 38
- Authentication Method page (Create VPN Profile Wizard), 277
- author's blogs, 332-333
- Automated Deployment Kit (ADK), 148, 319
- automatic client upgrade, 31
- automatic deployment rules (ADRs), 40-41
- Auto-Trigger VPN, 15
- available discovery and inventory data, 255-258
- Azure AD, 17-18, 199-200
 - Azure AD Premium, 17
 - namespace, creating, 200-204
 - synchronizing AD with, 200
 - Azure AD namespace, creating, 200-204

Directory Synchronization Tool, installing, 204-208
 Windows Intune instance, creating, 200-204

B

Background Intelligent Transfer Service (BITS), 120

Beaumont, Steve, 331

best practices

- application deployment, 112-115
- applications in task sequences, 115
- software installation, 112-115
- overview, 317

Bink, Steven, 331

BITS (Background Intelligent Transfer Service), 120

/BITSPriority option (CCMSetup.exe), 54

blogs, 331-333

boot images, 151-155

- down-level boot images, 152-154
- optional components within, 154-155

boot partitions, 176-177

Brady, Niall, 330, 332

BranchCache downloads, 57

bring your own device (BYOD), 5, 10-11.
 See *also* mobile device management

built-in task sequence variables, 175-176

BYOD (bring your own device), 5, 10-11. See *also* mobile device management

C

CAS (central administration site), 47-48

CCMAgent-DATE-TIME.log file, 145

ccmexec command, 143

CCMNotification-DATE-TIME.log file, 145

CCMPrefPane-DATE-TIME.log file, 145

CCMSetup.exe, 54-55

central administration site (CAS), 47-48

certificate enrollment profiles, 271-273

- configuring, 319
- creating, 96-97
- new features, 27

Certificate Registration Point site system role, 272

certificates

- certificate enrollment profiles, 271-273
- configuring, 319
- creating, 96-97
- new features, 27

Certificate Registration Point site system role, 272

OS X requirements, 122

Change Ownership action, 259

changes, monitoring, 42

- alerts, 43
- client operations, 45
- deployment status, 43
- distribution status, 43
- reporting, 43

Check Readiness task, 170-172

chmod command, 127

CIM (common information model), 119

classes (hardware inventory)

- custom classes, 138
- default classes, 137

Clendenen, Anthony, 331

client agents

- client agent uninstallation/reinstallation
- Linux/UNIX client, 132
- OS X client, 134

commands, 143

- cross-platform agent components, 134
 - hardware inventory, 136-142
 - settings management, 134-135
 - software inventory, 135
- cross-platform client agents, 126
 - Linux/UNIX client, 127-128
 - OS X client, 129-132
- downloading, 126
- settings, 120-121
- client enrollment. *See* enrollment (BYOD)
- client notification, 36-37
- client operations, monitoring, 45
- client settings
 - new features, 27-28
 - Resultant Client Settings, 34-35
 - wake-up proxy client settings, 27
- Client-DATE-TIME.log file, 144-145
- clients
 - Always On, Always Connected, 51-52
 - automatic client upgrade, 31
 - BranchCache downloads, 57
 - client agents
 - client agent uninstallation/reinstallation, 132-134
 - commands, 143
 - cross-platform agent components, 134-135
 - cross-platform client agents, 126-132
 - downloading, 126
 - settings, 120-121
 - client experience, 55
 - client notification, 36-37
 - client operations, monitoring, 45
 - company portal for Windows 8.x, 55-56
 - device support through Intune, 54
 - Linux and UNIX support, 49
 - metered Internet connections, 52-53
 - multiselect in Software Center, 56
 - OS X support, 49
 - reassigning, 36
 - required deployment to devices, 57
 - selective wipe, 57
 - settings
 - new features, 27-28
 - Resultant Client Settings, 34-35
 - wake-up proxy client settings, 27
 - setup/upgrade, 54-55
 - wake-up proxy client settings, 58
 - Windows 8.x modern applications, 54
 - Windows 8.x support, 51
 - Windows Embedded support, 49-51
 - Windows To Go (WTG), 54
- cloud. *See also* Azure AD
 - cloud-based distribution points, 28
 - cloud-only architecture (Windows Intune), 313-314
- Cloudusersync.log, 233-235, 291
- cmdlets, 32-34
- CMEnroll, 130-131
- CMTrace, 191
- collections, 34
- commands
 - cmexec, 143
 - chmod, 127
 - client agent commands, 143
 - su root, 127
 - sudo, 129, 134
 - tail, 144
- common information model (CIM), 119
- communication, cross-platform, 120
- Company Contact Information tab (Create Windows Intune Subscription Wizard), 229
- Company Logo tab (Create Windows Intune Subscription Wizard), 229-230

company portal websites, 287-288

company portals

- application deployment, 285-288

 - company portal websites, 287-288

 - on Windows 8.1 devices, 286

- company portal for Windows 8.x, 55-56

- Windows Intune, 309-310

company resource access, 37-38, 271

- certificate profiles, 271-273

- email profiles, 273-275

- Wi-Fi profiles, 278-280

company-owned devices, inventorying, 259.

