

Introducing Windows® 8

An Overview for IT Professionals

**Free
Preview**

Jerry Honeycutt

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

Copyright © 2012 Microsoft Corporation

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

ISBN: 978-0-7356-7050-1

This document is a preliminary release that may be changed substantially prior to final release. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet website references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user.

Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

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

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.

Project Editor: Valerie Woolley

Cover: Twist Creative • Seattle

Contents

Introduction.....	9
Acknowledgments.....	9
Errata & book support	9
We want to hear from you	10
Stay in touch.....	10
Chapter 1: Overview	11
Why Windows 8?	11
Experiences and devices	12
Enterprise-grade solutions.....	12
What's new for Windows 8?.....	12
End-to-end security.....	13
Manageability and virtualization	14
Hardware recommendations	16
Hardware innovation.....	16
Touch.....	16
Long battery life	17
Thinner, lighter, faster.....	17
Sensors and security.....	17
New form factors.....	17
Windows 8 editions.....	18
Getting started with Windows 8.....	18
Summary.....	19
Chapter 2: Experiencing Windows 8	20
Like Windows 7—Only better	20
Exploring the Weather app.....	21
Returning to the Start screen.....	22
Organizing Tiles into groups.....	22
Pinning Tiles to the Start screen	22

Showing administrative tools.....	23
Finding and launching apps quickly.....	24
Searching for files and settings.....	25
Switching between open apps.....	26
Using the App Switcher.....	26
Snapping apps to the screen edges.....	27
Closing an open app.....	28
Improvements to tools.....	29
File Explorer.....	29
Task Manager	30
Summary	31
Chapter 3: Windows 8 for IT pros.....	32
Reimagined system applications	32
Windows Task Manager.....	33
Windows Explorer	35
File history.....	36
Customizing and configuring Windows 8.....	36
Profile customization	37
Tile configuration	37
PC Settings.....	37
Client Hyper-V	38
Redesigned NTFS health model and chkdsk.....	39
Key design changes.....	39
New NTFS health model	40
Windows PowerShell 3.0	41
New features.....	41
Integrated Scripting Environment (ISE)	42
Networking enhancements	43
BranchCache	43
DirectAccess	44

Mobile broadband support	45
IPv6 Internet support.....	45
Remote Server Administration Tools	46
Windows Server 2012.....	46
Virtualization.....	47
ReFS.....	47
Summary.....	47
Chapter 4: Preparing for deployment.....	48
Windows 8 SKUs.....	48
Application compatibility.....	50
ACT 6.0 improvements.....	51
Common compatibility problems.....	51
User state migration	53
Deployment strategies.....	54
New deployment scenarios.....	56
Windows To Go.....	56
Virtual Desktop Infrastructure.....	56
Client Hyper-V.....	57
Summary.....	57
Chapter 5: Deploying Windows 8.....	59
Windows Assessment an Deployment Kit.....	59
Deployment and Imaging	59
Windows Preinstallation Environment.....	60
User State Migration Tool	60
Volume Activation Management Tool.....	61
Windows Performance Toolkit	61
Windows Assessment Toolkit.....	61
Windows Assessment Services.....	62
Deployment Options.....	62
Microsoft Deployment Toolkit 2012 Update 1.....	62

System Center 2012 Configuration Manager with SP1.....	63
Desktop Virtualization	64
Windows To Go	64
Preparation and Requirements.....	65
Management and Security.....	68
Windows To Go Workspace Creation	70
Summary	71
Chapter 6: Delivering Windows apps	73
A look at Windows apps.....	73
Windows app lifecycle.....	74
Building a Windows app	75
Using Visual Studio to build a Windows app	77
Distributing in the Windows Store.....	82
The certification process.....	82
The app purchase experience	83
Distributing within an Enterprise.....	83
Sideloading an app.....	84
Managing Windows apps.....	87
Summary	91
Chapter 7: Windows 8 recovery	92
The Windows Recovery Environment	92
Advanced options	94
Refresh and reset	96
Refresh your PC.....	97
Reset your PC.....	97
Customizing the Windows Recovery Environment	98
Building a customized Windows RE.....	98
Enhanced recovery with DaRT.....	100
Summary	103
Chapter 8: Windows 8 management	105

Windows PowerShell	107
Group Policy improvements	109
PowerShell GPO management	109
New functionality	110
AppLocker.....	111
System Center 2012 Configuration Manager	111
Redesigned management console	112
Infrastructure improvements.....	112
Expanded reporting options	113
Mobile device support.....	113
System Center 2012 Endpoint Protection.....	113
Windows Intune	114
Cloud management.....	114
Company portal.....	114
Summary.....	115
Chapter 9: Windows 8 security	116
Protecting the client against threats.....	116
Boot options for security	116
SmartScreen	118
Vulnerability mitigation and sandboxing	118
Protecting sensitive data	119
BitLocker.....	119
Advanced administration of BitLocker with MBAM	122
Secure access to resources.....	125
Virtual smart cards.....	125
Dynamic Access Control	125
Summary.....	126
Chapter 10: Internet Explorer 10	127
Using Internet Explorer for the desktop	127
Using Internet Explorer	128

New interface and new usage patterns	129
New Features in Internet Explorer 10	133
Group Policy in Internet Explorer 10.....	134
New Group Policies	134
Changed Group Policies.....	135
Summary	135
Chapter 11: Windows 8 virtualization.....	137
Virtual Desktop Infrastructure	137
Choosing the right VDI deployment.....	139
Complete desktop virtualization	141
Application virtualization.....	142
User state virtualization.....	143
Client Hyper-V	145
Summary	145

Introduction

The Windows 8 operating system is the newest member of the Microsoft Windows family. It differs from earlier Windows releases as much for what it does not change as for what it does change. That is, the features that IT pros loved about Windows 7 are still there in Windows 8—just better. The same keyboard shortcuts, management tools, security features, and deployment options are available in Windows 8. But in many cases, Windows 8 improves them in intuitive and significant ways. Some examples are the ribbon in File Explorer and faster disk encryption when using BitLocker Drive Encryption. This book describes these enhancements plus many of the new features in Windows 8.

Of course, everyone is talking about the elements of the new user interface in Windows 8: the Start screen, the modern looking Windows graphics, and so on. These are not replacements for the desktop, and it is not an either-or choice that you have to make. For desktop apps, the same desktop that you used in Windows 7 is still there in Windows 8. You can still pin apps to the taskbar, pin files to those apps, and so on. The keyboard and mouse work the same way as it did before on the desktop. But Windows 8 uses a Start screen instead of the tiny Start menu in Windows 7. The most obvious benefit is that there is more real estate available, so apps can display dynamic, live information on their Tiles (icons) to bring the latest information to you at a single glance.

Windows 8 also introduces Windows 8 apps. These are full screen, immersive apps that provide a different experience than you might be used to with traditional desktop apps. They do not have chrome. App commands (menu items) only appear when you need them. Importantly, Windows 8 and Windows 8 apps provide a first-class touch experience, so you can swipe, flick, and use other intuitive gestures to get around them.

This book describes these new and improved features. It focuses on IT pros, however, so we spend fewer pages talking about the new user interface and more talking about management, deployment, and security. This book is just an introduction—an overview. For more detailed information about any of the features and capabilities you learn about in this book, the one resource you need to know about is the Springboard Series on TechNet. The URL is simply <http://www.microsoft.com/springboard>.

Acknowledgments

We'd like to thank the following people who contributed content to this book: Doug Steen, Steve Suehring, Chris Howie. We'd also like to thank our reviewers: Brad McCabe, Chris Hallum, Craig Ashley, David Trupkin, Fred Pullen, Jason Leznek, Michael Niehaus, Richard Harrison, Skand Mittal, and Stephen Rose.

Errata & book support

We've made every effort to ensure accuracy of this preview ebook. When the final version is available

(November 2012), any errors that are reported after the book's publication will be listed on our Microsoft Press site at oreilly.com. At that point, you can search for the book at <http://microsoftpress.oreilly.com> and then click the "View/Submit Errata" link. If you find an error that is not already listed, you can report it to us through 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 is not offered through the addresses above.

We want to hear from you

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

<http://www.microsoft.com/learning/booksurvey>

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

Stay in touch

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

CHAPTER 1

Overview

Windows 8 is the newest member of the Windows family, and everyone at Microsoft is very excited about it. Microsoft reimagined Windows 8 to reflect the way people work and play, the devices they want to use, and the explosion of social media. You might be tempted to think that Windows 8 simply is a consumer release—and there are certainly a lot of great new features that consumers are going to love—but Windows 8 has a lot for businesses and IT pros, too.

