

Supporting Windows 8.1



Exam Ref

70-688

Joli Ballew

Exam Ref 70-688

Supporting Windows 8.1

Joli Ballew

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

Copyright © 2014 by Joli Ballew

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

Library of Congress Control Number: 2014940675
ISBN: 978-0-7356-8473-7

Printed and bound in the United States of America.

First Printing

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

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

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

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

Acquisitions Editor: Anne Hamilton

Developmental Editor: Karen Szall

Editorial Production: Box Twelve Communications

Technical Reviewer: Randall Galloway and Brian Svidergol

Cover: Twist Creative • Seattle

Contents at a glance

	<i>Introduction</i>	<i>ix</i>
	<i>Preparing for the exam</i>	<i>xiii</i>
CHAPTER 1	Support operating system and application installation	1
CHAPTER 2	Support resource access	93
CHAPTER 3	Support Windows clients and devices	217
	<i>Index</i>	<i>315</i>

This page intentionally left blank

Contents

Introduction	ix
<i>Microsoft certifications</i>	<i>ix</i>
<i>Acknowledgments</i>	<i>x</i>
<i>Errata, updates, & book support</i>	<i>x</i>
<i>We want to hear from you</i>	<i>xi</i>
<i>Stay in touch</i>	<i>xi</i>
Preparing for the exam	xiii
Chapter 1 Support operating system and application installation	1
Objective 1.1: Support operating system installation	2
Supporting Windows To Go	2
Managing boot settings	7
Working with multiboot systems	14
Managing desktop images	15
Customizing a Windows installation by using Windows Preinstallation Environment (Windows PE)	21
Objective summary	26
Objective review	26
Objective 1.2: Support desktop apps	29
Supporting desktop app compatibility by using ACT	29
Supporting desktop application coexistence	36
Supporting installation and configuration of User Experience Virtualization (UE-V)	45
Deploying desktop apps by using Windows Intune	47

What do you think of this book? We want to hear from you!
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:
www.microsoft.com/learning/booksurvey/

Objective summary	51
Objective review	51
Objective 1.3: Support Windows Store and cloud apps	53
Integrating a Microsoft account	53
Installing and managing software by using Office 365 and Windows Store apps	56
Sideloaded apps into online and offline images	68
Sideloaded apps by using Windows Intune	72
Deep linking apps by using Windows Intune	78
Objective summary	80
Objective review	81
Answers	84

Chapter 2 Support resource access 93

Objective 2.1: Support network connectivity	93
Understanding IPv4 and IPv6	94
Supporting names resolution	101
Supporting wireless networks and connections	106
Supporting network security	113
Objective summary	124
Objective review	125
Objective 2.2: Support remote access	127
Constructing a virtual private network (VPN)	127
Understanding Remote Desktop Protocol (RDP), including Remote Desktop Services Gateway access	131
Configuring and managing DirectAccess	134
Exploring remote administration	138
Supporting Network Access Protection (NAP)	141
Objective summary	148
Objective review	149
Objective 2.3: Support authentication and authorization	150
Understanding and supporting multifactor authentication	151
Distinguishing among workgroup vs. domain, homegroup, computer, and user authentication	156

Knowing when to use a local account vs. a Microsoft account	164
Configuring Workplace Join	165
Objective summary	166
Objective review	166
Objective 2.4: Support data storage	169
Supporting Distributed File System (DFS)	169
Understanding Storage Spaces	171
Optimizing data access by using BranchCache	173
Supporting OneDrive	175
Objective summary	178
Objective review	178
Objective 2.5: Support data security	180
Managing permissions	180
Supporting Encrypting File System (EFS)	186
Controlling access to removable media	190
Supporting BitLocker and BitLocker To Go	191
Objective summary	201
Objective review	202
Answers	205

Chapter 3 Support Windows clients and devices 217

Objective 3.1: Support operating system and hardware	217
Resolving hardware and device issues	218
Optimizing performance	224
Monitoring performance	227
Monitoring and managing printers	233
Remediating startup issues	237
Objective summary	240
Objective review	241
Objective 3.2: Support mobile devices	243
Supporting mobile device policies	243
Supporting mobile access and data synchronization	248
Supporting broadband connectivity	251
Supporting Mobile Device Management	255

Objective summary	261
Objective review	261
Objective 3.3: Support client compliance	262
Managing updates by using Windows Update and Windows Intune	263
Managing client security	269
Managing Internet Explorer 11 security	276
Supporting Group Policy application	281
Objective summary	287
Objective review	288
Objective 3.4: Manage clients by using Windows Intune	290
Managing user and computer groups	290
Managing remote computers with Windows Intune	302
Objective summary	304
Objective review	305
Answers.	307
 <i>Index</i>	 315

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

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

www.microsoft.com/learning/booksurvey/

Introduction

This book is written for IT professionals who want to earn the Microsoft Certified Solutions Associate Windows 8.1 certification. This certification includes two exams:

- **70-687** Configuring Windows 8.1
- **70-688** Supporting Windows 8.1

Exam 70-688, the focus of this book, serves as the second exam in the path to the Windows 8.1 MCSA certification. This book is written specifically for IT professionals who want to demonstrate that they have the primary set of Windows 8.1 skills, relevant across multiple solution areas in a business environment, to support Windows 8.1 across any size or type of enterprise. Starting in January 2014, this exam covers topics that include new features and capabilities introduced in Windows 8.1.

The two exams—Exam 70-687 and Exam 70-688—allow you to earn the Windows 8.1 MCSA certification without any prior certification. Together, these include 10 domains of broader skills and 35 more specific objectives, each having many subobjectives. The 70-688 exam tests three domains and 12 objectives that comprise the core knowledge needed to support a Windows 8.1 infrastructure. Each of the 12 objectives includes several subobjectives.

In order to create a book that is a manageable study tool, I've focused on covering the new features and capabilities of Windows 8.1, while not ignoring likely test subjects that were introduced in earlier versions of Windows 8.1. I cover every objective and subobjective here too, offering links to information you'll want to read that I didn't have room to add to this book.

While this book covers every exam objective, it does not cover every exam question. Only the Microsoft exam team has access to the exam questions themselves and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the links you'll find in the book to find more information—and then take the time to research and study the topic. Valuable information is available on MSDN, TechNet, and in blogs and forums.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design

and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO ALL MICROSOFT CERTIFICATIONS

For information about Microsoft certifications, including a full list of available certifications, go to <http://www.microsoft.com/learning/en/us/certification/cert-default.aspx>.

Acknowledgments

I have written nearly 60 books and I always say that it takes a good, strong, competent team to get it done. I just write the words. Behind the scenes are acquisition editors, project managers, technical editors, copy editors, layout designers, and many others I am sure that I don't even know about. I also have a supportive family, pets to keep me company while I write, and a group of friends that let me talk about tech stuff, even when I know they aren't really interested.

By name these people include Acquisitions Editor Karen Szall, Technical Editors Randall Galloway and Brian Svidergol, Copy Editor Susan Dunn, and Indexer Angie Martin. My Project Manager is Jeff Riley. My family includes Cosmo, Jennifer and Andrew, two lovely granddaughters, my 93-year-old father, and a handful of pets.

I'd like to thank everyone at Studio B, too, including my agent, Stacey Czarnowski, and the person who takes care of my money, Katrina Bevin. I also continue to acknowledge my (retired) agent, Neil Salkind, who managed my work for over a decade.

Errata, updates, & book support

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

<http://aka.ms/ER688R2>

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

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

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

We want to hear from you

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

<http://aka.ms/tellpress>

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

Stay in touch

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

This page intentionally left blank

Preparing for the exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. While there is no substitution for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you round out your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Training Guide and another study guide for your “at home” preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

This page intentionally left blank

Support operating system and application installation

You must pass two exams to earn the Microsoft Certified Solutions Associate (MCSA) certification. The first, Configuring Windows 8.1 (70-687), deals mainly with how to install and configure the operating system. The second, Supporting Windows 8.1 (70-688), deals mainly with how to support those installations and configurations for the long term. Because the common factor between these two exams is Windows 8.1, you'll see some overlap. For instance, you learn how to install Windows To Go while preparing for Exam 70-687, and you learn how to support Windows To Go while preparing for Exam 70-688. That's a fine line; make sure that as you work through this book you understand that installations and configurations might already have been performed, and that those who write the exam questions might simply assume that you know how to do it. That said, you will still see how to perform some installation and configuration tasks in this chapter, especially those you might not be familiar with.

IMPORTANT
*Have you read
page xiii?*

It contains valuable
information regarding
the skills you need to
pass the exam.

In this chapter you'll learn how to support various operating system installations that are, for the most part, already in place, ranging from the most basic Windows 8.1 installations to native virtual hard disks to specialty Windows installations unique to a single enterprise. You'll learn how to support desktop apps in many ways, too, including how to run those apps in virtual, cloud, or remote environments when running them on each workstation isn't ideal. Finally, you'll learn how network administrators can make their own apps available to users in a process called sideloading.

Objectives in this chapter:

- Objective 1.1: Support operating system installation
- Objective 1.2: Support desktop apps
- Objective 1.3: Support Windows Store and cloud apps

Objective 1.1: Support operating system installation

You can install an operating system in many ways beyond the familiar upgrade-with-a-DVD or boot-to-a-DVD method. You can install Windows 8.1 as Windows To Go, native virtual hard disk (VHD), and as part of a multiboot system, for example.

You also can customize an installation. As an enterprise network administrator, you can configure a reference computer exactly as you want it, install drivers, software, specialty screen savers, and so on, and then create an image of that computer to use for workstation installations. You can also perform installations via a network by enabling the computers to locate the installation files on a network server. Installations can be lite-touch and zero-touch, too, and include unique answer files to reduce the amount of human contact required during the installation process. In this objective you'll learn how to support many of these types of installations.

This objective covers how to:

- Support Windows To Go
- Manage boot settings, including native virtual hard disk (VHD) and multiboot
- Manage desktop images
- Customize a Windows installation by using Windows Preinstallation Environment (Windows PE)

Supporting Windows To Go

To create a Windows To Go workspace, you must have access to a Windows 8-based Enterprise edition computer. Windows 8.1 Enterprise has a Windows To Go Creator Wizard just for that purpose. You create and save the workspace to a certified Windows To Go USB flash drive. After it's created, you give authorized users the configured flash drive, which they can use to run Windows from a computer other than their own, assuming that the computer can be configured to start to a USB drive and run a compatible operating system.

MORE INFO CREATING A WINDOWS TO GO DRIVE

A step-by-step wiki available at TechNet explains how to create a Windows To Go USB drive: <http://social.technet.microsoft.com/wiki/contents/articles/6991.windows-to-go-step-by-step.aspx>. How to install Windows To Go is an objective on Exam 70-687, Configuring Windows 8.1.

A few things are unique about Windows To Go:

- You can create a Windows To Go workspace only from a Windows 8-based Enterprise edition computer, and you need the Windows 8-based Enterprise installation files

to do so. Installation files can be in the form of an International Organization for Standardization (ISO) file, installation media such as a DVD, or a Windows Image file (.wim).

- The Windows To Go drive can hold the same image used on your enterprise workstations.
- The USB drive must be at least 32 gigabytes (GB) or larger and must be Windows To Go certified.
- You can't use Trusted Platform Model (TPM) with Windows To Go drives. TPM protects a specific computer from unauthorized access, and Windows To Go is used on more than one. When BitLocker is used, though, you can configure a startup password.
- Hibernate and sleep aren't enabled by default, although they can be through Group Policy.
- Windows Recovery Environment (Windows RE) isn't available, nor is resetting or refreshing. You should reimage problematic drives.
- For Windows To Go images that run Windows 8.1 Enterprise edition, Windows Store apps can roam between multiple PCs on a Windows To Go drive.

Hosting Windows To Go

The host computer is the computer used to start to the Windows To Go USB drive. The host computer must:

- Have hardware that has been certified for use with either Windows 7 or Windows 8 operating systems
- Not be a Windows RT or Mac computer
- Be thought of as a temporary host, because Windows To Go is only a short-term solution when the user can't be at his or her workstation
- Meet additional requirements listed in Table 1-1 and Table 1-2

Note also that the host computer's internal hard disks aren't accessible. This is to ensure that data isn't accidentally or maliciously accessed by the temporary user. Likewise, Windows To Go won't be listed in File Explorer.

TABLE 1-1 Computer requirements when hosting Windows To Go

Item	Requirement
Startup and firmware	The computer must be able to start to a USB drive and firmware must be USB enabled.
Processor architecture	The architecture must support the image on the Windows To Go drive (see Table 1-2).
USB port	The host must have an available USB port that can't be part of a USB hub and must be 2.0 or later.
Processor, RAM, graphics	The host must meet minimum standards for Windows 8, including a 1-GHz processor or higher, 2 GB of RAM or higher, and a DirectX 9 graphics device with WDDM 1.2 or greater driver.

MORE INFO DEPLOYING AND PROVISIONING WINDOWS TO GO

You can learn plenty about Windows To Go, including image deployment and device provisioning. TechNet has a lengthy article at <http://technet.microsoft.com/en-us/library/jj592685.aspx>.

TABLE 1-2 Architecture requirements for hosting Windows To Go

Firmware/Processor	Compatible architecture
Legacy 32-bit BIOS	32-bit
Legacy 64-bit BIOS	32-bit and 64-bit
UEFI 32-bit BIOS	32-bit
UEFI 64-bit BIOS	64-bit

Starting to Windows To Go

If a host meets the requirements for starting to a Windows To Go USB drive, you should change the startup options on the host to ensure that it will do exactly that when a USB Windows To Go drive is inserted.

To change the Windows To Go startup options on a host running Windows 8.1, follow these steps:

1. Log on as an administrator.
2. Right-click the Start button and Control Panel.
3. Click Hardware And Sound.
4. Under Devices And Printers, click Change Windows To Go Startup Options.
5. Click Yes (see Figure 1-1).
6. Click Save Changes.

When you're ready, turn off the host computer, insert the Windows To Go USB drive into an applicable USB port, and restart the computer. During this first restart, the host scans for the Windows To Go drive and installs any required drivers. The information is cached so that next time the process won't be repeated. When the Windows To Go workspace opens, you use it as you would any Windows 8.1 installation, but understand the limitations detailed earlier (such as Hibernate being disabled and internal drives unavailable).

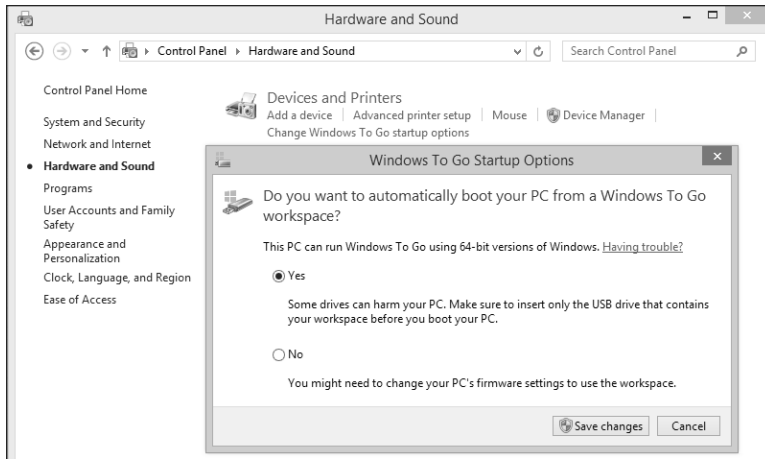


FIGURE 1-1 Configure the host computer to start to a Windows To Go workspace.

Configuring Group Policy for Windows To Go

Administrators configure and apply Group Policy to control what workers, guests, user groups, and even computer groups can do or access, either locally or on a domain. For example, you might use Group Policy to keep users from accessing the Windows Store or from copying data to removable drives. You might also require that all computers on a company network use a specific desktop background. Group Policy helps you maintain a secure (and sometimes identical) work environment for everyone. This makes managing large networks easier.

On domains, you configure Group Policy by using the Group Policy Management Console (gpmc.msc) or the Group Policy Editor (gpedit.msc). On a workgroup, you use the Local Group Policy Editor on each computer.

MORE INFO USING GROUP POLICY OBJECTS (GPOS)

At the highest level, network administrators create and configure Group Policy Objects (GPOs) to define settings that determine how users and computers will function. GPOs exist for Windows To Go as well. GPOs are then associated with Active Directory containers such as physical or virtual sites, entire domains, or other (perhaps smaller) organizational units.

Three Windows To Go settings are available:

- **Allow Hibernation (S4) When Starting From A Windows To Go Workspace** When this setting is enabled, the PC can go into hibernation mode when started from a Windows To Go workspace. If this setting is disabled or not configured, the PC can't.
- **Windows To Go Default Startup Options** When this setting is enabled, the host computer can start to a Windows To Go workspace when one is discovered during startup, and users can't change this setting in Control Panel. If this setting is disabled,

the host can't start to a Windows To Go workspace unless a user configures the option manually in the BIOS or other boot order configuration. If it's not configured, users who are members of the Administrators group can make changes using the Windows To Go Startup Options Control Panel item.

- **Disallow Standby Sleep States (S1-S3) When Starting From A Windows To Go Workspace** If this setting is enabled, when started from the Windows To Go workspace, Windows can't use standby states to let the computer sleep. If this setting is disabled or not configured, Windows can use standby states to make the PC sleep.

To locate and explore the available Windows To Go Local Group Policy settings, and to enable Windows To Go Default Startup Options, follow these steps:

1. Press Windows logo key+R to open a Run dialog box.
2. Type **gpedit.msc** and press Enter.
3. Navigate to Computer Configuration, Administrative Templates, Windows Components, Portable Operating System.
4. Double-click and explore each of the three available settings, and then return to the second one, Windows To Go Default Startup Options.
5. Click Enabled (see Figure 1-2).
6. Click OK.

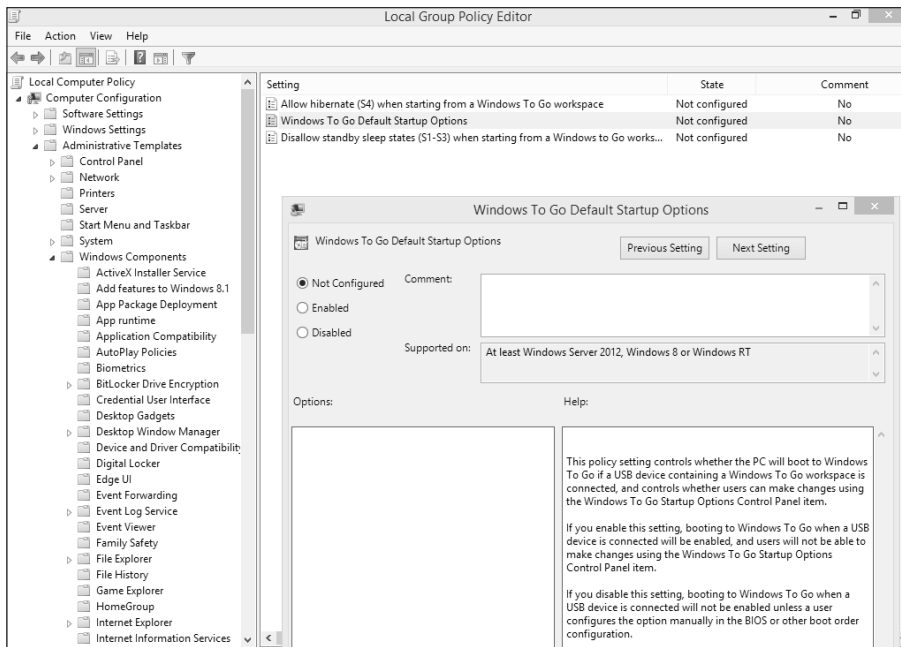


FIGURE 1-2 Locate and configure Windows To Go Local Group Policies.

Managing boot settings

Startup settings determine how a computer starts by default. When multiple operating systems are available, a list of startup entries generally appears from which users can choose what they want. BCDedit and BCDboot are command-line utilities used to configure and control the process. Startup configuration parameters are stored in the Boot Configuration Data (BCD) Store, which you manage with the BCD Editor (Bcdedit.exe).

Although these command-line tools might be new to you, you might already be familiar with a related end-user option available from the System tool in Control Panel. Click Advanced System Settings to see the dialog box shown in Figure 1-3 on the left, and click Settings under Startup and Recovery to see the Startup And Recovery dialog box shown on the right. The Startup And Recovery dialog box in Figure 1-3 also shows that Windows 8.1 is the default operating system. If multiple operating systems exist on the machine, the list of startup options remains on the screen (and available for selection) for 30 seconds before the default operating system automatically starts. When you need to make simple changes (such as changing the default operating system), you can make those changes in the Startup And Recovery dialog box.

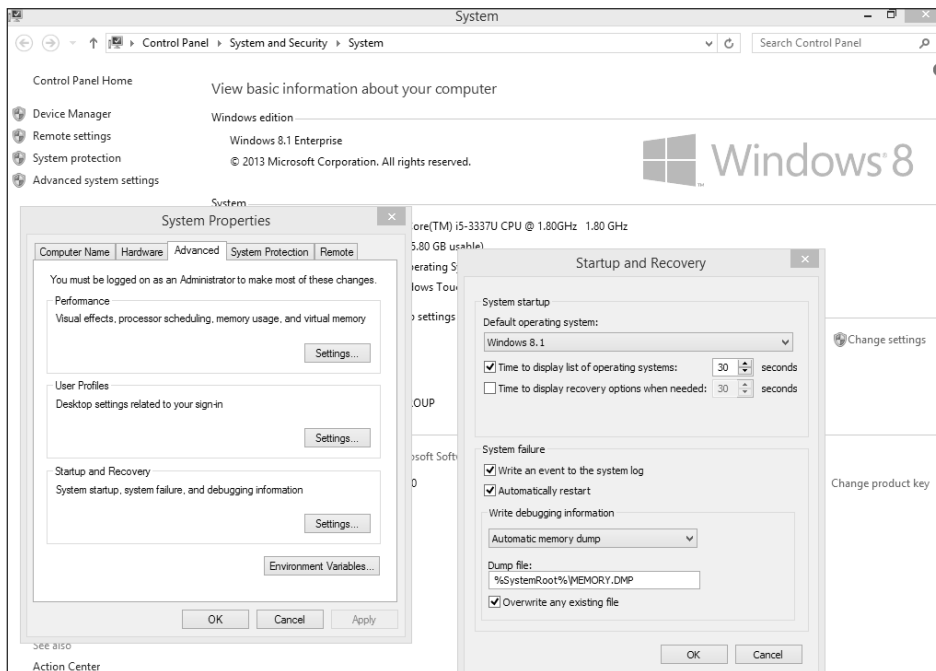


FIGURE 1-3 Change basic startup settings from the Startup And Recovery dialog box.

You can also change how Windows starts by using the System Configuration utility (Msconfig.exe) and the BCD Windows Management Instrumentation (WMI) provider. The System Configuration utility is more advanced than the Startup And Recovery dialog box and offers more tools with capabilities that include `/debug`, `/safeboot`, `/bootlog`, `/noguiboot`, `/basevideo`, and `/numproc`. The latter is a management interface that you can use to script utilities that modify BCD.

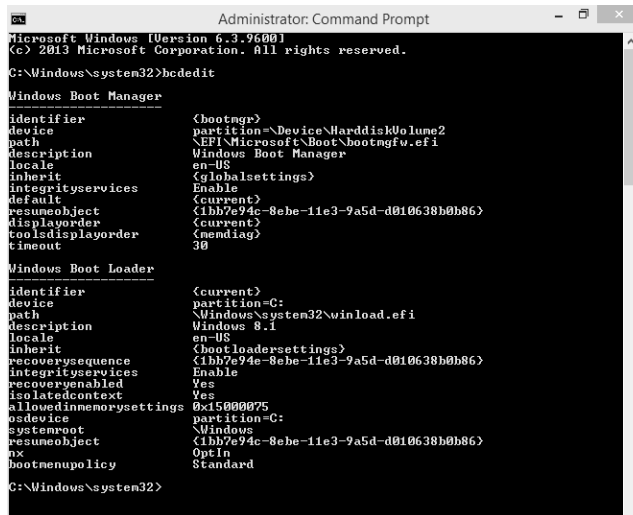


EXAM TIP

The BCD Store holds the startup configuration parameters. It replaces the older `ntldr/Boot.ini` file, so if you see this latter term on the exam, it's likely there to throw you off—that is, unless the question involves a multiboot system with something earlier than Windows Vista installed. `Bootcfg` is also an outdated term, now replaced with `BCDedit`. The BCD Store is located in one of two places on Windows Vista, Windows 7, and Windows 8-based machines. On legacy BIOS machines, it's in `\Boot\BCD`. On Extensible Firmware Interface machines, it's on the EFI system partition.

Using BCDedit

`Bcdedit.exe` is a command-line utility that replaced `Bootcfg.exe` in Windows Vista. Figure 1-4 shows this command and the resulting information regarding the BCD Store on a computer running only Windows 8.1 Enterprise. Notice the Administrator command prompt. The results show two entries: Windows Boot Manager and Windows Boot Loader.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>bcdedit

Windows Boot Manager
-----
identifier              {bootmgr}
device                  partition=\Device\HarddiskVolume2
path                    \EFI\Microsoft\Boot\bootmgfw.efi
description              Windows Boot Manager
locale                  en-US
inherit                  {globalsettings}
integrityservices        Enable
default                 {current}
resumeobject             {1bb7e94c-8ebe-11e3-9a5d-d010638b0b86}
displayorder            {current}
tooldisplayorder         {memdiag}
timeout                 30

Windows Boot Loader
-----
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.efi
description              Windows 8.1
locale                  en-US
inherit                  {bootloadersettings}
recoverysequence         {1bb7e94c-8ebe-11e3-9a5d-d010638b0b86}
integrityservices        Enable
recoveryenabled          Yes
isolatedcontext          Yes
allowedinmemorysettings {0x5000075}
osdevice                partition=C:
systemroot               \Windows
resumeobject             {1bb7e94c-8ebe-11e3-9a5d-d010638b0b86}
tx                       OptIn
bootmenupolicy           Standard

C:\Windows\system32>
```

FIGURE 1-4 Type `bcdedit` at an Administrator command prompt to view the BCD Store.

Windows Boot Manager lets you to choose which startup application to run and controls that process during startup. One of those applications is the Windows Boot Loader, which loads Windows—in this case, Windows 8.1 Enterprise.

You can do much more with the `bcdedit` command than simply showing the BCD Store information. You can do the following, for example:

- Add entries to an existing BCD Store, and modify or delete existing entries
- Export entries to a BCD Store or import from one

- Apply a global change (to all the entries)
- Change the default time-out value

You'll likely be tested on the various parameters you can use with the *bcdedit* command. Here are some with which you should be familiar (you can find a more complete list at [http://technet.microsoft.com/en-us/library/cc709667\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc709667(v=WS.10).aspx)):

- **/create store** Use this to create a new empty startup configuration store
- **/export** or **/import** Use */export* to export store information or */import* to restore using what you've saved from the */export* parameter
- **/copy** Use this to copy entries in the store
- **/delete** Use this to delete entries in the store
- **/boot sequence** Use this to configure a one-time startup sequence for the boot manager
- **/default** This sets the default startup entry
- **/displayorder** This sets the startup order in a multiboot system
- **/timeout** This sets the boot manager timeout value

Using BCDboot

Installing Windows 8.1 or any other operating system on a hard disk automatically creates partitions. The system partition contains the files required to start the operating system (as well as the Boot folder) that tells the computer where the operating system is stored. The boot partition contains the Windows operating system files. The active partition, a system partition, is the one used to start Windows. You can have multiple startup partitions—and you will if you have a multiboot system. BCDboot helps you manage these partitions.

Bcdboot.exe (as well as Bcdedit.exe) is located in the Windows\System32 folder of a Windows 8.1 computer. You can copy startup files from the Windows directory with this command:

```
x:\Windows\System32\bcdboot x:\Windows
```

You can use the *bcdboot* command to do the following, for example:

- Configure a computer to boot to a virtual hard disk (VHD) file
- Repair the system partition by replacing damaged files with undamaged copies
- Set up or repair the startup menu on a multiboot PC

You can view the parameters listed here by typing **bcdboot /Windows** at an Administrator command prompt, as shown in Figure 1-5.

```
Administrator: Command Prompt
C:\Windows\system32\bcdboot /windows
bcdboot - Bcd boot file creation and repair tool.
The bcdboot.exe command-line tool is used to copy critical boot files to the
system partition and to create a new system BCD store.
bcdboot <source> [/l <locale>] [/s <volume-letter>] [/f <firmware>] [/v]
[/m <OS Loader ID>] [/addlast]

source      Specifies the location of the windows system root.
/l          Specifies an optional locale parameter to use when
            initializing the BCD store. The default is US English.
/s          Specifies an optional volume letter parameter to designate
            the target system partition where boot environment files are
            copied. The default is the system partition identified by
            the firmware.
/v          Enables verbose mode.
/m          If an OS loader GUID is provided, this option merges the
            given loader object with the system template to produce a
            bootable entry. Otherwise, only global objects are merged.
/d          Specifies that the existing default windows boot entry
            should be preserved.
/f          Used with the /s command, specifies the firmware type of the
            target system partition. Options for <firmware> are 'UEFI',
            'BIOS', or 'ALL'.
/addlast    Specifies that the windows boot manager firmware entry
            should be added last. The default behavior is to add it
            first.