See also mobile device management

Completion tab (Create Windows Intune Subscription Wizard), 229-230

compliance

- ConfigMgr 2012 R2 settings, 37

- User Data and Profiles, 76

Computer rule type, 169

ConfigMgr 2012 R2

- administration changes

 - automatic client upgrade, 31

 - certificate profiles, 27

 - client settings, 27-28

 - database replication configuration, 20-24

 - DPs (distribution points), 28-31

 - Internet proxy server configuration, 24

 - Network Access accounts, 32

 - overview, 19

 - PowerShell support, 32-34

 - security, 28

 - software update points, 25-27

 - Windows Intune integration and extensions, 25

- application deployment. *See* application deployment

- Assets and Compliance, 34

 - client notification, 36-37

 - collections, 34

- company resource access, 37-38

- compliance settings, 37

- maintenance windows for software updates, 35

- Reassign Site option, 36

- Remote Connection Profiles, 37

- Resultant Client Settings, 34-35

- user data and profiles, 38

clients

- Always On, Always Connected, 51-52

- BranchCache downloads, 57

- client experience, 55

- company portal for Windows 8.x, 55-56

- device support through Intune, 54

- Linux and UNIX support, 49

- metered Internet connections, 52-53

- multiselect in Software Center, 56

- OS X support, 49

- required deployment to devices, 57

- selective wipe, 57

- setup/upgrade, 54-55

- wake-up proxy client settings, 58

- Windows 8.x modern applications, 54

- Windows 8.x support, 51

- Windows Embedded support, 49-51

- Windows To Go (WTG), 54

cross-platform support, 117

- client agent downloads, 126

- client agent settings, 120-121

- cross-platform agent architecture, 119-120

- cross-platform agent communication, 120

- firewall ports, 125

- Linux/UNIX requirements, 121

- OS X requirements, 121-125

- supported platforms, 117-119

- data protection, 13-14
 - enabling for custom inventory providers, 141-142
 - enabling users with, 9-13
 - BYOD registration and enrollment, 10-11
 - consistent access to corporate resources, 11-12
 - user connections to internal resources, 12-13
 - mobile device management
 - challenges, 244-246
 - company resource access, 271-280
 - configuration items for mobile devices, 259-268
 - deploying applications to mobile devices, 281-286
 - in-depth management, 243
 - enrolling devices, 248-254
 - inventorying mobile devices, 254-259
 - light management, 243
 - prerequisites, 246-248
 - remote connection profiles, 268-271
 - renaming devices, 248
 - retiring/wiping mobile devices, 288-290
 - supported platforms, 247-248
 - troubleshooting, 290-293
 - Monitoring, 42
 - alerts, 43
 - client operations, 45
 - deployment status, 43
 - distribution status, 43
 - reporting, 43
 - overview, 19
 - public forums, 333
 - reference URLs
 - Microsoft's Configuration Manager resources, 322-328
 - other Configuration Manager resources, 328-331
 - setup and recovery
 - CAS (central administration site), 47-48
 - database configuration, 45
 - migration capabilities, 47
 - scalability enhancements, 46-47
 - secondary sites, 48
 - support for new operating systems, 45
 - upgrade path, 47
 - Software Library, 38
 - Application Management, 38-39
 - OSD (operating system deployment), 41-42
 - software updates, 39-41
 - unifying environment with, 13
 - write filter support, 79-81
- configuration
- certificate enrollment profiles, 319
 - clients, 54-55
 - ConfigMgr 2012 R2
 - CAS (central administration site), 47-48
 - database configuration, 45
 - migration capabilities, 47
 - scalability enhancements, 46-47
 - support for new operating systems, 43
 - upgrade path, 47
 - cross-platform agent components, 134-135
 - database replication, 20
 - interval for replication data summary, 23
 - replication alerts, 23-24
 - SQL Server replication configuration, 20-21
 - support for distributed views, 22
 - transfer of site data across replication links, 21-22
 - Internet proxy server, 24
 - mobile device settings
 - Android devices, 261
 - custom configuration items, 267-268

- iOS configuration items, 263-264
- iOS security settings, 264
- remediation settings, 266
- remote connection profiles, 268-271
- Samsung KNOX devices, 261
- Windows 8.1 configuration items, 265
- Windows Phone 8 devices, 261
- Windows Phone 8.1 devices, 262
- MPs, 122
- SMSTSPreferredAdvertID variable, 335
- User Data and Profiles, 64
 - combined settings, 74
 - folder redirection, 64-67
 - offline files, 67-69
 - roaming user profiles, 70-74
- Windows Intune subscriptions, 314
- WinRM, 86
- Configuration Manager. *See* ConfigMgr 2012 R2
- confirming Windows Intune Connector site system role, 232-236
- Connection page (Create VPN Profile Wizard), 276
- connector (Intune). *See also* subscriptions (Windows Intune)
 - MDM prerequisites, 209-210
 - iOS device management, 215-220
 - Windows 8.1 device management, 210-212
 - Windows Phone 8.x device management, 212-215
 - overview, 199-200, 314
 - synchronizing AD with Microsoft Azure AD, 200
 - Azure AD namespace, creating, 200-204
 - Directory Synchronization Tool, installing, 204-208
 - Windows Intune instance, creating, 200-204
 - Windows Intune Connector site system role adding, 231-232
 - confirming installation of, 232-236
- ConnectorSetup.log, 233
- consistent access to corporate resources, 11-12, 14-15
- content prestaging, 189-190
- content staging, 188
- CoreTech, 329
- corporate resources, consistent access to, 11-12, 14-15
- CP Studio, 318
- Create a New Task Sequence Wizard, 173
- Create Application Wizard, 38
- Create Deployment Type Wizard, 82-83. *See also* sideloading applications
 - Apple App Store deployment type, creating, 90-91
 - application deployment type, 111
 - Google Play Store deployment type, creating, 92-93
 - Mac OS X deployment type, 105-107
 - Windows Phone Store deployment type, creating, 89-90
 - Windows Store deployment type, creating, 86-89
- Create Exchange ActiveSync Profile Wizard, 273-275
- Create Package and Program Wizard, 108-109
- Create Task Sequence Wizard, 156
- Create Virtual Environment page, 83-85
- Create Virtual Hard Disk Wizard, 180-181
- Create VPN Profile Wizard, 276-278
- Create Wi-Fi Profile Wizard, 278-280
- Create Windows Intune Subscription Wizard
 - Company Contact Information tab, 229
 - Company Logo tab, 229-230
 - Completion tab, 229-230

- General tab, 222-225
 - Information tab, 221
 - Platforms tab, 224-228
 - Subscription tab, 221
 - Summary tab, 229
 - CreateTSMedia.log, 182
 - cross-platform agent architecture, 119-120
 - cross-platform agent communication, 120
 - cross-platform agent components, 134
 - hardware inventory, 136-142
 - ConfigMgr site configuration, 141-142
 - custom classes, 138
 - custom inventory providers, 138-140
 - default classes, 137
 - non-Windows machine configuration, 140-141
 - OMI (open management infrastructure), 136
 - viewing results, 142
 - settings management, 134-135
 - software inventory, 135
 - cross-platform support, 117
 - client agent commands, 143
 - client agent deployment, 126
 - Linux/UNIX client, 127-128
 - OS X client, 129-132
 - client agent downloads, 126
 - client agent settings, 120-121
 - client agent uninstallation/reinstallation
 - Linux/UNIX client, 132
 - OS X client, 134
 - cross-platform agent architecture, 119-120
 - cross-platform agent communication, 120
 - cross-platform agent components, 134
 - hardware inventory, 136-142
 - settings management, 134-135
 - software inventory, 135
 - firewall ports, 125
 - Linux/UNIX requirements, 121
 - OS X requirements, 121-125
 - certificates, 122
 - client enrollment, 124-125
 - ConfigMgr Server, DP, and MP configuration, 122-123
 - HTTPS site roles, 123-124
 - supported platforms, 117-119
 - troubleshooting with log files
 - Linux/UNIX log files, 143-144
 - OS X log files, 144-145
 - verbose logs, 144
 - Crumbaker, Ron, 331
 - current drive letter set, viewing, 336
 - custom classes (hardware inventory), 138
 - custom configuration items (mobile devices), 267-268
 - custom inventory providers
 - configuring non-Windows machines for, 140-141
 - creating, 138-140
 - enabling ConfigMgr site to support, 141-142
- ## D
- data protection
 - with ConfigMgr and Windows Intune, 13-14
 - Microsoft's philosophy, 9
 - with Windows Server 2012 R2, 16
 - database configuration, 45
 - database replication, configuring, 20
 - configuring interval for replication data summary, 23
 - managing replication alerts, 23-24
 - modifying SQL Server replication configuration, 20-21