The new user interface and app model enable businesses to create their own line-of-business (LOB) apps to help improve users' productivity. The operating system improves on the fundamentals, such as speed, reliability, and security. Lastly, Windows 8 works with your existing infrastructure but also offers new ways to deploy and manage users' desktop environments.

This chapter provides an overview of Windows 8, beginning with answering the question, "Why?" Then it describes essential details, like hardware requirements and editions, and closes by telling you how you can begin evaluating it for your business today.

Why Windows 8?

Users have broad access to consumer devices (e.g., laptop PCs, tablet PCs, and mobile phones using modern technology) at home, and this device proliferation leads to higher user expectations of technology at work. You don't need an analyst to tell you that users have more personal computing devices and that those devices are often compelling.

The digital generation entering the work place raises these expectations to a whole new level. This is a generation that has grown up completely fluent with digital technology (e.g., texting, instant messaging, and social media). They are digital natives and have significantly different beliefs about the tools they should be able to use at work.

Digital natives are also increasingly mobile and operate at a very fast pace. Their quick pace, combined with ubiquitous connectivity, blurs the lines between people's work and personal lives. As those lines blur, their personalities and individual work styles impact how they get their work done and what technology they prefer to use. As a result, they want a say in the technologies they use to get their jobs done.

This trend is aptly called the "consumerization of IT." An example of consumerization is a Bring Your Own Device (BYOD) program, where users can bring their own laptop PC, tablet PC, or smartphone to work and use them to access a work desktop hosted in the datacenter. Another example is the use of social networking at work—for work.

It's certainly not a secret that people buy their own smartphones for work, use unapproved websites, or download unapproved applications on a work PC. They do so because the technology that they use at home is often better than the technology available on the job.

Consumerization of IT is great, as it unleashes people's productivity and passion, innovation, and competitive advantage. We believe in the power of saying "Yes" to users and their technology requests in a responsible way. Our goal at Microsoft is to partner with IT to enable you to embrace these trends but also ensure the environment remains secure and well managed.

While Microsoft knows that embracing the consumerization of IT can be challenging, the company's strategy can help overcome those challenges. That strategy is to:

- Provide the experiences and devices that users love and expect.
- Deliver enterprise-grade solutions that you can use to manage and secure them.

The following sections describe how Windows 8 is a key part of this strategy.

Experiences and devices

Microsoft knows that business users often have to choose between convenience and productivity. Windows 8 tablets (i.e., x86 tablets) offer users a no-compromise tablet experience. Windows 8 delivers a touch-first experience along with full support for mouse and keyboard. It's a no-compromise experience that gives users the convenience and mobility of a tablet combined with the power and familiarity of a full PC. Users can move effortlessly between work and personal activities. Not only that, but users can have a connected experience with apps from the Windows Store while continuing to use the same desktop LOB and productivity apps they currently use on Windows 7. Finally, Windows 8 offers new possibilities for mobile productivity.

Enterprise-grade solutions

Windows 8 also offers enterprise-grade solutions:

- **Enhanced end-to-end security** From the client device to back-end infrastructure, Windows 8 offers features that improve the security and reliability of the systems in your company. From power-on to power-off, Windows 8 can provide a more secure foundation to help keep businesses running and users productive.
- **Management and virtualization advancements** Windows 8 includes enhancements to manageability and virtualization features that help you manage client PCs. For example, Windows To Go provides new ways to give users a super mobile desktop experience on almost any PC. (For more information about Windows To Go, see Chapter 6, "Deploying Windows 8.")

What's new for Windows 8?

Windows 8 focuses on users' lives. It is beautiful. Fast. Fluid. It's also perfect for a range of devices. This includes PCs, of course, but also compact, touch-enabled tablet PCs, lightweight laptops, and large, powerful

all-in-one PCs with high-definition screens.

Windows 8 is smooth and intuitive. Users have instant access to the information they care about most, like their contacts, apps, and other information. They can spend less time looking for information and more time doing things with it.

But all that is the consumer story. What about IT pros? The following sections provide a quick look at some of the really interesting new features for IT pros. Of course, the remainder of this book provides more information about these features.

End-to-end security

The following list describes new and enhanced security features in Windows 8:

- **Trusted boot** Some malware programs target the boot process and insert themselves into the system before Windows or antimalware software is able to start. Because of this, the ability of Windows or the antimalware software to protect the system might be compromised. With UEFI 2.3.1 equipped devices, the UEFI Secure Boot feature helps to ensure that malware is not able to start before Windows 8. The Windows 8 Trusted boot feature protects the integrity of the remainder of the boot process, including the kernel, system files, boot critical drivers, and even the antimalware software itself. The system's antimalware software is the first third party application or driver to start. Moving antimalware into the Trusted boot process prevents it from being tampered with. In the event that malware is able to successfully tamper with the boot process, Windows can automatically detect and repair the system.
- **Measured boot** On Trusted Platform Module (TPM)-based systems, Windows 8 can perform a comprehensive chain of measurements during the boot process that can be used to further validate the boot process beyond Trusted boot. Measured boot process enables all aspects of the boot process to be measured, signed, and stored in a TPM chip. This information can be evaluated by a remote service to further validate a computer's integrity before granting it access to resources. This process is called Remote Attestation.
- **BitLocker Drive Encryption** BitLocker Drive Encryption is a data protection feature in Windows 8 Pro and Windows 8 Enterprise editions that helps protect data theft from lost, stolen, or inappropriately decommissioned computers. BitLocker now encrypts hard drives more quickly, helping to keep data safe without significantly interrupting worker productivity.

BitLocker now supports encrypted drives, which are hard drives that come pre-encrypted from the manufacturer. BitLocker offloads the cryptographic operations to hardware, increasing overall encryption performance and decreasing CPU and power consumption.

On devices without hardware encryption, BitLocker encrypts data more quickly. BitLocker allows you to choose to encrypt the used space on a disk instead of the entire disk. As free space is used, it will be encrypted. This results in a faster, less disruptive encryption of a hard drive, so that enterprises can more easily provision BitLocker, and they can do it with little time impact. In addition, the user experience is improved by allowing a standard user, one without administrative privileges, to reset the BitLocker PIN.

- **AppLocker** AppLocker is a simple and flexible mechanism that allows you to specify exactly which apps are allowed to run on users' PCs. Traditional access control technologies such as Active Directory Rights Management Services and Access Control Lists (ACLs) help control the data users are allowed to access. However, these technologies can't prevent users from installing or using non-standard software. In Windows 8 Enterprise editions, AppLocker enables you to create security policies through Group Policy to prevent potentially harmful or other non-approved apps from running. With AppLocker, you can set rules based on a number of properties, including the signature of the application's package or the app's package installer, and can more effectively control apps with less management.
- **Windows SmartScreen** Windows SmartScreen app reputation is a safety feature in Windows 8. This service provides application reputation-based technologies to help protect users from malicious software that they may encounter on the Internet. This technology checks the reputation on any new application, helping to keep users safe no matter what browser they use in Windows 8. This helps to prevent malware and other viruses from infiltrating your organization. The Windows SmartScreen app reputation feature works with the SmartScreen feature in Internet Explorer, which also protects users from websites seeking to acquire personal information such as usernames, passwords, and billing data.
- **Claim-based access control** Claim-based access control enables you to set up and manage usage policies for files, folders, and shared resources.

With Windows 8, you can dynamically allow users access to the data they need based on the user's role in the company. Unlike previous statically-controlled security groups, Claim-based access control allows you to dynamically control access to corporate resources based on the user and device properties that are stored in Active Directory. For example, a policy can be created that enables individuals in the finance group to have access to specific budget and forecast data, and the human resources group to have access to personnel files.

Chapter 11, "Windows 8 security," provides more information about these security features.

Manageability and virtualization

The following list describes some of the new manageability and virtualization features in Windows 8:

- **Client Hyper-V** Client Hyper-V on Windows 8 Pro and Windows 8 Enterprise is a robust virtualization platform that enables IT Pros and developers to run diverse client and server environments on their Windows 8 PCs. You can test and manage multiple environments from a single PC, allowing you to evaluate changes in a test environment in advance of deploying to a production environment. With support for wireless networking and sleep and hibernate modes, Client Hyper-V can run on any Second Level Address Translation (SLAT)-enabled 64-bit PC, including most Intel- and AMD-based laptops. Virtual Machines (VMs) can be migrated easily between server and Client Hyper-V without modification, making developers and IT pros more efficient. Client Hyper-V also supports both 32-bit and 64-bit guest operating systems. Client Hyper-V leverages the security enhancements in Windows 8 and can be managed easily by existing IT tools such as System Center. For more information about Client Hyper-V, see Chapter

13, "Windows 8 virtualization."