Examples: bcdboot c:\windows /l en-us
          bcdboot c:\windows /s h:
          bcdboot c:\windows /s h: /f UEFI
          bcdboot c:\windows /m {d58d18e6-df53-11dc-878f-00064f4f4e08}
          bcdboot c:\windows /d /addlast
C:\Windows\system32>
```

FIGURE 1-5 Type **bcdboot /windows** to view available parameters for the command.

You should be familiar with these *bcdboot* parameters:

- **/l** specifies an optional language for the BCD Store. The default is U.S. English.
- **/s** specifies a volume letter for the system partition. This shouldn't be used in typical deployment scenarios but can be used to specify a system partition for a drive on a USB flash drive or a secondary hard drive. The default is the partition designated in the firmware.
- **/v** specifies verbose mode, which provides details regarding what the computer is doing and what drivers and software it's loading during startup.
- **/m** specifies that you want to merge the values from an existing startup entry into a new startup entry. This option merges only global objects by default. You can specify an operating system loader GUID to merge a specific loader object.
- **/d** specifies that you want to preserve the existing startup entry.
- **/f**, when used with **/s**, specifies the firmware type. Options are *UEFI*, *BIOS*, and *ALL*.

You can view the current partitions for any Windows 8.1 computer in Disk Management, as shown in Figure 1-6.

MORE INFO BCDBOOT

TechNet offers a lot of information about BCDboot. You can start at <http://technet.microsoft.com/en-us/library/hh824874.aspx>.

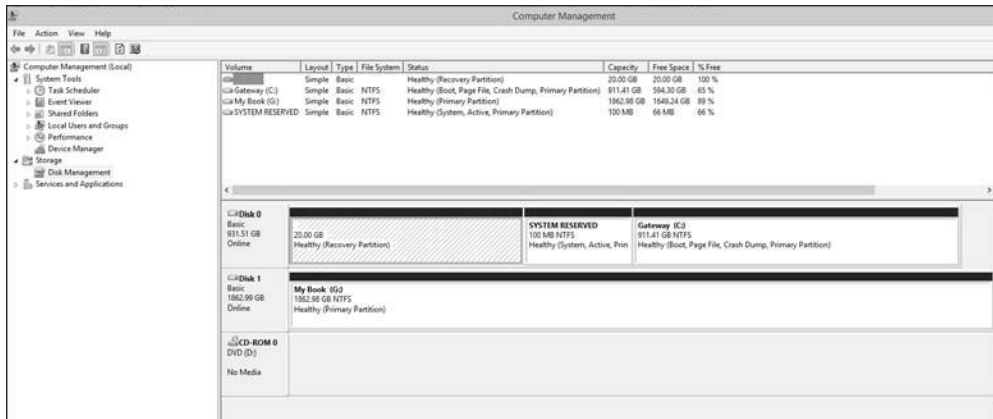


FIGURE 1-6 View partitions in Disk Management.

Adding a native VHD to the startup menu

A virtual hard disk (VHD) is a single file that functions as a unique, separate drive with its own operating system. If you studied for Exam 70-687, Configuring Windows 8.1, you learned how to create a VHD inside an existing operating system by using the Disk Management console, and then how to install Windows on it by using tools in the Windows Assessment and Deployment Toolkit (ADK). You learned how to attach the VHD and then run it “on top of” your Windows 8.1 default installation in its own separate window and space. In this instance, the VHD had a parent operating system.

VHDs can also run on their own, without the need for a parent operating system. These are called native VHDs. You can create a native VHD and use it to start by using the computer's actual hardware. This is easier to do if the computer already has an operating system on it, but it's not required that it does. In fact, you can run this kind of VHD on a computer with no existing virtual machine or hypervisor.



EXAM TIP

Read “Understand Virtual Hard Disks with Native Boot” at <http://technet.microsoft.com/en-us/library/hh825689.aspx>. You'll be glad you did.

Adding a native VHD to a computer with an operating system

If the computer has an operating system, you can create and attach a VHD by using the Disk Management console. From the Action menu select Create VHD to get started. Then use the Action menu again to attach the newly created VHD. (Creating a VHD was covered in *Exam Ref 70-687: Configuring Windows 8.1*.)

MORE INFO USING DISKPART

If you can't or don't want to create and/or attach the VHD via Disk Management, you can do it at an Administrator command prompt via DiskPart. You can also attach the VHD during a Windows installation by pressing Shift+F10 on the Where Do You Want To Install Windows page. There you use the DiskPart commands *select vdisk file=* and *attach vdisk*, among others. You can learn more about DiskPart at <http://support.microsoft.com/kb/300415>.

With the VHD created and attached, you can now work through the following general steps:

1. Start the computer by using a DVD or USB drive that contains a Windows 8.1 Enterprise image (or whatever you want to install). This can be a simple installation DVD or something you've created via other methods.
2. Opt to start to the DVD or USB drive, and start the installation process.
3. When you get to the Windows Setup page that asks where you want to install Windows, choose the partition that houses the VHD you created. If you don't see it, you might have to restart at step 1 and press Shift+F10 to attach the VHD.
4. Work through the rest of the installation process as prompted.
5. When installation is complete, on restart, you'll see two entries, one for the existing operating system and one for the new VHD. The new VHD should be on top.

Adding a native VHD to a computer without an operating system

If a computer doesn't have an operating system, you need some way to communicate with it and make the desired configurations—in this case, adding a native VHD to the startup menu. You do this by creating and using a Windows Preinstallation Environment (Windows PE) 8.1 disk and a Windows Image (.wim) file.

To get started, you need to install the Windows ADK on another Windows 7 or Windows 8-based technician computer. Use the Windows ADK to create the Windows PE disk. You use this disk and various tools to apply the .wim you want to install. You use the Deployment Image Service and Management (DISM) tool to apply an existing Windows 8 image, perhaps one you created for your enterprise (or to modify the image). This image can include drivers, for example.

IMPORTANT ADDING A NATIVE VHD

The steps described in this text for adding a native VHD should not be followed exactly, and should instead be adapted as required for your enterprise environment.

Assuming that the computer doesn't have an operating system on it and has at least 30 GB of free disk space, you first must use the DiskPart tool to create, attach, partition, and format a new virtual hard disk. At a command prompt, type the following, noting that you can generally use different parameters than what you see here for size, type, drive letter, and so on as desired:

```
Diskpart
create vdisk file=C:\windows.vhdx maximum=25600 type=fixed
select vdisk file=C:\windows.vhdx
attach vdisk
create partition primary
assign letter=v
format quick label=vhdx
exit
```

To apply the desired Windows image and to use the DiskPart tool to detach the virtual disk after applying it, type

```
Dism /apply-image /imagefile:install.wim /index:1 /ApplyDir:V:\
diskpart
select vdisk file=C:\windows.vhdx
detach vdisk
exit
```

To copy the VHDX file to a network share or USB hard drive, if applicable, type

```
net use n: \\server\share\
md N:\VHDXs
copy C:\windows.vhdx n:\VHDXs\
```

Start the destination computer with the Windows PE disk, and then format the hard disk and create a system and primary partition. Type

```
Diskpart
select disk 0
clean
create partition primary size=350
select partition 1
format fs=ntfs label="System" quick

active
create partition primary
format fs=ntfs label="Windows" quick
assign letter=c
exit
```

Copy the VHDX file and attach it on the destination computer by typing the following:

```
copy N:\VHDXs\Windows.vhdx C
diskpart
select vdisk file=C:\windows.vhdx
attach vdisk
```

Note the letter given to the VHD in the volume list. To exit the DiskPart tool, type

```
list volume
select volume <volume_number_of_attached_VHD>
assign letter=v
exit
```

Copy the boot-environment files from the \Windows directory in the VHD to the system partition. The BCDboot tool creates the BCD configuration required to start from the VHD.

Type

```
cd v:\windows\system32
bcdboot v:\windows
```

Use the DiskPart tool to detach the virtual disk and then restart the destination computer.

Type

```
Diskpart
select vdisk file=C:\windows.vhdx
detach vdisk
exit
```

On restart, the Boot Manager starts via the .vhdx file.



EXAM TIP

Spend some time studying the terms associated with hard disks: GPT, MBR, UEFI, BIOS, and so on.

Working with multiboot systems

A multiboot system has two or more operating systems installed on it. In a multiboot configuration, each operating system uses its own unique partition, and the operating systems are completely independent of one another. Most network administrators use (or formerly used) multiboot systems to test new operating systems and to determine compatibility with existing software and hardware. Most end users choose this type of setup when they need to run a legacy application that isn't compatible with Windows 8.1 and can't be forced into compatibility with Program Compatibility Mode. (Most users don't understand, have never heard of, or can't configure a VHD to resolve these kinds of problems.)

Creating a multiboot system is easier than you might think, assuming that your computer has a large enough hard drive to create a new partition for a second operating system. Only a few steps are involved: Shrink an existing partition so that you can use the new, unused space to create a second partition; create the new partition; and then install the operating system on it. You use Disk Management to shrink a partition:

1. Press the Windows logo key+R to open a Run dialog box.
2. In the Run dialog box, type **diskmgmt.msc**.

3. Select a partition, likely C, to shrink. Right-click this partition and select Shrink Volume (see Figure 1-7).

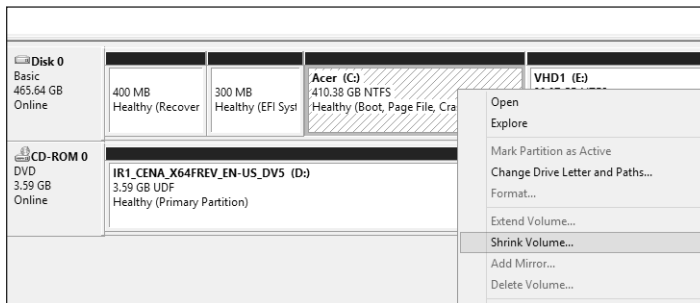


FIGURE 1-7 Shrink a volume to make room for a new partition.

4. Enter the amount of space to shrink in megabytes. You might opt for 40000. Click Shrink.
5. Right-click the new unallocated space and select New Simple Volume.
6. In the New Simple Volume Wizard, click Next, and then specify the volume size in megabytes. You can select the default size and click Next.
7. On the Assign Drive Letter Or Path page, leave Assign The Following Drive Letter selected and choose a letter. Click Next.
8. On the Format Partition page, leave the defaults selected, but type a name for the new partition in the Volume Label box. Click Next.
9. Click Finish.

You should see the new partition in the Disk Management window. You can now insert a bootable DVD that contains the operating system you want to install. Restart the computer, start to the DVD, and during the installation process select Custom to select the new partition. Windows installs the second operating system onto that partition. After the installation is complete, you should see the new operating system as an option at startup. Remember, you can change the defaults from the Startup And Recovery dialog box detailed earlier in this chapter.

Managing desktop images

Network administrators can opt to use a standard Windows Image (.wim) file to perform installations on their enterprise workstations. The standard image is the out-of-the-box installation file you receive when you purchase a Windows 8.1 DVD. When taking this route, you must then, using some method, also install the desired Office applications, device drivers, and so on, and configure each computer so that it meets company standards. Because this is quite time-consuming, enterprise administrators often opt to create a custom Windows image

that contains all these things and more, so that fewer after-the-installation tasks need to be completed.

Beyond building your own images, you must also design and implement a way to move existing user data from the old machine to the new or, if the installation is performed on a single PC, to move it off and then back on when the installation is complete. You can do this in several ways, including by using Windows Easy Transfer for small migrations or the User State Migration Tool (USMT) for large ones. If neither fits the scenario, you can opt to manually move data off the PC and then back on. Beyond even that, installations of images (and the folders that hold them) might also include custom answer files to limit the interaction required during the installation process.

Knowing what you'll see on the exam is difficult with regard to managing desktop images, because the area of study is extensive. You might need to know how to create or deploy a custom image, or only how to modify an existing image. You might be required to know how to include options to migrate user data during image deployment, or you might not. The goal of the next few pages is to introduce you to many of the facets of desktop imaging, but because everything can't be covered, links are provided where you can learn more.



EXAM TIP

With regard to USMT, which you'll learn about in this section, make sure that you are familiar with some of the terms associated with it, including but not limited to MigDocs, MigApp, /nocompress, /hardlink, and others that you'll find at <http://technet.microsoft.com/en-us/library/hh825256.aspx>.

Understanding desktop images

An image is an installation file. An image can be customized so that it is unique to the company and meets the company's specific needs. In larger enterprises, administrators likely create multiple desktop images. One image might be for the Sales team's laptop computers, another for the desktop computers in the Human Resources department, and another for the tablets used by high-ranking administrators. These images can be used for more than just installations, though. When a computer needs to be reimaged—perhaps when a user leaves the company or a computer becomes unstable—you can use the desired image to reinstall the computer quickly. By using data stored on network servers, you can quickly transfer user data also. Desktop images can also be serviced rather than rebuilt if an image itself becomes corrupt.

Images can contain device drivers, applications, specific settings for the desktop background, and so on. A *thin* image has little or no customization, and most of the device drivers, applications, and updates are installed by using another method on each client computer. A *thick* image includes applications, device drivers, and updates (for example) and requires much more planning, network bandwidth, and other resources than thin images. A *hybrid* image is lightly customized. It might be used as a base image for an entire organization's desktop computers. Thin images are recommended in most instances because they can

reduce installation time, maintenance time, storage requirements, and costs, for example. The Microsoft Deployment Toolkit (MDT) makes using thin images with the Lite-Touch, High-Volume Deployment strategy pretty straightforward for experienced network administrators. For more information, visit <http://technet.microsoft.com/en-us/windows/dn282138>.

Creating a desktop image

To create an image, you need the MDT, the Windows ADK, and a file server to hold the installation files (as a share). When you're ready to deploy that image, you need media that you can use to start the computers during deployment or a server configured with the Windows Deployment Services (WDS) role, and network cards on the PCs to upgrade that can start to the installation image. If you have all this in place, you should create an image and deploy it as Lite-Touch, High-Volume Deployment if your enterprise has between 200 and 500 computers, or use a Zero-Touch, High-Volume Deployment if your enterprise has 500 or more machines.



EXAM TIP

Although you won't be asked how to configure a WDS server, you might be asked how you would start a machine so that it could connect to it. Often the answer includes customizing a Windows PE image and booting the machine with it. The image can point the machine to the desired WDS server and deployment image, for example.

Many steps are involved in creating a custom installation, and a high-level outline is provided here:

1. On a technician computer, install the Windows ADK. (Note that you also can use Microsoft Hyper-V to build an image.)
2. Create a share on the network to hold the installation files and other files related to the deployment of Windows 8.1, such as the answer file. (An answer file can be created to answer some of the questions posed during the installation, such as the language or time zone, or even what partition to install the image to.)
3. Create a reference computer that can serve as a template for the desktop image you want to create, complete with all the software you want to install, language packs, settings, required device drivers, custom wallpapers, and anything else you want to include.
4. Prepare the reference computer for imaging by removing certain values unique to the reference computer. Use the following commands:
 - `Sysprep /generalize` to remove unique IDs. You might add other command-line options, such as `/oobe`, to give the installation an "out-of-the-box" experience.
 - `Copyype.cmd` to create a Windows PE startup disk, with the proper command-line options such as `c:\winpe` (to note the location of the required Windows PE files).

- *Oscdimg.exe* to package the Windows PE files into a sector-based image file, along with proper command-line options.
- 5. Capture an image of the reference computer that results in an image file. By using this file, you can install as many desktops as you want and apply your image to all of them to create uniformity. Use these commands in place of the deprecated command *ImageX* along with *net use*, appropriately adapted for your enterprise:
 - *Dism /Capture-Image /ImageFile:c:\myimage.wim /CaptureDir:C:\ /Name:"Myimagecapture"*
 - *Dism /Capture-Image /ImageFile:s:\mysystempartition.wim /CaptureDir:S:\ /Name:"Mysystempartition"*
 - *Net use* with command-line options including something like *z: \\server\share* to denote the location of the network share where the files are stored
- 6. Create an answer file to automate the installation partially or an unattended answer file to completely automate the answers asked during installation. Use tools including Windows System Image Manager (SIM, available in Windows ADK) to select the image and create and apply the answer file.
- 7. Start the target computers with either a Windows PE disk or a boot image that the computer can download from the server.
- 8. Apply the reference computer image to create your duplicate workstations. This can include copying and applying the desired image.



EXAM TIP

You will probably see questions that ask when you would use a specific tool such as SysPrep, a Windows PE disk, DISM, and so on. Make sure that you understand what each tool is used for, why, when, and how.

Modifying or repairing a desktop image

If you create an image and then need to modify it, you can use the DISM command-line tool, available from the Windows ADK. You learned a little about this tool earlier in the chapter when you saw how to add a native VHD to a computer without an operating system. There, you used it to mount the installation file.

You should know some more facts about DISM:

- You can use it to install, uninstall, configure, and update Windows features, packages, drivers, and international settings in an existing .wim file.
- You can use the DISM servicing commands to make changes to a VHD.
- DISM commands are generally used on offline images, but servicing a running operating system is possible.
- You can use DISM to repair an image.

Use the commands in Table 1-3 to repair an image.

TABLE 1-3 Commands for repairing an image

Action	Command
To check for corruption	<i>Dism /Online /Cleanup-Image /ScanHealth</i>
To check whether corruption has been detected	<i>Dism /Online /Cleanup-Image /CheckHealth</i>
To repair an offline image by using a mounted image as a repair source	<i>Dism /Image:C:\offline /Cleanup-Image /RestoreHealth /Source:c:\test\mount\windows</i>
To repair an image by using your own sources without involving Windows Update	<i>Dism /Online /Cleanup-Image /RestoreHealth /Source:c:\test\mount\windows /LimitAccess</i>

To modify an image, you need to know quite a bit more about DISM. You can find command sets that enable you to do the following:

- Add or remove drivers.
- Enable or disable Windows features.
- Add or remove language packs.
- Sideload apps.
- Customize the Start screen.

This isn't a complete list, of course. Each modification requires that you type a set of commands. For example, to add or remove a language pack, assuming that your image is already mounted (this is the easiest to achieve), you would follow this sequence:

1. On the Start screen, type **Deployment**, and then right-click Deployment and Imaging Tools Environment.
2. Click Run As Administrator.
3. Type the following commands, in order:

```
Dism /Get-MountedImageInfo
```

```
Dism /Image:C:\test\offline /ScratchDir:C:\Scratch /Add-Package /PackagePath:C:\packages\package1.cab /PackagePath:C:\packages\package2.cab ...
```

```
Dism /Commit-Image /MountDir:C:\test\offline
```

4. To configure international settings, type these commands, in order:

```
Dism /Mount-Image /ImageFile:C:\test\images\install.wim /Index:1 /MountDir:C:\test\offline
```

```
Dism /Image:C:\test\offline /Set-SKUIntlDefaults:en-us
```

```
Dism /Unmount-Image /MountDir:C:\test\offline /Commit
```

The Windows image is now ready to be deployed.

MORE INFO USING DISM

You can learn more about DISM at <http://technet.microsoft.com/en-us/library/hh824821.aspx>. You can learn how to perform tasks such as adding or removing drivers or customizing the Start screen at <http://technet.microsoft.com/en-us/library/hh825239.aspx>.



EXAM TIP

The MDT includes DISM PowerShell cmdlets, DISM API, Windows SIM, and OSCDIMG. It also includes the Volume Activation Management Tool (VAMT), Windows Performance Toolkit (WPT), Windows Assessment Toolkit, and Windows Assessment Services. Make sure that you are familiar with these tools. An overview is available at <http://msdn.microsoft.com/en-us/library/windows/hardware/hh825486.aspx>.

Using Windows Easy Transfer and the User State Migration Tool

You can use the Windows Easy Transfer (WET) Wizard to migrate user data (such as profile information) off a computer to complete a clean installation on it. After the installation is complete, you can migrate the data back. You also can use WET to move data from one computer to another. You would use this method to migrate data only for a small number of computers; you wouldn't want to use it in an enterprise.



EXAM TIP

You can't use WET to transfer files from a 64-bit operating system to a 32-bit operating system (USMT doesn't work either). In this case, you should back up files manually.

You can use the scriptable command-line User State Migration Tool (USMT) to migrate user data from a previous edition of Windows to Windows 8.1. By using USMT, you can copy the user data you select, exclude any data that doesn't need to be migrated, and then transfer the selected data back to the computer after it's installed clean with Windows 8.1. You can also transfer the data to a brand new or newly installed Windows 8.1 computer.

USMT provides much of the same functionality as Windows Easy Transfer. However, although USMT has the same basic capabilities as WET, USMT is a command-line tool and WET is graphical. This isn't a disadvantage in a large organization, because administrators can use USMT to incorporate USMT tasks into scripts, which are better suited for domains, enterprises, and automated deployments. (Scripts, task sequences, answer files, and so on are what help automate a deployment.) Two tools included with USMT are ScanState and LoadState, both command-line tools. When you use USMT, you'll also use Windows PE, which you learn about next.



EXAM TIP

Windows PE and USMT are available in the Windows ADK; you might be required to know this to select the proper solution, given a scenario. You also might see an exam question regarding ScanState and LoadState and their related parameters. To learn about the parameters available for these two commands, refer to the USMT Technical Reference sheet offered at <http://technet.microsoft.com/en-us/library/hh825256.aspx>.

MORE INFO USING MDT

No matter how many images you create and store, you can use MDT to manage and maintain them. MDT 2013 supports the Windows ADK for Windows 8.1, supports the deployment of Windows 8.1, and supports zero-touch installations if you also use System Center 2012 R2 Configuration Manager.

Customizing a Windows installation by using Windows Preinstallation Environment (Windows PE)

When you create a custom installation, you also create a Windows PE disk. It's unique to your image. You can use the Windows PE disk to start the installation process on a client computer. Before focusing more on this, though, you should look at what Windows PE actually is.

Exploring Windows PE

The startup process has changed over the years. When Windows ME was retired, so was MS-DOS. Windows 8, Windows 7, and Windows Vista no longer rely on MS-DOS for any part of the installation and startup process. To replace MS-DOS, Windows uses Windows PE, a minimal operating system that you can use to prepare a computer for a Windows installation. Windows PE can start a computer that has no operating system or has other problems. When deploying Windows 8.1, you can use Windows PE to partition and format hard drives, copy disk images to a computer, and initiate Windows Setup from a network share. You can create a Windows PE disk by using the tools in the Windows ADK. With regard to USMT, you use a customized Windows PE startup disk to start the source computer (the computer that holds the files to migrate) and use the tools available on the disk to collect the data you want to migrate.



EXAM TIP

Windows PE can help you deploy custom Windows 8.1 images to computers. It can also help you create disk partitions and format hard drives, but most notably it helps initiate an installation from a network share. Also, something called the Windows Recovery Environment (Windows RE) is built from Windows PE, which makes sense. Both assist in installations (and recovery).

Windows PE offers the following improvements and advantages over MS-DOS. As you read through this list, think about how important each item is to automated and custom operating system deployments:

- Native 32-bit or 64-bit support (MS-DOS is a 16-bit operating system)
- Native 32-bit and 64-bit driver support, or the ability to use the same drivers as a full Windows 8 installation
- Internal networking support
- Internal NTFS support
- Scripting language support for a subset of Win32 application programming interface (API), Windows Management Instrumentation (WMI), Windows Data Access Components (Windows DAC), HTML Applications (HTAs), and Windows Script Host (You can create scripts that are much more robust than the MS-DOS batch files.)
- Myriad startup options, including CDs, DVDs, USB devices such as flash drives, a temporary folder on a hard disk, RAM disk, network share, and Windows Deployment Services (WDS) server
- Support for offline sessions and offline servicing of images
- Inclusion of Hyper-V drivers (except display drivers), which enables Windows PE to run in a hypervisor (support includes mass storage, mouse integration, and network adapters)

Windows PE has various restrictions, not limited to the following:

- It restarts after 72 hours, so it can't be used as an operating system for the long term.
- It supports TCP/IP and NetBIOS over TCP/IP, but doesn't support other methods, such as the Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) network protocol.
- It doesn't support applications that are packaged via Windows Installer (.msi) files.
- It doesn't support cross-platform scenarios, like installing a 64-bit Windows image on a 32-bit computer (among others).

MORE INFO WINDOWS PE

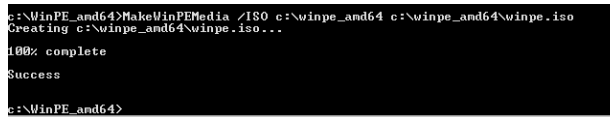
Visit <http://technet.microsoft.com> and type **What is Windows PE?** in the Search box to locate related technical information.

Copying the Windows PE files and creating a standard Windows PE DVD disk

You need to copy the Windows PE files to your computer before you can work with them or create a custom Windows PE disk. You can copy and create 32-bit or 64-bit sets, or both, using the *Copype* command as detailed in the following steps. You can also create an ISO file if you want to create a standard, bootable Windows PE DVD. You must complete steps 1–3 before you can continue with the next section.

To create a standard, bootable Windows PE DVD disk, follow these steps:

1. Install the Windows ADK from www.microsoft.com/en-us/download/details.aspx?id=39982. Also be sure to install the necessary deployment tools: Deployment and Imaging Tools Environment and Windows PE.
2. At the Start screen, type **Deploy** and then right-click Deployment And Imaging Tools Environment. Click Run As Administrator.
3. Type **copyype amd64 C:\WinPE_amd64** (or replace with 32 as applicable). Press Enter.
4. Insert a writeable DVD into the appropriate drive.
5. Type **MakeWinPEMedia /ISO C:\winpe_amd64 c:\winpe_amd64\winpe.iso**. Press Enter.
6. Verify that Success appears (see Figure 1-8).



```
c:\WinPE_amd64>MakeWinPEMedia /ISO c:\winpe_amd64 c:\winpe_amd64\winpe.iso
Creating c:\winpe_amd64\winpe.iso...
100% complete
Success
c:\WinPE_amd64>
```

FIGURE 1-8 Create a Windows PE ISO file.

7. If desired, in File Explorer, navigate to C:\winpe_amd64, right-click winpe.iso, and select Burn To Disc.
8. Follow the prompts to create a DVD. Alternatively, you can wait and customize Windows PE by working through the next section.

Mounting and modifying Windows PE

You can customize Windows PE to meet your own needs. A more common customization is to add device drivers, but you can also add languages, add an app, replace the background image, add answer file settings, add a startup script, and more. Before you continue here, however, make sure that you've installed the required Windows ADK tools and worked through steps 1–3 in the preceding section to install the Windows ADK and copy the appropriate Windows PE files to your hard drive.

As an example of what you can do, you can follow these steps to mount and modify a Windows PE image specifically to change the desktop background:

1. At the Start screen, type **Deploy** and then right-click Deployment And Imaging Tools Environment. Click Run As Administrator.
2. Mount the PE Image. Type **Dism /Mount-Image /ImageFile:"C:\WinPE_amd64\media\sources\boot.wim" /index:1 /MountDir:"C:\WinPE_amd64\mount"** (see Figure 1-9).

```

C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment
Tools>diskpart /mount-image /imagefile:"C:\winpe_amd64\media\sources\boot.wim" /ind
ex=1 /mountdir:"C:\winpe_amd64\mount"

Deployment Image Servicing and Management tool
Version: 6.2.9200.16384

Mounting image
[=====100.0%=====]
The operation completed successfully.