- scheduling transfer of site data across replication links, 21-22
- support for distributed views, 22
- deep linking, 78
- default classes (hardware inventory), 137
- defining application information, 282-284
- deleting
 - subscriptions (Windows Intune), 236-241
 - Wi-Fi profiles, 280
- Deploy Software Wizard, 80
- deployment
 - ADRs (automatic deployment rules), 40-41
 - application deployment
 - to Apple OS X computers, 105-107
 - best practices, 112-115
 - definition of application, 77-78
 - DTs (deployment types), 78
 - to Linux and UNIX computers, 108-109
 - to mobile devices, 85-104, 281-286
 - new features, 78-79
 - overview, 77
 - sideloading applications, 93-103
 - virtual applications, 81-85
 - VPN profiles, 104
 - web applications, 111
 - write filter support, 79-81
 - certificate profiles, 96-97
 - client agent uninstallation/reinstallation
 - Linux/UNIX client, 132
 - OS X client, 134
 - cross-platform client agents, 126
 - Linux/UNIX client, 127-128
 - OS X client, 129-132
 - deployment status, 43
 - deployment types (DTs), 78
 - Apple App Store deployment type, 90-91
 - application deployment type, 111
 - App-V 5 deployment type, 82-83
 - Google Play Store deployment type, 92-93
 - Windows Phone Store deployment type, 89-90
 - Windows Store deployment type, 86-89
 - OSD (operating system deployment), 41-42
 - built-in task sequence variables, 175-176
 - content prestaging, 189-190
 - deployment control, 160-164
 - deployment monitoring, 164-166
 - Driver Package Export and Import, 186-187
 - offline servicing, 185-186
 - overview, 147-148
 - prerequisites, 148-155
 - prestaged media, 188-189
 - task sequences size ceiling, 190
 - task types, 166-173
 - troubleshooting hints and tips, 190-195
 - unknown computer cleanup, 187-188
 - VHDs (virtual hard disks), 180-182
 - Windows setup support change, 155-158
 - WTG (Windows To Go), 183-185
 - required deployment to devices, 57
 - UEFI (Unified Extensible Firmware Interface) support, 176-179
 - User Data and Profiles, 75
- deployment status, 43
- deployment types (DTs), 78
 - Apple App Store deployment type, creating, 90-91
 - application deployment type, 111
 - App-V 5 deployment type, creating, 82-83

- Google Play Store deployment type, creating, 92-93
- Windows Phone Store deployment type, creating, 89-90
- Windows Store deployment type, creating, 86-89
- DeployToVHD.log, 182
- in-depth mobile device management, 243
- device inventory
 - overview, 13
 - Windows Intune, 301-303
- device retirements (Windows Intune), 310-311
- devices
 - application deployment, 85-86
 - Apple App Store deployment type, 90-91
 - Google Play Store deployment type, 92-93
 - sideloading applications, 93-103
 - Windows Phone Store deployment type, 89-90
 - Windows Store deployment type, 86-89
 - mobile device management, 268-271
 - challenges, 244-246
 - company resource access, 271-280
 - configuration items for mobile devices, 259-268
 - deploying applications to mobile devices, 281-286
 - in-depth management, 243
 - enrolling devices, 248-254
 - inventorying mobile devices, 254-259
 - iOS device management, 215-220
 - light management, 243
 - prerequisites, 246-248
 - remote connection profiles, 268-271
 - renaming, 248
 - retiring/wiping mobile devices, 288-290
 - supported platforms, 247-248
 - troubleshooting, 290-293
 - Windows 8.1 device management, 210-212
 - Windows Phone 8.x device management, 212-215
 - settings, enabling and enforcing, 13
 - Windows Intune support, 54
 - direct device management (Windows Intune), 301
 - DirectAccess, 15
 - Directory Synchronization Tool, installing, 204-208
 - DirSync, 312
 - Directory Synchronization Tool, installing, 204-208
 - DirSync Configuration Wizard, 204-208
 - installing, 204-208
 - DirSync Configuration Wizard, 204-208
 - disable deadline randomization, 27
 - disabling Windows Intune extensions, 236
 - discovery data (mobile device inventory), 255-258
 - disks
 - online disk deduplication, 15
 - partitioning, 176-177
 - dismgr.log, 291
 - distributed views, support for, 22
 - distribution points. See DPs (distribution points)
 - distribution status, 43
 - Dmpdownloader.log, 233, 235, 291
 - Dmpuploader.log, 233, 235, 291
 - domain-joined machines, sideloading applications, 95
 - down-level boot images, 152-154
 - downloading
 - BranchCache downloads, 57
 - client agents, 126
 - /downloadtimeout option (CCMSetup.exe), 54