- **Windows PowerShell** Management tasks are simplified with Windows PowerShell automation. Windows PowerShell provides easy-to-learn language syntax. New features in the Windows PowerShell Integrated Scripting Environment (ISE) make it easier and faster for both new and experienced users to author clear, maintainable, production-ready automation scripts. IntelliSense tap completion, snippets, and GUI based search features provide improved cmdlet discovery, making it easier to find and run any of the 1,200 new high-level, task-oriented cmdlets. For more information about Windows PowerShell, see Chapter 10, "Windows 8 management."
- **Testing, deployment, and migration** Deploying Windows 8 in your organization is faster and easier than Windows 7. Enhanced tools help you make the right decisions with minimal downtime for users. A new version of the Application Compatibility Toolkit (ACT) helps you understand potential application compatibility issues by identifying which apps are or are not compatible with Windows 8. ACT helps you to deploy Windows 8 more quickly by helping to prioritize, test, and detect compatibility issues with your apps.

Migrating user data from a previous Windows installation can be automated with the User State Migration Tool (USMT). This tool now supports migrating user data from Windows XP installations. With the end of support for Windows XP approaching, now is a great time to plan your migration to Windows 8.

For more information about deploying Windows 8, see Chapter 6, "Deploying Windows 8."

- **Refresh and Reset your PC** Windows 8 helps streamline the recovery process for PCs. Refresh your PC and Reset your PC allow users to restore their Windows 8 installation and more easily get their systems up and running again. Even when Windows 8 cannot start, you can use these new features from within the Windows Recovery Environment (Windows RE). Refresh your PC allows users to reinstall Windows 8 while maintaining their personal files, accounts, and personalization settings. These features make it faster and easier to get a PC up and running again. For more information about Refresh your PC and Reset your PC, see Chapter 9, "Windows 8 recovery." This chapter also describes the Microsoft Diagnostics and Recovery Toolset, which provides more advanced troubleshooting and recovery tools that are built into Windows 8.
- **Virtual Desktop Infrastructure (VDI)** Powered by Window Server 8, Microsoft VDI provides the best value for virtual desktops today. The new Remote Desktop client in Windows 8 works with VDI. Windows Server 8 provides customers with deployment choices through a single platform and a consistently rich user experience. Setting up a VDI environment is easy with the simple setup wizard, and managing your VDI environment is simple with administration, intelligent patching, and unified management capabilities. Features such as user profile disks and Fair Share ensure high performance and flexibility, while support for lower cost storage and sessions help reduce the cost of VDI. In addition, Microsoft RemoteFX provides users with a rich, local-like desktop experience, with the ability to play multimedia, 3D graphics, use USB peripherals, and touch-enabled devices across any type of network (LAN or WAN). All of these benefits are available across different types of VDI desktops (personal VM, pooled VM, or session-based desktops). For more information about Windows 8 in a VDI environment, see Chapter 13,

"Windows 8 virtualization."

Hardware recommendations

Windows 8 provides a terrific experience on the same hardware that runs Windows 7. Table 1-1 describes the hardware recommendations for Windows 8. In fact, you might even notice that PCs seem to work even better after upgrading from Windows 7 to Windows 8.

Table 1-1 Windows 8 Hardware Recommendations

COMPONENT	RECOMMENDATION
Processor	1 GHz or faster
Memory	32-bit PCs: 1 GB 64-bit PCs: 2 GB
Hard disk space	32-bit PCs: 16 GB 64-bit PCs: 20 GB
Graphics card	Microsoft DirectX 9 graphics device with WDDM driver

Additionally, some Windows 8 features require other hardware components:

- To use touch, you need a tablet or a monitor that supports multi-touch.
- To access the Windows Store to download and run apps, you need an active Internet connection and a screen resolution of at least 1024 x 768.
- To snap apps, you need a screen resolution of at least 1366 x 768.

Hardware innovation

Hardware innovation is broad in Windows 8, and there are a few key areas where Microsoft has worked extensively with its partners. The following sections describe some of the things you and your users will notice quickly about PCs built for Windows 8—either at work or at a retail store.

Touch

Touch is clearly front-and-center for Microsoft. For example, the company is requiring that touch displays support a minimum of five-fingers, and it is working with its partners to deliver touch-optimized devices. To ensure a great user experience with touch, Microsoft has done extensive research into:

- The response times required for touch.
- The sensitivity and precision required of a digitizer.
- The user experience of a flush bezel.

These requirements are enforced with the Windows 8 Hardware Certification Requirements. You can learn more about these requirements on the "Windows Hardware Certification" page at <http://msdn.microsoft.com/en-us/library/windows/hardware/gg463010.aspx>.

Long battery life

One of the key design tenets of Windows 8 is to enable long battery life. With Windows 8, a new class of ultrathin PCs and tablets can turn on instantly, can run all day on a single charge, and stay connected to the Internet—so users' PCs are ready when they're ready.

Thinner, lighter, faster

As you have seen with today's ultrabooks, PCs are already thinner and lighter than ever. This will only continue with Windows 8. There will be thin and light tablets and ultra-portables that start and run faster than today's PCs. Even installing Windows 8 on an existing PC will improve its performance because of the improvements we've made in the core operating system.

Sensors and security

With Windows 8, Microsoft will enable developers to take advantage of hardware innovation such as:

- Low-power Bluetooth
- GPS
- Gyroscopes
- Accelerometer

You'll also be able to take advantage of security hardware technologies like Trusted Platform Module (TPM) and Unified Extensible Firmware Interface (UEFI) boot.

New form factors

Microsoft believes that users should have a choice. To that end, PCs will come in a variety of form factors, from tablets to convertibles to ultra-portables to all-in-one PCs. One day, you might even see designs that you would not have thought possible. Together with its OEM partners, Microsoft will provide great devices for every work style:

- Devices for executives that are innovative, portable, powerful.
- Devices optimized for enterprise knowledge workers and everyday business tasks.
- Devices that are specialized and unique for specific tasks.
- Industrial devices like ruggedized machines in oil rigs and manufacturing lines.
- Varieties of companion devices that present new and fun possibilities.

Devices for Windows 8 are about choices, because Microsoft believes the device has to fit the job. Microsoft and its ecosystem are committed to providing choices to our customers.

Windows 8 editions

Chapter 5, "Preparing for deployment," contains a table that describes the specific features you will find in each edition of Windows 8. For now, the following list summarizes them:

- **Windows 8** Windows 8 is the basic stock-keeping unit (SKU) for home users. It includes the core feature set that home users require but does not include key business features, such as support for the ability to join domains, process Group Policy, and so on.
- **Windows 8 Pro** Windows 8 Pro is for small- and medium-sized businesses. It delivers new levels of productivity, security, and mobility—without sacrificing performance or choice. It provides enhanced features that help to easily connect to company networks, access files on the go, encrypt data, and more.
- **Windows 8 Enterprise** Windows 8 Enterprise edition is available through Windows Software Assurance. It includes all the capabilities of Windows 8 Pro, plus premium features designed to meet the mobility, productivity, security and manageability, and virtualization needs of today's large businesses. Key examples are Windows To Go, DirectAccess, BranchCache, AppLocker, VDI, and Windows 8 app deployment. You will learn about these features in this book.
- **Windows RT Devices** Windows RT Devices run low-powered ARM processors, which helps OEMs build devices with long battery lives and new form factors (thin, light, and sleek devices). Also, Windows RT Devices are built on a new paradigm (preconfigured system on certified hardware), which helps ensure that users have high-quality and predictable experiences over time. While Windows RT Devices offer the great benefits this chapter just mentioned, they have commonality and shared code with Windows 8, offering a consistent, great Windows experience. For example, Windows RT Devices support the new UI (including desktop). Both Windows RT Devices and Windows 8 can run apps from the Windows Store. Windows RT Devices are compatible with most peripherals, since they include class drivers for most peripherals, and the majority of mice, keyboards, printers, and USB storages are supported out of the box.