C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment
Tools>

```

FIGURE 1-9 Use DISM to mount Windows PE.

Before you can customize Windows PE by replacing the background image, you must first change the security permissions of the background image file so that you can modify it. The default image file is at `\windows\system32\winpe.jpg`. Follow these steps to make the required modifications:

1. In File Explorer, navigate to `C:\WinPE_amd64\mount\windows\system32`.
2. Right-click the `winpe.jpg` file and select Properties, Security tab, Advanced.
3. Next to Owner, select Change.
4. In the Enter The Object Name To Select box, type **Administrators** and press Enter.
5. Click Apply and then OK. Click OK again.
6. Right-click the `winpe.jpg` file and select Properties, Security tab, Advanced.
7. Click Administrators and then Edit.
8. Click Administrators, and select the Full Control Allow check box to give Administrators full access (see Figure 1-10).

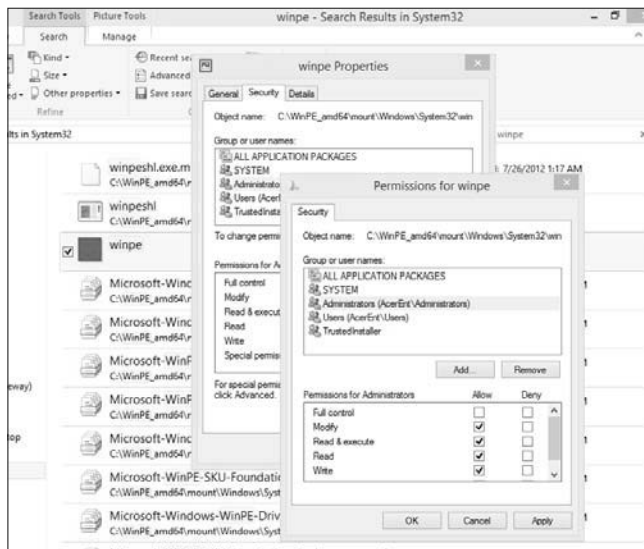


FIGURE 1-10 Change required permissions.

9. Click OK twice.

10. Replace the winpe.jpg file with your own image file.

To learn how to perform other customizations, you can refer to the steps at <http://technet.microsoft.com/en-us/library/hh824972.aspx>. You'll find the commands you need to modify other areas of Windows PE. For example, to add device drivers to the Windows PE image, use these commands at the DISM Administrator prompt:

- To add a device driver: *Dism /Add-Driver /Image:"C:\WinPE_amd64\mount" /Driver:"C:\SampleDriver\driver.inf"*
- To verify that driver packages have been added: *Dism /Get-Drivers /Image:"C:\WinPE_amd64\mount"*

To add an app, use these commands:

- To create an app directory: *md "C:\WinPE_amd64\mount\windows\<MyApp>"*
- To copy the app files: *Xcopy C:\<MyApp> "C:\WinPE_amd64\mount\windows\<MyApp>"*
- To test the app by booting Windows PE and running the application from the X directory: *X:\Windows\System32> X:\Windows\<MyApp>*



Thought experiment

Testing a Windows Image before deployment

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You created a Windows Image (.wim) file that you want to deploy across your organization. You want to test it thoroughly before performing the deployment—specifically, you want to test it against the same hardware your desktops use. You want to do this with a VHD. You've chosen to use a computer that now has no operating system on it.

1. What term is used to describe a VHD that you install on a computer with no parent operating system?
2. What application should you use to create the required Windows PE disk?
3. Your image is ready to go. What application or tool can you use to apply that image?
4. How much free hard disk space does this computer need to have to support this VHD?

Objective summary

- You can use Windows To Go to work from any computer that enables you to start to a USB drive and meets Windows To Go host requirements.
- You can use Group Policy to control how Windows To Go and the host interact.
- Startup settings determine how a computer starts by default, and many tools are available to help you manage the startup process, including but not limited to BCDedit and BCDboot.
- You can add a native VHD to the startup menu and start to it, even if no parent operating system exists.
- Multiboot systems house two or more operating systems, each on its own partition.
- Enterprise administrators often create specialized, personalized installation images for deployment in their organizations.
- You can modify and repair desktop images rather than rebuild them.
- Windows PE is a preinstallation environment that you can use to install a new operating system, for example, or repair one. It replaces the older MS-DOS and offers many more features.
- You can create customized Windows PE images and add your own drivers, apps, Start screen configurations, and more.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. Which of the following are true regarding Windows To Go? (Choose all that apply.)
 - A. You can create a Windows To Go workspace only from a Windows 8-based Enterprise edition computer, and you need the Windows 8-based Enterprise installation files to do so.
 - B. The USB drive must be at least 32 GB or larger and must be Windows To Go certified.
 - C. You can't use a Trusted Platform Model (TPM) with Windows To Go drives.
 - D. When a Windows To Go drive starts having problems, you can refresh or restore it by using recovery options in PC Settings.
 - E. You can use Windows To Go when a Windows RT computer is the host.

- 2.** You want to host Windows To Go on your personal computer but don't want to allow the computer to hibernate. How should you configure Local Group Policy?
- A.** Disable Allow Hibernate (S4) when starting from a Windows To Go workspace or leave the default, Not Configured.
 - B.** Enable Allow Hibernate (S4) when starting from a Windows To Go workspace.
 - C.** Disable Disallow Standby Sleep States (S1-S3) when starting from a Windows To Go workspace.
 - D.** Enable Disallow Standby Sleep States (S1-S3) when starting from a Windows To Go workspace.
- 3.** Where are the startup configuration parameters stored?
- A.** Boot.ini
 - B.** BCD Editor (BCDedit)
 - C.** BCDboot
 - D.** BCD Store
- 4.** You need to create a new, empty startup configuration store and configure what starts by default. You plan to use BCDedit. What two command parameters do you use?
- A.** */import*
 - B.** */create store*
 - C.** */boot sequence*
 - D.** */default*
 - E.** */displayorder*
 - F.** */new*
- 5.** You have a Windows 8.1 computer with a 500-GB hard drive, all available from the C drive. You're using only a small portion of that hard drive now. You want to create a multiboot system that runs both the existing Windows 8.1 operating system and Windows 7. What do you do first?
- A.** Start to the Windows 7 DVD.
 - B.** Create a new simple volume.
 - C.** Open Disk Management and shrink the C partition.
 - D.** Format the drive.

6. What type of custom image includes many applications, device drivers, and updates and requires a lot of planning, network bandwidth, and other resources?
- A. Thin
 - B. Thick
 - C. Hybrid
 - D. All custom images include these things.
7. Which of the following do you need to create your own custom image?
- A. MDT
 - B. Windows ADK
 - C. A network share
 - D. A reference computer
 - E. All of the above
 - F. B, C, and D
8. To create an image and then modify it, you need the DISM command-line tool, which is available from which of the following?
- A. MDT
 - B. Windows ADK
 - C. SIM
 - D. ACT
9. Which of the following commands might you use to copy the Windows PE files from Windows ADK to your hard drive?
- A. *copyype amd64 C:\WinPE_amd64*
 - B. *copyype amd32 C:\WinPE_amd32*
 - C. *MakeWinPEMedia /ISO C:\winpe_amd64 c:\winpe_amd64\winpe.iso*
 - D. *Dism /Get-MountedImageInfo*
10. Which of the following does MDT include?
- A. DISM PowerShell cmdlets
 - B. DISM API
 - C. Windows System Image Manager (Windows SIM)
 - D. OSDIMG
 - E. The Volume Activation Management Tool (VAMT)
 - F. All of the above
 - G. Only A, B, C, and D

Objective 1.2: Support desktop apps

Although Windows 8.1 comes with a set of default apps on the Start screen, these aren't widely used in large enterprises by end users who need to perform work. Instead, administrators often opt to install traditional desktop apps. This isn't to say that apps aren't used at all; they are. In fact, administrators can (and do) create their own apps and make them available using a process known as sideloading, detailed later in Objective 1.3. However, this objective focuses on supporting only desktop apps.

Quite a few issues can arise while supporting desktop apps. The desktop app might not be compatible, period. Because you need to know this sooner rather than later, you use the Application Compatibility Toolkit (ACT) to determine how widespread the problem is and learn how to fix it before proceeding with an organization-wide installation of Windows 8.1 or the application after the fact. Other issues include the need to run two or more versions of an app side by side, and in these cases and similar scenarios you might opt for technologies such as Hyper-V, RemoteApp, and AppV. You might also opt to run a problematic or noncompliant app virtually or remotely. Other options available for additional desktop app scenarios and functionality include User Experience Virtualization (UE-V) and Windows Intune, which also are discussed in this section.

This objective covers how to:

- Support desktop app compatibility by using ACT, including shims and compatibility databases
- Support desktop application coexistence by using Hyper-V, RemoteApp, and App-V
- Support installation and configuration of User Experience Virtualization (UE-V)
- Deploy desktop apps by using Windows Intune

Supporting desktop app compatibility by using ACT

ACT is included with the Windows ADK and can be used to detect which enterprise applications, devices, and computers will likely be incompatible (or cause problems) with Windows 8.1 after installation. ACT can also help you find solutions to those problems.

ACT is used in stages:

1. You have to install all of the required software and set up or have previously set up an ACT database.
2. You need to inventory computers and applications in your enterprise. This lets ACT know what to test.

3. You need to gather compatibility information based on what's found by testing for compatibility on the desired platform and comparing that to known issues.
4. You need to test applications and obtain compatibility results.
5. You need to analyze the data.
6. You finally can implement solutions and test again.

Before you dive into the inventory process (the first step to using ACT), look at what ACT includes.

NOTE PREPARING FOR THE ACT

If you haven't yet installed Windows ADK on your computer, do that before continuing. Alternatively, you can download and install just ACT for Windows 8.1. To use ACT, you also need an active and compatible SQL Server database.

Understanding ACT tools and how to get started

You should be familiar with several ACT tools before working with the program:

- The Windows Assessment Console is a graphical user interface that enables you to group assessments, create and run jobs, and view and manage the results of those jobs.
- Assessments are a combination of files that induce specific states on a computer for the purpose of measuring activities during testing. These assessments provide a starting point for necessary remediation.
- The Assessment Platform comprises the items necessary to develop assessments, extend assessments, and reliably run jobs and display results.

As noted previously, you have to set up or have previously set up an ACT database before you can use ACT. The requirements for doing so include having in place a SQL Server database that stores your enterprise inventory, as well as .NET Framework 4. If you have all of that, you can begin to work through the wizard available from the Microsoft Application Compatibility Manager, which guides you through the setup process. The wizard also helps you create an ACT log share, where the collected log files can be stored, and set up an ACT Log Processing Service user account, which has read and write access. To get started, at the Start screen type **application compat**, and click Application Compatibility Manager. (You need to run this with elevated privileges.)

Creating an inventory collector package

You create an inventory collector package to collect information about the computers in your enterprise. The data collected includes hardware information such as memory capacity and processor speed, as well as information about the make and model of those PCs. Of course, it also inventories the installed software so that you can later determine whether that software

is compatible with the Windows edition you want to install. (If you have hundreds of computers, you can likely inventory them all; however, if you have thousands, you can opt to inventory representative groups of computers. You can do this only if you have groups of computers on similar platforms and with similar installations.)

To create an inventory collector package, follow these steps:

1. Open the Microsoft Application Compatibility Manager.
2. Click File, and then click New.
3. Click Inventory Collection Package.
4. Input the required information (name, output location, and label) and click Create.
5. Browse to the location to save the required Windows Installer (.msi) file for the package. You might opt for a network share that can be reached by client computers.
6. Type a name for the file and click Save.
7. Click Finish.

Deploying the inventory collector package

Now you must deploy the package you created. If your network isn't too large and your users are computer-savvy, you might opt to send an email with a link to the deployment folder and let the users install the package themselves. You could also burn the .msi file to a DVD or other removable media and pass that around. Users need administrator privileges either way. Alternatively, you can opt for a Group Policy software installation. This requires more infrastructure, but you would probably already have the required items in place in a large organization. For Group Policy to work, the computers you want to inventory need to be part of the Active Directory forest; you'll need to create a Group Policy Object (GPO) for publishing; you'll need to assign the GPO to the appropriate organizational units (OUs); and you'll need to create and publish the software installation.

More complicated ways require scripting or using additional hardware. You can, for instance, assign a logon script. You can also deploy the package by using System Center Configuration Manager.

Creating a runtime-analysis package

The testing compatibility process involves a few steps, all of which must be completed before creating the runtime-analysis package:

1. Decide which applications to test. You can use information gathered from the previous steps to make those decisions.
2. Use the Microsoft Compatibility Exchange to get the latest compatibility ratings.
3. Organize the applications you want to test.

With that complete, you are ready to create your runtime-analysis package:

1. In ACM, click Collect.
2. Click File, and then click New.
3. Click Runtime Analysis Package.
4. Provide the required information (name, output location, and label) and click Create.
5. Browse to the location to save the required Windows Installer (.msi) file for the package.
6. Type a file name for the .msi file, and then click Save.
7. Click Finish.

MORE INFO USING THE MICROSOFT COMPATIBILITY EXCHANGE

During the inventory and testing process, you need to use the Microsoft Compatibility Exchange to compare what you found on your own network with what others also encountered. The exchange collects and stores compatibility data from many places including Microsoft, software vendors, and ACT users (who opt to be part of the ACT community and document and share their own experiences and results). You can sync the data you've collected with data in the exchange from the ACM to share what you've learned with others too:

1. Navigate to the Analyze screen.
2. Click Send And Receive.
3. Click Review The Data Before Sending.
4. (Optional) Click Review All Data.
5. Type a name for the .txt file and click Save.
6. Review the file, as desired.
7. When you are ready to send the data, click Send.

Review what's offered as results arrive and use the information to help your decision-making processes. After your first sync, subsequent syncs include only the changes made since the last synchronization. The process won't resend all the information. Again, updates might be available, or you might be notified that no updates exist.

Deploying a runtime-analysis package

You can now deploy the package. You can use Group Policy, Configuration Manager, a logon script, removable media, a network share, and so on to do so. If you opt to let users work with the package, they'll need to run Microsoft Compatibility Monitor. However you opt to deploy, Compatibility Monitor needs to be run.

To run a deployed runtime-analysis package, follow these steps:

1. On the target computer, open Microsoft Compatibility Monitor. Note that if you run the .msi file Microsoft Compatibility Monitor installs automatically.
2. Click Start Monitoring.
3. Use each application that you want to test for a few minutes.
4. After you test the required applications, click Stop Monitoring. Data is sent automatically to the ACT database.

Reviewing report data

You view application compatibility reports from the ACM. Several types of reports are available, with names such as Computers, Devices, and Internet Explorer Add-ons. What you're interested in here is the Applications report. To open this report, follow these steps:

1. Open ACM.
2. In the Quick Reports pane, click Analyze.
3. In the same pane, under the operating system heading, click Applications.

Here are a few things you'll see in this report:

- Application names
- Application vendors
- Application versions
- The count of active issues for the application
- Whether the information for the application is included in the synchronization process with the Microsoft Compatibility Exchange
- Compatibility ratings unique to your organization
- Compatibility ratings provided by the vendor
- The number of computers that have the application installed

Fixing problems

When application compatibility problems are uncovered, you have to decide how you will deal with them. It might be time to move from a little-known office application suite to something more mainstream, such as Microsoft Office. It might be time to simply retire an application. Or, you might decide (and likely will in most cases) to fix the problem and

continue to use the application. Fixing the problem can involve modifying the code or applying shims.

A common way to fix a compatibility issue is to alter the code. Microsoft recommends this over changing Registry settings or trying other risky or short-term workarounds. Changing the code requires resources (like money and time) on the front end, but the result might be worth it in the end, at least for a while. If you change the source code for Windows, however, you do create a long-term challenge for yourself and future administrators on many levels, including a risk of causing unexpected problems with other applications you run, with Windows Updates, and so on. A better option to consider is to create shims.

UNDERSTANDING SHIMS

If you opt to use the Shim Infrastructure, you can apply the fix (shim) to a specific application and application version only. Shims you create remain independent of the core Windows functions. (If you're unsure of what the word "shim" means, consider this real-life example: When you fold up a piece of paper and place it under a single table leg that is uneven and causing the table to wobble, you're creating a shim.)

Technically, but on a high level, Shim Infrastructure involves application programming interface (API) hooking; the shim redirects API calls from Windows to some other code, which is the shim itself. Windows manages and secures shims just as it would the original application code. Thus, you can't use shims to work around security mechanisms already in place by the operating system, including User Account Control (UAC) prompts. You also can't use a shim to fix kernel-mode code, specifically to fix issues with device drivers. Shims can fix compatibility issues, though, and are often applied as the desired solutions to compatibility problems.

KNOWING WHEN TO USE SHIMS

Deciding to use shims is a process, like anything else. You must first decide whether the problem merits a shim and is worth the time it takes to create it. Here are a few reasons you might opt for a shim:

- The vendor who created the application is out of business and no updates are available. The source code isn't available either, so shims are the only option.
- Your company created the application. If you don't have the time available to rewrite the code, a shim is the next best alternative.
- The vendor is still in business but has yet to create an update or fix, or a company-created application can be modified in the future, but no immediate update is available. In these cases, a shim can work temporarily, until an update or fix becomes available in the future.

CREATING SHIMS

Teaching you how to create a shim for an application is beyond the scope of this book; besides, the number of applications that might need shims is seemingly endless. So, rather than try to address this specifically, this section offers an overview and then points you to a few TechNet articles that can offer overviews and provide solution options.

One tool you might opt to use to resolve application compatibility issues is Compatibility Administrator, available from ACT (see Figure 1-11).

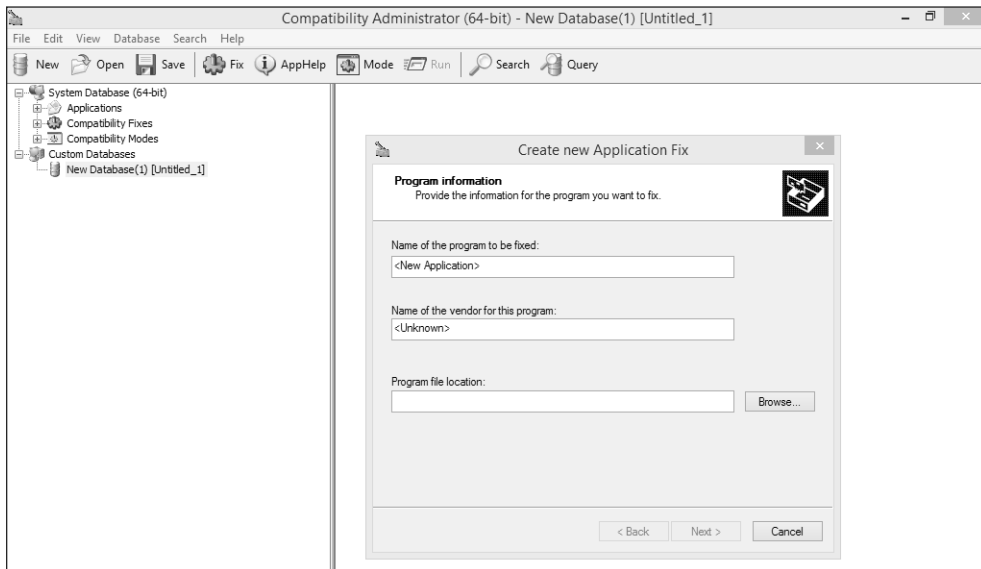


FIGURE 1-11 Compatibility Administrator enables you to create and apply application compatibility fixes.

This tool provides

- Compatibility fixes, compatibility modes, and AppHelp messages that you use to resolve specific compatibility issues
- Tools that enable you to create your own customized compatibility fixes, compatibility modes, AppHelp messages, and compatibility databases
- A tool that you can use to query and search for installed compatibility fixes on your organization's computers

To use this tool, you first create a new compatibility database (.sdb), select your problematic application, and then select and apply the desired fix. You then test that fix and, when you're ready, deploy it throughout your organization. To learn how to use this tool, refer to the Compatibility Administrator Users' Guide at <http://technet.microsoft.com/en-us/library/hh825182.aspx>.



EXAM TIP

If you discover that problems are the result of UAC issues, you can use the Standard User Analyzer (SUA) Wizard to guide you through the process of locating and fixing compatibility issues. Alternatively, you can use the SUA tool (without a wizard) with which you can perform an in-depth analysis first, and then then fix issues on your own. You use the SUA tool to test applications, monitor API calls, and detect issues related to UAC in Windows.

The following TechNet articles provide more detail:

- Compatibility Fixes for Windows 8, Windows 7, and Vista at <http://technet.microsoft.com/library/dn383989.aspx>
- Managing Shims in an Enterprise at <http://technet.microsoft.com/en-us/windows/jj863250.aspx>
- Application Compatibility at <http://technet.microsoft.com/en-us/windows/application-compatibility.aspx>
- Create Shim Database-Management Strategies at [http://technet.microsoft.com/en-us/library/dd835543\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd835543(v=ws.10).aspx)
- Custom Shim Database Deployment at [http://technet.microsoft.com/en-us/library/dd837647\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd837647(v=ws.10).aspx)

Supporting desktop application coexistence

You can further test and run applications on new operating systems by using technologies such as Client Hyper-V, RemoteApp, and App-V. Client Hyper-V lets you run applications on virtual machines (VMs) in a dedicated space you can easily manage. RemoteApp lets you access applications remotely through Remote Desktop Services, and the apps themselves are housed and managed on network servers. App-V lets you virtualize applications so that you can use the applications side by side on the same system. All three options let you test applications in various scenarios before deployment. You can then make decisions based on what solution and environment works best in your enterprise.

Understanding and supporting Client Hyper-V

With Windows 8.1 Pro and Windows 8.1 Enterprise, you can create virtual machines that are housed inside a single operating system on a single computer. These virtual machines can run their own operating systems, and you can separate and secure them with virtual switches. A hypervisor keeps these “child” operating systems separate from the parent operating system. This enables network administrators to combine multiple machines into one, which saves money, power consumption, resources, space, and so on. In Windows 8.1, this technology is called Client Hyper-V and is a free element. With regard to supporting applications, you will install applications that you want to test in these environments to check compatibility, perhaps after shims or other fixes are applied.

To use Client Hyper-V, you’ll need the following:

- Windows 8.1 Pro or Windows 8.1 Enterprise, 64-bit
- Second Level Address Translation (SLAT) processor
- 4 GB of RAM
- BIOS-level hardware virtualization support

If you have a compatible computer, you can create and configure a virtual machine. However, you must first enable Client Hyper-V from Control Panel, under Programs And Features.

Click Turn Windows Features On Or Off, locate Hyper-V, and select all related entries (see Figure 1-12). When it's enabled, click OK and restart the computer. After restarting, you'll have access to two new tiles when you log on as an administrator: Hyper-V Manager and Hyper-V Virtual Machine Connection.

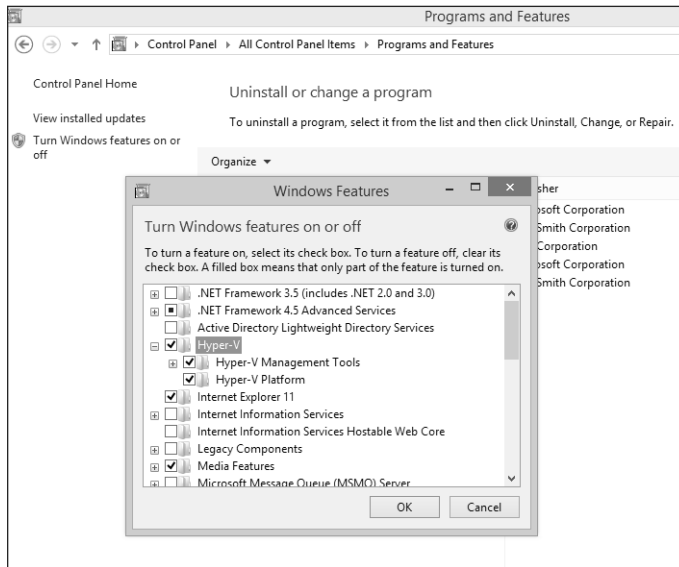


FIGURE 1-12 Enable Hyper-V.

NOTE

You might have to enter the BIOS to enable virtualization support.



EXAM TIP

You can enable Hyper-V in Windows PowerShell with the *Enable-WindowsOptionalFeature -FeatureName Microsoft-Hyper-V -All* command.

IMPORTANT WHEN HYPER-V PLATFORM IS UNAVAILABLE

If you don't see any entries for Hyper-V in the Windows Features dialog box, the computer is either Windows 8.1 (not Pro or Enterprise) or is 32-bit. If you see everything but Hyper-V Platform is unavailable for selection, everything else is okay, but the computer's processor isn't SLAT.

How to create, configure, and then install virtual machines by using the Hyper-V Manager is covered in the book, *Exam Ref 70-687: Configuring Windows 8.1*. This book also covers the

types of virtual switches available and how to create them. You can create three types of virtual switches (from the Action pane, click Virtual Switch Manager):

- External, to let the VM connect to a network interface controller (NIC) on the computer to communicate with the external network, perhaps for the purpose of connecting to the Internet. If you want, it can also be configured to connect to the host computer. The physical NIC can connect to only one network in this scenario.
- Internal, to let the VM communicate with other VMs and to the host computer.
- Private, to let the VM communicate with other VMs but not the host computer.



EXAM TIP

More than likely you'll see something about the three types of virtual switches on the exam: External, Internal, and Private. You also should know that pretty much anything you want to do in the Hyper-V Manager requires you to log on with an administrator account.

Because creating and installing VMs were objectives for Exam 70-687, you wouldn't think you would need to know how to do these things for Exam 70-688. But as you learned earlier in this chapter, the exams will likely have quite a bit of overlap. So learning how to perform these tasks is in your best interest, specifically creating a VM, installing a VM, running a VM, and creating a virtual switch. This section, however, focuses only on supporting application compatibility with Client Hyper-V.

You can install applications on a virtual machine the same way you would install one in any other circumstance. You open Hyper-V Manager, right-click the desired VM and select Connect, in the VM window click Action and then Start, and then perform the desired application installation. During the testing process you can use the Hyper-V snapshot feature to take a snapshot of the original state of the VM so that you can return to a known state after application testing. (Snapshots are now called *checkpoints*.) You manually create a checkpoint to save the state of a virtual machine. This saves all the hard disk's contents, including application data files, settings, and configurations. When you're sure you don't need the checkpoint anymore, you can delete it (because these files can be quite large). Also, checkpoints are portable.

To create a checkpoint, follow these steps:

1. In Hyper-V Manager, click the new VM you just created and configured.
2. As needed, click Action and then Start, or click Action and then Connect.
3. Right-click the VM and select Checkpoint.
4. In the Checkpoints pane, right-click the new checkpoint and select Rename.
5. Name the checkpoint appropriately (Day1AfterInstall, for instance).

To test a checkpoint, follow these steps:

1. Inside the virtual machine, make a change, such as the desktop background.

2. In Hyper-V Manager in the Virtual Machines pane, right-click the VM and select Revert.
3. Click Revert again to verify.
4. Return to the running VM and note that the change has been undone.



EXAM TIP

A *differencing disk* is a virtual hard disk you create to quarantine changes you've made to a virtual hard disk or the guest operating system. You store these changes in a separate file. The differencing disk is associated with an existing virtual hard disk and can be any kind of virtual disk. You choose the disk when you create the differencing disk. This virtual hard disk is called the parent disk and the differencing disk is the child disk.