DPs (distribution points), 28-31

- cloud-based DPs, 28

- configuration, 122

- pull DPs, 28-31

Driver Package Export and Import, 186-187

DSC (dynamic suite composition), 83

DTs (deployment types), 78

- Apple App Store deployment type, 90-91

- application deployment type, 111

- App-V 5 deployment type, 82-83

- Google Play Store deployment type, 92-93

- Windows Phone Store deployment type, 89-90

- Windows Store deployment type, 86-89

Dynamic Access Control, 16

dynamic resolution change, 15

dynamic suite composition (DSC), 83

E

ECM (Enterprise Client Management), 316

editing device ownership, 259

email profiles, 273-275

Enable BitLocker task, 173

enabling

- device settings, 13

- users, 14-16

- Windows Intune extensions, 238-240

Endpoint Protection, 40

enforcing device settings, 13

enrollment (BYOD), 248. *See also*

- cross-platform support; deployment

- Android devices, 254

- with ConfigMgr and Windows Intune, 10-11

- iOS devices, 252-253

- OS X requirements, 124-125

- Windows 8.1 devices, 251-252

- Windows Phone 8 devices, 249

Enterprise Client Management (ECM), 316

Enterprise Firmware Interface System Partition (ESP), 177

environment, unifying for people-centric IT

- with ConfigMgr and Windows Intune, 13

- Microsoft's philosophy, 8

- with Windows Server 2012 R2, 16

Error logging level, 144

Erskine, Samuel, 332

ESP (Extensible Firmware Interface System Partition), 177

Exchange ActiveSync page (Create Exchange ActiveSync Profile Wizard), 273-274

/ExcludeFeatures option (CCMSetup.exe), 54

extensions (Windows Intune), 25, 238-240

- disabling, 240

- enabling, 241-239

Extensions for Windows Intune tab, 238-240

F

FAQShop.com, 316

files

- .appx file format, 101

- install.wim image file, 155-158

- log files

 - Linux/UNIX log files, 143-144

 - mobile device management, 290-293

 - OS X log files, 144-145

 - SMSPXE.log, 191-192

 - SMSTSErrorDialogTimeout, 192-193

 - SMSTS.log, 191

- verbose logs, 144
- VHD-specific logs, 182
- Windows Intune, 235-240
- offline files, 67-69
 - scxcm.conf file, 144
- filters, write filter support, 79-81
- firewall ports, 125
- Flexera AdminStudio, 331
- folder redirection, 64-67
- Folder Redirection Health Report, 76
- folders
 - folder redirection, 64-67
 - Folder Redirection Health Report, 76
 - OfflineImageServicing, 186
 - OfflineImageServicing folder, 335
 - Work folders, 16
- /forceinstall option (CCMSetup.exe), 54
- /forcereboot option (CCMSetup.exe), 54
- forums, 333

G

- general resource reference URLs, 315-322
- General tab (Create Windows Intune Subscription Wizard), 222-224
- Get-Command, 33
- Google Play Store deployment type, 92-93

H

- hardware inventory
 - cross-platform agent components, 136-142
 - ConfigMgr site configuration, 141-142
 - custom classes, 138
 - custom inventory providers, 138-140

- default classes, 137
- non-Windows machine configuration, 140-141
- OMI (open management infrastructure), 136
 - viewing results, 142
- overview, 13
- Windows Intune, 301-303
- hidden task sequences, 164
- Hite, Don, 331
- Hobbs, Cliff, 316
- HTTPS site roles, 123-124
- Hudson, Matthew, 331
- hypervisor support, 153

I

- images
 - boot images, 151-155
 - down-level boot images, 152-154
 - optional components within, 154-155
 - install.wim image file, 155-158
 - thin versus thick images, 156
- Info logging level, 144
- Information tab (Create Windows Intune Subscription Wizard), 221
- InformIT website, 315
- Infrastructure Optimization (IO), 318
- installation wrappers, 114
- installing
 - Directory Synchronization Tool, 204-208
 - software. See application deployment
- install.wim image file, 155-158
- integrating Active Directory, 13
- “Integrating Virtual Application Management with App-V 5 and Configuration Manager 2012 SP1” (whitepaper), 82

internal resources, user connections to, 12, 15-16

internal WSUS server, specifying as synchronization source, 26-27

Internet proxy server, configuring, 24

interval for replication data summary, configuring, 23

Intune. See Windows Intune

inventory, 13

device inventory

overview, 13

Windows Intune, 301-303

hardware inventory

cross-platform support, 136-142

overview, 13

Windows Intune, 301-303

mobile devices, 254-259

available discovery and inventory data, 255-258

personal versus company-owned devices, 259

software inventory

cross-platform agent components, 135

personal versus company-owned devices, 259

IO (Infrastructure Optimization), 318

iOS device management, 215-220, 248

enrolling devices, 252-253

log files, 291-292

mobile device settings

iOS configuration items, 263-264

iOS security settings, 264

retiring/wiping mobile devices, 289

sideloading applications, 101-103

iPad. See iOS device management

iPhone. See iOS device management

iPod. See iOS device management

IT Ninja website, 113

J

Jones, Don, 328

Jones, Garth, 331

K

kbalertz, 316

key licensing requirements (sideloading), 210-211

Kissinger, Sherry, 331

L

LDIFDE, 318

libraries. See Software Library

licensing

reference URLs, 321-322

Windows Intune, 311

Windows Intune Add-on for System Center Configuration Manager license, 248

light mobile device management, 243

Linux support, 49

client agent uninstallation/
reinstallation, 132

cross-platform agent requirements, 121

cross-platform client agent deployment, 127-128

deploying applications to, 108-109

log files, 143-144

live links (online content), 336

Location rule type, 169

log files

Linux/UNIX log files, 143-144

- mobile device management, 290-293
 - log files on Android devices, 292
 - log files on iOS devices, 291-292
 - log files on site server, 291
 - log files on Windows 8.x devices, 292
 - Windows 8.1 OMA-DM devices, 293
- OS X log files, 144-145
- SMSPXE.log, 191-192
- SMSTSErrorDialogTimeout, 192-193
- SMSTS.log, 191
- verbose logs, 144
- VHD-specific logs, 182
- Windows Intune, 232-236
- /logon option (CCMSSetup.exe), 54

M

- maintenance windows for software updates, 35
- Make and Model rule type, 170
- managing
 - devices. See mobile device management
 - replication alerts, 23-24
- “Managing Embedded Devices with Write Filters in Configuration Manager Service Pack 1” (TechNet), 81
- Martinez, Santos, 43, 330
- MDM. See mobile device management
- MDT (Microsoft Deployment Toolkit), 166
- Mead, Wally, 326
- Meringer, Torsten, 332
- metered Internet connections, 27, 52-53
- metro applications, 54
- Microsoft Azure Active Directory
 - overview, 199-200
 - synchronizing AD with, 200
 - Azure AD namespace, creating, 200-204
 - Directory Synchronization Tool, installing, 204-208
 - Windows Intune instance, creating, 200-204
- Microsoft Configuration Manager. See Configuration Manager
- Microsoft Deployment Guys blog, 332
- Microsoft Deployment Toolkit (MDT), 166
- Microsoft Operations Framework (MOF), 318
- Microsoft Reserved Partition (MSR), 177
- Microsoft Security Compliance Manager (SCM), 318
- Microsoft server-cloud blog, 332
- Microsoft System Center Configuration Manager product group blog, 332
- Microsoft VDI (virtual desktop infrastructure), 15
- migration capabilities (ConfigMgr 2012 R2), 47
- mobile device management, 243, 300
 - application deployment, 85-86, 281-282
 - Apple App Store deployment type, 90-91
 - with company portal, 285-288
 - defining application information, 282-284
 - Google Play Store deployment type, 92-93
 - sideloading applications, 93-103
 - Windows Phone Store deployment type, 89-90
 - Windows Store deployment type, 86-89
 - challenges, 244-246
 - company resource access, 271
 - certificate profiles, 271-273
 - email profiles, 273-275
 - VPN profiles, 275-278
 - Wi-Fi profiles, 278-280
 - in-depth management, 243
 - enrolling devices, 248
 - Android devices, 254
 - iOS devices, 252-253