Getting started with Windows 8

Microsoft makes getting started with your Windows 8 evaluation easy. MSDN and TechNet subscribers can download Windows 8 from the subscriber downloads area. You can also download a Windows 8 Enterprise evaluation from the Downloads page on TechNet at <http://www.microsoft.com/technet/downloads>.

You can evaluate Windows 8 in a VM. By doing so, you will experience the vast majority of features that this book describes. If you want to experience touch, however, then you must install Windows 8 on a PC with a touch-enabled display or a tablet PC.

Summary

As this chapter described, Windows 8 offers strong value to IT pros. Microsoft is delivering on its commitment to deliver experiences and devices that users want, along with enterprise-grade solutions that provide end-to-end security, management, and security. The remainder of this book provides more information about the features you learned about in this chapter.

Experiencing Windows 8

Consumers often say that they have to choose between the full productivity experience of a PC and the convenience of a tablet. Tablets historically presented productivity challenges, because most business desktop apps don't run on non-Windows tablets. Tablets also challenged IT because it can be difficult to manage and secure non-Windows tablets.

However, with an x86 Windows 8 tablet, users can have a no-compromise tablet experience, so choosing between productivity and convenience is no longer necessary. Microsoft Windows 8 gives users productivity, convenience, and mobility. They can use the familiar Windows user interface, their desktop line-of-business (LOB) and productivity apps, and peripherals that they use today on Windows 7.

Windows 8 delivers a touch-first experience, along with full support for mouse and keyboard, enabling users to move between work and personal activities easily and effortlessly. The Windows 8 user interface provides quick access to critical data, and Windows 8 apps are always on and always connected to help keep them up-to-date.

IT pros don't need to compromise either. Windows 8 provides the manageability and security that you need. Also, you can take advantage of your existing management and security infrastructure for managing Windows 8 tablets.

In both cases, features that were great in Windows 7 are even better in Windows 8. With Windows 8, users have the best of both worlds: a powerful new way of working with their PCs and the flexibility and power of the Windows desktop. And Windows 8 extends the deployment, management, and virtualization capabilities of Windows 7 with new capabilities.

Like Windows 7—Only better

Windows 8 uses the same management tools that you already use to support Windows 7 in your organization. Tools like System Center 2012 Configuration Manager, Microsoft Deployment Toolkit (MDT) 2012, and the Microsoft Diagnostics and Recovery Toolset (DaRT) have been updated for Windows 8—not just updated, but really enhanced.

Additionally, Windows 8 contains all of the security and reliability features that you've come to expect from Windows. As you'll learn in this book, the changes in Windows 8 are incremental from Windows 7. For an IT pro, these changes enhance supportability and security. For example, there are new refresh and recovery options available with Windows 8. This means that you'll spend less time supporting Windows 8.

The Windows 7 desktop features you love, like Jump Lists, the Taskbar, and Snapping, are still there in Windows 8. You can pin items to the taskbar in Windows 8 and you can use thumbnails in Windows 8 too. The desktop experience is just like Windows 7.

To provide a no-compromise tablet experience, the Windows 8 user interface is optimized for touch. But the keyboard and mouse are still first-class input methods in Windows 8. Figure 2-1 illustrates how you can perform the same tasks with both the touch interface and by using the mouse. The important thing to remember about the Windows 8 user interface is:

- Touch is about the edges.
- Mouse is about the corners.

To be more specific, you can swipe in from the top, bottom, left, or right edges of the screen to perform tasks. But you can also click the corners of the screen with the mouse to accomplish the same tasks. For example, to search for a file, you can swipe in from the right edge and tap the Search icon or you can click the top-right corner of the screen and click the Search icon. Whereas you swipe in from the top edge of the screen to display app commands, you simply right-click with the mouse (just like you do in Windows 7).

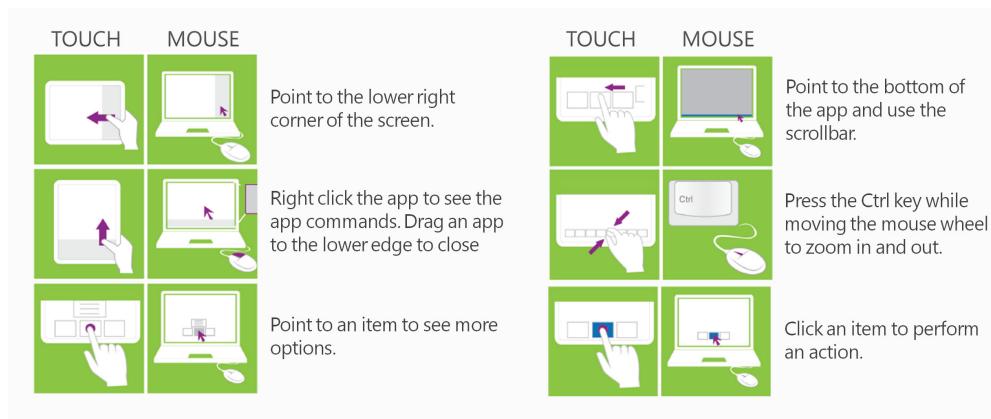


FIGURE 2-1. TOUCH GESTURES AND THE MOUSE

Using Windows 8 is intuitive and easy. However, Windows 8 provides excellent Help that you can use to learn about the gestures, mouse, and keyboard shortcuts available. The following sections provide a brief hands-on tour of the Windows 8 user interface, which can help you get up to speed quickly if you follow along on your own PC running Windows 8.

Exploring the Weather app

Windows 8 apps put content before chrome. They are elegant. They are immersive. And they provide a consistent, compelling user experience. Complete the following steps to open and use the Windows 8 Weather app:

1. On the Start screen, click (or tap) the Weather app. Notice how the Weather app uses the full screen.
2. Move your mouse to the bottom of the screen and scroll the app left and right (or drag your finger right and left) to reveal more of the Weather app.
3. Click the minus sign (-) in the bottom-right corner of the screen (or pinch the Weather app with two fingers), and click or tap Hourly Forecast.

4. To see the app commands available for the Weather app, right-click anywhere in the app (or swipe in from the top edge of the screen).
5. Click (or tap) Places, to view weather in different areas.
6. Right-click (or swipe from the top edge of the screen), and then click (or tap) World Weather to see the weather for different locations around the world.

Returning to the Start screen

The new Start screen has all of the information you care about in one place. Real-time updates about things like news, the weather, and what your friends are doing are all available right here. No searching is necessary—Tiles are the quick way to see it all. Returning to the Start screen in Windows 8 is just like opening the Start menu in Windows 7. The only difference is the addition of touch gestures. For example, you can use any of the following methods to return to the Start screen at any time:

- Swipe in from the right edge of the screen and tap Start.
- Move the mouse to the lower-right or upper-right corner of the screen, and click Start.
- Move the mouse to the lower-left corner of the screen, and click.
- Press the Windows logo key.

Organizing Tiles into groups

On your PC, the Start screen will eventually have many Tiles on it. You can group Tiles to make them quicker and easier to find. Try the following on your Start screen:

- Drag a Tile upward with your mouse or finger until it snaps out of place; then, drag it to left or right until you see a white separator, and drop it.
- Drag a Tile to the bottom edge of the screen, but do not release it. Notice how the Start screen zooms out so you can see all of your groups and app Tiles. Continue dragging the Tile to the one that you moved previously. After the Start screen zooms back in, drop the second Tile below the first one.
- Click the minus sign (-) in the lower-right corner of the screen to zoom out; then, right-click a group and click Name Group.
- To change the size of the Weather app Tile, right-click it (or swipe it a short distance up [flick it]); then, click or tap Smaller in the App Commands. Notice that the Calendar app Tile is now half its original size.

Pinning Tiles to the Start screen

The Start screen displays your most-used apps and live Tiles. Live Tiles update in real time to keep you constantly connected to the information you care about most. It is like pinning apps to the Start menu in Windows 7, but in a way that is alive with activity. Just like in Windows 7, you can pin additional apps to the Start screen anytime. Complete the following steps to pin the Computer app to the Start screen:

1. Right-click anywhere on the Start screen, and click All apps in App commands.

2. In the Windows System group, right-click Computer. Notice the commands available in the App Commands.
3. Click Pin to Start.
4. Return to the Start screen. Notice on the right end of the Start screen the Computer desktop app Tile. When you pin Windows 8 or desktop app Tiles to the Start screen, Windows 8 adds them to the right end of the Start screen.
5. Right-click the Computer desktop app Tile, and click Manage in App commands to open Computer Management.