Understanding and supporting RemoteApp

Remote Desktop Services (RDS) lets you virtualize a computing session. You can opt to virtualize the entire desktop or, in this chapter, only individual applications. You use RemoteApp tools and technologies to virtualize applications. When you do, applications look and feel as though they're running on the computer a user is sitting in front of, but in reality the app is being hosted elsewhere. As you might guess, this could be used to resolve compatibility problems with specific apps, as well as provide another means to test the apps before deployment. You can use RemoteApp with local apps, and they can be added to the Start screen.

RemoteApp programs are stored on an RD Session Host server; virtual desktops are hosted on an RD Virtualization Host server. These virtual environments can be accessed remotely from a configured client machine. The Windows server running the RDS role must have the following services configured and available:

- RD Session Host enables a server to host the desired applications (and perhaps full desktops). Users connect to this server to run the programs. Users also save files and access other network resources available on the server, as applicable.
- RD Virtualization Host, with Hyper-V, hosts the virtual machines and makes them available to users as virtual desktops. These virtual desktops can be provided in a pool on a first-come, first-served basis, or you can assign a specific desktop to a specific user.
- RD Web Access enables users to access RemoteApp and Desktop Connection through their computer's Start screen.
- RD Licensing is used to manage the RDS client access licenses. A license must exist for a user to connect to the RD Session Host server.
- RD Gateway enables users to access the internal enterprise network remotely from an Internet-connected device such as a tablet or laptop.
- RD Connection Broker helps manage session load balancing and reconnection. It also provides access to the RemoteApp programs and virtual desktops.

Beyond the reasons stated already are other reasons to use RDS:

- You can consolidate all apps to manage them more easily. When an app needs to be updated or otherwise serviced, you can perform the needed work on the RD Session Host server instead of on every client desktop.
- You can simplify deployment when applications are difficult to manage, perhaps because they are updated often or prone to problems.
- You can use fewer resources on client computers and simplify management by hosting rarely used applications.
- You can allow access to company applications remotely, for instance, from home, from tablets or other limited hardware, or while traveling on business.

Windows 8.1 Enterprise offers a Control Panel icon when you opt to view by large or small icons: RemoteApp And Desktop Connections. Users click this icon to access available remote desktops or remote applications. Figure 1-13 shows Control Panel and this icon (in the right column), the RemoteApp And Desktops Connections window, and the area where users type an email address or connection URL. (You can put icons on the desktop or tiles on the Start screen so that users can directly access virtualized apps.)

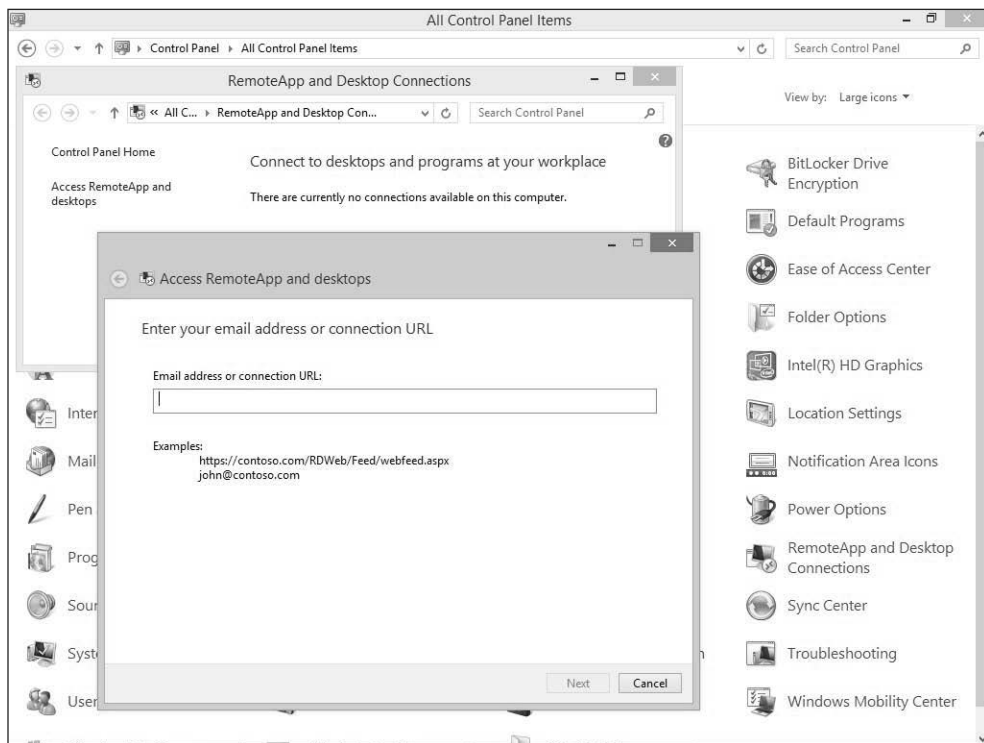


FIGURE 1-13 RemoteApp And Desktop Connections lets users connect to RemoteApp.

Understanding and supporting App-V

In some instances, you might need to run several applications side by side on a single computer. Doing so is generally okay, unless those applications conflict with one another. Such a conflict almost always occurs when you need to run multiple versions of the same application. This could certainly happen and is common in testing environments. In other cases, applications simply don't play well together; this might not have anything to do with versioning and could be caused by something completely different and difficult to diagnose. App-V helps you resolve these kinds of problems. Specifically, App-V lets you virtualize an application so that it remains independent of others but can still live on the same machine without causing conflict.

Application virtualization, as you've already learned, can also mean that users can access an application that's installed elsewhere from almost anywhere an Internet connection and compatible hardware can be used, and both users and administrators gain many benefits in doing so. Virtualization keeps applications off client machines, which means that the users' computers remain "clean" and administrators can manage the apps centrally (rather than have to manage every client in the enterprise). After App-V is set up and configured for use, a Windows 8.1 Enterprise user can install App-V client software to access and use the desired applications. As with other virtualization technologies, the running apps appear to the user to be installed and running on their own machines.

MORE INFO ADMINISTRATORS DETERMINE WHO CAN ACCESS VIRTUALIZED APPS

As soon as apps are virtualized, authorized users can access them through the App-V client application. If more than one app is available, a list appears from which they can select. Administrators set the required limitations on users and the apps they can access.

You must perform plenty of steps before end users can access virtualized applications. Setting up the actual infrastructure is beyond the scope of this book and is best left to experienced network administrators, but you must understand the fundamental task sequence and the hardware, software, and services required.

Using Microsoft Desktop Optimization Pack (MDOP)

App-V is available from Microsoft Desktop Optimization Pack (MDOP). MDOP is available as a subscription for Software Assurance (SA) customers, although you can download an evaluation to experiment with if you are an MSDN or TechNet subscriber. If you want to work through this part of the chapter, you'll want to download and install MDOP before continuing. Specifically, you need these elements, which are all part of App-V Server:

- App-V Management Server for managing App-V
- App-V Publishing Server to host virtual applications
- App-V Reporting Server to run and view applicable reports

- App-V Reporting Database Server to work with database deployments and report management

Beyond the required software, the hardware also must meet minimum requirements. The computer on which MDOP is installed must have the following:

- Microsoft .NET Framework 4.5
- Windows PowerShell 3.0
- Update for Windows KB2533623

Each element also must meet specific requirements. For example, the App-V client, Remote Desktop Services client, and the App-V server must all have the applicable Microsoft Visual C++ Redistributable Package installed. To see all requirements, refer to this article on TechNet: <http://technet.microsoft.com/en-us/library/jj713458.aspx>.

MORE INFO SOFTWARE ASSURANCE (SA)

Software Assurance is generally associated with an enterprise's ability to obtain the next version of Windows software as part of their enterprise agreement as a fee associated with qualified products. Some of the most popular additional benefits are free technical training, licenses for home users, online training, and 24x7 support. SA also provides deployment-planning services and other benefits.

Installing the App-V Sequencer and getting ready for sequencing

You should install MDOP and the App-V Sequencer on a 64-bit Windows 8.1 Enterprise computer. From the MDOP installation folder, navigate to App-V, Installers, 5.0_SP2 (or applicable version), and then run the setup program. As soon as it's installed, obtain the installer files for the application that you want to sequence. Copy those files to the computer that's running the sequencer. Create a new VM to use for the sequencing tasks, and make a backup copy of it before you start.

When you're ready, locate the Microsoft Application Virtualization Sequencer from the All Apps screen on your Windows 8.1 Enterprise computer. Click to open. Figure 1-14 shows the Microsoft Application Virtualization Sequencer as well as an open VM.

You can now do the following:

- Create virtual packages that can be deployed to computers that run the App-V 5.0 client.
- Upgrade and edit configuration information for packages you've already created.
- Convert virtual packages.

Creating a package also creates the following files:

- An .msi file that you'll use to install the virtual package on client computers
- A Report.xml file that contains all issues, warnings, and errors that were discovered during sequencing, in case you need to troubleshoot the package

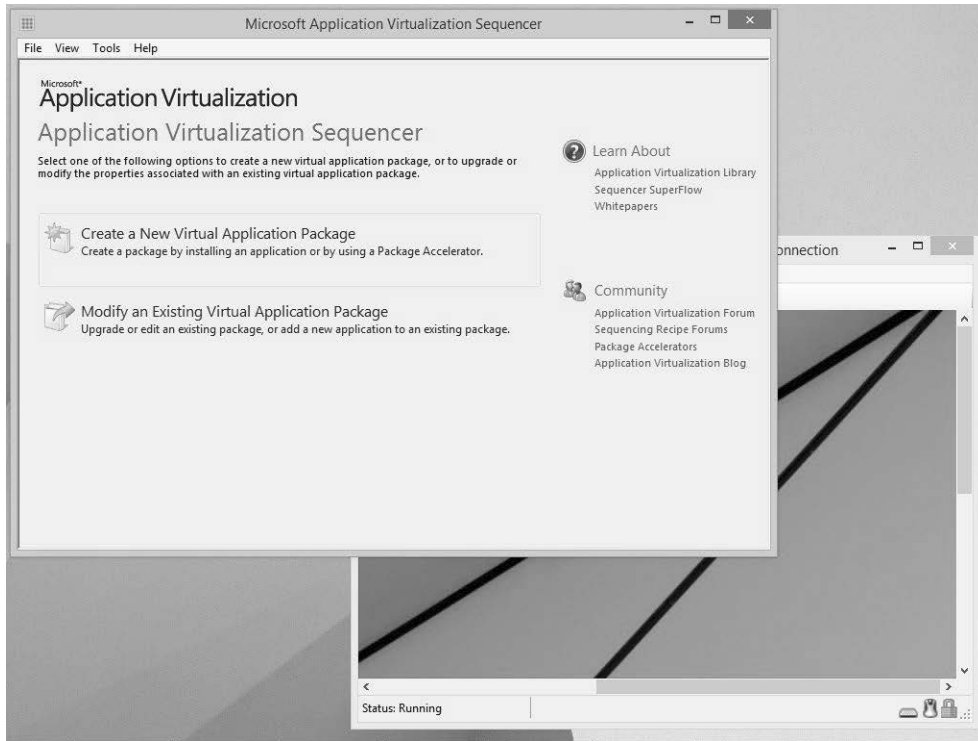


FIGURE 1-14 The Microsoft Application Virtualization Sequencer window helps you create or modify a new virtual application package.

- An .appv file, which is the virtual application file
- A deployment configuration file that regulates how virtual application is deployed
- A user configuration file that regulates how the virtual application runs

Sequencing an application

You can create virtualized application packages for standard applications, add-ons or plug-ins, and middleware. Creating packages for standard applications is the most common and what is detailed here. The following steps create one of the simplest types of packages. They don't configure every aspect available, including the option to stream the virtualized application; that experimentation is up to you. From the computer that has the sequencer installed, perform these steps:

1. At the Start screen, type **App-V**, and in the results click Microsoft Application Virtualization Sequencer.
2. Click Create A New Virtual Application Package. You can see this option in Figure 1-14.
3. Select Create Package (Default), and then click Next.

4. Resolve all listed issues that can cause the creation of the package to fail (see Figure 1-15).

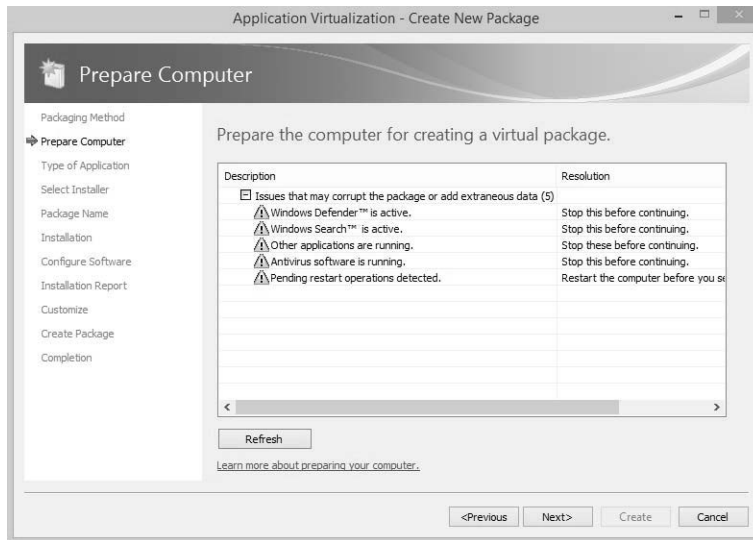


FIGURE 1-15 Prepare the computer for application sequencing.

5. Click Refresh and, if all problems are resolved, click Next.
6. Select the Standard Application (Default) check box, and then click Next.
7. Click Browse to find the installation file for the application. (If the application doesn't have an associated installer file, select the Perform A Custom Installation check box, and then click Next. Continue as prompted.)
8. Type a name for the package.
9. Click Browse to find the Primary Virtual Application Directory. Navigate to the location where the file would be installed by default, perhaps `c:\ProgramFiles\<application name>`. Note that you are navigating to this in the VM you already created.
10. Click Next three times. At the Create A Basic Package Or Customize Further page (see Figure 1-16), select Customize, and then click Next.
11. Click Next to bypass the option to run the program briefly.
12. Select Allow This Package To Run Only On The Following Operating Systems, and then select Windows 8.1 32-bit and Windows 8.1 64-bit. Notice the other options, such as the option to Allow The Package To Run On Any Operating System.
13. Click Next.
14. Click Create.
15. When the Package Completed page appears, click Close.

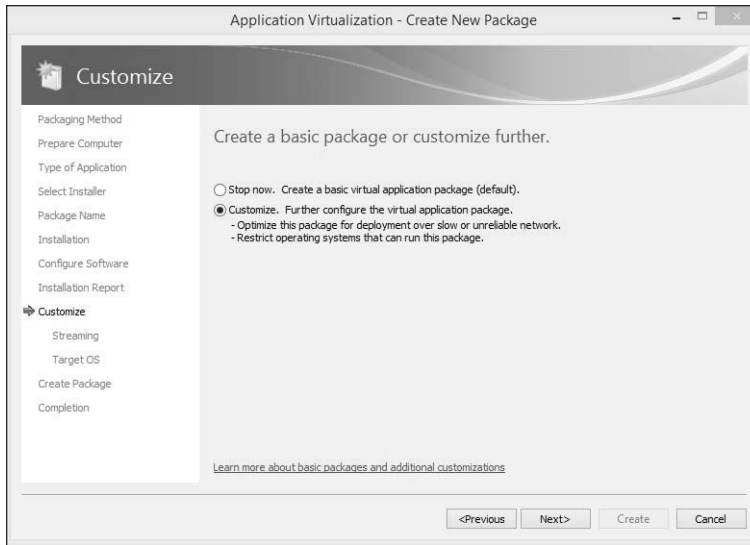


FIGURE 1-16 Opt to customize your package.

With the package created, you are now ready for deployment. You can deploy App-V packages by using an Electronic Software Distribution (ESD) solution. When you opt for an ESD, you eliminate the need for an App-V 5.0 management server, management database, and publishing server. Alternatively, you can use Windows PowerShell to deploy a virtualized application. You can, for example, also opt to install the virtual application on a single computer, deploy it through Group Policy, or use it with Configuration Manager.

MORE INFO DEPLOYING VIRTUAL APPLICATION PACKAGES

To learn more about deploying App-V packages via ESD, refer to this article on TechNet: <http://technet.microsoft.com/en-us/library/jj713482.aspx>.

Supporting installation and configuration of User Experience Virtualization (UE-V)

Users are more mobile than ever, and the trend will continue. Making the user experience the same no matter where the users log on—whether it's on a laptop, desktop, or tablet—would be valuable to users and enhance productivity. Network administrators have been doing so for quite some time by incorporating roaming user profiles, making the user's files and folders available offline, configuring syncing when a user reconnects to the network, and incorporating folder redirection. Quite a bit of this was covered in my previous book, *Exam Ref 70-687: Configuring Windows 8.1*. This exam doesn't focus on these technologies from what I've seen via the list of objectives; instead, it focuses on User Experience Virtualization (UE-V).

Microsoft UE-V monitors the Windows operating system, monitors apps and application settings that are applied when users are at their computers, and captures those settings. The information is saved to a defined storage location such as a network share folder. (This data isn't saved to OneDrive, a USB drive, or similar mechanism.) The settings are then applied (or can be applied) to the different computers and devices assigned to the user. What is synchronized (and where) and what apps and applications are included (or not) is determined by the settings location templates (XML files) that the network administrator creates and configures, in combination with what the applications' developers make available for synchronization.

Here are a few additional things to understand about UE-V:

- A user can change personal settings from any device included in the UE-V synchronization group. Those changes will be applied to the other computers the next time the user logs on to them.
- The user can use UE-V with a Windows 7 or Windows 8 computer. Applicable and compatible settings will sync automatically.
- Changes are saved to a file, and the file is synced on log on. Nothing is actually "virtualized."
- Application settings that can be synced can come from applications installed on the device, applications that are sequenced with App-V, and RemoteApp applications.
- Settings can be used as part of a recovery process when a machine is reimaged or reinstalled.
- You can incorporate Windows PowerShell and WMI to configure and deploy UE-V agents. Refer to this article to learn more: <http://technet.microsoft.com/en-us/library/dn458904.aspx>.
- UE-V includes application settings templates for various editions of Microsoft Office, Internet Explorer, Windows Accessories, desktop settings, ease of use settings, and more.



EXAM TIP

You might see exam questions with answers that include App-V, Roaming Profiles, RemoteApp, UE-V, Windows Intune, Office 365, and similar technologies that you'll learn about in this chapter. These questions will include a scenario that includes something specific the user needs and that you want to provide (perhaps retrieving application settings from the cloud, with the ability to change those settings and sync them back as is possible with UE-V). You must be able to choose the ideal technology when you are asked to provide a specific option or feature for users.

Several elements must be in place for UE-V to work. A UE-V Agent must be used. This agent watches what changes and saves those changes as applicable. A settings package is also necessary to store the application and operating system settings and application template information. Finally, a UE-V Generator must exist where you can create your own custom templates. This might seem a little vague because it is. A lot of planning and resources are

required to put this technology into place. Looking at it from a high level, deployment includes the following:

1. Deploy the Settings Storage Location.
2. Deploy the UE-V Agent.
3. Install the Group Policy templates.
4. Install the Agent Generator.
5. Deploy the Settings Template Catalog.
6. Deploy Settings Location Templates.
7. Administer UE-V, including but not limited to understanding how to
 - Manage frequency of scheduled tasks.
 - Restore application and Windows settings.
 - Configure applicable Group Policy objects.
 - Manage settings packages.
 - Incorporate App-V applications.
 - Incorporate Configuration Manager as applicable.

Deploying desktop apps by using Windows Intune

Not all companies have the money, time, or resources to set up and maintain an intricate server infrastructure, the ability or know-how to set up personal VMs, or the ability to set up a UE-V substructure to synchronize various user settings. However, those same companies might still want to virtualize applications. Keeping applications off users' desktops, especially with so many of them mobile and using multiple devices, can lighten the load required of network administrators (as well as support staff). This is where Windows Intune really shines. Any size company can use Windows Intune to virtualize applications.

In this section you'll learn just enough about Windows Intune to understand what it is and how you can use it. Later in this chapter and book you'll learn a lot more. Here are the highlights. With Windows Intune, a company can:

- Use a single web-based administrator console to manage computers and mobile devices via the cloud.
- Simplify the management of various devices, including Windows laptops, desktops, tablets, and phones—and even Apple iOS and Android devices.
- Make following company guidelines easier by using the cloud to manage all devices.
- Download Windows Intune client software when necessary, using a Microsoft account and password, from the administration page. (Client software can be deployed in many ways, including manually, through Group Policy and by using Configuration Manager.)

- Make software available to users, requiring all users to have the software or making it optional, while at the same time requiring no user interaction for installing it.
- Make software available through the company portal so that Windows RT users can install applications as needed.
- Create, upload, publish, and deploy software packages; configure and manage security policies; manage inventory; and create inventory reports when combined with Configuration Manager.

Unlike most of what you've seen so far in this objective, you can get a free 30-day trial of Windows Intune even if you don't have a Software Assurance plan or a subscription to TechNet or MSDN. After you set it up (and possibly install Microsoft Silverlight if you didn't have it already), go to <https://manage.microsoft.com/WindowsIntune>, log on, and work through the setup processes. Your logon name should look something like *administrator@yourname.onmicrosoft.com*. Figure 1-17 shows the Windows Intune Administrator Console, with System Overview selected. Notice the alerts, system status, updates, agent health, and more, just from this one tab.

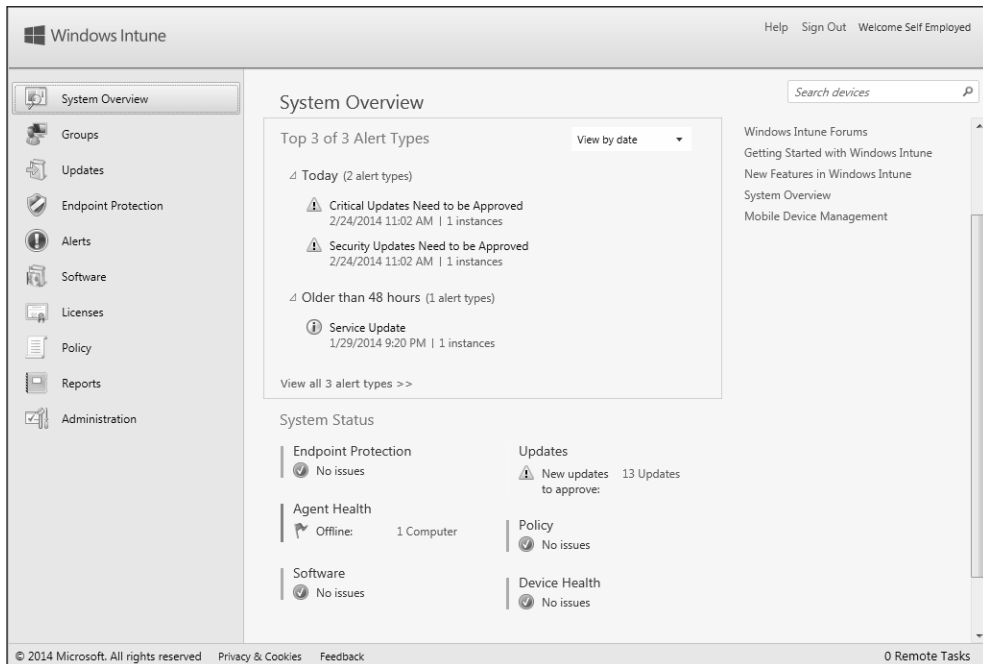


FIGURE 1-17 The Windows Intune Administrator Console consolidates the available tools and makes them easy to work with.

From the other tabs available in the Windows Intune Administrator Console, you can manage clients easily. Table 1-4 details the tabs available.

TABLE 1-4 Tabs available in the Windows Intune Administrator Console

Windows Intune tab	Available tools and options
System Overview	Read notices regarding the functionality of Windows Intune; view summaries of Alerts, Endpoint Protection, Agent Health, Policy, Device Health, Software, and Updates; view Computer Summary and Mobile Device Summary
Groups	Create groups; view hardware reports; see a Mobile Device Summary that includes Alerts, Update Status, Policy, Software Status, and Device Health Status; view information on available disk space, top five manufacturers, and top five operating systems used in your enterprise
Updates	View Update Status and Cloud Storage Status; perform update tasks; sort updates by type (Critical, Security, Definition, and so on)
Endpoint Protection	Review Malware Status and Computer Status to see if any issues exist; see Top Malware Instances
Alerts	See a list of Alerts that you can sort in various ways, including View By Date
Software	Review Software Status and Cloud Storage Status; manage cloud storage; perform tasks such as adding software and managing software deployment
Licenses	Review Licenses Overview specific to your organization; add agreements; create a License Group; view Purchase Report; view Installation Report
Policy	Configure policies to manage settings on computers and mobile devices (after it's configured, you can deploy the policy to groups of devices, or deploy mobile device policies to mobile users)
Reports	View various reports: Update, Detected Software, Computer Inventory, Mobile Device Inventory, License Purchase, and License Installation
Administrator	Access Administration Overview, including the name of the account, status, number of enrolled devices, and Cloud Storage Status; learn more about these items

If you've set up a free trial of Windows Intune, click the Software tab. Under Tasks, click Add Software. Download and install the Microsoft Intune Software Publisher, log on, and read the introductory screen. This should give you an idea of how to publish software with Windows Intune. Click Next; you see the screen shown in Figure 1-18, except the path to the location of the software setup files is blank. You learn how to complete this process later in the chapter.

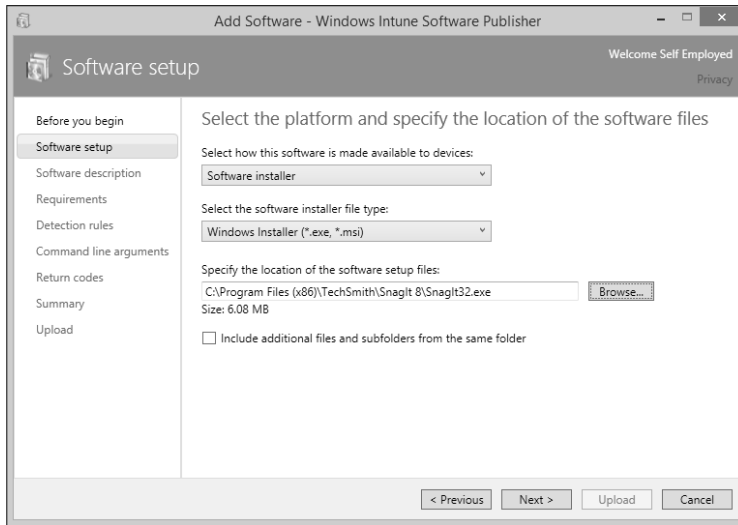


FIGURE 1-18 Use the Windows Intune Software Publisher to publish software.



Thought experiment

Choosing the best method for hosting a desktop application

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You have been commissioned by a large organization to help prepare for an enterprise-wide rollout of Windows 8.1. Company employees use myriad desktop applications, two of which were written by a developer who's no longer in business. The company wants you to help test the applications to see whether they are or can be made compatible with Windows 8.1.

- 1.** What tool will you choose to determine whether the applications in question are compatible?
- 2.** What type of database must also be available for this technique to work successfully?
- 3.** Several steps are involved in using this tool. What is the second step you'll take to use this tool to test the applications and determine compatibility, after performing the installation and setting up the applicable database?
- 4.** After you create and deploy the appropriate collector package, what kind of package do you create and deploy next?
- 5.** Where can you review the application compatibility reports?

Objective summary

- You can determine application compatibility and deal with problems that arise in many ways, including using ACT and creating shims.
- Applications can coexist with others that would usually cause compatibility issues or simply aren't compatible with the current operating system. The technologies to consider include Client Hyper-V, RemoteApp, and App-V. Each offers something unique and is used in specific circumstances to provide solutions.
- You can give users a consistent desktop and user experience with UE-V.
- You can use Windows Intune to host applications and manage computer inventory, even if you don't have a server structure in place.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You are planning for a Windows 8.1 deployment and have learned that one desktop application your company relies on heavily isn't compatible. The application vendor is still in business and promised an update soon, but you don't want to wait for that update. What can you do to make the application compatible until an update is available? Choose all that apply.
 - A. Create a shim for the application.
 - B. Create and deploy a runtime-analysis package.
 - C. Run the program in Program Compatibility mode.
 - D. Use RemoteApp for the application.
2. You have discovered that an application is incompatible with Windows 8.1 and the issue involves User Account Control. Which of the following tools can you use to resolve the issue?
 - A. Create a shim with ACT.
 - B. Use the Standard User Analyzer Wizard.
 - C. Create a shim with App-V.
 - D. None of the above; you can't resolve this kind of issue.
3. Which of the following lets you store and manage applications on your own network servers while also making them available to users?
 - A. Client Hyper-V
 - B. App-V
 - C. RemoteApp
 - D. Windows Intune

4. You try to enable Client Hyper-V on a workstation and can select Hyper-V and the Hyper-V Management tools, but you can't select Hyper-V Platform. Why?
- A. You aren't logged on as an administrator.
 - B. The computer's processor isn't SLAT.
 - C. The computer's architecture is 32 bit.
 - D. The computer is running Windows 8.1, but not the Pro or Enterprise edition.
5. RemoteApp programs are stored on a(n) _____ and virtual desktops are hosted on a(n) _____.
- A. RD Virtualization Host server; RD Session Host server
 - B. App-V Publishing Server; App-V Management Server
 - C. App-V Management Server; App-V Publishing Server
 - D. RD Session Host server; RD Virtualization Host server
6. You want to monitor Windows operating system, app, and application settings that are applied when users are at their computers. You want to capture those settings and then allow users to access those settings to provide a consistent user experience no matter where they log on. Which of the following are parts of the solution you will put into place to make this happen?
- A. A working Active Directory and network share
 - B. A UE-V Agent
 - C. A UE-V Generator
 - D. A Settings Storage Location
 - E. All of the above
 - F. Only B and C
7. When you deploy UE-V, which of the following is the first thing you must do?
- A. Deploy the Settings Storage Location.
 - B. Deploy the UE-V Agent.
 - C. Install the Group Policy templates.
 - D. Install the Agent Generator.
 - E. Deploy the Settings Template Catalog.
 - F. Deploy Settings Location Templates.
8. For Windows Intune, what does Endpoint Protection refer to?
- A. Malware
 - B. Updates
 - C. Policy
 - D. Licensing

Objective 1.3: Support Windows Store and cloud apps

The previous objective covered supporting desktop apps. This objective covers supporting apps from the Windows Store and Office 365, sideloading apps, and managing the apps you want to use. You'll also see more about how to sync settings unique to a user by incorporating the cloud, specifically with a Microsoft account and a trusted PC.

This objective covers how to:

- Integrate a Microsoft account, including personalization settings and trusted PCs
- Install and manage software by using Office 365 and Windows Store apps
- Sideload apps into online and offline images
- Sideload apps by using Windows Intune
- Deep link apps by using Windows Intune

Integrating a Microsoft account

These days, almost all Windows 8 and Windows 8.1 users have Microsoft accounts that they use to log on to their personal Windows 8-based computers and tablets. These accounts enable them to sync certain settings related to their user experience, including but not limited to the Start screen layout, app data, account picture, web browser favorites, and some passwords. Settings are stored via OneDrive. Consumers can use their Microsoft accounts to manage billing for their Xbox accounts, the Store app, and even connect their Xbox gamer tags. Users also receive cloud services when they sign up for the account, including a calendar, contact list, and similar features and tools. They can decide what to sync by using PC Settings on their local computers.



EXAM TIP

If a scenario on the exam asks you to troubleshoot why a user can't sync passwords with other accounts and computers, make sure the scenario states that they are using a Microsoft account first. Local accounts can't be used to sync to the cloud. If a Microsoft account is in use, check to see whether the PC is a trusted PC (or if others are).

Network administrators can integrate users' Microsoft accounts into the workplace to help users incorporate what they've configured with these accounts with their domain accounts. Network administrators can also opt not to let users connect to their Microsoft accounts by setting limitations in Group Policy. This section looks at the Group Policy options first, followed by how users can tweak what they want to sync and how to trust various PCs, and then how users connect their Microsoft accounts to the domain account.

Exploring Group Policy settings

You configure Group Policy to allow or deny Microsoft accounts in a domain by using the \ or Group Policy Management Editor. You open the Group Policy Management Editor window, and then expand Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, Security Options. You also can use the Local Group Policy Editor to allow or block Microsoft accounts on local computers by navigating to Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options. Figure 1-19 shows the path to the latter.

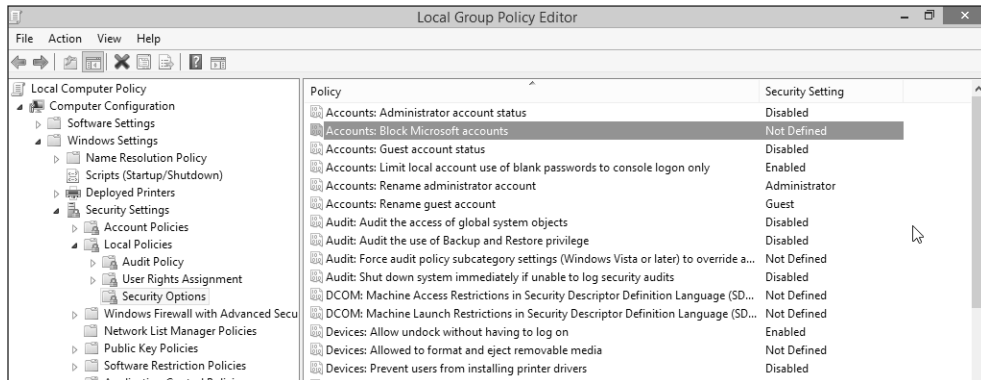


FIGURE 1-19 Navigate to the Local Group Policy setting Accounts: Block Microsoft Accounts.

Double-clicking the entry Accounts: Block Microsoft Accounts presents three options:

- **This Policy Is Disabled** If you apply this setting or don't configure any others, users can use Microsoft accounts.
- **Users Can't Add Microsoft Accounts** If you apply this setting, users can't create new Microsoft accounts, switch from local accounts to Microsoft accounts, or connect domain accounts to Microsoft accounts. This is the best option to choose if you want to limit the use of Microsoft accounts in your enterprise.