- Windows 8.1 devices, 251-252
- Windows Phone 8 devices, 249
- inventorying mobile devices, 254-255
 - available discovery and inventory data, 255-258
 - personal versus company-owned devices, 259
- iOS devices, 215-220
- light management, 243
- managing mobile device settings, 259-260
 - Android configuration items, 261
 - custom configuration items, 267-268
 - iOS configuration items, 263-264
 - iOS security settings, 264
 - remediation settings, 266
 - remote connection profiles, 268-271
 - Samsung KNOX configuration items, 261
 - Windows 8.1 configuration items, 265
 - Windows Phone 8 configuration items, 261
 - Windows Phone 8.1 configuration items, 262
- prerequisites, 209-210, 246-248
 - iOS device management, 215-220
 - Windows 8.1 device management, 210-212
 - Windows Phone 8.x device management, 212-215
- renaming devices, 248
- retiring/wiping mobile devices, 288-290
 - company content removed when retiring Android devices, 289
 - company content removed when retiring iOS devices, 289
 - company content removed when retiring Windows-based devices, 289
- supported platforms, 247-248

- troubleshooting, 290-293
 - log files on Android devices, 292
 - log files on iOS devices, 291-292
 - log files on site server, 291
 - log files on Windows 8.x devices, 292
 - Windows 8.1 OMA-DM devices, 293
- Windows Intune
 - application distribution, 309-310
 - company portal, 309-310
 - device inventory, 301-303
 - device retirement and remote wipe, 310-311
 - direct device management, 301
 - policy settings management, 303-309
- Modify Virtual Hard Disk Wizard, 181
- modifying
 - SQL Server replication configuration, 20-21
 - VHDs (virtual hard disks), 181
- MOF (Microsoft Operations Framework), 318
- monitoring changes, 42
 - alerts, 43
 - client operations, 45
 - deployment status, 43
 - distribution status, 43
 - OSD (operating system deployment), 164-166
 - reporting, 43
- Moss, Scott, 332
- MP configuration, 122
- MP_ClientRegistration record, 127
- MP_RegistrationManager.log file, 127
- MSIs, repackaging, 113
- MSR (Microsoft Reserved Partition), 177
- multiple software update points, 26
- multiselect in Software Center, 56
- myITforum.com, 315

N

namespaces, Azure AD, 200-204
 Network Access accounts, 32
 Network Load Balancing Deployment guide, 320

O

offline files, 67-69
 offline servicing, 185-186
 OfflinelImageServicing folder
 creating, 335
 overview, 186
 Oh, Marcus, 330, 332
 OMA-URI (Open Mobile Alliance - Uniform Resource Identifier), 319
 OMI (open management infrastructure), 119, 136
 online content, 335
 live links, 336
 pause.vbs script, 336
 Set_SMSTSPreferredAdvertID.vbs VBScript, 335
 View_Current_Drive_Letter_Set.ps1 PowerShell script, 336
 WMI_Create_OfflinelImageServicing_folder.ps1 PowerShell script, 335
 online disk deduplication, 15
 open management infrastructure (OMI), 119, 136
 Open Mobile Alliance - Uniform Resource Identifier (OMA-URI), reference URL, 319
 operating system deployment. See OSD (operating system deployment)
 operating systems
 cross-platform support, 117
 client agent settings, 120-121
 cross-platform agent architecture, 119-120
 cross-platform agent communication, 120
 Linux/UNIX requirements, 121
 OS X requirements, 121-125
 supported platforms, 117-119
 deployment. See OSD (operating system deployment)
 mobile devices. See mobile device management
 support for new operating systems, 43
 version support, 149-150
 Oppalfens, Kim, 331
 OS X Computer Enrollment Wizard, 131-132
 OS X support, 49
 client agent uninstallation/reinstallation, 134
 cross-platform agent requirements, 121-125
 client enrollment, 124-125
 ConfigMgr Server, DP, and MP configuration, 122
 HTTPS site roles, 123-124
 cross-platform client agent deployment, 129-132
 CMEnroll, 130-131
 OS X Computer Enrollment Wizard, 131-132
 deploying applications to, 105-107
 log files, 144-145
 OS X 10.9 (Mavericks), 119
 OSD (operating system deployment), 41-42, 147
 built-in task sequence variables, 175-176
 content prestaging, 189-190
 deployment control, 160-164
 deployment monitoring, 164-166
 Driver Package Export and Import, 186-187
 offline servicing, 185-186
 overview, 147-148

- prerequisites, 148
 - boot images, 151-155
 - operating system version support, 149-150
- prestaged media
 - content staging, 188
 - staged content use, 189
- task sequences
 - pausing, 193-195
 - size ceiling, 190
- task types, 166-173
 - Check Readiness, 170-172
 - Enable BitLocker, 173
 - Pre-provision BitLocker, 172-173
 - Run PowerShell Script, 167-168
 - Set Dynamic Variables, 168-170
- troubleshooting hints and tips, 190-195
 - pausing task sequences, 193-195
 - power scheme, 193
 - SMSPXE.log, 191-192
 - SMSTSErrorDialogTimeout, 192-193
 - SMSTS.log, 191
 - Windows 8.1 wireless network prompt, 195
- UEFI (Unified Extensible Firmware Interface) support, 176-179
- unknown computer cleanup, 187-188
- VHDs (virtual hard disks), 180
 - creating, 180-181
 - modifying, 181
 - updating, 181-182
 - uploading to VMM, 182
 - VHD-specific logs, 182
- Windows setup support change, 155-158
- WTG (Windows To Go), 183-185

OSD Support Team blog, 331

OSDBitLockerPIN variable, 184

OSDPreserveDriveLetter, 175

OSs. See operating systems

outgoingcontentmanager.log, 235, 238, 291

overriding subscriptions (Windows Intune), 236-241

ownership of mobile devices, editing, 259

P

Package parameter (Run PowerShell Script task), 167

Parameters parameter (Run PowerShell Script task), 168

partitions, 176-177

password synchronization, enabling, 208

pause.vbs script, 336

pausing task sequences, 336, 193-195

PCIT (people-centric IT). See people-centric IT (PCIT)