Showing administrative tools

IT pros like to keep their administrative tools handy. They also like keyboard shortcuts. Not only can you add administrative tools to the Start screen, but you can also open a menu of administrative tools quickly. Complete the following steps to see how you can quickly access administrative tools by using just the keyboard:

1. On the Start screen, press the Windows logo key + I, click Tiles.
2. Click Show administrative tools to change it to Yes.
3. Return to the Start screen. Notice all of the administrative tools on the right end of the Start screen.
4. Now press the Windows logo key + X. Notice the menu of administrative tools in the lower-left corner of the screen (Figure 2-2). Press Esc to close the menu.

NOTE You can also open the menu of administrative tools by using the mouse. Place the mouse pointer in the lower-left corner of the screen, and right-click to open it.

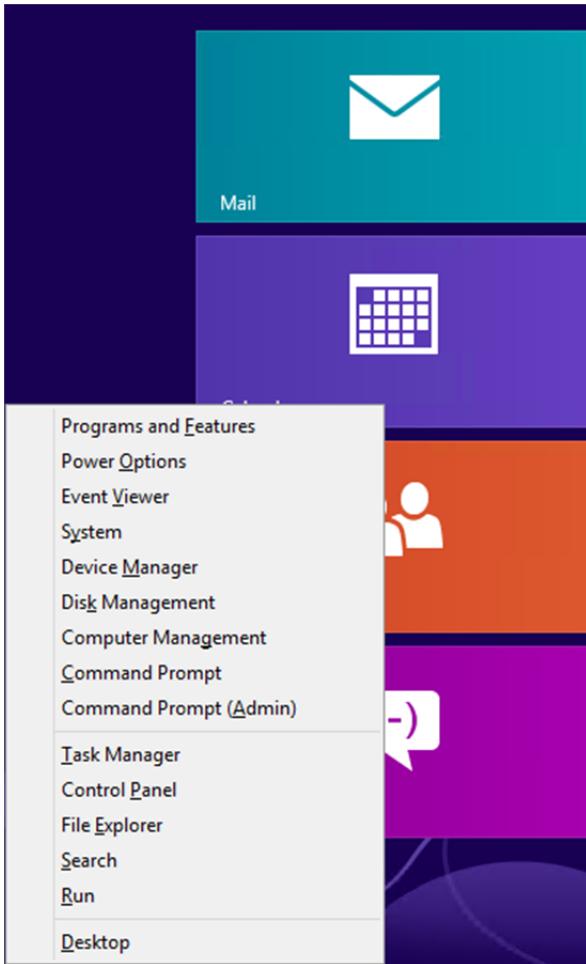


FIGURE 2-2. ADMINISTRATIVE TOOLS

Finding and launching apps quickly

In Windows 7, you can quickly run apps by pressing the Windows logo key, typing the name of the app, and pressing Enter. You can do the same thing in Windows 8. Complete the following steps to launch an app by searching for it:

1. On the Start screen, type **maps**, and press Enter. Notice that the Windows 8 Maps app opens immediately.
2. Return to the Start screen, and type **powershell**.
3. With Windows PowerShell already selected, press Ctrl + Shift + Enter.
4. On the User Account Control dialog box, click Yes. Notice that Windows PowerShell opened with elevated permissions.

5. Close Windows PowerShell.

Searching for files and settings

When you search in Windows 8, the results will include apps, settings, and files. You can even search across your apps. As a result, you can find the apps, files, and information you care about most—quickly and simply. Complete the following steps to search for results that contain the word Windows, not just in your files but also across your apps:

1. On the Start screen, type **windows**. Notice how Windows 8 displays a list of apps that contains the word "Windows." By default, the Start screen displays results for Apps.
2. On the right side of the search results, click Files. Notice that the search results show all files on the computer that contain the word Windows in their file names or metadata.
3. On the left side, click Documents to limit the results to just documents.
4. Click **Videos** to limit the results to just pictures, as shown in Figure 2-3.
5. Press the Windows logo key + F, and click Internet Explorer. Notice that the Windows 8 Internet Explorer app displays search results that contain the word "Windows."
6. Click News. Notice that the News app displays articles that contain the word "Windows."

TIP By default, the Start screen searches apps when you start typing. To search settings, press the Windows logo key + W. To search files, press the Windows logo key + F.

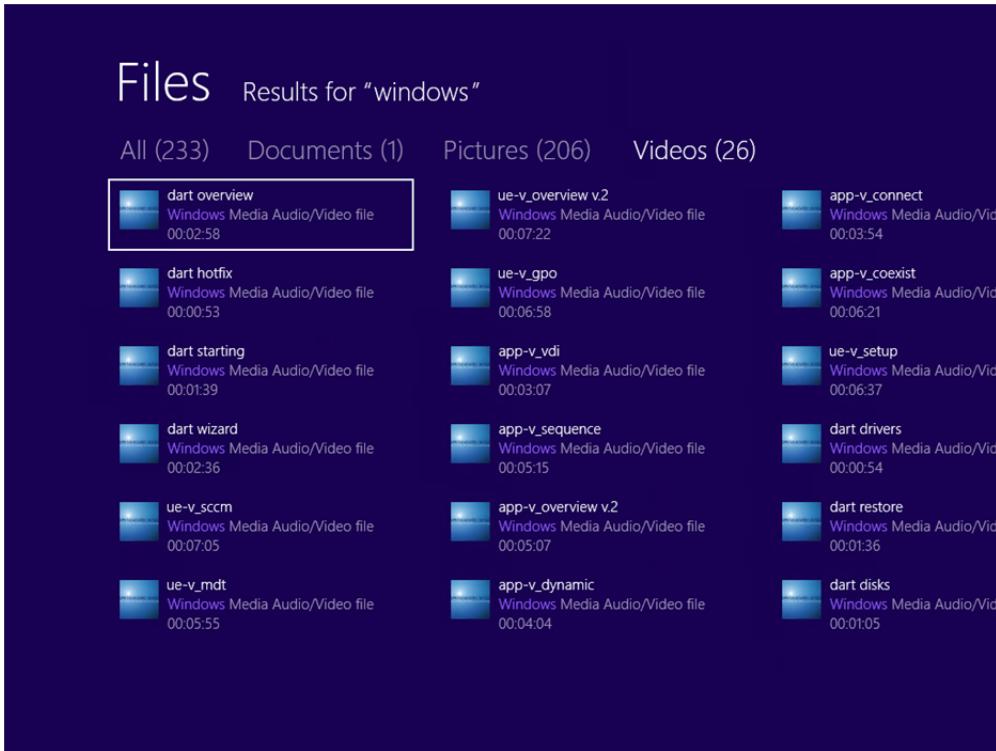


FIGURE 2-3. SEARCHING FOR FILES AND SETTINGS

Switching between open apps

You can switch to open Windows 8 apps by swiping in from the left edge of the screen. It's a quick way to cycle through your open apps. To try it yourself:

1. On the Start screen, click Weather.
2. Return to the Start screen, and click News.
3. Return to the Start screen, and click Internet Explorer.
4. Swipe in from the left edge of the screen to switch to the next Windows 8 app.
5. Repeat step 3 to cycle through each open Windows 8 app.

Using the App Switcher

The App Switcher (Figure 2-4) displays a thumbnail of each open Windows 8 app. Do any of the following to open the App Switcher and open a running Windows 8 app:

- Swipe in from the left edge of the screen and, without lifting your finger, drag the app back to the left edge of the screen. (The motion feels like drawing a right bracket [>]). Notice the App Switcher on the left edge of the screen. You see a thumbnail for each open Windows 8 app. At the bottom of the App Switcher, you see the Start screen.

- Press and hold the Windows logo key, repeatedly press Tab to highlight each running Windows 8 app; then, release both keys to open the selected apps full screen.
- Press Alt + Tab, just like you did in Windows 7, to quickly switch between apps.
- Move the mouse pointer to the upper-left corner of the screen. Notice in the upper-left corner of the screen a thumbnail for the next Windows 8 app. Also notice the hint along the left edge of the screen that the App Switcher is available. Click the mouse in the upper-left corner of the screen to bring in the next open app, or move the mouse pointer straight down the left edge of the screen to open the App Switcher.