- **Users Can't Add Or Log On With Microsoft Accounts** If you apply this setting, users who have existing Microsoft accounts can't log on to Windows. This can limit even the administrators' ability to log on.

Locating and managing what's synced with a Microsoft account

Users can change what items they opt to sync to and from the personal computers they log on to with their Microsoft accounts. Users can access the options on their personal computers via PC Settings, the OneDrive tab, and Sync settings (see Figure 1-20). (Press Windows logo key+C to access the charms and click Change PC Settings.) Users will encounter additional sync options when they connect with their domain accounts.

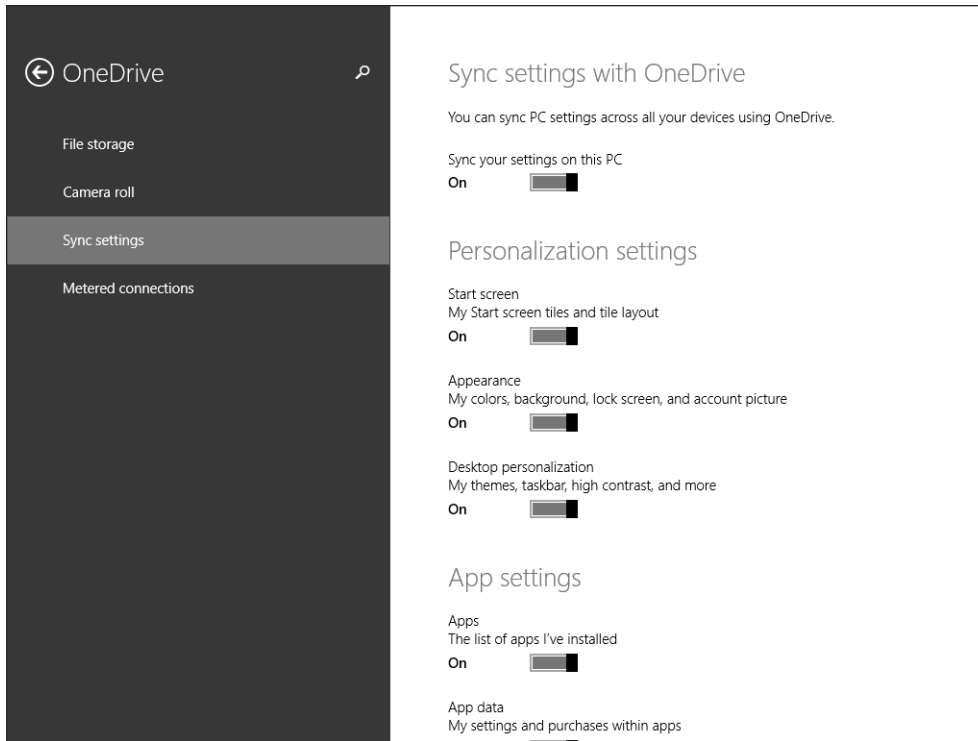


FIGURE 1-20 Change what syncs from PC Settings.

Configuring trusted PCs

User settings are synced via Microsoft accounts and OneDrive. OneDrive also enables users to configure and sync passwords with trusted PCs. You can use a configured trusted PC (sometimes called a *trusted device*) to synchronize passwords and to reset the Microsoft account password if it's forgotten or compromised. Users decide which of their devices should be trusted. Two scenarios are involved.

In the first scenario, users log on to a new computer with a new Microsoft account (or an account that's new to that computer). In this instance, users are prompted to enter a security code. Microsoft generates this code and sends it to a backup email address or cell phone number already configured for the account. After the users type the code, they can then opt to state that the PC being configured is one they log on to often and should thus be trusted.

In another scenario, users opt not to sync passwords while configuring a PC, for whatever reason. In this case, when they try to sync passwords later, they see a message that states the passwords can't be synced until the PC is trusted. When the users opt to trust the PC, the same process completes as noted before with the generation of a code they must type.

Finally, users can log on to their Microsoft account online via a web browser, navigate to Security info, and then gain access to options for recovering passwords and setting up

additional trusted devices. Users can also remove all trusted devices associated with an account, should the account be compromised.

Connecting a Microsoft account with a domain account

If users have domain accounts in the workplace, they can connect their Microsoft accounts to them and see the same desktop background, browser history, and other account settings they've already configured on their home PCs. They also can use Microsoft account services from their domain PCs without signing in to them.

To connect a Microsoft account with a domain account, follow these steps:

1. Access the charms and click Change PC Settings.
2. Under PC Settings, click Accounts.
3. Click Connect To A Microsoft Account.
4. Clear the check boxes for items you don't want to sync, and click Next.
5. Enter the applicable email address and click Next.
6. Enter the password and click Next.
7. Complete the security information requirements and type in the generated code.
8. Click Next, and then click Finish.

Installing and managing software by using Office 365 and Windows Store apps

Network administrators who manage large enterprises of computers and users don't carry physical media from machine to machine to install software. Instead, they opt for more practical solutions. You've already learned about several of those options in this chapter. More ways are available than what's been covered so far, however; administrators can install and manage software using Office 365, and they can make their apps available from the Windows Store.

Installing software by using Office 365

Office 365 in its multiple editions is Microsoft Office. But it is Microsoft Office in the cloud, accessible via a user-based paid subscription. Because it's cloud-based, users can access the Microsoft Office products that are licensed to them on up to five compatible devices (with Office 365 ProPlus). Office 365 ProPlus is designed to run locally on PCs, so a persistent connection to the Internet isn't required.

MORE INFO THE VARIOUS EDITIONS OF OFFICE 365

Office 365 comes in many editions: Small Business, Small Business Premium, Midsize Business, and various Enterprise editions. You can learn more about which edition to choose and how much it costs per user at <http://office.microsoft.com/en-us/business/compare-office-365-for-business-plans-FX102918419.aspx>.

Many compatible platforms are available, including Windows, Mac, and compatible mobile devices. With Office 365, updates are applied automatically, so enterprise administrators never have to worry about updating computers or other devices manually, although they are still in control of those updates and can decide how and when they'll be offered to users. Just about every other maintenance task you can encounter when you host Office 365 in your enterprise is also handled without any interaction from you (after Office 365 is set up). Beyond that, administrators can also decide where users' data should be stored: on a company's onsite data servers or private cloud, in the public cloud, or a combination of these.

The reality is that Office 365 is "application virtualization." And you know about virtualization, and that virtualized applications run in their own space. This means that users can run the latest version of Office in the cloud while at the same time leaving older versions installed and available on their own PCs. It also means that users can have the same user experience from wherever they log on while using the hosted apps.

MORE INFO FAMILIARIZING YOURSELF WITH OFFICE 365 FEATURES

This book isn't the place to tell you what Office 365 offers beyond installing Office products—such as online conferencing, business class email solutions, secure file sharing, public website development, and using virtually any web browser to create Office documents—but you need to be familiar with them just the same. You can learn more at <http://office.microsoft.com/en-us/business/what-is-office-365-for-business-FX102997580.aspx>.

You can get a free trial of Office 365 Small Business Premium or Office 365 Midsize Business here: <http://office.microsoft.com/en-us/business/compare-office-365-for-business-plans-FX102918419.aspx?tab=1>. Setting up Office 365 involves creating an account, creating an administrator logon and domain name, and requesting and then typing in a security code from Microsoft. Figure 1-21 shows the Office 365 Admin Center.

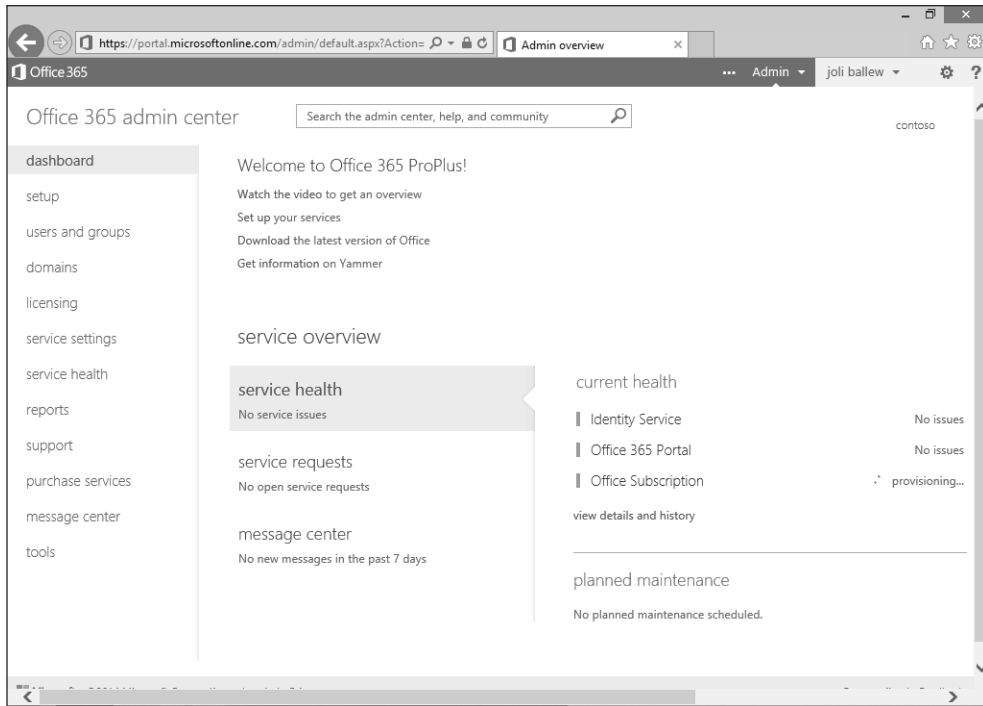


FIGURE 1-21 The Office 365 ProPlus Admin Center offers the tools you need in a single console.

Before you can go much further, you need to create at least one user account. That user will then log on to the Office 365 portal with a temporary password and create a new password. Then the user can download whatever parts of Office you want to license that user to use.

To perform the initial setup tasks and to create a user and assign a license (after signing up for a free trial, completing the administration requirements, and logging on to the portal at <https://portal.microsoftonline.com>), follow these steps:

1. Click the Settings icon in the top right corner and click Office 365 Settings.
2. Click Setup.
3. From the Quick Start section, click Start.
4. Choose the desired domain and click Next.
5. Click Add users and assign licenses.
6. Choose an option to add users. For this example, choose Add Users One At A Time. Click Next.
7. Input user details and click Next (see Figure 1-22).

FIGURE 1-22 Create a new user before deploying software.

- 8.** Choose the new user's status (administrator or not) and set the user location. Click Next.
- 9.** Leave Office 365 ProPlus selected under Assign Licenses, and then click Next.
- 10.** Read the information on the final page and click Create.
- 11.** Write down the temporary password (which is good for 90 days).
- 12.** Click Finish.

The new user can now install Office Professional on one or more computers. The easiest way to do this is to let users install Office 365 directly from the Office 365 portal, as outlined here. You can also opt to download the software to a network share and deploy it to users in any applicable manner you prefer. An overview of how that's done comes later.

Before you start, though, you might want to explore the admin portal for a few minutes. Specifically, look at the Service Settings tab, where you can clear check boxes for Office products that you don't want users to have permission to install, if you have a software package that offers this as a feature. The list depends of the software package that the enterprise has obtained. Office 365 ProPlus includes Access, Excel, InfoPath, Lync, OneNote, Outlook, PowerPoint, Publisher, and Word, and installs as a single package. You can't select only one or two here. Whatever the case, you should check it out anyway.



EXAM TIP

If you don't want users to run a particular program but don't have the option to pick and choose what programs your users can install, as in the case of Office 365 ProPlus, you can use AppLocker to control it. You can also opt to deploy Office 365 ProPlus through App-V.

To let the new user install Office 365 ProPlus from the Office 365 portal, follow these steps:

1. Log on as an administrator to a local computer where you want to install Office 365.
2. With Internet Explorer, navigate to <https://portal.microsoftonline.com>.
3. Type the user ID and temporary password, and then click Sign In.
4. Type the old password, input a new password, and confirm it. Click Save.
5. Follow the applicable instructions to install the software and connect to Office 365.
6. Select the 32-bit version of Office 365 and the language to install. The 32-bit version is recommended. Click Install.
7. Click Run to start the installation, click Yes to continue, and click Next to start the wizard.
8. Select No Thanks to not send updates to Microsoft, and then click Accept.
9. Click Next in the Meet OneDrive screen.
10. Click Next to accept defaults, select No Thanks, and then click All Done.



EXAM TIP

When users install from the Office 365 portal, updates are installed automatically in the background. You can't change this behavior. Also, as an administrator, you can't control which computers the user installs the software on.

Other deployment options exist beyond this self-service method. For large organizations with a domain and Active Directory, administrators can save the installation files on a local network share. For this method to work, however, you need the Office Deployment Tool, available from the Microsoft Download Center. You can use this tool to create a Configuration.xml file that contains information about what language to download or what architecture to use. It can also include where the software is located on the network, how updates are applied after Office is installed, and what version of the software to install. As soon as the files are available, deployment can include Group Policy, startup scripts, or Configuration Manager.

MORE INFO LEARN MORE ABOUT DEPLOYMENT

To learn more about the different ways that you can deploy Office 365 ProPlus, visit [http://technet.microsoft.com/en-us/library/ee624360\(v=office.15\).aspx](http://technet.microsoft.com/en-us/library/ee624360(v=office.15).aspx).

On a high level, deployment via a network share involves these steps:

1. You create a network share, `\\yourservername\Officeversion\Source`, and the files are extracted there. The extraction command is `microsoftoffice.exe /extract:"pathtosourcefiles"`.

2. You download additional required files, such as template files and Office Customization Tool files.
3. You configure these files, complete installation, and copy the necessary data to the shared folder in a new folder called Admin.
4. You then start the Office Customization Tool, using the command `\\yourservername\Officeversion\Source\setup.exe /Admin`, and customize Office. Changes are saved to a customization files (.msp). This is also saved to the shared folder.
5. Users log on to the Office 365 portal and run MicrosoftOffice.exe from the network share.

Managing software by using Office 365

When you set up Office 365, you are the Global Administrator. You have the power to create users who are administrators and users who aren't, and to perform any other task associated with Office 365. You can create several types of administrators, as outlined in Table 1-5. Creating these administrators and delegating responsibilities is part of managing Office 365. Each administrator has specific permissions.

TABLE 1-5 Administrator roles in Office 365

Permission	Admins who can manage	Admins who can't manage
View information related to the organization and users	Billing; Global; Password; Service; User Management	Not applicable
Manage support tickets	Billing; Global; Password; Service; User Management	Not applicable
Manage user passwords (reset)	Global; Service; User Management can reset passwords for Password and User Management admins	Billing
Manage billing and purchasing	Billing; Global	Password; Service; User Management
Manage user views	Global; User Management	Billing; Password; Service
Manage user licenses	Global; User Management with limitations (can't delete a global admin or create admins)	Billing; Password; Service
Manage domains	Global	Billing; Password; Service; User Management
Manage organization information	Global	Billing; Password; Service; User Management
Create and manage admin roles	Global	Billing; Password; Service; User Management
Use directory synchronization	Global	Billing; Password; Service; User Management

After you delegate responsibilities and roles to the various members of your administration team, you're ready to start managing the product. This involves many facets. To see these facets, click each tab in the Office 365 Admin Center. A few examples include the following:

- **Users And Groups tab** From the Active Users tab (see Figure 1-23), you can set up single sign-on, set up Active Directory synchronization, create password policies, and configure multifactor authentication requirements. You can also add users, filter users, and search for users, as well as edit user information. The Delete Users, Security Groups, and Delegated Admins tabs each have their own available management tasks. (Click Learn More to the right of Single Sign-on to learn what this feature offers; you might be asked about this on the exam.)

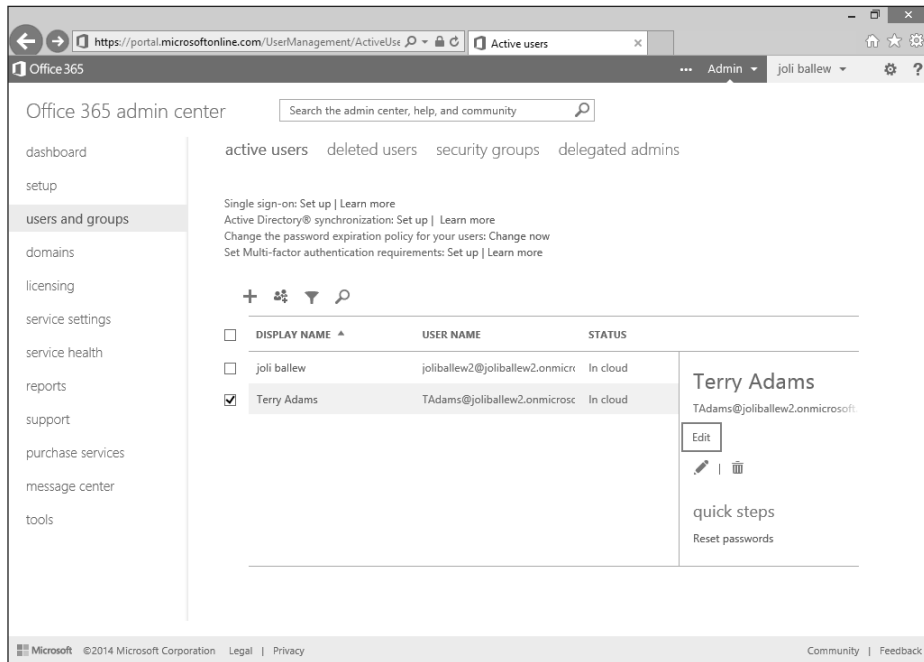


FIGURE 1-23 You can perform many management tasks from every tab and subtab in the Office 365 Admin Center.

- **Domains tab** Use this tab to manage your domain, add a domain, buy a domain, and perform similar tasks.
- **Licensing tab** Here, you can review your current subscription; view the number of licenses that are valid, expired, and assigned; and manage your subscription.
- **Service Settings** Here, you can manage user software, including choosing which software your users can download directly from Office 365 (see Figure 1-24). You also can configure a password expiration policy.

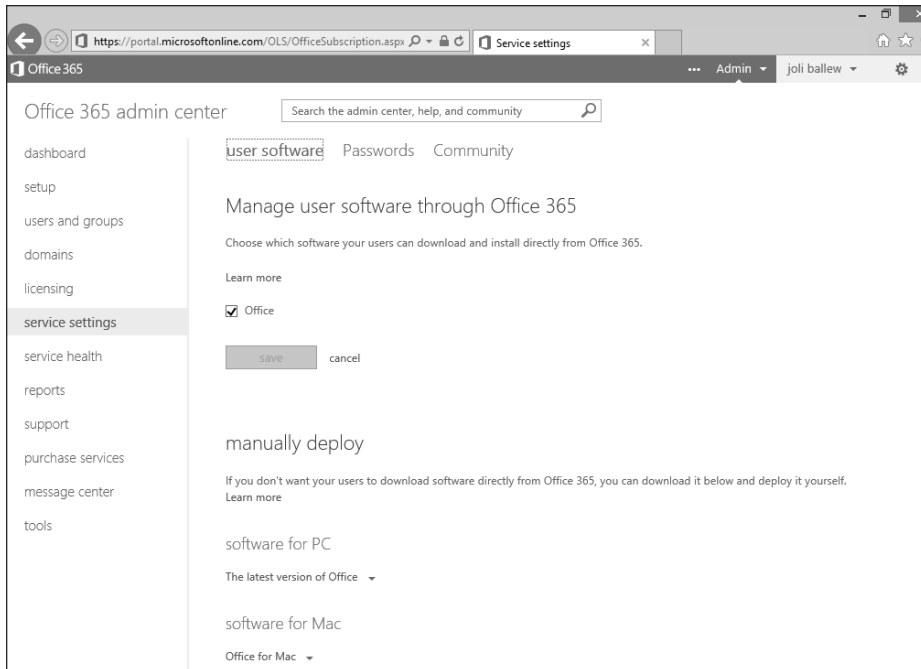


FIGURE 1-24 There are many options available from the Service Settings tab in the Office 365 Admin Center.

- **Service Health tab** You can see the status of the Office 365 service in relation to use as categorized by day. You also can review planned maintenance.
- **Message Center tab** You can access messages provided by Microsoft, including messages regarding new features in Office 365 and information about available upgrades.

As you can see, you can manage Office 365 in many ways. You should become familiar with how to perform certain tasks, such as resetting a user's password, configuring a password expiration policy, and creating new admins. Spend some time now exploring, and perform these tasks as time allows. Notice that the Dashboard tab, the first one on the left, offers access to videos for performing tasks as well as setting up services. For an introduction, the following steps walk you through one task: resetting a user's password.

To reset a user password, follow these steps:

1. From the Office 365 Admin Center, click Users And Groups.
2. Select the user you want to modify.
3. Click Reset Password.
4. Click Finish.

Performing other tasks is similar. You click the tab that offers the resource you need (perhaps Service Settings, and the Password tab you find there to set a password expiration policy), and then you click to view, edit, create, or configure the option desired.

Before you leave this Office 365 discussion, here are a few more things to familiarize yourself with:

- **Click-to-Run** Traditionally when you install Office, you have to wait until the whole Office product is installed before you can use it. Click-to-Run allows you to stream installations, which means users can open and start to use the product before the entire product is installed.
- **Other features** You might be familiar with features beyond Word, Excel, PowerPoint, and others. For example, large enterprises might also use Exchange Online, SharePoint Online, Lync Online, and opt to incorporate other services such as Yammer.
- **Windows PowerShell management** You can manage Office 365 with Windows PowerShell. Read this TechNet article to familiarize yourself with this: <http://technet.microsoft.com/en-us/library/dn568002.aspx>.
- **Desktop versions** Many Office 365 plans also include the latest desktop versions of Office. If your users can't always be online, this option is something to consider.
- **Mobile apps** Many mobile apps support Office 365, including but not limited to Office Mobile, Outlook Mobile, OneNote, and Lync Mobile.



EXAM TIP

In the past, Microsoft certification exams included questions that ask you to choose which Windows PowerShell command in a list of commands can be used to perform tasks. Whether you'll be asked this isn't known. To be on the safe side, read this article about performing common tasks with Windows PowerShell, such as licensing users, adding users, and adding domains: <http://technet.microsoft.com/en-us/library/dn568028.aspx>.

Installing software by using the Windows Store

You should know how to install software from the Windows Store as a consumer. You simply click the Store tile from the Start screen, navigate to the app to install, click it, and choose Install. These apps are also called packaged apps. If you aren't yet familiar with the Store, press the Windows logo key to access the Start screen, click the Store tile, and install a few apps before continuing here. Figure 1-25 shows the Store and the results that appear after searching for "Microsoft."

The Windows Store has the following characteristics and features:

- It's a central depository for publicly created apps available for free, as a trial, and for purchase.
- Users must have a Microsoft account to obtain Store apps.

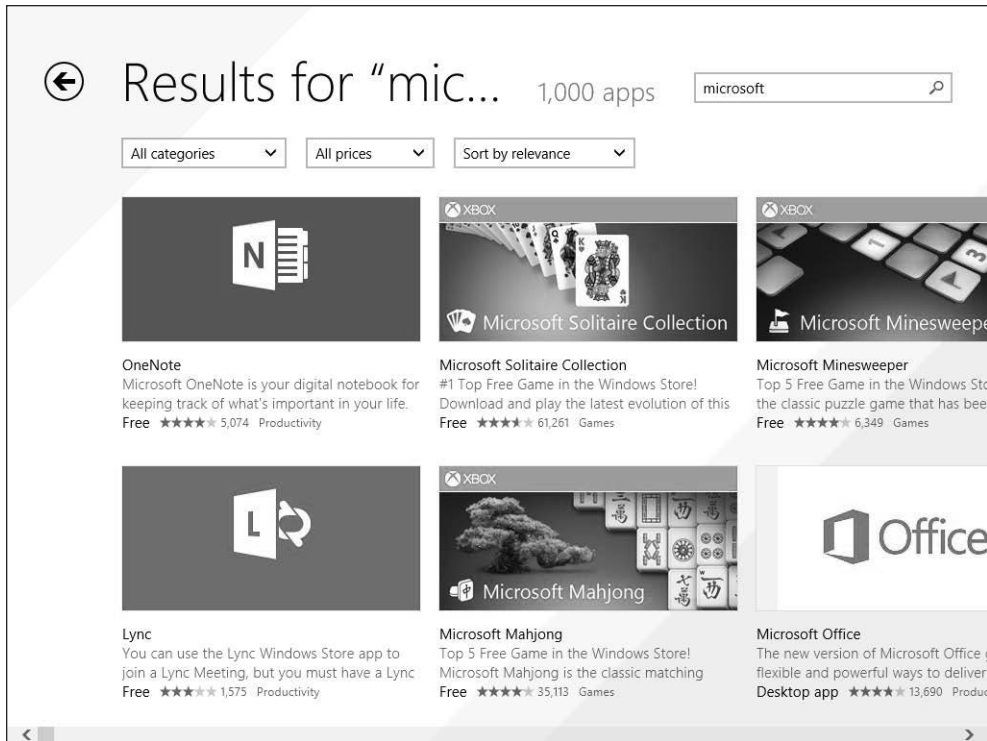


FIGURE 1-25 The Windows Store offers apps made available to the public.

- Publicly created apps must pass Microsoft's certification and compatibility tests before they can be published to the Store.
- Installed apps appear on the All Apps page. (They no longer appear automatically on the Start screen like they did in Windows 8.)
- Your enterprise can offer Line of Business (LOB) apps through the Store. You can certify your apps through Microsoft to make public, or choose not to certify them and make them private and available only to your employees.
- As an administrator, you need to configure Group Policy to define how you want your users to interact with the Store with devices you provide and those they bring to work ("bring your own device," or BYOD). See "Managing software by using the Windows Store," next.

Managing software by using the Windows Store

By default, all users can access the Windows Store. You might want to change this behavior. You can modify access in two ways. You can configure it so users can't access the Windows Store at all, or you can limit their use by allowing them to acquire only specific apps. If you opt to let users access the Store, you can disable app updates, if you want.



EXAM TIP

To disable users' access to the Store completely, you need to configure Group Policy. To restrict access to only some of the Windows Store content, you have to use AppLocker. AppLocker is available only for domain-joined machines and can't be used to manage users' computers when they are at home on their local network.

DISABLE APP UPDATES

You might opt to let users access Store apps but choose to disable app updates (they are installed automatically in Windows 8.1). You can do this by using Group Policy in a domain, via the Local Group Policy Editor in a workgroup, or from a single computer using the Store app options. First, look at how to achieve this on a single computer. This is really the only setting relevant to single users at a single PC.

To disable updates on a single client computer, follow these steps:

1. From the Start screen, click the Store app.
2. Press Windows logo key+I to open the Settings charm.
3. Click App Updates.
4. Move the slider under Automatically Update My Apps from Yes to No.

If you need to manage a group of computers in a workgroup or domain, you need to apply Group Policy. The location of the Group Policy setting is in the same place whether you use the Local Group Policy or the related Group Policy Management Console on your domain server. The path to the Local Group Policy setting (in `gpedit.msc`) is Computer Configuration, Administrative Templates, Windows Components, Store. If you enable the setting Turn Off Automatic Download Of Updates On Win8 Machines, updates are disabled (see Figure 1-26).

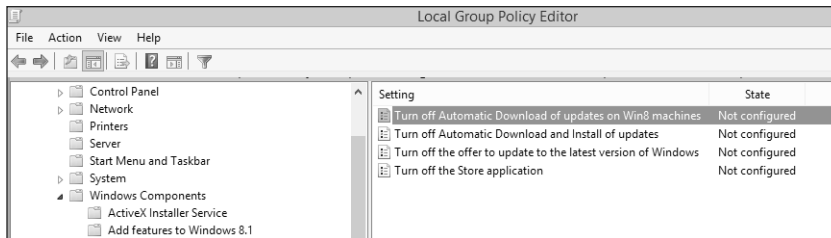


FIGURE 1-26 Use Group Policy to manage Store settings.



EXAM TIP

When you configure Local Group Policy, your changes might not take effect immediately. Use the command `gpupdate /force` to refresh the policies.

DISABLING ACCESS THROUGH GROUP POLICY

You can't disable access to the Windows Store from the Settings charm like you can when disabling app updates. To disable access, you must use the applicable Group Policy Editor. You might want to do this if your employees are downloading and installing games, for example. You might need to disable access to meet a company's security needs. You can disable the Store for computers, users, and/or groups. Whatever the case, to disable access to the Windows Store using the Local Group Policy Editor, follow these steps:

1. On the Start screen, type **gpedit.msc** and click it in the results. (You can also use the Run box on the desktop.)
2. In the Group Policy Editor, expand the following nodes: Computer, User Configuration, Administrative Templates, Windows Components, and Store.
3. Double-click Turn Off The Store Application.
4. Click Enabled.
5. Click OK.



EXAM TIP

The exam will have questions that ask how to open all manner of features, using various text-based shortcuts. For instance, rather than search for the Local Group Policy Editor on the Start screen of a workstation computer, you might be expected to know that you can also use Windows logo key+R, and in the Run box that opens, type **gpedit.msc**. So, as you work through this book and perform any task, know that likely other ways are available to do it. Here are a few examples you can type in the Run box or on the Start screen to open a few of the popular Administrative Tools and Computer Management tools:

- File Signature Verification: **Sigverif**
- Group Policy Editor: **gpedit.msc**
- Local Security Settings: **secpol.msc**
- System Configuration Utility: **msconfig**
- Task Manager: **taskmgr**
- Computer Management: **compmgmt.msc**
- Event Viewer: **eventvwr.msc**
- Performance Monitor: **perfmon.msc**
- Disk Management: **diskmgmt.msc**

To find more, perform a web search for "List Run command for Windows 8."

Sideload apps into online and offline images

Companies sometimes create their own apps. These apps have the same characteristics as the apps you find on the Start screen and from the Store (which aren't desktop apps). These apps are meant to be used by employees to do work. As noted earlier, enterprise administrators can make these apps available publicly if they want to go through the Microsoft certification process, or they can make them available to their enterprise users through a process known as *sideloading*. Tools such as DISM, Windows PowerShell, Configuration Manager, and Windows Intune help with sideloading.

As a new technology, sideloading can be used only with Windows Server 2012, Windows 8 and Windows 8.1 Enterprise, and Windows 8 and Windows 8.1 Pro. You can also do sideloading on Windows RT tablets, but with a few tweaks. Sideloading is easiest if the devices are also joined to an Active Directory domain, but you can work around this if you need to. Beyond that, you must enable a specific Group Policy setting, which you'll learn about shortly, and the app must be signed by a Certificate Authority (CA) trusted by the PCs on your network (at least the ones you want to offer the app to). If the PCs aren't domain-joined or are Windows RT devices, you'll also need a sideloading product activation key. You can get this key from Microsoft's Volume Licensing Service Center (VLSC).

Setting Group Policy

To set Group Policy so that computers can accept and install sideloaded apps that you created for your enterprise, on a Windows 8-based Enterprise or Pro machine, navigate to Computer Configuration, Administrative Templates, Windows Components, App Package Deployment. Double-click Allow All Trusted Apps To Install. Figure 1-27 shows this in the Local Group Policy Editor. When enabled, any LOB Windows Store app (signed by a CA that the computer trusts) can be installed. To perform this task for multiple computers in your enterprise, use the Group Policy Management Console (GPMC) and navigate to Computer Configuration, Policies, Administrative Templates, Windows Components, App Package Deployment.

MORE INFO CREATING A WINDOWS STORE APP

You create apps by using Microsoft Visual Studio Express 2012 for Windows 8 or something similar. If you're interested, you can find a tutorial to help you get started at <http://msdn.microsoft.com/en-us/library/windows/apps/dn631757.aspx>

Another tutorial is at <http://technet.microsoft.com/en-us/windows/jj874388.aspx>.

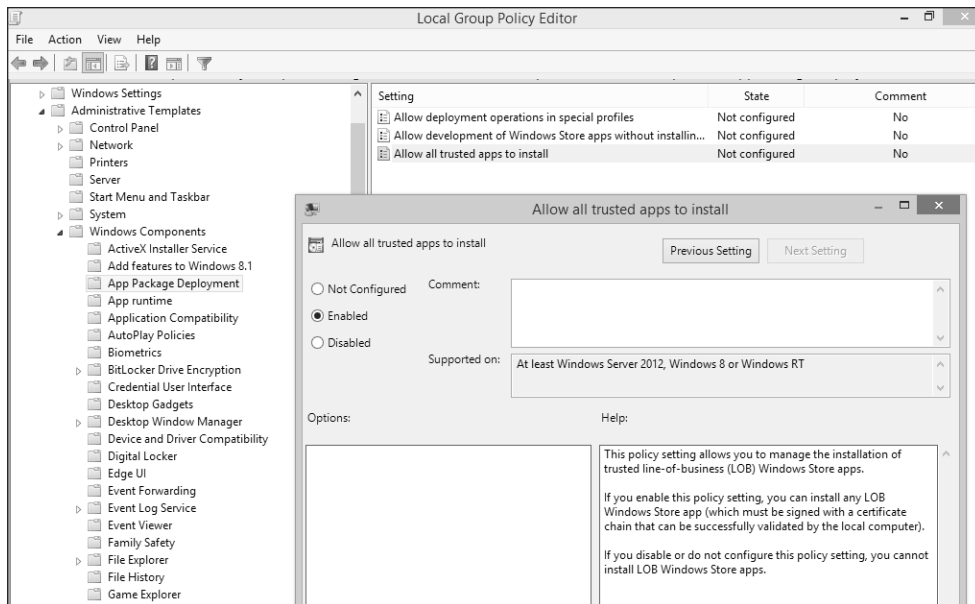


FIGURE 1-27 You must enable the applicable Group Policy setting Allow All Trusted Apps To Install to incorporate sideloading.

Activating a sideloading key

To enable sideloading on a Windows 8 or Windows 8.1 Enterprise computer that's not joined to a domain or on any Windows 8 or Windows 8.1 Pro computer, you must use a sideloading product activation key. To enable sideloading on a Windows RT device, you must also use a sideloading product activation key.

To add a sideloading product key and then activate it with the generic activation Globally Unique Identifier (GUID), follow these steps:

1. Open an elevated command prompt.
2. Type **slmgr /ipk <sideloading product key>**.
3. Type **slmgr /ato ec67814b-30e6-4a50-bf7b-d55daf729d1e**.

Sideloading the app

After you configure the necessary Group Policy settings and create your app package, you're ready to sideload the app. You can do this manually, per user, or you can do it for multiple users at one time.



EXAM TIP

Some exam questions require you to put two or more technologies together to form a solution. For example, you might be asked how you would deploy an app to all client computers in a domain, configure that app to access network resources, and “minimize administrative effort.” The answer will then be twofold, perhaps one that includes applying a specific Group Policy Object (Allow All Trusted Apps To Install) along with a specific Windows PowerShell cmdlet (such as *add-appxpackage*).

If you want to manually sideload the app to the current user, in Windows PowerShell you must add the appx module and then add the app package, as follows:

1. Type **Import-module appx**. Press Enter.
2. Type **Add-appxpackage “path and name of the app”** to add the app. Press Enter. Table 1-6 shows the available appx cmdlets. If you need to add app dependencies, the command should look more like this: *add-appxpackage C:\MyApp.appx -DependencyPath C:\appplus.appx*.

TABLE 1-6 Appx module cmdlets

Cmdlet	Description
<i>Add-AppxPackage</i>	To add a signed app package to a single user account
<i>Get-AppxLastError</i>	To review the last error reported in the app package installation logs
<i>Get-AppxLog</i>	To review the app package installation log
<i>Get-AppxPackage</i>	To view a list of the app packages installed for a user profile
<i>Get-AppxPackageManifest</i>	To read the manifest of an app package
<i>Remove-AppxPackage</i>	To remove an app package from a user account

The app installs and then is available to the user. This must be done for each user if multiple users share a single computer. Figure 1-28 shows a Windows PowerShell session with two typed commands: *import-module appx* and *add-appxpackage*.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Joli> import-module appx
PS C:\Users\Joli> add-appxpackage "MyNewApp"
```

