Kerrie Meyler
Jason Sandys
Greg Ramsey

Foreword by Wally Mead

Powered by

CLEARPointe

# System Center 2012 R2 Configuration Manager

## UNLEASHED


FREE SAMPLE CHAPTER

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

SAMS | 800 East 96th Street, Indianapolis, Indiana 46240 USA

## System Center 2012 R2 Configuration Manager Unleashed



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



### Warning and Disclaimer



### 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

# Contents

# 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 Surksum**, 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.vansurksum.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** begin 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

IN THIS APPENDIX



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.

## 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 blog 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 smartphone 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 ANNOUCEMENT**

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 | WP8 | 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: SIDELOADING 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.

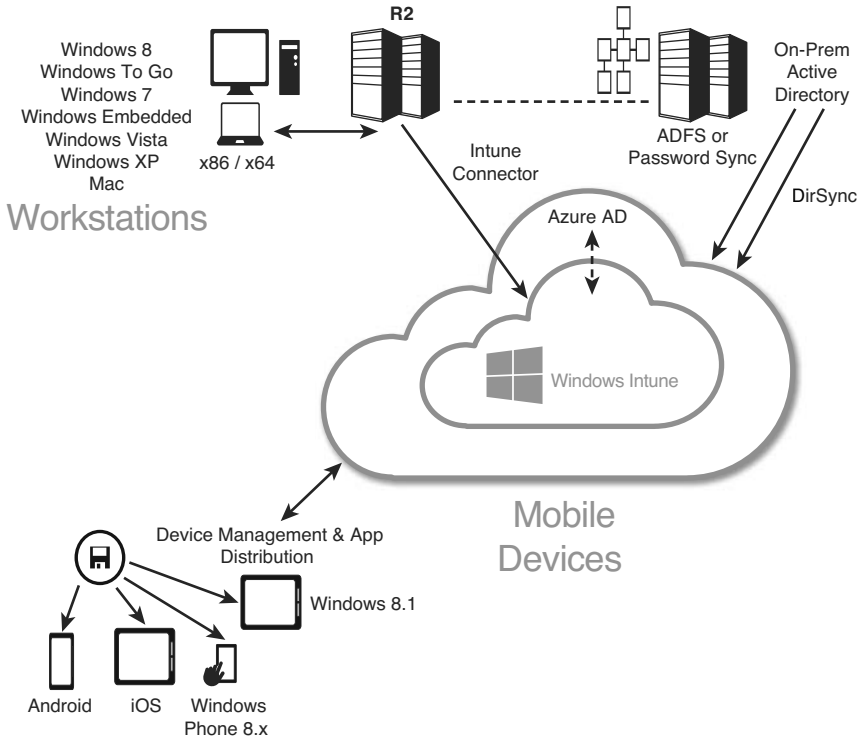


FIGURE A.1 UDM components.

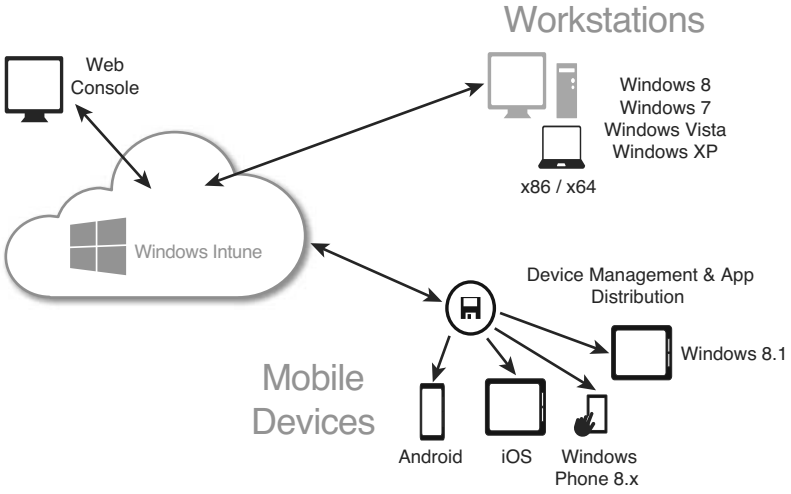


FIGURE A.2 Cloud-only components.

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



## A

## B



## C

# D

## E



## F

## G



## H



## I

## J



## K



## L

# M

# N



# O

# P

## Q-R

# S

# T



# U

# V

# W-X-Y-Z