Pearson, Michael, 317

Pederson, Ronni, 331

people-centric IT (PCIT), 6-9, 316

- data protection
 - with ConfigMgr and Windows Intune, 13-14
 - with Windows Server 2012 R2, 16
- enabling users for
 - with ConfigMgr and Windows Intune, 9-13
 - Microsoft's philosophy, 7-8
 - with Windows Server 2012 R2, 14-16

Microsoft Azure Active Directory, 17-18

Microsoft's philosophy, 6-7

- data protection, 9
- enabled users, 7-8
- unified environment, 8

- unifying environment for
 - with ConfigMgr and Windows Intune, 13
 - Microsoft's philosophy, 8
 - with Windows Server 2012 R2, 16
- performance and tuning guidelines (reference URLs), 316-317
- personal devices. *See also* mobile device management, inventorying, 259
- philosophy of people-centric IT, 6-7
 - data protection, Microsoft's philosophy, 9
 - enabled users, 7-8
 - unified environment, 8
- platforms. *See* operating systems
- Platforms tab (Create Windows Intune Subscription Wizard), 224-228
- policies
 - policy to enable sideloading on domain-joined machines, 95
 - PowerShell execution policies, 168
 - Windows Intune policy settings management, 303-309
- ports, firewall, 125
- power scheme, 193
- powercfg.exe, 193-195
- PowerShell
 - PowerShell Execution Policy, 27
 - support in ConfigMgr 2012 R2, 32-34
- PowerShell Execution Policy parameter (Run PowerShell Script task), 168
- Pre-provision BitLocker task, 172-173
- prestaged media, content staging, 188
- profiles
 - certificate enrollment profiles
 - configuration, 319
 - creating, 96-97
 - new features, 27
 - overview, 271-273
 - email profiles, 273-275
 - Remote Connection Profiles, 37

- remote connection profiles, 268-271
- roaming user profiles, 70-74
- User Data and Profiles, 38
 - compliance reporting, 76
 - configuration, 64-74
 - deployment, 75
 - overview, 61-62
 - prerequisites, 62-64
 - settings, 27
- VPN profiles, 104
- Wi-Fi profiles, 278-280
- protecting data
 - with ConfigMgr and Windows Intune, 13-14
 - Microsoft's philosophy, 9
 - with Windows Server 2012 R2, 16
- Proxy Settings page (Create VPN Profile Wizard), 277
- public forums, 333
- pull DPs (distribution points), 28-31

Q-R

- Rachui, Steve (blog), 329-330, 332
- RDP (Remote Desktop Protocol), 15
- Reassign Site option, 36
- reassigning clients, 36
- recovery (ConfigMgr 2012 R2)
 - CAS (central administration site), 47-48
 - database configuration, 45
 - migration capabilities, 47
 - scalability enhancements, 46-47
 - secondary sites, 48
 - support for new operating systems, 43
 - upgrade path, 47
- redirection (folder), 64-67

reference URLs, 315

- blogs, 331-333
- general resources, 315-322
- IT Ninja, 113
- Microsoft's Configuration Manager resources, 322-328
- online live links, 336
- other Configuration Manager resources, 327-331
- public forums, 332
- utilities, 333-334

registration (BYOD), 10-11. *See also* mobile device management

reinstalling clients

- Linux/UNIX client, 132
- OS X client, 134

remediation settings (mobile devices), 266

Remote Access Role service, 14

remote applications, 15

Remote Connection Profiles, 37, 268-271

Remote Desktop Protocol (RDP), 15

remote wipe (Windows Intune), 310-311

RemoteApp, 15

removing

- subscriptions (Windows Intune), 236-240
- Wi-Fi profiles, 280

renaming devices, 248

repackaging MSIs, 113

replication alerts, managing, 23-24

reporting

- overview, 43
- User Data and Profiles compliance, 76

required deployment to devices, 57

Resultant Client Settings, 34-35

retiring/wiping mobile devices, 288-290

- company content removed when retiring Android devices, 289

- company content removed when retiring iOS devices, 289
- company content removed when retiring Windows-based devices, 289

rights management services (Active Directory), 16

roaming user profiles

- overview, 70-74
- Roaming User Profiles Health Report, 76

Roaming User Profiles Health Report, 76

roles

- Certificate Registration Point site system role, 272
- Windows Intune Connector site system role adding, 231
- confirming installation of, 232-236

Run PowerShell Script task, 167-168

S

Samsung KNOX devices configuration items, 261

Santiago, Carlos, 331

Saukko, Panu, 332

scalability enhancements (ConfigMgr 2012 R2), 46-47

SCEP (Simple Certificate Enrollment Protocol), 271

scheduling transfer of site data across replication links, 21-22

Schurling, Stefan, 332

SCM (Security Compliance Manager), 318

Script Name parameter (Run PowerShell Script task), 168

scripts

- pause.vbs, 336
- Set_SMSTSPreferredAdvertID.vbs VBScript, 335

- View_Current_Drive_Letter_Set.ps1
 - PowerShell script, 336
- WMI_Create_OfflineImageServicing_folder.ps1 PowerShell script, 335
- scxcm.conf file, 144
- SCXCM.log, 143-144
- scxcmprovider.log, 143-144
- secondary sites, recovering, 48
- security
 - ConfigMgr 2012 R2, 28
 - people-centric IT (PCIT)
 - data protection with ConfigMgr and Windows Intune, 13-14
 - Microsoft's philosophy, 9
- Security Compliance Manager (SCM), 318
- Security Configuration page (Create Wi-Fi Profile Wizard), 279
- selective wipe, 57
- session shadowing, 15
- Set Dynamic Variables task, 168-170
- Set_SMSTSPreferredAdvertID.vbs VBScript, 335
- settings (mobile devices), 259-260. *See also* configuration
 - Android configuration items, 261
 - custom configuration items, 267-268
 - iOS devices
 - iOS configuration items, 263-264
 - iOS security settings, 264
 - Windows 8.1 configuration items, 265
 - remediation settings, 266
 - remote connection profiles, 268-271
 - Samsung KNOX configuration items, 261
 - Windows Phone 8 configuration items, 261
 - Windows Phone 8.1 configuration items, 262
- setup. *See* configuration
- sideloading applications
 - for Android devices, 103
 - for Apple iPhone, iPod, and iPad devices, 101-103
 - certificate profiles, 96-97
 - domain-joined machines, 95
 - key licensing requirements, 210-211
 - overview, 78, 93-94, 210
 - sideloading enhancements, 319
 - for Windows and Windows RT devices, 94-95
 - Windows modern applications, 97-99
 - for Windows Phone devices, 99-101
- sideloading keys (Windows), 39
- Sienaert, Nico, 326
- Silect Software, 318
- Simple Certificate Enrollment Protocol (SCEP), 271
- Simple Mail Transfer Protocol (SMTP), testing, 317
- site roles (HTTPS), 123-124
- size ceiling for task sequences, 190
- /skippreq option (CCMSetup.exe), 54
- SMSPXE.log, 191-192
- SMSTSAssignmentsDownloadInterval, 175
- SMSTSAssignmentsDownloadRetry, 175
- SMSTSDownloadRetryCount, 176
- SMSTSDownloadRetryDelay, 176
- SMSTSErrorDialogTimeout, 192-193
- SMSTS.log, 191
- SMSTSPostAction, 175
- SMSTSPreferredAdvertID variable
 - overview, 160-164, 184
 - setting, 335
- SMSTSSUdaUsers variable, 115
- SMTP (Simple Mail Transfer Protocol), testing, 317