FIGURE 1-28 Use Windows PowerShell to sideload an app to the current user.

NOTE

In larger enterprises you would use the *Add-AppxPackage* cmdlet as part of an automated software-distribution deployment plan. The command can also be incorporated into scripts.

If you want to sideload the apps to multiple computers, use DISM. You can use DISM commands to manage app packages (.appx or .appxbundle) in a Windows image. The .appxbundle is new for Windows 8.1 and combines both app and resource packages to enhance the app experience. When you use DISM to provision app packages, those packages are added to a Windows image and are installed for the desired users when they next log on to their machines.

You should be familiar with the DISM syntax when servicing a Windows image, whether a computer is offline or online. Table 1-7 lists a few to keep in mind.

TABLE 1-7 DISM syntax for servicing a Windows image

Command	Purpose
<i>DISM.exe [/Image:<path_to_image_directory> /Online] [dism_global_options] {servicing_option} [<servicing_argument>]</i>	To service a Windows image with DISM
<i>DISM.exe /Image:<path_to_image_directory> [/Get-ProvisionedAppxPackages /Add-ProvisionedAppxPackage /Remove-ProvisionedAppxPackage /Set-ProvisionedAppxDataFile]</i>	To service an app package (.appx or .appxbundle) for an offline image
<i>DISM.exe /Online [/Get-ProvisionedAppxPackages /Add-ProvisionedAppxPackage /Remove-ProvisionedAppxPackage /Set-ProvisionedAppxDataFile]</i>	To service an app package (.appx or .appxbundle) for a running operating system



EXAM TIP

When you need to make a company app available to the public, you have to certify and publish the app to the Windows Store.

Other command-line service options include */Get-ProvisionedAppxPackages*, */FolderPath*, */PackagePath*, */LicensePath*, and */Add-ProvisionedAppxPackage*. Becoming familiar with these is extremely important because you'll likely be tested on them. You can learn about all available commands and options at <http://technet.microsoft.com/en-US/library/hh824882.aspx>. Review this article and make sure that you can make sense of commands you might see, perhaps one that looks like

```
Dism /Online /Add-ProvisionedAppxPackage /FolderPath:C:\Test\Apps\MyUnpackedApp  
/SkipLicense
```

or like

```
Dism /Image:C:\test\offline /Add-ProvisionedAppxPackage /FolderPath:c:\Test\Apps\  
MyUnpackedApp /CustomDataPath:c:\Test\Apps\CustomData.xml
```

**EXAM TIP**

You must install an app package (.appx) on an operating system that supports Windows 8 apps. You can install an app bundle package (.appxbundle) on an operating system that supports Windows 8.1 apps. Apps aren't supported in Windows PE 4.0.

Sideload apps by using Windows Intune

Windows Intune lets you sideload apps via the cloud and make them available to any authorized, compatible device that's connected to the Internet. You need to perform several steps to sideload apps (If you want to follow along, you can download Windows Intune for free and use it for 30 days without a subscription to TechNet or MSDN, or even without using a credit card):

1. Work through the available wizard to upload your software.
2. Add users and create groups, if applicable.
3. Choose the users, groups, computers, and devices that can download the software, and link them (user-to-device).
4. For the self-service model in this example, choose how to deploy the app. It can be available, or available and required.
5. Verify that the app is available in the Windows Intune Company Store.

NOTE FORCING APP INSTALLATION

Windows Intune is a self-service model. This means that you cannot use it to force apps to be installed on client machines. You can create groups and assign the apps to the groups, but the user will still need to approve the installation.

Adding a user

To get the full Windows Intune experience, you need to create a few users and, perhaps, add them to groups. From the Admin Overview page shown in Figure 1-29, click Add Users. Notice that the Admin page is selected at the top. Fill in the fields to create your new user. Type a first and last name, a display name, a user name, and any additional details you want to include. Assign the desired role, perhaps Billing Administrator or User Administrator, or simply create a new user. Finally, select the Windows Intune user group—by default, only one, Windows Intune (although you can create your own). Watch for an email that contains a temporary password for the new user.

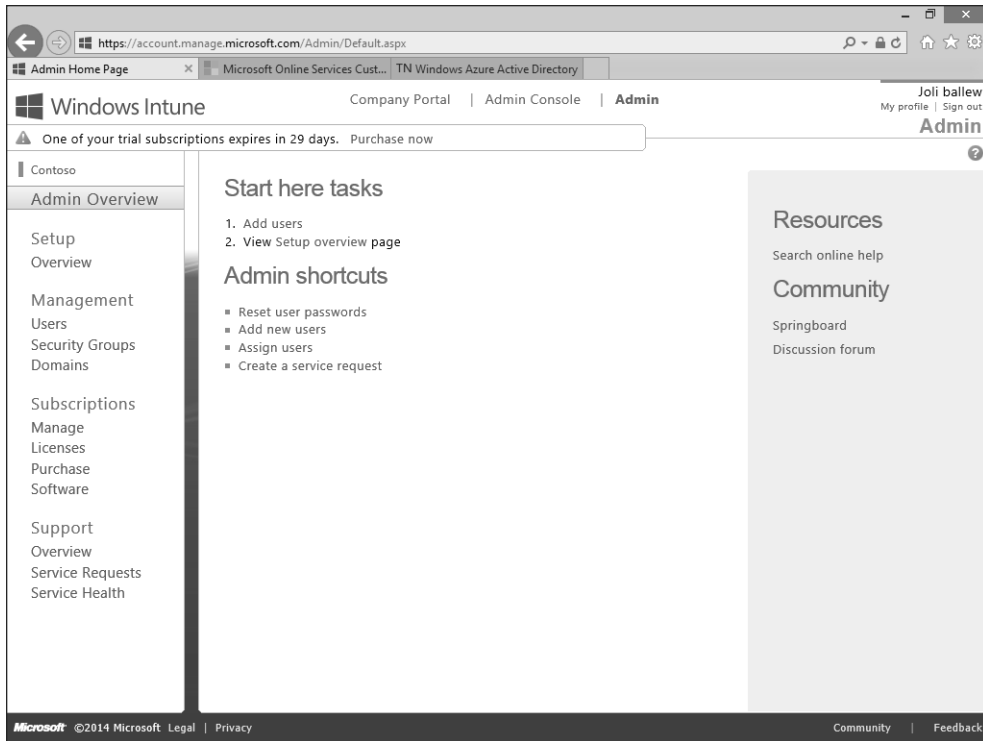


FIGURE 1-29 Add users and perhaps put them into groups before uploading software.

Uploading software

In the Windows Intune Admin page shown in Figure 1-29, click Admin Console at the top of the page. (Notice also a link to the Company Portal.) This opens a new window with many more tools and opportunities to personalize Windows Intune for your enterprise (see Figure 1-30). Click each tab in the left column, including System Overview, Groups (you might want to create a group now), Updates, Endpoint Protection, Alerts, Software, Licenses, Policy, Reports, and Administration. You'll be expected to be familiar with each tab when taking the exam. Now, click the Software tab.

To upload the desired software, follow these steps:

1. Click Add Software (on the Software Overview page).
2. If prompted, sign in with your Windows Intune Administrator account.
3. Read the information on the Before You Begin page and click Next.

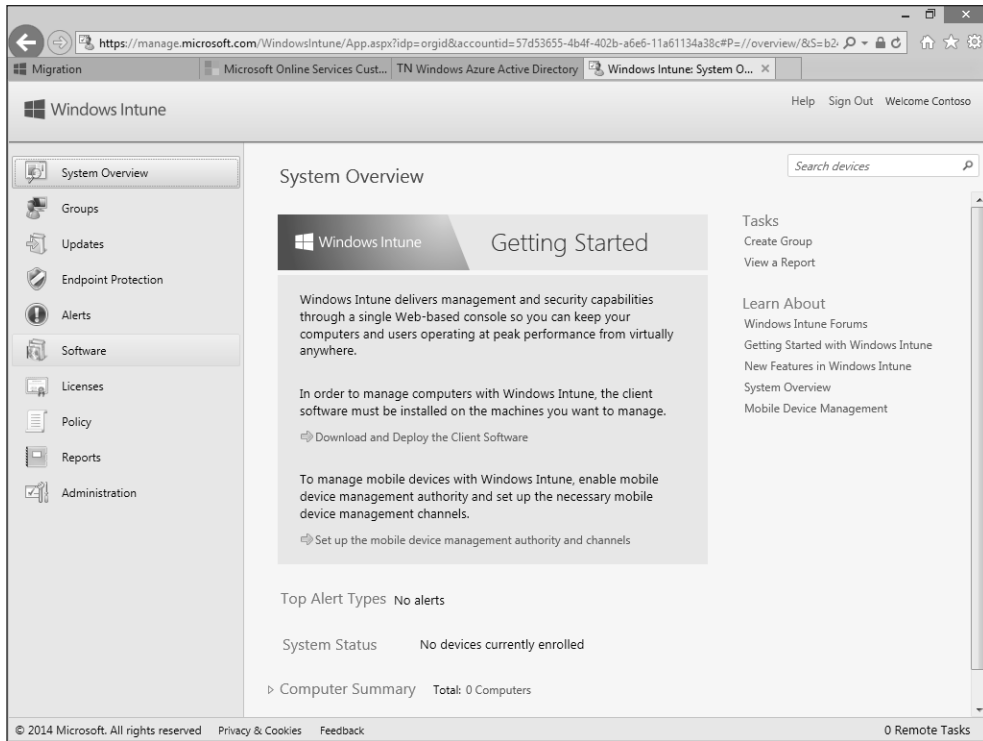


FIGURE 1-30 Review the options in the Windows Intune Admin Console page.

4. Make the desired choices from the Select The Platform And Specify The Location Of The Software Files page, including:
 - A. How this software is made available to devices: Software Installer or External Link. Choose Software Installer here.
 - B. The type of installer file type you'll use: Windows Installer (*.exe, *.msi) or Windows App Package (*.appx, *.appxbundle). Choose Windows Installer (*.exe, *.msi) here.
 - C. Click Browse and locate the software file to install. You might browse to something like C:\Program Files as a start.
 - D. Click Open.
 - E. Click Next.
5. Continue to work through the wizard, adding information about the publisher, application name, architecture, operating system, and so on, clicking Next as applicable.
6. When you are at the end of the wizard, click Upload (see Figure 1-31).

7. Click Close.
8. Back on the Software Overview page, click Managed Software to see the uploaded file(s).

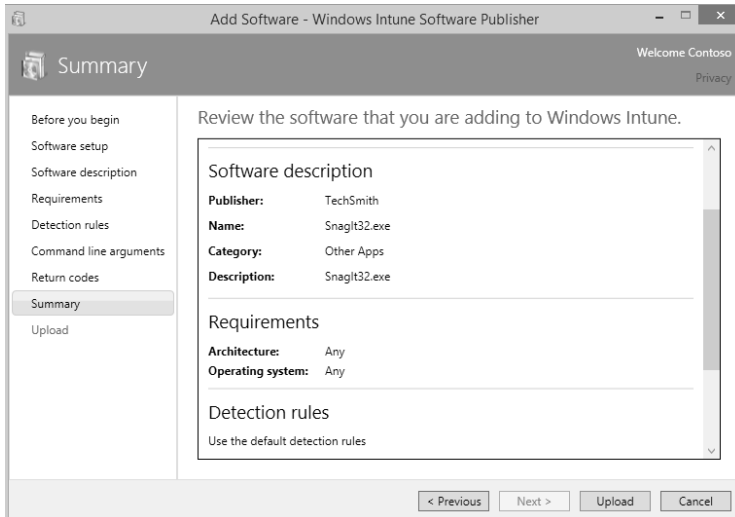


FIGURE 1-31 Upload software at the end of the wizard.



EXAM TIP

Detection rules let you specify how you want Windows Intune to determine whether the software already exists on the client. This ensures that the software isn't installed twice. You can opt for the default detection rules or create your own. The three rule types are File Exists, MSO Product Code Exists, and Registry Key Exists. If you are asked about these rules, first eliminate answers that don't have anything to do with those three things. Also, Registry key names that start with HKEY_LOCAL_MACHINE are okay to use in a detection rule, but other options aren't recommended because they aren't applied directly to the machine. Likewise, when using a path to create a rule, don't choose a path specific to a user; instead, choose a path that has to do with where program files are stored.

Selecting users and/or groups and deploying your app

With the software uploaded, you're ready to choose the users, groups, computers, and/or devices to which you want to deploy the application. You can use Active Directory synchronization to populate the account portal if you want. If you don't have that option, however, open the Windows Intune Admin Console, shown in Figure 1-30, click the Software tab and from Software workspace click Managed Software. From there you can manage deployment.



EXAM TIP

To use Windows Intune to manage a user's computer directly, you must first download and install (automatically or manually) the Windows Intune client software package on it. The computer can be a physical computer or a virtual machine. You can get this software from the Windows Intune Admin Console on the Administrator tab. The directions offered instruct you to wait 30 minutes before verifying that the computers appear in the Windows Intune Administrator Console.

Now you can select the users, groups, and computers that can access the software. If you are following along here, click Ungrouped Users and then click Add. Otherwise, select any group you've created or other applicable choices. From the Select The Deployment Settings For This Software page, shown in Figure 1-32, click the arrow beside each entry that shows Do Not Install and click Available Install or Required Install as applicable. Then, you can click Finish (not shown).

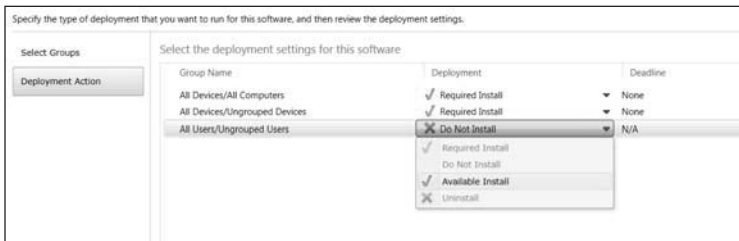


FIGURE 1-32 Make the software available to users.

Review the results. From the Managed Software page you can see how many users have this software available. Now, as an administrator you must link the users to a device (or devices) in your inventory. You do this from the Groups tab, from All Computers, and by clicking Link User. From there you select the desired device to link. The user is almost ready to log on and access your app. (You need to wait a half hour or so for all the information to sync.)

To test your new configuration, log on as the standard user you created at the Windows Intune Company Portal. If you created an administrator account, log on using either the Windows Intune Administrator Console or the Windows Intune Account Portal. All these links are available in the email the user received with his or her temporary password. After logon, users must click the option to enroll the device they're using. Following that, click All Apps to see the available app. Figure 1-33 shows the Windows Intune Company Portal.

Finally, you can review how many computers have installations pending and how many users have the deployed software available. Figure 1-34 shows the Managed Software tab in the Windows Intune Administrator Console, with a deployed application selected and the current status of the software showing at the bottom of the page.

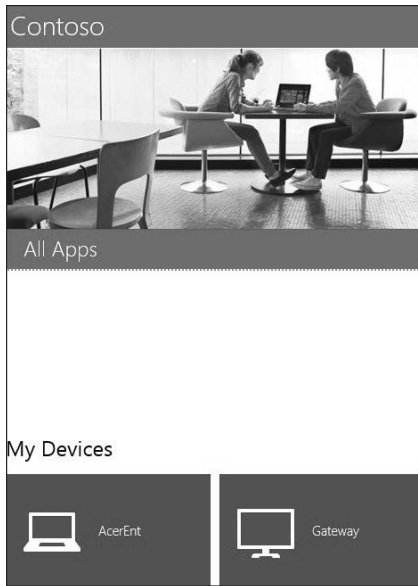


FIGURE 1-33 The user logs on to the Windows Intune Company Portal from an approved device to access the All Apps option.

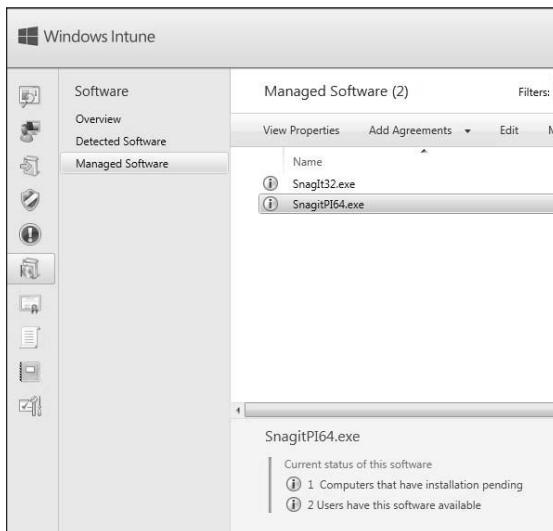


FIGURE 1-34 Administrators can keep track of the status of their deployed software easily.

MORE INFO USING WINDOWS INTUNE AND CONFIGURATION MANAGER

You can use Windows Intune to sideload apps in conjunction with System Center 2012 SP1 Configuration Manager by also incorporating the Windows Intune connector. This tool enables you to manage your apps with the Configuration Manager console. For more information, visit <http://technet.microsoft.com/en-us/windows/dn223286.aspx>.

Before moving on, you need to know a few more things about Windows Intune:

- You can embed Windows Intune in an operating system deployment image.
- After you install the Windows Intune client software, you must restart the PC.
- You can enroll mobile devices from the Administration tab.
- Windows Intune client software can be installed only on computers that are running the following:
 - Windows XP Professional, Service Pack (SP) 3
 - Windows Vista Enterprise, Ultimate, or Business editions
 - Windows 7 Enterprise, Ultimate, or Professional editions
 - Windows 8 Enterprise or Pro editions
 - Windows 8.1 Enterprise or Pro editions
- Windows Intune supports the following mobile devices:
 - Windows Phone 8
 - iOS
 - Android
 - Windows RT
- When you opt to deploy an application by using an external link, you can provide a link to an application on the Windows Store or to a web-based application that runs in a user's web browser.
- Users can contact IT from the Windows Intune Company Portal.
- After installing client software and performing other tasks, you might have to wait for a while before you see the changes in the Windows Intune Administrator Console.

Deep linking apps by using Windows Intune

You can make Windows Store apps available to your Windows RT users in your company portal by using Windows Intune as well as Configuration Manager. This section focuses on Windows Intune. You'll follow the same basic process as you did when deploying an app via the Installed Software option, but this time you choose External Link when you get to the Select The Platform And Specify The Location Of The Software Files page. Before you begin, decide which Windows Store app you want to deploy. For this example, choose OneDrive for Business.

The first part of the process requires you to obtain the link to the app you want to add to your company portal. To obtain the link for OneDrive for Business, follow these steps:

1. From the Start screen, click Store.
2. Search for OneDrive for Business, and then click it to access the installation page.
3. From the charms (Windows logo key+C), click Share.
4. Click Mail.
5. The email contains the link. Send this link to yourself, copy the link and paste it into Notepad, or otherwise make the link accessible for later.

The second part of the deep-linking process involves adding the app to add to Windows Intune:

1. Log on to the Windows Intune Administrator Console.
2. Click the Software tab, Managed Software, Add Software.
3. From the Select The Platform And Specify The Location Of The Software Files page, under Select How This Software Is Made Available To Devices, select External Link.
4. In the Specify The URL box, paste the link to OneDrive for Business. Click Next.
5. Carefully input the information to describe the software. What you input can be viewed by your employees. Click Next when finished.
6. Verify that the information is correct (see Figure 1-35). Click Upload.

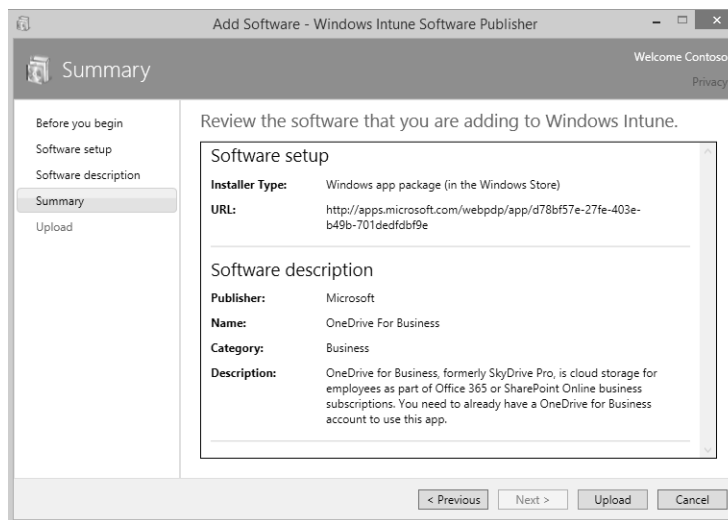


FIGURE 1-35 Add a Windows Store app to Windows Intune for deploying to users.

7. Click Close.

8. From the Managed Software screen, verify that OneDrive For Business is selected, and click Manage Deployment.
9. Click All Users, Add, and then click Next.
10. Under Approval, click the arrow and select Available Install.
11. Click Finish.

Your Windows RT users can now open their company portal app (which they've previously obtained from the Windows Store), log on, locate the deployed app, and install it.



Thought experiment

Managing Microsoft Office in a small business

In this thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You manage a small business that has seven employees, and each employee has multiple devices that they use to perform work. You don't have an Active Directory domain. Sometimes the users are at the company, sometimes at home, and often in a hotel. Users don't always have Internet access.

Users complain that they can't always access their work documents and that when they use Microsoft Office on their devices, they get a difference user experience on all of them. Their settings and preferences continually need to be reset for each device as they change them. You want to resolve these problems (and others, including mandating Microsoft Office updates), but you don't have a lot of money to spend.

1. What should you set up to resolve all these issues, all without incurring a lot of expense?
2. Where would you store the users' data?
3. If you want to delegate some of the responsibilities for managing your solution, what types of administrator would you create to manage support tickets?

Objective summary

- Network administrators can integrate users' Microsoft accounts into the workplace to enable users to incorporate what they've configured with these accounts with their domain accounts.
- You can manage desktop apps in many ways, such as by using Office 365, Configuration Manager, DISM, and Windows Intune.

- You can sideload apps to offer them to your users without going through the Windows Store certification process.
- You can configure Group Policy settings to manage your desktop apps, to manage access to the Windows Store, and to enable sideloading.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. Where can you configure a Group Policy that restricts the use of Microsoft accounts for a specific group of users in an Active Directory domain?
 - A. In the Group Policy Management Editor window, by expanding Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, Security Options
 - B. In the Group Policy Management Editor window, by expanding Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, User Rights Assignment
 - C. In the Local Group Policy Editor, by navigating to Computer Configuration, Windows Settings, Security Settings, Local Policies, Security Options
 - D. In the Local Group Policy Editor, by navigating to Computer Configuration, Windows Settings, Security Settings, Local Policies, User Rights Assignment
2. Where can users opt to connect a Microsoft account with a domain account?
 - A. Users can't do this; an administrator must perform this task for them in Active Directory.
 - B. From their local computer, in PC Settings, from the Accounts tab
 - C. In the Group Policy Management Editor window, by expanding Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, Security
 - D. From their local computer, in PC Settings, from the OneDrive tab
3. Which of the following can you manage in the Office 365 Admin Center?
 - A. Active Directory synchronization
 - B. Valid, expired, and assigned licenses
 - C. User passwords, including resetting
 - D. All of the above
 - E. B and C only

4. You need to disable access to the Windows Store for one group of employees in your workgroup. How do you do this?
- A. Configure a Group Policy setting that disables the policy Turn On The Store Application.
 - B. Configure a Group Policy setting that enables the policy Turn On The Store Application.
 - C. Configure a Group Policy setting that disables the policy Turn Off The Store Application.
 - D. Configure a Group Policy setting that enables the policy Turn Off The Store Application.
5. Which of the following tools and technologies can help you sideload company apps?
- A. DISM
 - B. Windows PowerShell
 - C. Configuration Manager
 - D. Windows Intune
 - E. All of the above
 - F. Only C and D
6. What Group Policy setting do you have to enable before users can install apps you've sideloaded?
- A. None
 - B. Allow All Trusted Apps To Install
 - C. Allow Development Of Windows Store Apps
 - D. Block Microsoft Accounts
7. When you offer a sideloaded app to a Windows RT device, which of the following commands must you run at an elevated command prompt?
- A. `slmgr /ipk <sideload product key>`
 - B. `slmgr /ato ec67814b-30e6-4a50-bf7b-d55daf729d1e`
 - C. `import-module appx`
 - D. `Add-AppxPackage`
 - E. All of the above

- 8.** True or false: You can make sideloaded apps mandatory and force their installation on to clients by applying the applicable settings in Windows Intune.
- A.** True
 - B.** False
- 9.** You want to manage a user's computer by using Windows Intune, on a computer running Windows 7 Professional. What must you do first?
- A.** Install the Windows Intune client software package on it.
 - B.** Install the Windows Intune connector.
 - C.** Upgrade the computer to Windows 7 Enterprise or Windows 8 Enterprise.
 - D.** Install the company portal from the Windows Store.
- 10.** Which of the following describes the purpose of deep linking an app?
- A.** To push out specific Windows Store apps to your Windows RT users
 - B.** To make Windows Store apps available to your Windows RT users in your company portal
 - C.** To add your company apps to the Windows Store
 - D.** None of the above

Answers

This section contains the solutions to the thought experiments and answers to the objective review questions in this chapter.

Objective 1.1: Thought experiment

1. Native VHD.
2. Windows ADK. You can install this on another Windows 7 or Windows 8-based technician computer and use it to create the Windows PE disk.
3. DISM. You will use the Deployment Image Service and Management (DISM) tool to apply an existing Windows 8 image—in this case, the one you created.
4. 30 GB.

Objective 1.1: Review

1. **Correct answers:** A, C
 - A. **Correct:** You must use a Windows 8-based computer, and you need the Windows 8-based installation files.
 - B. **Incorrect:** The drive must be 32 GB or larger, not 64 GB.
 - C. **Correct:** TPM protects a specific computer from unauthorized access, and Windows To Go is used on more than one.
 - D. **Incorrect:** Resetting or refreshing isn't supported. Problematic drives should be reimaged.
 - E. **Incorrect:** Windows To Go isn't supported on Windows RT or Mac computers.
2. **Correct answer:** A
 - A. **Correct:** Because hibernation is disabled by default, leaving Not Configured or changing the policy to Disabled is correct.
 - B. **Incorrect:** If you enable this policy, hibernation becomes enabled.
 - C. **Incorrect:** Sleep and hibernate are different. Thus, the Group Policy for sleep isn't the proper policy to configure.
 - D. **Incorrect:** Sleep and hibernate are different. Thus, the Group Policy for sleep isn't the proper policy to configure.

3. Correct answer: D

- A. Incorrect:** Boot.ini is no longer used.
- B. Incorrect:** BCDedit and BCDboot are command-line utilities used to configure and control the process.
- C. Incorrect:** BCDedit and BCDboot are command-line utilities used to configure and control the process.
- D. Correct:** Startup parameters are stored in the BCD Store.

4. Correct answers: B, D

- A. Incorrect:** */import* is used to restore a store, using what you've obtained before using the */export* parameter.
- B. Correct:** Use */create store* to create a new empty startup configuration store.
- C. Incorrect:** */boot sequence* is used to configure a one-time startup sequence for the boot manager.
- D. Correct:** */default* defines the default startup entry.
- E. Incorrect:** */displayorder* sets the startup order in a multiboot system.
- F. Incorrect:** */new* isn't a valid parameter.

5. Correct answer: C

- A. Incorrect:** Although you could likely start to the Windows 7 DVD and begin an installation, you couldn't create a second partition or shrink the existing one while performing that installation.
- B. Incorrect:** Before you can create a new volume from unallocated space, you must first make that space available by shrinking the existing partition.
- C. Correct:** You must first open Disk Management and shrink the existing partition.
- D. Incorrect:** Multibooting with an operating system older than Windows 7 required a specific order, but that is not a requirement now. Thus, there is no need to format the drive first.

6. Correct answer: B

- A. Incorrect:** Thin images include little or no customization, and most of the device drivers, applications, and updates are installed by using another method on each client computer.
- B. Correct:** Thick images are loaded with applications, drivers, and customizations and require a lot of planning, lots of bandwidth for rollout, and much more time to create and manage.
- C. Incorrect:** Hybrid images are like thin images, but with a few more customizations. Hybrid images aren't thick images.
- D. Incorrect:** A custom image might include only one device driver and one background image.

7. Correct answer: E

- A. Incorrect:** MDT is required, but so is Windows ADK, a network share, and a reference computer.
- B. Incorrect:** Windows ADK is required, but so is MDT, a network share, and a reference computer.
- C. Incorrect:** A network share is required, but so is a reference computer, MDT, and Windows ADK.
- D. Incorrect:** A reference computer is required but so is a network share, MDT, and Windows ADK.
- E. Correct:** All of the above are required.
- F. Incorrect:** You do need MDT.

8. Correct answer: B

- A. Incorrect:** MDT doesn't include DISM but does include tools needed to automate desktop deployments.
- B. Correct:** The Windows ADK includes DISM.
- C. Incorrect:** SIM, or System Image Manager, is used to create answer files and is available from the Windows Automated Installation Kit (AIK).
- D. Incorrect:** The Application Compatibility Toolkit (ACT) is used to verify compatibility of applications and computers with Windows 8.1.

9. Correct answers: A, B

- A. Correct:** *copyype amd64 C:\WinPE_amd64* is a valid command for copying Windows PE files.
- B. Correct:** *copyype amd32 C:\WinPE_amd32* is a valid command for copying Windows PE files.
- C. Incorrect:** *MakeWinPEMedia /ISO C:\winpe_amd64 c:\winpe_amd64\winpe.iso* is used to create an ISO file from the Windows PE files.
- D. Incorrect:** *Dism /Get-MountedImageInfo* is used when mounting an image.

10. Correct answer: F

- A. Incorrect:** DISM PowerShell cmdlets and all other choices are included in MDT.
- B. Incorrect:** DISM API and all other choices are included in MDT.
- C. Incorrect:** Windows System Image Manager (Windows SIM) and all other choices are included in MDT.
- D. Incorrect:** OSCDIMG and all other choices are included in MDT.
- E. Incorrect:** The Volume Activation Management Tool (VAMT) and all other choices are included in MDT.
- F. Correct:** All of the above are included in MDT.
- G. Incorrect:** Everything listed is included with MDT.

Objective 1.2: Thought experiment

1. ACT.
2. SQL Server (to create an ACT database).
3. Inventory the computers and applications in the enterprise.
4. First you create and deploy an inventory collector package, and then you create and deploy a runtime-analysis package.
5. The ACM.

Objective 1.2: Review

1. **Correct answers:** A, D
 - A. **Correct:** A shim can be used as a short-term solution for application incompatibility.
 - B. **Incorrect:** You create a runtime-analysis package to test compatibility, not to fix compatibility problems.
 - C. **Incorrect:** You can use Program Compatibility Mode to manage compatibility issues by letting the applications run in an older operating system space, but you can't configure it to resolve compatibility issues in newer ones.
 - D. **Correct:** This is an option, but would require a lot of work to set up. When you use RemoteApp, the application is run on a remote server and is made available for clients from there.
2. **Correct answer:** B
 - A. **Incorrect:** Shims can fix quite a few types of problems but can't fix issues that are related to UAC.
 - B. **Correct:** This tool lets you fix problems related to UAC.
 - C. **Incorrect:** App-V is used to virtualize applications but can't be used to create shims.
 - D. **Incorrect:** You can resolve the problem with SUA.
3. **Correct answer:** C
 - A. **Incorrect:** Client Hyper-V lets you run and manage applications in a virtual machine that you manage.
 - B. **Incorrect:** App-V lets you virtualize applications so that you can use the applications side by side on the same system.
 - C. **Correct:** RemoteApp lets you access applications remotely through Remote Desktop Services, and the apps themselves are housed and managed on network servers.
 - D. **Incorrect:** Windows Intune lets you manage apps in the cloud, not on your own network servers.