FIGURE 2-4. APP SWITCHER

Snapping apps to the screen edges

You can snap Windows 8 apps to the left or right edges of the screen to share the screen with a second app (Figure 2-5), including desktop apps running on the Desktop. Complete the following steps to snap an app to the screen edges:

1. On the Start screen, click a Windows 8 app, such as the Weather app. The app will open full screen.
2. Press the Windows logo key + period (.) to snap the app to the right edge.
3. Press the Windows logo key + period (.) to snap the app to the left edge.

4. Press the Windows logo key + period (.) to restore the app to full screen.
5. Move the mouse to the top of the app, and notice that the mouse pointer has changed to a hand. Drag the app to the right edge of the screen to snap it to the right edge.
6. On the Start screen, click another Windows 8 app, such as the News app. Notice that the first app snapped to the right edge of the screen never changes as you open multiple apps. (For example, you can snap the Calendar app to the right edge of the screen, and keep it there while you work with multiple other apps.)
7. To make one app bigger and the other small, simply drag the app divider from one side of the screen to the other, and release it.
8. Drag the app divider to the left edge of the screen to unsnap the apps.

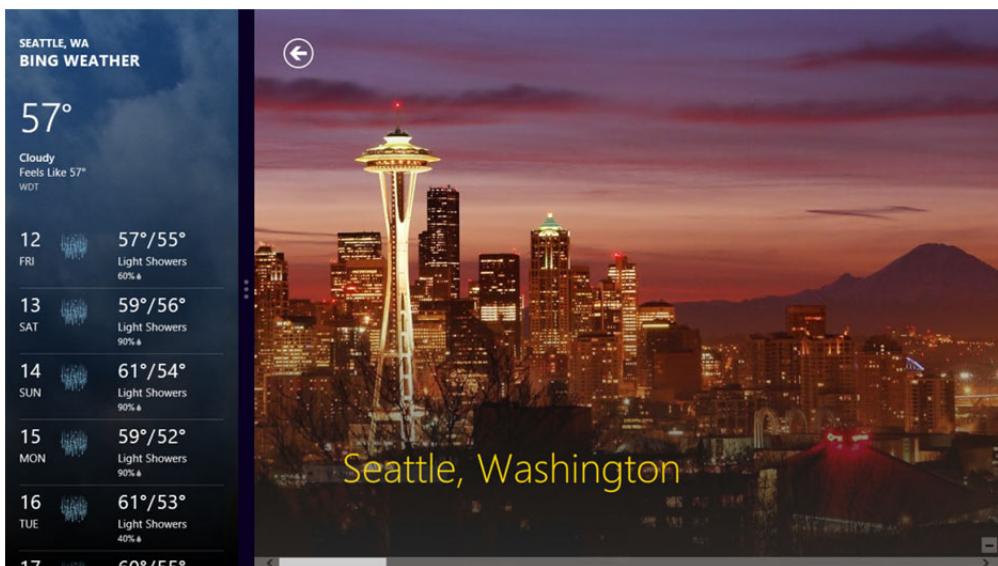


FIGURE 2-5. SNAPPING APPS SIDE BY SIDE

Closing an open app

Windows 8 can suspend Windows 8 apps when they are idle in the background; however, you can close a Windows 8 app by throwing it away. Do either of the following to close an open Windows 8 app by throwing it away:

- Swipe in from the top of the screen and, without lifting your finger, drag the app to the bottom of the screen.
- You can also close an app by using the mouse: Place the mouse pointer at the top edge of the screen. (The mouse pointer changes to a hand.) Drag the app to the bottom of the screen to throw it away.

Improvements to tools

The Windows 8 experience is about more than just the Start screen and Windows 8 apps. It also offers improvements to the tools that you use every day, like File Explorer and Task Manager. The following sections describe some of these improvements.

File Explorer

File Explorer is the new Windows Explorer. File Explorer has quite a history, going all the way back to the days of MS-DOS. Over the years, the tool now known as File Explorer has evolved. It used to be called File Manager, and for a long time it was called Windows Explorer. With the release of Windows 8, Windows Explorer is now known as File Explorer.

File Explorer is used for file management tasks. Whether the task is to copy or move a file, to delete it or get its properties, when people use File Explorer they're working with files and folders. With this in mind, File Explorer has been optimized for file management tasks. Frequently used commands, such as those related to copying and moving files, are available in a ribbon. Commands for accessing properties and creating new files and folders are available in the same ribbon (Figure 2-6).

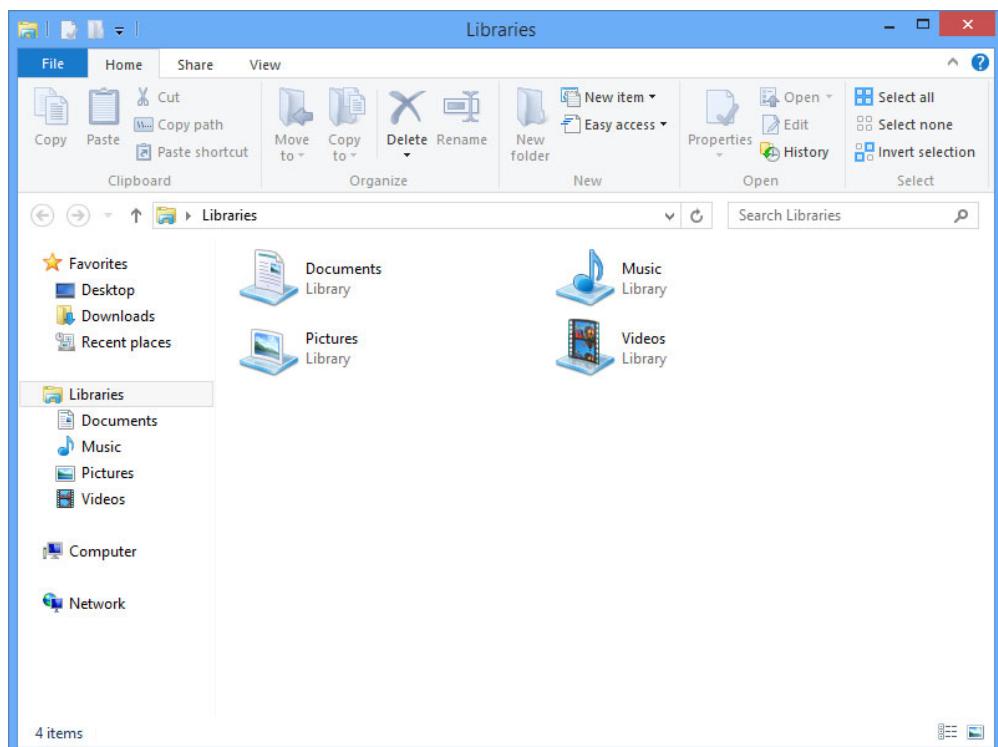


FIGURE 2-6. RIBBONS IN FILE EXPLORER

People share files more frequently today, and File Explorer provides a new Share menu that contains frequently used commands such as zip and email, along with advanced sharing and security.

View options, which are also frequently used, have their own menu in File Explorer. You no longer need to go into Folder and Search Options and search through complex menus just to see hidden items or file name extensions; those are now available with check boxes right in the View menu.

File Explorer also has contextual menu options. When viewing a library such as the Picture library, you'll see tools that make sense for working with pictures. There are contextual tools available for things like Video and other libraries as well. This gives you the tools you need for the types of files you're working with at a given time.

Task Manager

With the new Task Manager, you can quickly see running programs and can also end tasks if there is an issue. But IT pros and power users frequently want to see more information about the running tasks and the overall status of the system.

By clicking More Details, you see a significant amount of information about the processes running on your PC, its performance, and so on (Figure 2-7). Merely looking at the available tabs reveals that there is a lot of information and many options here. Like File Explorer, the Task Manager interface has been redesigned to serve the needs of all types of users.

The screenshot shows the Windows Task Manager window with the "Details" tab selected. The table displays various processes across six columns: Name, Status, CPU, Memory, Disk, and Network. The "CPU" column is currently sorted in descending order, with "News" at 56% and "Task Manager" at 1%. The "Memory" column is also sorted, with "Weather" using 86.3 MB.