- Software Center, multiselect, 56
- software installation. See application deployment
- software inventory, cross-platform agent components, 135
- Software Library, 38
 - Application Management, 38-39
 - App-V virtual environments, 39
 - overview, 38
 - Windows sideloading keys, 39
 - OSD (operating system deployment), 41-42
 - software updates, 39-41
- software update points, 25-27
 - multiple software update points, 26
 - specifying internal WSUS server as synchronization source, 26
 - in untrusted forests, 26-27
- software updates
 - maintenance windows for software updates, 35
 - Software Library, 39-41
 - software update points, 25-27
 - multiple software update points, 26
 - specifying internal WSUS server as synchronization source, 26-27
 - in untrusted forests, 26-27
 - VHDs (virtual hard disks), 181-182
- solution accelerators, 320
- SQL Server
 - replication configuration, modifying, 20-21
 - SQL Server Service Broker port, 21
 - SSRS (SQL Server Reporting Services), 317
- SQL Server Service Broker port, 21
- SSRS (SQL Server Reporting Services), 317
- staged content use, 189
- status
 - deployment status, 43
 - distribution status, 43
 - storage tiering, 15
 - su root command, 127
 - Subscription tab (Create Windows Intune Subscription Wizard), 221
 - subscriptions (Windows Intune)
 - creating, 220-230
 - Company Contact Information tab, 229
 - Company Logo tab, 229-230
 - Completion tab, 229-230
 - General tab, 222-224
 - Information tab, 221
 - Platforms tab, 224-228
 - Subscription tab, 221
 - Summary tab, 229
 - overview, 314
 - removing or overriding, 236-240
 - sudo command, 129, 134
 - Sullivan, Kevin, 332
 - Summary tab (Create Windows Intune Subscription Wizard), 229
 - Support Tool for Windows Intune Trial Management, 321
 - SUPs. See software update points
 - Symantec, 331
 - Synchronization Settings page (Create Exchange ActiveSync Profile Wizard), 274-275
 - synchronizing AD with Microsoft Azure AD, 200
 - Azure AD namespace, creating, 200-204
 - Directory Synchronization Tool, installing, 204-208
 - Windows Intune instance, creating, 200-204
 - Sysinternals website, 318
 - System Center 2012 Configuration Unleashed*, 244
 - System Center Central, 316
 - System Center Orchestrator, 129
 - System Center Virtual User Group, 316

T

- tail command, 144
- Task Sequence Variable rule type, 170
- task sequences
 - applications in, 115
 - built-in task sequence variables, 175-176
 - hidden task sequences, 164
 - new task types, 166-173
 - Check Readiness, 170-172
 - Enable BitLocker, 173
 - Pre-provision BitLocker, 172-173
 - Run PowerShell Script, 167-168
 - Set Dynamic Variables, 168-170
 - pausing, 336, 193-195
 - size ceiling, 190
 - SMSTSPreferredAdvertID task sequence, 160-164
- templates, virtualization, 182
- Tenant ID, 291
- testing SMSTSPreferredAdvertID variable, 317
- thick versus thin images, 156
- thin versus thick images, 156
- Thompson, Steve, 332
- Thomsen, Paul, 332
- Trace logging level, 144
- training, 328
- transfer of site data across replication links, scheduling, 21-22
- Transmission ID, 291
- troubleshooting with log files
 - Linux/UNIX log files, 143-144
 - mobile device management, 290-293
 - log files on Android devices, 292
 - log files on iOS devices, 291-292
 - log files on site server, 291
 - log files on Windows 8.x devices, 292
 - Windows 8.1 OMA-DM devices, 293
 - OS X log files, 144-145
 - OSD (operating system deployment), 190-195
 - power scheme, 193-195
 - SMSPXE.log, 191-192
 - SMSTSErrorDialogTimeout, 192-193
 - SMSTS.log, 191
 - Windows 8.1 wireless network prompt, 195
 - verbose logs, 144
- trusted CA certificates, 271
- tuning, 316-317

U

- UDA (user device affinity), 115
- UDM (unified device management), 311-313
- UEFI (Unified Extensible Firmware Interface), 42, 176-179, 318
- unattended software installation, 113
- unified architecture, 311-313
- unified device management (UDM), 311-313
- Unified Extensible Firmware Interface (UEFI), 42, 176-179, 318
- unifying environment
 - with ConfigMgr and Windows Intune, 13
 - Microsoft's philosophy, 8
 - with Windows Server 2012 R2, 16
- uninstalling clients
 - Linux/UNIX client, 132
 - OS X client, 134
- UNIX support, 49
 - client agent uninstallation/reinstallation, 132
 - cross-platform agent requirements, 121
 - cross-platform client agent deployment, 127-128

- deploying applications to, 108-109
 - log files, 143-144
- unknown computer cleanup, 187-188
- untrusted forests, software update points, 26-27
- updating
 - software
 - maintenance windows for software updates, 35
 - Software Library, 39-41
 - VHDs (virtual hard disks), 181-182
- upgrade path (ConfigMgr), 47
- upgrading
 - automatic client upgrade, 31
 - clients, 54-55
 - ConfigMgr 2012 SP 1, 47
 - Windows 8 to Windows 8.1, 158
- uploading VHDs (virtual hard disks), 182
- URLs. *See* reference URLs
- User Data and Profiles
 - compliance reporting, 76
 - configuration, 64
 - combined settings, 74
 - folder redirection, 64-67
 - offline files, 67-69
 - roaming user profiles, 70-74
 - deployment, 75
 - overview, 38, 54, 61-62
 - prerequisites, 62-64
 - settings, 27
 - User Data and Profiles Health Report, 76
- user device affinity (UDA), 115
- users
 - enabling for people-centric IT
 - with ConfigMgr and Windows Intune, 9-13
 - Microsoft's philosophy, 7-8
 - with Windows Server 2012 R2, 14-16