4. Correct answer: B

- A. Incorrect:** If you can't provide administrator credentials you wouldn't have gotten as far as selecting the first two options.
- B. Correct:** The computer's processor isn't SLAT.
- C. Incorrect:** If the computer's architecture is 32 bit, you wouldn't see the first two entries at all.
- D. Incorrect:** If the computer is running Windows 8.1 (not the Pro or Enterprise edition), you wouldn't see the first two entries at all.

5. Correct answer: D

- A. Incorrect:** These two are required but are listed out of order.
- B. Incorrect:** The required technology is RemoteApp, not App-V.
- C. Incorrect:** The required technology is RemoteApp, not App-V.
- D. Correct:** These two servers are required and are listed in the proper order.

6. Correct answer: E

- A. Incorrect:** A working Active Directory and network share are required, but so are the other listed elements.
- B. Incorrect:** A UE-V Agent is required, but so are the other listed elements.
- C. Incorrect:** A UE-V Generator is required, but so are the other listed elements.
- D. Incorrect:** A Settings Storage Location is required, but so are the other listed elements.
- E. Correct:** All of the above are parts of the UE-V solution.
- F. Incorrect:** All of the listed elements are required.

7. Correct answer: A

- A. Correct:** Deploy the Settings Storage Location is the first thing you do.
- B. Incorrect:** Deploy the UE-V Agent is the second thing you do.
- C. Incorrect:** Install the Group Policy templates is the third thing you do.
- D. Incorrect:** Install the Agent Generator is the fourth thing you do.
- E. Incorrect:** Deploy the Settings Template Catalog is the fifth thing you do.
- F. Incorrect:** Deploy the Settings Location Templates is the sixth thing you do.

8. Correct answer: A

- A. Correct:** Endpoint Protection refers to malware.
- B. Incorrect:** Endpoint Protection involves malware, not updates.
- C. Incorrect:** Policy does refer to security, but it has more to do with creating security policies than it does with malware specifically.
- D. Incorrect:** Licensing is an important element of Windows Intune, but Endpoint Protection refers to malware.

Objective 1.3: Thought experiment

1. Office 365.
2. Most likely using the cloud, with options that enable the user to sync that data even when they aren't online.
3. Billing; Global; Password; Service; User Management.

Objective 1.3: Review

1. **Correct answer:** A
 - A. Correct:** Options to restrict the use of Microsoft accounts for a group of users in a domain are in the Group Policy Management Editor window. Expand Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies, Security Options.
 - B. Incorrect:** The User Rights Assignment node doesn't provide options for restricting Microsoft accounts.
 - C. Incorrect:** To restrict a group of users in an Active Directory domain you need to access Group Policy, not Local Group Policy.
 - D. Incorrect:** To restrict a group of users in an Active Directory domain, you need to access Group Policy, not Local Group Policy. Also, User Rights doesn't offer the options you need.
2. **Correct answer:** B
 - A. Incorrect:** Users can do this from their local computers.
 - B. Correct:** This is the correct answer; from their local computers, in PC Settings, from the Accounts tab.
 - C. Incorrect:** You can't connect a Microsoft account using Group Policy.
 - D. Incorrect:** This is achieved in PC Settings, but not from the OneDrive tab.
3. **Correct answer:** D
 - A. Incorrect:** Active Directory synchronization is one of the things can you manage in the Office 365 Admin Center, but others are correct here.
 - B. Incorrect:** Valid, expired, and assigned licenses is one of the things can you manage in the Office 365 Admin Center, but others are correct here.
 - C. Incorrect:** User passwords, including resetting, is one of the things can you manage in the Office 365 Admin Center, but others are correct here.
 - D. Correct:** All of the above can be configured in the Office 265 Admin Center.
 - E. Incorrect:** All the answers are correct, not just B and C.

4. Correct answer: D

- A. Incorrect:** Access to the Store is on by default, and the policy listed here doesn't exist anyway.
- B. Incorrect:** Access to the Store is on by default, and the policy listed here doesn't exist anyway.
- C. Incorrect:** You need to enable this policy, not disable it.
- D. Correct:** You need to configure Group Policy to enable the policy Turn Off The Store Application.

5. Correct answer: E

- A. Incorrect:** DISM is only one of the correct options listed.
- B. Incorrect:** Windows PowerShell is only one of the correct options listed.
- C. Incorrect:** Configuration Manager is only one of the correct options listed.
- D. Incorrect:** Windows Intune is only one of the correct options listed.
- E. Correct:** All of the above
- F. Incorrect:** "Only C and D" isn't correct because A and B are correct also.

6. Correct answer: B

- A. Incorrect:** Special Group Policies are required.
- B. Correct:** Allow All Trusted Apps To Install is the required Group Policy setting that must be enabled.
- C. Incorrect:** Allow Development Of Windows Store Apps isn't the correct Group Policy setting to enable.
- D. Incorrect:** You should not block Microsoft accounts; you should enable the Group Policy setting listed for answer B.

7. Correct answers: A, B

- A. Correct:** `slmgr /ipk <sideloading product key>` loads the product key, which is required for Windows RT devices.
- B. Correct:** `slmgr /ato ec67814b-30e6-4a50-bf7b-d55daf729d1e` is the second requirement, and the entry here is the GUID.
- C. Incorrect:** `import-module appx` is a Windows PowerShell command used with sideloading, but isn't run at an elevated command prompt and isn't the correct answer here.
- D. Incorrect:** `Add-AppxPackage` is a Windows PowerShell command used with sideloading, but isn't run at an elevated command prompt and isn't the correct answer here.
- E. Incorrect:** All of the above isn't correct because C and D are incorrect.

8. Correct answer: B

- A. Incorrect:** You cannot make sideloaded apps mandatory and force their installation on to clients by applying the applicable settings in Windows Intune.
- B. Correct:** This statement is false.

9. Correct answer: A

- A. Correct:** You must first install the Windows Intune client software package on it.
- B. Incorrect:** To use Windows Intune to sideload apps in conjunction with System Center 2012 SP1 Configuration Manager, you must also incorporate the Windows Intune connector. It's not required in this scenario, though.
- C. Incorrect:** You don't need to upgrade the computer to Windows 7 Enterprise or Windows 8 Enterprise; Windows 7 Professional is compatible.
- D. Incorrect:** You don't achieve this by installing the company portal from the Windows Store.

10. Correct answer: B

- A. Incorrect:** You don't use deep linking to push out specific Windows Store apps to your Windows RT users.
- B. Correct:** To make Windows Store apps available to your Windows RT users in your company portal, you use deep links.
- C. Incorrect:** You don't use deep linking to add your company apps to the Windows Store. It's used to make Windows Store apps available through the company portal.
- D. Incorrect:** "None of the above" isn't correct. B is correct.

This page intentionally left blank

Index

Symbols

6to4 transition technology, 99–100
802.1x wireless technology standard, 110
802.11ac wireless technology standard, 110
802.11a wireless technology standard, 109
802.11b wireless technology standard, 109
802.11g wireless technology standard, 110
802.11i wireless technology standard, 110
802.11n wireless technology standard, 110
/? parameter (Cipher.exe command), 188

A

Accelerators (Manage Add-Ons dialog box), 280
access control lists (ACLs), 181
accessing resources
 authentication and authorization, 150–165
 account policies, 160–161
 computer authentication vs user authentication, 159–160
 credential caching, 161–162
 Credential Manager, 162–164
 homegroups, workgroups, and domains, 156–159
 local accounts vs Microsoft accounts, 164–165
 multifactor authentication, 151–156
 Secure Channel, 160
 Workplace Join, 165
data security, 180–200
 BitLocker Drive Encryption, 191–200
 EFS (Encrypting File System), 186–189
 permissions, 180–186
 removable devices, 190
data storage, 169–177
 BranchCache, 173–175

DFS, 169–170
OneDrive, 175–177
Storage Spaces, 171–173
network connectivity, 93–123
 automatic IP address assignment, 96–97
 IPv4, 94–96
 IPv6, 97–99
 names resolution, 101–106
 security, 113–123
 transition technologies, 99–101
 wireless networks, 106–113
remote access, 127–147
 DirectAccess, 134–138
 NAP, 141–147
 RDP, 131–134
 remote administration, 138–141
 VPNs, 127–131
Access (Office 365), 59
access policies, mobile devices, 246–247
Account Lockout Duration policy, 161
Account Lockout Policies, 161
Account Lockout Threshold policy, 161
account policies, authentication and authorization, 160–161
Accounts: Block Microsoft Accounts setting, 165
ACLs (access control lists), 181
ACT (Application Compatibility Toolkit), 29–36
 fixing problems, 33–36
 inventory collector packages, 30–31
 reviewing report data, 33
 runtime-analysis packages, 31–33
 tools, 30
activating sideloading key, 69–72
Active Directory Certificate Services (AD CS), 151
Active Directory Users And Computers snap-in, 160
active partitions, 9
AD CS (Active Directory Certificate Services), 151

Add-AppxPackage cmdlet

- Add-AppxPackage cmdlet, 70
- add-appxpackage command, 70
- ad hoc scenario, connecting to wireless networks, 111
 - administration
 - monitoring and managing printers, 233–235
 - remote access, 138–141
- Administrator Roles, Office 365, 61–64
- Administrator tab (Windows Intune), 49
- Admin Overview page (Windows Intune), 72
- Advanced Encryption Standard (AES), 187
- advantages, Windows PE, 22
- AES (Advanced Encryption Standard), 187
- AH (Authentication Headers) protocol, 120
- alerts, setting with Windows Intune, 294–298
- Alerts tab (Windows Intune), 49
- Alert Status, Windows Intune monitoring, 295
- Allow Hibernate (S4) When Starting From A Windows To Go Workspace setting (Windows To Go), 5
- Allow permissions, 182
- Alt key, Internet Explorer, 280
- APIPA (Automatic Private IP Addressing) range, 96
- App History tab (Task Manager), 230
- Application Compatibility Manager, 30
- Application Compatibility Toolkit. *See* ACT (Application Compatibility Toolkit)
- Applications report, 33
- application virtualization, 41
- AppLocker, 59
- applying
 - NTFS permissions, 181–185
 - Share permission, 180–181
- apps, desktop. *See* desktop applications
- App-V, 41
- App-V Management, 41
- App-V Publishing Server, 41
- App-V Reporting, 42
- App-V Reporting Server, 41
- App-V Sequencer installation, 42–43
- appx module cmdlets, 70
- architecture requirements, Windows To Go, 4
- Assessment Platform, 30
- Assessments tool (ACT), 30
- asynchronous processing, 284
- authentication, 150–165
 - account policies, 160–161
 - computer authentication vs user authentication, 159–160
 - credential caching, 161–162

- Credential Manager, 162–164
- homegroups, workgroups, and domains, 156–159
- local accounts vs Microsoft accounts, 164–165
- multifactor authentication, 151–156
- Secure Channel, 160
- VPN protocols, 128–129
- Workplace Join, 165
- Authentication Exemption rule, 121–122
- Authentication Headers (AH) protocol, 120
- authorization, 150–165
 - account policies, 160–161
 - computer authentication vs user authentication, 159–160
 - credential caching, 161–162
 - Credential Manager, 162–164
 - homegroups, workgroups, and domains, 156–159
 - local accounts vs Microsoft accounts, 164–165
 - Secure Channel, 160
 - Workplace Join, 165
- automatic IP address assignment, 96–97
- Automatic Private IP Addressing (APIPA) range, 96
- Automatic Update Approval rules, creating, 266
- autonomous host configuration, IPv6, 98

B

- backing up credentials, 163
- backup and recovery, EFS (Encrypting File System), 187–189
- Backup-CARoleService cmdlet, 153
- base 10 numbers, converting binary octets to, 94
- Base64-encoded X.509, 164
- basic NTFS permissions, 182–183
- BCDboot command-line tool, 9–11
- BCD (Boot Configuration Data) Store, 7
- BCDedit command-line tool, 8–9
- binary octets, converting to base 10, 94
- binding, 151
- biometrics, 155–156
- BIOS interfaces, 239
- BitLocker Drive Encryption, 191–200
 - BitLocker To Go, 196–197
 - configuring
 - command-line tools, 195–196
 - control panel, 193–195
 - data recovery, 198–199

- MBAM (Microsoft BitLocker Administration and Monitoring), 200–201
- startup key storage and recovery options, 197–198
- BitLocker To Go
 - configuring, 196–197
 - data recovery, 198–199
- Boot Configuration Data (BCD) Store, 7
- /boot sequence parameter (BCDedit command), 9
- boot settings, 7–14
 - adding native VHD to startup menu, 11
 - adding VHD to a computer with an operating system, 11–12
 - adding VHD to computers without an operating system, 12–14
- BCDboot, 9–11
- BCDedit, 8–9
- BranchCache, 173–175
- broadband connectivity, mobile devices, 251–254

C

- /c parameter (Cipher.exe command), 188
- CA (Certificate Authority), 151
- caching
 - credentials, 161–162
 - Group Policy, 285–286
- central access policies, DAC, 186
- central access rules, DAC, 186
- Certificate Authority (CA), 151
- Certificate Enrollment Policy Web Service, 153
- certificates
 - import/export operations, 164
 - multifactor authentication, 151–153
- CertMgr command, 152
- Challenge Handshake Authentication Protocol (CHAP), 129
- Change Group Policy Processing Ro Run
 - Asynchronously When A Slow Network Connection Is Detected setting, 286
- changePIN parameter (manage-BDE command), 195
- Change Share permission, 180–181
- CHAP (Challenge Handshake Authentication Protocol), 129
- checkpoints, 38
- ChkDsk, 221–222
- Cipher.exe command, 186–188
- claims, DAC, 186
- Class A addresses, 95
- Class B addresses, 95
- Class C addresses, 95
- Click-to-Run (Office 365), 64
- client caching, DFS, 170
- client compliance, 262–285
 - client security, 269–276
 - Group Policy application, 281–286
 - configuring caching, 285–286
 - policy processing, 283–284
 - RSOP (Resultant Set of Policy), 281–283
- Internet Explorer 11 security, 276–280
- managing updates, 263–270
 - Windows Intune, 265–269
 - Windows Update, 264–266
- Client Hyper-V, 36–39
- client management, Windows Intune
 - configuring monitoring and setting alerts, 294–298
 - policies, 299–303
 - remote computers, 302–303
 - users and groups, 290–294
- clients, NAP (Network Access Protection), 143–147
- CMAK (Connection Manager Administration Kit), 129
- cmdkey /add command-line tool, 163
- cmdlets. *See also* commands
 - appx module, 70
 - Backup-CARoleService, 153
 - DISM API, 20
 - Enable-WindowsOptionalFeature, 37
 - Get-Printer, 236
 - Get-PrintJob, 236
 - Install-WindowsFeature BranchCache, 173
 - Invoke-GPUUpdate, 283
 - ipconfig, 96–97
 - OSCDIMG, 20
 - Remove-PhysicalDisk, 171
 - Remove-PrintJob, 236
 - Repair-VirtualDisk, 171
 - Restore-CARoleService, 153
 - Set-PhysicalDisk, 171
 - Windows SIM, 20
- coexistence, desktop applications, 36–45
 - App-V, 41
 - App-V Sequencer installation, 42–43
 - Client Hyper-V, 36–39
 - MDOP, 41–42
 - RemoteApp, 39–40
 - sequencing applications, 43–45

command-line tools, configuring BitLocker Drive Encryption, 195–196

commands. *See also* cmdlets

add-appxpackage, 70

CertMgr, 152

Cipher.exe, 186–188

Cotype, 22–23

Disable-BC, 174

Enable-BCDistributed, 174

Enable-BCHostedClient, 174

Enable-BCHostedServer, 174

Enable-BCLocal, 174

Get-BCDataCache, 174

Get-BCStatus, 174

icacls.exe, 184–185

import-module appx, 70

manage-BDE, 195–196

manage-bde -forcerecovery <Volume>, 198

Mstsc.exe, 132

netsh nap client, 145, 146–147

Pnputil.exe, 221–222

Set-BCCache, 174

Sigverif.exe, 220

Xbootmgr.exe, 226

Xperf.exe, 226

XperfView.exe, 226

command sets (DISM tool), 19

Company Portal, Windows Intune, 76–77

compatibility, desktop applications, 29–36

Compatibility Administrator, 35–36

Computer And User (Kerberos V5) authentication method, 121

computer authentication, 159–160

computer groups, 292–293

Computer (Kerberos V5) authentication method, 121

Computer Management tool (DaRT), 238

Computer Name/Domain Changes dialog box, 158

Computer Name tab (System Properties dialog box), 157

computers, recovering, 238–239

Computer Summary, Windows Intune monitoring, 295

Configure Group Policy Slow Link Detection Policy setting, 284

Configure Group Policy Slow Link Detection setting, 286

Configure Logon Script Delay setting, 286

Configure User Group Policy Loopback Processing Mode setting, 286

configuring

advanced Wi-Fi settings, 108

BitLocker Drive Encryption

command-line tools, 195–196

control panel, 193–195

BitLocker To Go, 196–197

BranchCache, 173–175

DirectAccess, 134–138

deployment options, 136–137

new features, 136

understanding how DirectAccess works, 135

Windows 8.1 users, 137–138

EFS (Encrypting File System), 187

Group Policy caching, 285–286

Group Policy for Windows To Go, 5–6

inactive profiles, 117

monitoring, Windows Intune, 294–298

NAP clients, 143–147

RD Gateway Server Settings, 133–134

trusted PCs, 55–56

virtual smart cards, 154–155

conflicting policies, Windows Intune, 301

Connection Manager Administration Kit (CMAC), 129

connections, broadband connectivity

metered connections, 253–255

personal broadband connections, 252

shared personal hotspots, 252

Connection Security Rules, Windows Firewall With

Advanced Security window, 116

Content tab (Internet Explorer 11 security), 276

contradicting explicit permissions, 184

Control Panel

configuring BitLocker Drive Encryption, 193–195

monitoring Windows Firewall, 114

converting binary octets to base 10, 94

/copy parameter (BCDedit command), 9

copying Windows PE files, 22–23

Cotype command, 22–23

Crash Analyzer tool (DaRT), 238, 239–240

Create A New Policy Wizard, 245

creating

Automatic Update Approval rules, 266

checkpoints, 38

computer groups, 292–293

connection security rules, 121–123

Data Collector Sets, 227–230

desktop images, 17–18

picture passwords, 155

- security groups, 293–294
- shims, 34
- standard Windows PE DVD disks, 22–23
- storage pools, 172
- user groups, 292–293
- VPNs, 127–131
 - authentication protocols, 128–129
 - CMAK, 129
 - user profiles, 129–131
- Windows Store apps, 68
- Credential Manager, 162–164
- credentials
 - backing up, 163
- caching, 161–162
 - saving, 162
- critical alerts, 297
- Cryptographic Message Syntax Standard (PKCS#7), 164
- Custom (Connection security rule), 123
- custom installations, 17
- custom rules, 117
- customizing Windows installation using Windows PE, 21–25

D

- /d parameter
 - BCDboot command, 10
 - Cipher.exe command, 187
- DAC (Data Access Control), 185–186
- DaRT (Diagnostics and Recovery Toolkit) 8.1, 237–240
- DaRT recovery disks, 238–239
- DaRT Recovery Image Wizard, 238
- data
 - recovery
 - BitLocker Drive Encryption, 198–199
 - BitLocker To Go, 198–199
 - security, 180–200
 - BitLocker Drive Encryption, 191–200
 - EFS (Encrypting File System), 186–189
 - permissions, 180–186
 - removable devices, 190
 - storage, 169–177
 - BranchCache, 173–175
 - DFS, 169–170
 - OneDrive, 175–177
 - Storage Spaces, 171–173
 - synchronization, mobile devices, 248–251
- Data Access Control (DAC), 185–186
- Data Collector Sets, 227–230
- Data Protection (Quick Mode) settings, IPsec, 120
- Data Recovery Agent (DRA), 186
- DCA (DirectAccess Connectivity Assistant), 137
- deep linking apps, Windows Intune, 78–80
- /default parameter (BCDedit command), 9
- Defender tool (DaRT), 238
- deferred procedure calls (DPCs), 224
- /delete parameter (BCDedit command), 9
- Deny permissions, 182
- deployment
 - desktop applications, Windows Intune, 47–50
 - DirectAccess, 136–137
 - Windows Intune, 75–78
 - Windows To Go, 4
- Deployment Image Service and Management (DISM)
 - tool, 12, 18–19
- DER (Distinguished Encoding Rules)-encoded binary X.509, 164
- desktop applications, 29–50
 - accessing OneDrive, 176
 - ACT, 29–36
 - fixing problems, 33–36
 - inventory collector packages, 30–31
 - reviewing report data, 33
 - runtime-analysis packages, 31–33
 - tools, 30
 - coexistence, 36–45
 - App-V, 41
 - App-V Sequencer installation, 42–43
 - Client Hyper-V, 36–39
 - MDOP, 41–42
 - RemoteApp, 39–40
 - sequencing applications, 43–45
 - deployment using Windows Intune, 47–50
 - UE-V (User Experience Virtualization), 45–47
- desktop images, 15–21
 - creating, 17–18
 - modifying and repairing, 18–20
 - understanding images, 16–17
 - WET and USMT, 20–21
- desktop versions, Office 365, 64
- Details tab (Task Manager), 231
- detection rules, 75
- Device Backups setting, OneDrive, 177
- device drivers, 218–221
 - Pnputil.exe command-line tool, 221–222

- troubleshooting and updating with Device Manager
 - drivers, 218–219
 - unsigned drivers, 220
- Device Health Status, Windows Intune monitoring, 295
- Device Manager, troubleshooting and updating
 - drivers, 218–219
- Device Registration Service (DRS), 165
- devices, support
 - client compliance, 262–285
 - client security, 269–276
 - Group Policy application, 281–286
 - Internet Explorer 11 security, 276–280
 - managing updates, 263–270
 - mobile devices, 243–259
 - access policies, 246–247
 - broadband connectivity, 251–254
 - configuring policies, 243–248
 - mobile access and data
 - synchronization, 248–251
 - Mobile Device Management, 255–259
 - Remote Wipe, 247
 - operating system and hardware
 - monitoring and managing printers, 233–237
 - monitoring performance, 227–233
 - optimizing performance, 224–226
 - remediating startup issues, 237–240
 - resolving hardware and device issues, 221–227
- Windows Intune, 290–303
 - configuring monitoring and setting
 - alerts, 294–298
 - managing remote computers, 302–303
 - managing users and groups, 290–294
 - policy management, 299–303
- DFS (Distributed File System), 169–170
- DFS Management MMC, 170
- DFS Namespaces (DFSN or DFS-N), 170
- DFS-N (DFS Namespaces), 170
- DFSN (DFS Namespaces), 170
- DFS-R (DFS Replication), 170
- DFSR (DFS Replication), 170
- DFS Replication (DFSR or DFS-R), 170
- Dfsutil.exe command-line tool, 170
- DHCP (Dynamic Host Configuration Protocol), assigning
 - IP addresses to networks, 96
- diagnosing system failures, 239–240
- Diagnostic Console, Windows Performance
 - Analyzer, 225
- Diagnostics and Recovery Toolkit (DaRT) 8.1, 237–240
 - dialog boxes
 - Computer Name/Domain Changes, 158
 - Manage Add-Ons, 279
 - Startup And Recovery, 7
 - System Properties, 157
 - VPNTest Properties, 130–131
 - Wi-Fi Properties, 107–108
 - Wi-Fi Status, 108
 - Wi-Fi Wireless Network Properties, 108
 - Windows Firewall with Advanced Security, 117–118
 - differencing disks, 39
 - digital certificates, 151
 - DirectAccess, 134–138
 - deployment options, 136–137
 - new features, 136
 - understanding how DirectAccess works, 135
 - Windows 8.1 users, 137–138
 - DirectAccess Connectivity Assistant (DCA), 137
 - Disable-BC command, 174
 - disabling app updates, Windows Store, 66
 - Disallow Standby Sleep States (S1-S3) When Starting
 - From A Windows To Go Workspace setting (Windows To Go), 6
 - Disk Commander tool (DaRT), 238
 - DiskPart tool, 12
 - Disk Wipe tool (DaRT), 238
 - DISM API cmdlet, 20
 - DISM (Deployment Image Service and Management) tool, 12, 18–19
 - /displayorder parameter (BCDedit command), 9
 - Distinguished Encoding Rules (DER)-encoded binary X.509, 164
 - Distributed File System (DFS), 169–170
 - DNS clients, 105
 - DNSSECs (Domain Name System Security Extensions), 104–106
 - DNS servers, 105
 - DNS zones, 105
 - domain accounts, connecting with Microsoft
 - accounts, 56
 - Domain Name System Security Extensions (DNSSECs), 104–106
 - Domain Profile tab (Windows Firewall With Advanced Security dialog box), 117–118
 - domains, 101, 156–159
 - Domains tab (Office 365 Admin Center), 62
 - DPCs (deferred procedure calls), 224
 - DRA (Data Recovery Agent), 186

- Driver Catalog files, driver packages, 221
- driver files, 221
- driver packages, 221–222
- DRS (Device Registration Service), 165
- Dynamic Host Configuration Protocol (DHCP), assigning IP addresses to networks, 96

E

- EAP-MS-CHAPv2, 129
- EAP-TLS (Extensible Authentication Protocol-Transport Layer Security), 128
- Easy Transfer, 20–21
- editions, Office 365, 57
- EFS (Encrypting File System), 186–189
 - backup and recovery, 187–189
 - encryption, 186–187
- Electronic Software Distribution (ESD) solutions, 45
- Enable-BCDistributed command, 174
- Enable-BCHostedClient command, 174
- Enable-BCHostedServer command, 174
- Enable-BCLocal command, 174
- Enable-WindowsOptionalFeature cmdlet, 37
- enabling
 - BitLocker, 191–192
 - BranchCache, 173
 - Hyper-V, 37
- Encapsulating Security Payload (ESP) protocol, 120
- Encrypting File System (EFS), 186–189
 - backup and recovery, 187–189
 - encryption, 186–187
- encryption
 - Encrypting File System (EFS), 186–187
 - wireless network protocols, 110–111
- Endpoint Protection
 - alerts, 297
- Overview tab (Windows Intune), 296
 - System Center, 275–277
 - Windows Intune, 271–274
- workspace, 272
- Endpoint Protection tab (Windows Intune), 49
- end users, monitoring and managing printers, 233–235
- ESD (Electronic Software Distribution) solutions, 45
- ESP (Encapsulating Security Payload) protocol, 120
- Event Trace Sessions option, creating Data Collector Sets, 229

- Excel (Office 365), 59
- Exchange Access For Mobile tab, Windows Intune Policy workspace, 302
- Explicit permissions, 182, 184
- Explorer tool (DaRT), 238
- /export parameter (BCDedit command), 9
- export operations, certificates, 164
- expressions, DAC, 186
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), 128
- external virtual switches, 38

F

- /f parameter (BCDboot command), 10
- Fast Startup feature, 285
- Federated Search, 137
- File Exists detection rules, 75
- file formats, certificate import/export operations, 164
- File Restore tool (DaRT), 239
- File Search tool (DaRT), 239
- Filter By, Windows Firewall With Advanced Security window, 116
- filters, network security, 114–119
- fingerprints, biometrics, 155
- Firewall, monitoring, 114
- Folder Redirection, 137
- forcing app installation, 72
- forcing a sync, mobile devices, 251
- formats, certificate import/export operations, 164
- free trials, Office 365, 57
- Full Control NTFS permission, 182
- Full Control Share permission, 180–181
- full wipe (Remote Wipe), 247

G

- General tab
 - Internet Explorer 11 security, 276
 - Windows Intune, 295
- gestures, picture passwords, 165
- Get-AppxLastError cmdlet, 70
- Get-AppxLog cmdlet, 70
- Get-AppxPackage cmdlet, 70
- Get-AppxPackageManifest cmdlet, 70
- Get-BCDataCache command, 174

- Get-BCStatus command, 174
- Get-Printer cmdlet, 236
- Get-PrintJob cmdlet, 236
- Global Administrators, Office 365, 61–64
- GPMC (Group Policy Management Console), 54
- GPOs (Group Policy Objects), 5
- GPT (GUID Partition Table), 239
- Group Policy
 - biometric settings, 155
 - BranchCache settings, 174
 - client compliance, 281–286
 - configuring caching, 285–286
 - policy processing, 283–284
 - RSOP (Resultant Set of Policy), 281–283
 - configuring BitLocker To Go, 196–197
 - configuring for Windows To Go, 5–6
 - configuring settings, 147–148
 - disabling access to Windows Store, 67
 - integrating Microsoft accounts, 54
 - Internet Explorer 11 security settings, 277–281
 - managing metered connections, broadband connectivity, 253–254
 - managing NAP, 147
 - managing Windows Store settings, 66
 - setting for acceptance of sideloaded apps, 68–69
- Group Policy Management Console (GPMC), 54
- Group Policy Management Editor window, 54
- Group Policy Objects (GPOs), 5
- groups
 - managing with Windows Intune, 290–294
 - selection, Windows Intune, 75–78
- Groups tab (Windows Intune), 49
- Groups workspace, Windows Intune, 291
- GUID Partition Table (GPT), 239

H

- hardware support, 217–239
 - monitoring and managing printers, 233–237
 - monitoring performance, 227–233
 - optimizing performance, 224–232
 - remediating startup issues, 237–240
 - resolving hardware and device issues, 218–224
 - Reality Monitor, 223–224
 - STOP errors, 221–222
- health status updates, 142
- History tab (Windows Defender), 270
- homegroups, 156–159
- Home tab (Windows Defender), 270
- host computers, Windows To Go, 3
- host ID (TCP/IP) definitions, 96
- hosting Windows To Go, 3–4
- Hotfix Uninstall tool (DaRT), 239
- hotspots, broadband connectivity, 252
- hybrid images, 16
- Hyper-V Virtual Machine Connection, 37

I

- IANA (Internet Assigned Network Authority), 96
- lcacls.exe command, 184–185
- IKEv2 (Internet Key Exchange, Version 2), 128
- images, desktop, 15–21
 - creating, 17–18
 - modifying and repairing, 18–20
 - understanding images, 16–17
 - WET and USMT, 20–21
- /import parameter (BCDedit command), 9
- Import/Export/Restore/Diagnose/Repair Policies, Windows Firewall With Advanced Security window, 116
- import-module appx command, 70
- import operations, certificates, 164
- improvements, Windows PE, 22
- inactive profiles, configuring, 117
- Inbound Rules, Windows Firewall With Advanced Security window, 116
- InfoPath, 59
- informational alerts, 297
- infrastructure mode, connecting to wireless networks, 111
- inheritance, permissions, 184
- installation
 - App-V Sequencer, 42–43
 - operating system, 2–25
 - customizing with Windows PE, 21–25
 - desktop images, 15–21
 - multiboot systems, 14–15
 - Windows To Go, 2–6
 - RSAT (Remote Server Administration Tool), 139
 - software
 - Office 365, 56–61
 - Windows Store, 64–65
- Install-WindowsFeature BranchCache cmdlet, 173