Name	Status	1% CPU	56% Memory	0% Disk	0% Network
Apps (6)					
Bing		0%	0.7 MB	0 MB/s	0 Mbps
Microsoft Application Virtualiza...		0%	10.7 MB	0 MB/s	0 Mbps
News		0%	1.1 MB	0 MB/s	0 Mbps
Task Manager		0%	8.3 MB	0 MB/s	0 Mbps
Travel		0%	1.4 MB	0 MB/s	0 Mbps
Weather		0%	86.3 MB	0 MB/s	0 Mbps
Background processes (11)					
Device Association Framework ...		0%	0.2 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	3.3 MB	0 MB/s	0 Mbps
Microsoft Application Virtualiza...		0%	17.7 MB	0 MB/s	0 Mbps
Microsoft Application Virtualiza...		0%	1.0 MB	0 MB/s	0 Mbps
Microsoft Windows Search Inde...		0%	8.0 MB	0 MB/s	0 Mbps
RDP Clipboard Monitor		0%	3.3 MB	0 MB/s	0 Mbps

[Up] Fewer details End task

FIGURE 2-7. MORE DETAILS IN TASK MANAGER

Summary

Windows 8 reflects changes in today's workplace by providing an immersive experience that you and your users will love. It gives people the freedom to get their work done the way they want on the types of devices they want. Windows 8 builds on the foundation set by Windows 7. Features like File Explorer and Task Manager have been updated and enhanced for today's users. These and other tools give you the ability to be more productive.

Windows 8 for IT pros

Microsoft Windows 8 is optimized for making your life as an IT pro easier. Increased functionality and innovative new features distinguish Windows 8 from all other previous operating systems. Windows 8 provides reimagined system applications, expanded user customization, new tools such as Windows PowerShell 3.0, and new functionality, such as integrated mobile broadband support. These additions, alongside redesigned Windows Server 2012 remote management features, make Windows 8 one of the most advanced operating system offerings from Microsoft—ever.

IT pros that have experience in Windows 7 will have no problem quickly learning to navigate through Windows 8. Its enhanced usability and new features make everything you need readily available. In addition to feature upgrades, accessibility, and expanded functionality, significant improvements have been made in areas such as startup and shutdown times and general performance. This chapter explains some of the key improvements and added features for the Windows 8 operating system that are specifically important to IT pros.

Reimagined system applications

For IT pros, Windows 8 is just like Windows 7—but better. Features that were great in Windows 7 were redesigned to be even more efficient and provide more functionality. Windows 8 provides a flexible platform for a wide variety of applications and devices. Most of the familiar applications that IT pros use are exactly the same but with a renewed, simplified layout. Many system features such as Performance Monitor or Windows Services, look nearly identical to their Windows 7 predecessors. Some applications have gained increased functionality. For example, Windows Defender now offers malware protection as well as spyware protection. If you were a Windows 7 expert, then Windows 8 is going to be simple for you to learn and implement.

Making the transition from Windows 7 to Windows 8 is much easier than transitioning from Windows XP to Windows Vista or 7. Windows 8 is packed with new features that make your life as an IT pro easier. Some quick access and navigation features that are heavily used as an IT pro are still the same, such as Window key + R to open the Run dialog box. Also, many new quick access features have been added for convenience (e.g., Windows key + X to open a menu of administrator tools). Throughout this chapter are tips on new quick access features that make navigating Windows much quicker. Additionally, in an effort to improve Windows functionality, two of the most commonly used applications—Windows Task Manager and Windows Explorer—have been infused with new features to enhance the user experience.

Windows Task Manager

Windows Task Manager is one of the most widely used tools in the Windows operating system. For IT pros, Windows Task Manager performs a vital role in maintaining healthy systems through troubleshooting resource issues. Virtually every IT pro has used Task Manager at some point to close an application or kill a process.

Since its introduction in Windows NT, it has been polished and improved with each operating system revision. Before Windows 8, IT pros were forced to use other tools to compliment Windows Task Manager, such as Sysinternals Process Explorer.

TIP To quickly access Windows Task Manager and many other system features in Windows 8, press **Windows key + X**.

The redesigned Windows Task Manager introduces new functionality, detailed data visualization, and an optimized user experience. It provides a simple "fewer details" option for standard users and a "more details" option that contains all of the intricate data that IT pros have been seeking from additional software. Figure 3-1 shows the redesigned Windows Task Manager found in Windows 8.

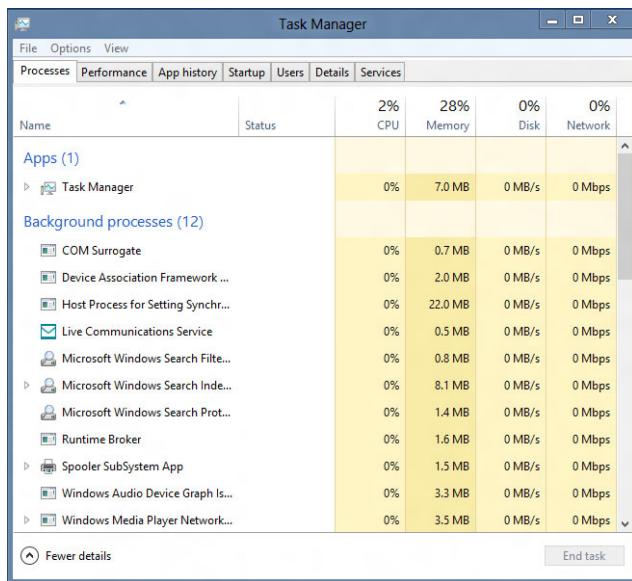


FIGURE 3-1 The new Windows 8 Windows Task Manager.

The redesigned Windows Task Manager is vastly more user friendly than previous versions. Top-level application windows can now be broken down into their components. This provides users with the capability to close specific windows in an application, without closing the application entirely.

In addition, commonly named processes like "svchost.exe" have also received this improved, more detailed layout. Also, friendly application and process names have replaced unrecognizable ones found in previous

versions. For example, you will see "Print driver host for applications" in the place of its previous name "splwow64.exe." Table 3-1 offers a quick description of the features found under each tab in Windows Task Manager.

TIP Don't understand what a process, service, or application is? The new Windows Task Manager has a built in "search online" feature. Simply right-click a process that you would like explained and select "search online." You will automatically be directed to your default search engine's results.

Table 3-1 Windows Task Manager Tabs

TAB NAME	DESCRIPTION
Processes	This tab displays all active applications and processes. It also shows the status and cpu, memory, disk, and network usage for each. Memory, disk, and network usage values can be filtered by percent or raw value. Using the new heat map feature, background color intensity of the data indicates higher usage. This feature quickly identifies resource-intensive applications and processes.
Performance	This tab displays a system overview of resources, broken down into cpu, memory, disk drives, and Ethernet categories. You can also access the resource monitor from this page.
App History	This new Windows Task Manager feature shows the cpu time and network usage for each installed application. The network usage is broken down by metered, upload/download, and tile update usage. This information can help troubleshoot network slowness possibly caused by an application.
Startup	The startup tab was previously available in the system configuration menu in earlier versions of Windows. It allows for customization of which programs run and their impact at startup. This feature has been improved by simplifying the provided information and filtering it by application name, publisher, status, and startup impact.
Users	This feature of Windows Task Manager has been completely redesigned in Windows 8. Instead of only providing the name of active users, resources used by profile and active applications within the profile are also visible. This improves visibility of resource allocation on machines with multiple user accounts.
Details	This familiar tab is a remake of the previous performance tab found in the Windows 7 task manager. The details tab provides information regarding resource usage and user activation for the status of each application and process.

Services

The services tab shares the same layout as in Windows 7. It allows users to start, stop, and view the status of all Windows services.

Windows Explorer

The redesigned Windows Explorer, named File Explorer, has been optimized for file management tasks. It provides a streamlined command experience but remains a powerful tool. New features include advanced folder customization options, previously hidden explorer features, and the ability to pause file transfers to free cpu usage.

One of the biggest changes in Windows Explorer is the ribbon tool bar. As found in Microsoft Office 2010, menu options are displayed in an icon-filled ribbon toolbar for easy access.

TIP If you don't know where an application, setting, or file is located, **Windows key + Q** navigates to Windows Search.

The reimagined toolbar hosts many hidden features that existed but were never used in previous versions of Windows Explorer toolbars. The new ribbon toolbar is laid out for maximum efficiency, placing the most popular commands in its most prominent parts and grouping them by context and relevance. This grouping makes finding commands predictable and reliable. The ribbon layout also exposes a large set of commands while maintaining a pleasant visual appearance. Specific sets of commands are visible when a user is working with specific file and folder types. For example, Figure 3-2 shows the toolbar available when inside a user's pictures folder.