- user connections to internal resources, 15-16
- User Data and Profiles, 38
 - compliance reporting, 76
 - configuration, 64-74
 - deployment, 75
 - overview, 61-62
 - prerequisites, 62-64
 - remote connection profiles, 268-271
 - settings, 27
- user experience, 55
- VPN connections, 12-13
- USMT 8.1, 320
- utilities, 333-334. *See also specific utilities*

V

- van Surksum, Kenneth, 332
- variables, built-in task sequence
 - variables, 175-176
- VDI (virtual desktop infrastructure), 15
- verbose logs, 144
- VHDs (virtual hard disks), 42, 180
 - creating, 180-181
 - modifying, 181
 - updating, 181-182
 - uploading to VMM, 182
 - VHD-specific logs, 182
- View_Current_Drive_Letter_Set.ps1 PowerShell script, 336
- viewing
 - current drive letter set, 336
 - hardware inventory results, 142
- virtual applications, deploying, 81-82
 - App-V 5 deployment type, 82-83
 - App-V virtual environments, 83-85

virtual desktop infrastructure (VDI), 15
 virtual environments. See App-V virtual environments
 virtual hard disks. See VHDs (virtual hard disks)
 Virtual Machine Manager (VMM), uploading VHDs to, 182
 virtualization templates, 182
 Visual Studio Report Designer, 320
 VMM (Virtual Machine Manager), uploading VHDs to, 182
 VPN connections, 12-13
 VPN profiles, 104

W-X-Y-Z

WAIK (Windows Automated Installation Kit), 153, 319
 wake-up proxy client settings, 27, 58
 Warning logging level, 144
 Wayback Machine, 336, 315
 WBEM (web-based enterprise management), 119
 Web Application Proxy, 14, 15, 16, 321
 web applications, deploying, 111
 web-based enterprise management (WBEM), 119
 websites. See reference URLs
 Wi-Fi profiles, 278-280
 Wiles, Michael, 332
 Windows 8.x support, 51
 company portal, 55-56
 company portals, 286
 device management, 210-212, 247
 enrolling devices, 251-252
 log files, 292
 mobile device configuration items, 265
 retiring/wiping mobile devices, 289
 sideloading applications, 94-95
 upgrading Windows 8 to Windows 8.1, 158
 Windows 8.x modern applications, 54
 Windows 8.1 OMA-DM devices, troubleshooting, 293
 wireless network prompt, 195
 Windows Automated Deployment Kit (ADK), 319
 Windows Automated Installation Kit (WAIK), 153, 319
 Windows Embedded support
 overview, 49-51
 write filter support, 79-81
 Windows Intune
 data protection, 13-14
 device support through Intune, 54
 enabling users with, 9-13
 BYOD registration and enrollment, 10-11
 consistent access to corporate resources, 11-12
 user connections to internal resources, 12-13
 extensions, 25, 238-340
 disabling, 240
 enabling, 239-240
 integration with ConfigMgr 2012, 25
 Intune connector
 adding Windows Intune Connector site system role, 231-232
 confirming installation of Windows Intune Connector site system role, 232-236
 overview, 199-200, 314
 licensing, 311
 log files, 232-236
 mobile device management features, 300
 application distribution, 303-310
 company portal, 303-310
 device inventory, 301-303

- device retirement and remote wipe, 310-311
- direct device management, 301
- policy settings management, 303-309
- mobile device management prerequisites, 209-210
 - iOS device management, 215-220
 - Windows 8.1 device management, 210-212
 - Windows Phone 8.x device management, 212-215
- overview, 297-300
- reference URLs, 321
- subscriptions
 - creating, 220-230
 - overview, 314
 - removing or overriding, 236-241
- supported architectures
 - cloud-only architecture, 313-314
 - unified architecture, 311-313
- synchronizing AD with Microsoft Azure AD, 200
 - Azure AD namespace, creating, 200-204
 - Directory Synchronization Tool, installing, 204-208
 - Windows Intune instance, creating, 200-204
- unifying environment with, 13
- Windows Intune Add-on for System Center Configuration Manager license, 248
- Windows Intune Connector site system role adding, 231
 - confirming installation of, 232-236
- Windows IT Pro, 319
- Windows Management Instrumentation (WMI), 320
- Windows modern applications, sideloading, 97-99
- Windows Partition, 177
- Windows Phone 8.x devices
 - device management, 212-215, 247
 - enrolling, 249
 - mobile device settings, 261-262
 - sideloading applications, 99-101
- Windows Phone Store deployment type, creating, 89-90
- Windows RT devices
 - mobile device management, 247
 - sideloading applications, 94-95
- Windows Server 2012 R2
 - data protection, 16
 - enabling users for people-centric IT, 14-16
 - BYOD registration and enrollment, 14
 - consistent access to corporate resources, 14-15
 - user connections to internal resources, 15-16
 - VDI (virtual desktop infrastructure), 15
 - unifying environment with, 16
 - Web Application Proxy, 14
 - Workplace Join, 14
- Windows Server technical library, 318
- Windows sideloading keys, 39
- Windows Store deployment type, creating, 86-89
- Windows To Go (WTG), 42, 54, 183-185, 318
- Windows XP, end of support, 147
- WinRM configuration, 86
- wiping mobile devices, 288-290
 - company content removed when retiring Android devices, 289
 - company content removed when retiring iOS devices, 289
 - company content removed when retiring Windows-based devices, 289

- wireless network prompt, 195
- wizards. See *specific wizards*
- WMI (Windows Management Instrumentation), 320
- WMI Query Language (WQL), 320
- WMI_Create_OfflineImageServicing_folder.ps1
PowerShell script, 335
- Work folders, 16
- Workplace Join
 - overlapping ranges, 14
 - reference URLs, 321
- WQL (WMI Query Language), 320
- wrappers (installation), 114
- write filter support, 79-81
- WTG (Windows To Go), 42, 54, 183-185
- WTGCreator.exe, 185

- XML Notepad 2007, 318