- integrating apps, 53–80
 - deep linking apps using Windows Intune, 78–80
 - Microsoft accounts, 53–56
 - Office 365 and Windows Store apps, 56–67
 - sideloading apps into online/offline images, 68–72
 - sideloading apps using Windows Intune, 72–78
- internal virtual switches, 38
- Internet Assigned Network Authority (IANA), 96
- Internet domains, 101
- Internet Explorer 11 security, client
 - compliance, 276–280
- Internet Key Exchange, Version 2 (IKEv2), 128
- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 100
- inventory collector packages, 30–31
- inventory refreshing, remote computers, 304
- Invoke-GPUupdate cmdlet, 283
- IP addresses
 - automatic assignment, 96–97
 - filters and rules, 114
- ipconfig cmdlet, 96–97
- IP-HTTPS transition technology, 100
- IPsec, 119–123
- IPsec Settings tab (Windows Firewall With Advanced Security dialog box), 117–118
- IPv4, 94–96
- IPv6, 97–99
- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol), 100
- Isolation (connection security rule), 122

K

- KDC (Key Distribution Center), 159
- Kerberos v5 Authentication methods, 121
- Key Distribution Center (KDC), 159
- Key Exchange (Main Mode) settings, IPsec, 119

L

- /l parameter (BCDboot command), 10
- L2TP (Layer 2 Tunneling Protocol), 128
- Layer 2 Tunneling Protocol (L2TP), 128
- legacy hardware management, 220
- Licenses tab (Windows Intune), 49, 296
- Licensing tab (Office 365 Admin Center), 62

- Link Referrals (DFS), 170
- Link Targets (DFS), 170
- List Folder Contents NTFS permission, 182
- LoadState, 20
- local accounts, authentication and
 - authorization, 164–165
- Local Group Policy Editor, 5, 54
- Local Security Authority (LSA), 158
- lock parameter (manage-BDE command), 195
- Locksmith tool (DaRT), 239
- logging mode, RSOP, 281–282
- logging on, Windows8-based computers, 165
- LSA (Local Security Authority), 158
- Lync, 59

M

- /m parameter (BCDboot command), 10
- MAC (Media Access Control) address, 98
- Main Mode (Key Exchange) settings, IPsec, 119
- Manage Add-Ons dialog box, 279
- manage-BDE command, 195–196
- manage-bde -forcerecovery <Volume> command, 198
- management
 - DirectAccess, 134–138
 - deployment options, 136–137
 - new features, 136
 - understanding how DirectAccess works, 135
 - Windows 8.1 users, 137–138
 - legacy hardware, 220
 - printers, 233–237
 - end users and administrators, 233–235
 - NFC, 237
 - shared printers, 235–236
 - remote computers, Windows Intune, 302–303
 - software
 - Office 365, 61–64
 - Windows Store, 65–67
 - users and groups, Windows Intune, 290–294
- MBAM (Microsoft BitLocker Administration and Monitoring), 200–201
- MDOP (Microsoft Desktop Optimization Pack), 41–42
- MDT (Microsoft Deployment Toolkit), 17
- Media Access Control (MAC) address, 98
- Membership Criteria, Windows Intune monitoring, 295
- Message Center tab, 63
- metered connections, broadband connectivity, 253–255

- Microsoft accounts
 - authentication and authorization, 164–165
 - integrating apps, 53–56
- Microsoft BitLocker Administration and Monitoring (MBAM), 200–201
- Microsoft Compatibility Exchange, 32
- Microsoft Deployment Toolkit (MDT), 17
- Microsoft Desktop Optimization Pack (MDOP), 41–42
- mirror spaces (storage), 172
- mobile apps, Office 365, 64
- Mobile Device Management, 255–259
- Mobile Device Security Policies, 299
- mobile devices, support, 243–259
 - access policies, 246–247
 - broadband connectivity, 251–254
 - configuring policies, 243–248
 - mobile access and data synchronization, 248–251
 - Mobile Device Management, 255–259
 - Remote Wipe, 247
- modes, wireless connections, 111–113
- modifying
 - desktop images, 18–20
 - Windows PE, 23–25
- Modify NTFS permission, 182
- monitoring
 - performance, 227–233
 - Data Collector Sets, 227–230
 - Resource Monitor, 232–233
 - Task Manager, 229–231
 - printers, 233–237
 - end users and administrators, 233–235
 - NFC, 237
 - shared printers, 235–236
 - Windows Firewall, 114
- Monitoring rules, Windows Firewall With Advanced Security window, 116
- mounting Windows PE, 23–25
- MS-CHAP v2, 129
- MSO Product Code Exists detection rules, 75
- Mstsc.exe command, 132
- multiboot systems, 14–15
- multifactor authentication, 151–156

N

- Name Resolution Policy Table (NRPT), 105
- names resolution, 101–106
 - DNSSECs, 104–106

- PNRP (Peer Name Resolution Protocol), 104
- NAP Agents, 142
- NAP Client Configuration console, 143–145
- NAP (Network Access Protection), 141–147
 - using NAP on the client, 143–147
 - using NAP on the server, 142–143
- NAT (Network Address Translation), 96
- NDES (Network Device Enrollment Service), 153
- near field communication (NFC) Tap-to-Pair, 233, 237
- netsh command-line tool, 145–147, 174
- Network Access Protection. *See* NAP
- Network Address Translation (NAT), 96
- network connectivity, 93–123
 - automatic IP address assignment, 96–97
 - IPv4, 94–96
 - IPv6, 97–99
 - names resolution, 101–106
 - security, 113–123
 - filters and rules, 114–119
 - IPsec, 119–123
 - Windows Firewall, 114
 - transition technologies, 99–101
 - wireless networks, 106–113
 - connection options and modes, 111–113
 - encryption protocols, 110–111
 - W-Fi connections, 106–109
 - Wi-Fi technology standards, 109–110
- Network Device Enrollment Service (NDES), 153
- network ID (TCP/IP) definitions, 96
- network location server (NLS), DirectAccess and, 135
- Network Unlock (BitLocker), 198
- New Rules, Windows Firewall With Advanced Security window, 116
- NFC (near field communication) Tap-to-Pair, 233, 237
- NLS (network location server), DirectAccess and, 135
- notices (alerts), 297
- NRPT (Name Resolution Policy Table), 105
- NTFS permissions, 181–185

O

- on parameter (manage-BDE command), 195
- off parameter (manage-BDE command), 195
- Office 365
 - editions, 57
 - features, 57
 - ProPlus Admin Center, 58
 - software installation, 56–61

- software management, 61–64
- Office Customization Tool files, 61
- Office Deployment Tool, 60
- Office File Formats setting, OneDrive, 177
- Office Professional, 59
- on-demand remote scans, 272
- OneDrive, 175–177
- OneDrive app, 176
- OneNote, 59
- one-to-one remoting, 141
- operating system installation, 2–25
 - boot settings, 7–14
 - adding native VHD to startup menu, 11
 - adding VHD to a computer with an operating system, 11–12
 - adding VHD to computers without an operating system, 12–14
 - BCDboot, 9–11
 - BCDedit, 8–9
 - customizing with Windows PE, 21–25
 - desktop images, 15–21
 - creating, 17–18
 - modifying and repairing, 18–20
 - understanding images, 16–17
 - WET and USMT, 20–21
 - multiboot systems, 14–15
 - Windows To Go, 2–6
 - configuring Group Policy for, 5–6
 - hosting, 3–4
 - startup options, 4–5
- operating system support, 217–239
 - monitoring and managing printers, 233–237
 - monitoring performance, 227–233
 - optimizing performance, 224–226
 - remediating startup issues, 237–240
 - resolving hardware and device issues, 218–224
- optimization, performance, 224–232
 - WPT (Windows Performance Toolkit), 224–226
 - Xbootmgr.exe command-line tool, 226
 - Xperf.exe command-line tool, 226
 - XperfView.exe command-line tool, 226
- OSCDIMG cmdlet, 20
- Outbound Rules, Windows Firewall With Advanced Security window, 116
- Outlook (Office 365), 59
- Overview tab (Resource Monitor), 232

P

- PAP (Password Authentication Protocol), 129
- parity spaces (storage), 172
- password parameter (manage-BDE command), 195
- Password Authentication Protocol (PAP), 129
- passwords
 - picture, 155
 - remotely resetting, 303
- pause parameter (manage-BDE command), 195
- Peer Name Resolution Protocol (PNRP), 104
- People Tagging setting, OneDrive, 177
- performance
 - monitoring, 227–233
 - Data Collector Sets, 227–230
 - Resource Monitor, 232–233
 - Task Manager, 229–231
 - optimization, 224–232
 - WPT (Windows Performance Toolkit), 224–226
 - Xbootmgr.exe command-line tool, 226
 - Xperf.exe command-line tool, 226
 - XperfView.exe command-line tool, 226
- Performance tab (Task Manager), 230
- permissions, 180–186
 - DAC (Data Access Control), 185–186
 - NTFS, 181–185
 - proposed, DAC, 186
 - Share, 180–181
- personal broadband connections, 252
- personal hotspots, broadband connectivity, 252
- Personal Information Exchange (PKCS#12), 164
- picture passwords, 155, 165
- PKCS#7 (Cryptographic Message Syntax Standard), 164
- PKCS#12 (Personal Information Exchange), 164
- PKI (Public Key Infrastructure), 151, 187
- planning mode, RSoP, 281–282
- Plans setting, OneDrive, 177
- Pnputil.exe command-line tool, 221–222
- PNRP (Peer Name Resolution Protocol), 104
- Point-to-Point Protocol (PPP), 128
- Point-to-Point Tunneling Protocol (PPTP), 128
- policy alerts, 297
- Policy Conflicts tab, Windows Intune Policy workspace, 302
- policy management, Windows Intune, 299–303
- policy processing, Group Policy application, 283–284
- Policy tab (Windows Intune), 49
- port numbers, 115

- port rules, 117
- Ports option, configuring printers, 233
- PowerPoint (Office 365), 59
- PPP (Point-to-Point Protocol), 128
- PPTP (Point-to-Point Tunneling Protocol), 128
- predefined rules, 117
- printers, monitoring and management, 233–237
 - end users and administrators, 233–235
 - NFC, 237
 - shared printers, 235–236
- Print Management console, 234–235
- Privacy tab (Internet Explorer 11 security), 276
- private network ranges, 96
- private virtual switches, 38
- Processes tab (Task Manager), 230
- program rules, 116
- ProPlus Admin Center (Office 365), 58
- ProPlus (Office 365), 59
- proposed permissions, DAC, 186
- protocols, 94, 115
- protocol suite, defined, 94
- provisioning Windows To Go, 4
- Public Key Infrastructure (PKI), 151, 187
- Publisher (Office 365), 59

Q

- Quick Mode (Data Protection) settings, IPsec, 120

R

- /r:<nameof recoveryagent> parameter (Cipher.exe command), 188
- RD Connection Broker, 39
- RDC (Remote Desktop Connection) client, 131
- RD Gateway, 39
- RD Gateway Server Settings, configuring, 133–134
- RD Licensing, 39
- RDP (Remote Desktop Protocol), 131–134
 - entering RD Gateway Server Settings and connecting, 133–134
 - opening Remote Desktop Connection on the client, 132–133
- RD Session Host, 39
- RDS (Remote Desktop Services), 39
- RD Virtualization Host, 39
- RD Web Access, 39
- Read & Execute NTFS permission, 182
- Read NTFS permission, 183
- read-only domain controllers (RODCs), credential caching, 161
- Read Share permission, 180–181
- Reality Monitor, 223–224
- recovering
 - computers, 238–239
 - data
 - BitLocker Drive Encryption, 198–199
 - BitLocker To Go, 198–199
 - recoverykey parameter (manage-BDE command), 195
 - recovery keys, BitLocker, 193
 - recoverypassword parameter (manage-BDE command), 195
- Referral cache (DFS), 170
- referrals (DFS), 170
- refreshing inventory remotely, 304
- Registry Editor tool (DaRT), 239
- Registry Key Exists detection rules, 75
- remediating startup issues, 237–240
- remote access, 127–147
 - DirectAccess, 134–138
 - deployment options, 136–137
 - new features, 136
 - understanding how DirectAccess works, 135
 - Windows 8.1 users, 137–138
 - NAP, 141–147
 - using NAP on the client, 143–147
 - using NAP on the server, 142–143
 - RDP, 131–134
 - entering RD Gateway Server Settings and connecting, 133–134
 - opening Remote Desktop Connection on the client, 132–133
 - remote administration, 138–141
 - VPNs, 127–131
 - authentication protocols, 128–129
 - CMAK, 129
 - user profiles, 129–131
- remote administration, 138–141
- RemoteApp, 39–40
- Remote Assistance alerts, 297
- remote computer management, Windows Intune, 302–303
- Remote Desktop Connection (RDC) client, 131
- Remote Desktop Protocol (RDP), 131–134

- entering RD Gateway Server Settings and connecting, 133–134
- opening Remote Desktop Connection on the client, 132–133
- Remote Desktop Services (RDS), 39
- remote locks, 302
- remote scans, 272
- Remote Server Administration Tool (RSAT), 139–140
- Remote Wipe, 247
- Remoting (Windows PowerShell), 140–141
- removable devices, access, 190
- Remove-AppxPackage cmdlet, 70
- Remove-PhysicalDisk cmdlet, 171
- Remove-PrintJob cmdlet, 236
- repairing desktop images, 18–20
- Repair-VirtualDisk cmdlet, 171
- report data, application compatibility, 33
- Reports tab (Windows Intune), 49
- requirements
 - hosting Windows To Go, 3
- Reset Account Counter After policy, 161
- resetting passwords remotely, 303
- resolving
 - hardware and device issues, 218–224
 - Reality Monitor, 223–224
 - STOP errors, 221–222
 - IP addresses, 101
- resource access
 - authentication and authorization, 150–165
 - account policies, 160–161
 - computer authentication vs user authentication, 159–160
 - credential caching, 161–162
 - Credential Manager, 162–164
 - homegroups, workgroups, and domains, 156–159
 - local accounts vs Microsoft accounts, 164–165
 - multifactor authentication, 151–156
 - Secure Channel, 160
 - Workplace Join, 165
- data security, 180–200
 - BitLocker Drive Encryption, 191–200
 - EFS (Encrypting File System), 186–189
 - permissions, 180–186
 - removable devices, 190
- data storage, 169–177
 - BranchCache, 173–175
 - DFS, 169–170

- OneDrive, 175–177
- Storage Spaces, 171–173
- network connectivity, 93–123
 - automatic IP address assignment, 96–97
 - IPv4, 94–96
 - IPv6, 97–99
 - names resolution, 101–106
 - security, 113–123
 - transition technologies, 99–101
 - wireless networks, 106–113
- remote access, 127–147
 - DirectAccess, 134–138
 - NAP, 141–147
 - RDP, 131–134
 - remote administration, 138–141
 - VPNs, 127–131
- Resource Monitor, 232–233
- resource ownership, 185
- restarting computers remotely, 303
- Restore-CARoleService cmdlet, 153
- restrictions, Windows PE, 22
- Resultant Set of Policy (RSOP), 281–283
- resume parameter (manage-BDE command), 195
- reviewing Data Collector Sets, 228
- RODCs (read-only domain controllers), credential caching, 161
- root domain management, 101
- Root Referrals (DFS), 170
- RSAT (Remote Server Administration Tool), 139–140
- RSOP (Resultant Set of Policy), 281–283
- Rules, network security, 114–119
- runtime-analysis packages, 31–33

S

- /s parameter (BCDboot command), 10
- status parameter (manage-BDE command), 195
- /s:<directory> parameter (Cipher.exe command), 188
- SAM (Security Account Manager) database, 158
- SA (Software Assurance), 42
- saving
 - credentials, 162
 - startup keys, 197–198
- ScanState, 20
- scans, Windows Intune Endpoint Protection, 272–274
- Schannel (Secure Channel), 160

scheduling scans, Windows Intune Endpoint Protection, 273

Scripting Center, 141

Search Providers (Manage Add-Ons dialog box), 280

Secure Channel (Schannel), 160

Secure Socket Tunneling Protocol (SSTP), 128

security

authentication and authorization, 150–165

account policies, 160–161

computer authentication vs user

authentication, 159–160

credential caching, 161–162

Credential Manager, 162–164

homegroups, workgroups, and

domains, 156–159

local accounts vs Microsoft accounts, 164–165

multifactor authentication, 151–156

Secure Channel, 160

Workplace Join, 165

client compliance, 269–276

data, 180–200

BitLocker Drive Encryption, 191–200

EFS (Encrypting File System), 186–189

permissions, 180–186

removable devices, 190

network connectivity, 113–123

filters and rules, 114–119

IPsec, 119–123

Windows Firewall, 114

Security Account Manager (SAM) database, 158

security groups, 293–294

Security option, configuring printers, 233

Security Policy, Accounts: Block Microsoft Accounts
setting, 165

Security tab (Internet Explorer 11 security), 276

selective wipe (Remote Wipe), 247

self-recovery, 198

sequencing applications, 43–45

servers, NAP (Network Access Protection), 142–143

Server-to-server (Connection security rule), 122

Service Health tab (Office 365 Admin Center), 63

Service Set Identifier (SSID), 106

Service Settings (Office 365 Admin Center), 62

Services tab (Task Manager), 231

Set-BCCache command, 174

Set Group Policy Refresh Interval For Computers
setting, 286

Set-PhysicalDisk cmdlet, 171

setting alerts, Windows Intune, 294–298

Settings tab (Windows Defender), 270

SFC Scan tool (DaRT), 239

shared personal hotspots, broadband connectivity, 252

shared printers, 235–236

Share permissions, 180–181

Sharing option, configuring printers, 233

Shim Infrastructure, 34

shims, 34

sideloaded apps, 257

online/offline images, 68–72

Windows Intune, 72–78

sideloading key, activating, 69–72

signing zones, DNS, 105

Sigverif.exe command-line tool, 220

simple spaces (storage), 172

SkyDrive, 175

smart cards, 153–155

snapshots, 38

software

installation

Office 365, 56–61

Windows Store, 64–65

management

Office 365, 61–64

Windows Store, 65–67

uploading, Windows Intune, 73–75

Software Assurance (SA), 42

Software Publisher (Windows Intune), 49–50

Software Status, Windows Intune monitoring, 295

Software tab (Windows Intune), 49, 296

SoH (statements of health), 142

Solution Wizard tool (DaRT), 239

Specify Startup Policy Processing Wait Time
setting, 286

SSID (Service Set Identifier), 106

SSTP (Secure Socket Tunneling Protocol), 128

Standard User Analyzer (SUA) Wizard, 35

standard Windows PE DVD disks, 22–23

Startup And Recovery dialog box, 7

Startup Event Trace Sessions option, creating Data
Collector Sets, 229

startup issues, remediating, 237–240

Startup key only authentication strategy, 193

startup keys, 197–198

startup options, Windows To Go, 4–5

Startup tab (Task Manager), 231

stateful configuration, 98

- stateless configuration, 98
- statements of health (SoH), 142
- STOP errors, resolving, 221–222
- storage, data, 169–177
 - BranchCache, 173–175
 - DFS, 169–170
 - OneDrive, 175–177
 - Storage Spaces, 171–173
- storage pools, 172
- Storage setting, OneDrive, 177
- Storage Spaces, 171–173
- SUA (Standard User Analyzer) Wizard, 35
- subnet masks, 95
- support
 - desktop applications, 29–50
 - ACT, 29–36
 - coexistence, 36–45
 - deployment using Windows Intune, 47–50
 - UE-V (User Experience Virtualization), 45–47
 - integrating apps, 53–80
 - deep linking apps using Windows Intune, 78–80
 - Microsoft accounts, 53–56
 - Office 365 and Windows Store apps, 56–67
 - sideloading apps into online/offline images, 68–72
 - sideloading apps using Windows Intune, 72–78
 - operating system installation, 2–25
 - boot settings, 7–14
 - customizing with Windows PE, 21–25
 - desktop images, 15–21
 - multiboot systems, 14–15
 - Windows To Go, 2–6
 - resource access
 - authentication and authorization, 150–165
 - data security, 180–200
 - data storage, 169–177
 - names resolution, 101–106
 - network connectivity, 93–123
 - remote access, 127–147
 - Windows clients and devices
 - client compliance, 262–285
 - mobile devices, 243–259
 - operating system and hardware, 217–239
 - Windows Intune, 290–303
- Sync Center, mobile device synchronization, 250–251
- sync conflicts, mobile devices, 251
- synchronizing data, mobile devices, 248–251
- System alerts, 297

- System Center
 - Endpoint Protection, 275–277
 - set up, 275–276
- System Center Configuration Manager, 31
- System Configuration utility, 7
- system failures, diagnosing, 239–240
- System option, creating Data Collector Sets, 228
- System Overview tab (Windows Intune), 49, 295
- system partitions, 9
- System Properties dialog box, 157

T

- tabs, Windows Intune administrator console, 49
- Task Manager, 229–231
- TCP/IP Config tool (DaRT), 239
- TCP/IP (Transmission Control Protocol/IP Protocol), 94
- Temporal Key Integrity Protocol (TKIP), 123
- Teredo tunneling technology, 100
- testing checkpoints, 38–39
- thick images, 16
- thin images, 16
- /timeout parameter (BCDedit command), 9
- TKIP (Temporal Key Integrity Protocol), 123
- TLS (Transport Layer Security)/SSL (Secure Sockets Layer) security, 160
- Toolbars And Extensions (Manage Add-Ons dialog box), 280
- top-level Internet domains, 101
- TPM only authentication strategy, 193
- TPM + startup key authentication strategy, 193
- TPM + startup PIN authentication strategy, 193
- TPM + startup PIN + startup key authentication strategy, 193
- TPM (Trusted Platform Model), 3
- TPM (Trusted Platform Module) chip, 153
- Tpmvscmgr.exe command-line tool, 154
- Tracking Protection (Manage Add-Ons dialog box), 280
- transition technologies, network connectivity, 99–101
- Transmission Control Protocol/IP Protocol (TCP/IP), 94
- Transport Layer Security (TLS)/Secure Sockets Layer (SSL) security, 160
- trials, Office 365, 57
- trust anchors, 105
- trusted PCs, configuring, 55–56
- Trusted Platform Model (TPM), 3
- Trusted Platform Module (TPM) chip, 153

- Trusted Root Certification Authorities store, 152
- Tunnel (Connection security rule), 122
- Turn Off Background Refresh Of Group Policy setting, 286
- Turn Off Local Group Policy Objects Processing setting, 286
- Turn Off Resultant Set Of Policy Logging setting, 286

U

- /u parameter (Cipher.exe command), 188
- UEFI (Unified Extensible Firmware Interface), 192
- UEFI (Unified Extensible Firmware Interface), 239
- UE-V Agents, 46–47
- UE-V Generators, 46
- UE-V (User Experience Virtualization), 45–47
- /u /n parameter (Cipher.exe command), 188
- Unified Extensible Firmware Interface (UEFI), 192, 239
- unsigned drivers, 220
- updates, client compliance, 263–270
 - Windows Intune, 265–269
 - Windows Update, 264–266
- Updates alerts, 297
- Update Software Packages, 268
- Updates tab (Windows Intune), 49, 296
- Update Status, Windows Intune monitoring, 295
- Update tab (Windows Defender), 270
- uploading software, Windows Intune, 73–75
- user authentication, 159–160
- User Experience Virtualization (UE-V), 45–47
- user groups, 292–293
- User Interface Settings (NAP Client Configuration console), 144
- User (Kerberos V5) authentication method, 121
- user profiles, VPNs, 129–131
- users, Windows Intune
 - adding, 72–73
 - managing, 290–294
 - selection, 75–78
- Users And Groups tab (Office 365 Admin Center), 62
- Users tab (Task Manager), 231
- User State Migration Tool (USMT), 16, 20–21
- USMT (User State Migration Tool), 16, 20–21

V

- /v parameter (BCDboot command), 10
- VAMT (Volume Activation Management Tool), 20
- Verisign, 151
- VHDs (virtual hard disks)
 - adding to a computer with an operating system, 11–12
 - adding to computers without operating systems, 12–14
 - adding to startup menu, 11
- View section, Windows Firewall With Advanced Security window, 116
- virtual hard disks (VHDs)
 - adding to a computer with an operating system, 11–12
 - adding to computers without operating systems, 12–14
 - adding to startup menu, 11
- virtual private networks. *See* VPNs (virtual private networks)
- virtual smart cards, 153–155
- virtual switches, 38–39
- VLSC (Volume Licensing Service Center), 68
- Volume Activation Management Tool (VAMT), 20
- Volume Licensing Service Center (VLSC), 68
- VPNs (virtual private networks)
 - constructing, 127–131
 - authentication protocols, 128–129
 - CMAK, 129
 - user profiles, 129–131
 - DirectAccess and, 135
- VPNTTest Properties dialog box, 130–131

W

- warnings (alerts), 297
- WBF (Windows Biometric Framework), 155
- web browsers, accessing OneDrive, 176
- WEP encryption protocol, 110
- WET (Windows Easy Transfer), 20–21
- W-Fi connections, 106–109
- Wi-Fi Properties dialog box, 107–108
- Wi-Fi Status dialog box, 108
- Wi-Fi technology standards, 109–110

- Wi-Fi Wireless Network Properties dialog box, 108
- Windows ADK (Windows Assessment and Deployment Kit), 224
- Windows Assessment and Deployment Kit (Windows ADK), 224
- Windows Assessment Console, 30
- Windows Assessment Services, 20
- Windows Assessment Toolkit, 20
- Windows Biometric Framework (WBF), 155
- Windows Boot Loader, 8
- Windows Boot Manager, 8
- Windows clients, support
 - client compliance, 262–285
 - client security, 269–276
 - Group Policy application, 281–286
 - Internet Explorer 11 security, 276–280
 - managing updates, 263–270
 - mobile devices, 243–259
 - access policies, 246–247
 - broadband connectivity, 251–254
 - configuring policies, 243–248
 - mobile access and data
 - synchronization, 248–251
 - Mobile Device Management, 255–259
 - Remote Wipe, 247
 - operating system and hardware, 217–239
 - monitoring and managing printers, 233–237
 - monitoring performance, 227–233
 - optimizing performance, 224–232
 - remediating startup issues, 237–240
 - resolving hardware and device issues, 218–224
- Windows Intune, 290–303
 - configuring monitoring and setting alerts, 294–298
 - managing remote computers, 302–303
 - managing users and groups, 290–294
 - policy management, 299–303
- Windows Easy Transfer (WET), 20–21
- Windows Firewall, monitoring, 114
- Windows Firewall Settings policies, 299
- Windows Firewall With Advanced Security dialog box, 117–118
- Windows Firewall With Advanced Security window, 115
- Windows Intune
 - client management, 290–303
 - configuring monitoring and setting alerts, 294–298
 - policies, 299–303
 - remote computers, 302–303
 - users and groups, 290–294
- Company Portal, 76–77
- connector tool, 78
- creating custom firewall policies, 246–247
- creating security policies for mobile devices, 244–246
- deep linking apps, 78–80
- deploying desktop applications, 47–50
- Endpoint Protection, 271–274
- managing client updates, 265–269
- Remote Wipe, 247
- sideloading apps, 72–78
- Windows Intune Agent Settings policies, 299
- Windows Intune Center Settings policies, 299
- Windows Management Instrumentation (WMI) provider, 7
- Windows Performance Analyzer (WPA), 224–226
- Windows Performance Recorder (WPR), 224–226
- Windows Performance Toolkit (WPT), 20, 224–226
- Windows PE (Windows Preinstallation Environment), 12, 21–25
- Windows PowerShell
 - DirectAccess and, 136
 - remote access, 140–141
- Windows PowerShell Remoting, 140
- Windows Preinstallation Environment. *See* Windows PE
- Windows Recovery Environment (Windows RE), 3
- Windows RE (Windows Recovery Environment), 3
- Windows SIM cmdlet, 20
- Windows Store
 - creating apps, 68
 - disabling access through Group Policy, 67
 - disabling app updates, 66
 - features, 64–65
 - installing and managing software, 56–67
 - software installation, 64–65
 - software management, 65–67
- Windows To Go, 2–6
 - configuring Group Policy for, 5–6
 - hosting, 3–4
 - startup options, 4–5
- Windows To Go Default Startup Options setting (Windows To Go), 5
- Windows Update, managing client updates, 264–266

wireless networks, connections

- wireless networks, connections, 106–113
 - connection options and modes, 111–113
 - encryption protocols, 110–111
 - W-Fi connections, 106–109
 - Wi-Fi technology standards, 109–110
- wizards
 - Create A New Policy, 245
 - DaRT Recovery Image, 238
 - SUA (Standard User Analyzer), 35
 - Windows Easy Transfer, 20–21
- WMI (Windows Management Instrumentation)
 - provider, 7
- Word (Office 365), 59
- Work Folders, mobile device synchronization, 248–249
- workgroups, 156–159
- Workplace Join, 165
- WPA2 encryption protocol, 111
- WPA encryption protocol, 110
- WPA-Enterprise mode, connecting to wireless networks, 113
- WPA-Personal mode, connecting to wireless networks, 112
- WPA (Windows Performance Analyzer), 224–226
- WPR (Windows Performance Recorder), 224–226
- WPT (Windows Performance Toolkit), 20, 224–226
- Write NTFS permission, 183

X

- /x parameter (Cipher.exe command), 188
- Xbootmgr.exe command-line tool, 226
- Xperf.exe command-line tool, 226
- XperfView.exe command-line tool, 226

Z

- zones, DNS, 105

About the author



JOLI BALLEW is an award-winning, best-selling author of over 50 books, including *Windows 8.1 Step By Step* and *Windows 8.1 Plain and Simple*, both with Microsoft Press. Joli is a Microsoft MVP (10 years) and holds many Microsoft certifications, starting with the original MCSE for Windows Server 2000. Joli is a Microsoft Certified Trainer and a professor at Brookhaven Community College, where she also serves as the Microsoft Academy Coordinator. Joli teaches certification classes, including the class related to this exam, Supporting Windows 8.1 (70-688) and the one that precedes it, Configuring Windows 8.1 (70-687).

This page intentionally left blank




From technical overviews to drilldowns on special topics, get *free* ebooks from Microsoft Press at:

www.microsoftvirtualacademy.com/ebooks

Download your free ebooks in PDF, EPUB, and/or Mobi for Kindle formats.

Look for other great resources at Microsoft Virtual Academy, where you can learn new skills and help advance your career with free Microsoft training delivered by experts.

Microsoft Press



Now that
you've
read the
book...

Tell us what you think!

Was it useful?

Did it teach you what you wanted to learn?

Was there room for improvement?

Let us know at <http://aka.ms/tellpress>

Your feedback goes directly to the staff at Microsoft Press,
and we read every one of your responses. Thanks in advance!



Microsoft