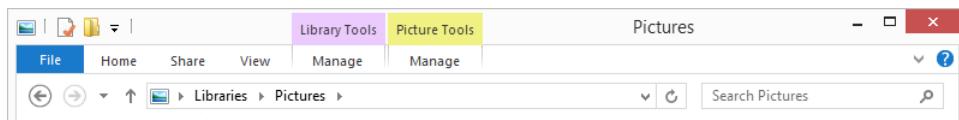


FIGURE 3-2 File Explorer.

As shown in the figure, both Library Tools and Picture Tools menus are available. The new Windows File Explorer toolbar focuses on the commands that are most used and combines them with additional commands relevant to the current folder contents. For example, there is no reason to have music tools available when you are in the videos folder.

For this reason, when you create a folder the new Windows File Explorer allows the folder to be optimized for different content, as shown in Figure 3-3. To optimize a folder, simply right-click the folder and select Properties. Optimizing the folder for pictures will force the picture toolbar to appear when you enter the folder.

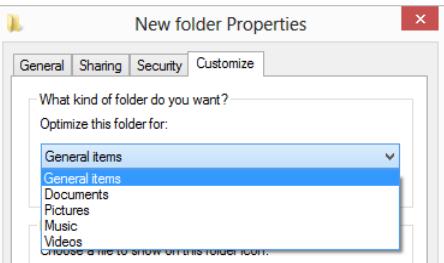


FIGURE 3-3 Folder optimization.

File history

File history is a new feature in Windows 8. It allows a user to back up files to removable media or a networked repository and retrieve them if they are lost or damaged. The user can customize exactly which folders are backed up and where the backup is stored. It also has an integrated recovery feature that will cache backed up files on the primary volume for offline access. For Enterprise use, this feature works well with DirectAccess because it allows remote file share back up.

For more information on DirectAccess, see the section titled "DirectAccess" later in this chapter.

Customizing and configuring Windows 8

Windows 8 is full of improvements that IT pros can appreciate. Just some of its many improvements include:

- Better resource allocation.
- Expanded device compatibility.
- Innovative and completely customizable desktop.
- Vastly improved Windows features.

Most advanced configuration options are exactly the same as in Windows 7. For example, IT pros using features such as Key Management Service (KMS) and Multiple Activation Key (MAK) volume activation still have those features available. Also available is the familiar desktop found in Windows 7. Desktop applications run on the desktop, just like before.

TIP To navigate directly to the desktop, from any application, press **Window Key + D**.

Along with the familiar desktop, the same security and reliability features found in Windows 7 exist in Windows 8. Windows 8 simply takes the stable and reliable core of Windows 7 and makes it better by adding advanced features and improved functionality. With Windows 8, all of the information and program shortcuts are found in one place—the new Windows Start screen. This new Start screen is easily customized and transferred to the default profile via the System Preparation (Sysprep) tool.

NOTE Sysprep allows system administrators to take a specialized image for one PC and generalize it for use on other PCs. For more information on Sysprep go to: <http://technet.microsoft.com/en-us/library/hh824816.aspx>.

Profile customization

Profile customization in Windows 8 is simple. Both roaming and local profiles are available in Windows 8. Roaming profiles allow user customizations to be saved remotely and accessed on any Windows 8 machine. Local profiles are stored locally on the file system volume just like those in previous versions of Windows. To manage the user experience for generated local profiles, Sysprep is available in Windows 8. Default customizations can be packaged, just like in Windows 7, and redeployed in the out-of-box experience (OOBE) after system imaging is performed.

One new profile customization feature reduces the necessity for multiple images in an environment. Using Group Policy objects (GPOs) and AppLocker, limitations and user restrictions can be set on individual programs. Instead of having various images for different types of users, this option allows you to deploy general images to your environment and simply limit program availability to different groups. For more information about AppLocker, see Chapter 8, "Windows 8 management."

Tile configuration

The new Windows Start screen is fully customizable with "Tiles." Some Tiles can be activated to provide real-time updates of applications such as Microsoft Outlook. Windows 8 is an event-driven operating system, meaning that it provides information and options right when you need them. Right-clicking a Tile brings up its menu with available options. Figure 3-4 shows the menu available when right-clicking a Live Tile.



FIGURE 3-4 Live Tile menu.

The Windows 8 Tile layout makes tasks like uninstalling an application very simple. Right-click the Tile of the program that you want to uninstall, and then select Uninstall. For programs not designed for Windows 8, uninstallation can be performed through the Add/Remove Programs feature in the Control Panel.

PC Settings

The PC Settings menu can be accessed by dragging the mouse pointer to the bottom right corner of the screen and selecting Settings. (You can also simply press Windows key + I to open Settings.) You will notice that a settings menu comes up. This settings menu is the settings for the active window. At the bottom of the menu, you will notice "Change PC Settings."

TIP To navigate directly to the settings menu press **Window Key + I** or by pressing **Window key + C** and selecting **Settings**.

Using this interface, you can:

- Customize features such as lock screen and Start screen appearance.
- Manage user accounts.
- Edit application notifications and search history.
- Share applications.
- Edit general settings such as system time and language.
- Refresh your Windows installation or fully reinstall Windows.
- Edit privacy settings for location services and other information.
- Manage devices.
- Change Home group and profile sync settings.
- Check for Windows updates.

Client Hyper-V

Client Hyper-V is an innovative virtualization platform available in Windows 8. It provides IT pros and developers with a local environment to test applications and client–server deployment scenarios without requiring a Hyper-V server. For example, you can build, host, and test an entire infrastructure on your local machine and then export the virtual machines directly into production. Additionally, tools that were created for Hyper-V in Windows Server, such as VMM P2V (Virtual Machine Manager Physical-to-Virtual) and Sysinternals DisktoVHD, can also be used in Client Hyper-V. Windows PowerShell scripts and Hyper-V virtual switch extensions that are developed and tested on Client Hyper-V can also be used in Windows Server 2012.

Because Client Hyper-V is the same technology as found in Windows Server, IT pros and developers do not need to learn any new tools or commands to implement and use this technology. The availability of Client Hyper-V allows cross compatible virtual machines (VMs) to be imported and exported between Client Hyper-V and Hyper-V Server. This simplifies application and deployment testing and troubleshooting across an enterprise. Client Hyper-V supports USB media, as well as other new Windows features such as Windows To Go. Turning on the Windows 8 Hyper-V feature also installs a VM management tool called Hyper-V Manager.

To enable Client Hyper-V from Control Panel:

9. From the Control Panel, click Programs, then select Programs and Features.
10. Select Turn Windows Features on or off.
11. Click Hyper-V, then OK, and then Close.

To enable Client Hyper-V using Windows PowerShell:

12. In the Windows PowerShell command line, type the following:

Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V

Once Hyper-V is enabled, you must fully shut down and restart your computer to complete installation. Upon restart, you will be able to create and manage VMs through Hyper-V Manager or the Hyper-V Module

for Windows PowerShell. You can also use Virtual Machine Connection to remotely connect to VMs. Not all features found in Hyper-V are available in Client Hyper-V; see Chapter 11, "Windows 8 virtualization" for more information.

Redesigned NTFS health model and chkdsk

While increasingly rare, disk corruptions can occur due to a variety of unique causes. Whether caused by hard disk or transient memory errors, corruptions can occur within the file system's metadata, which links physical disk blocks to virtual data. To restore access to the corrupted data, Windows must isolate and correct the issue using the chkdsk tool. Windows 8 vastly improves the resolution time of system errors by implementing a new NTFS health model and Check Disk resolution strategies.

Key design changes

In previous versions of the Windows operating system, NTFS implemented a simple health model which indicated two states for a volume; healthy or not. In this health model, the corrupted volume had to be taken offline for however long was necessary to resolve the issue. The downtime of the volume was directly proportional to its number of files, which for some systems was quite large. Windows Vista and Windows 7 made significant improvements to this process that ultimately decreased the resolution time. However, with hard drive capacities rapidly expanding, using the current resolution method has spanned several hours in some cases.

A redesigned NTFS health model and chkdsk was necessary to correlate with the rapidly expanding storage capacities. The new chkdsk design makes administrators aware of file system health at all times and provides convenient scheduled resolution with nearly zero downtime. Using this new design, downtime for correcting typical corruptions is less than two seconds. The correction process is now split into the following phases to ensure coordinated, rapid, and transparent corruption resolution. Figure 3-5 shows that in the green phases, the volume remains online. The final phase requires the volume to be offline for only seconds (which is indicated in red). In the previous model, the entire resolution process would be red rather than the stripe.

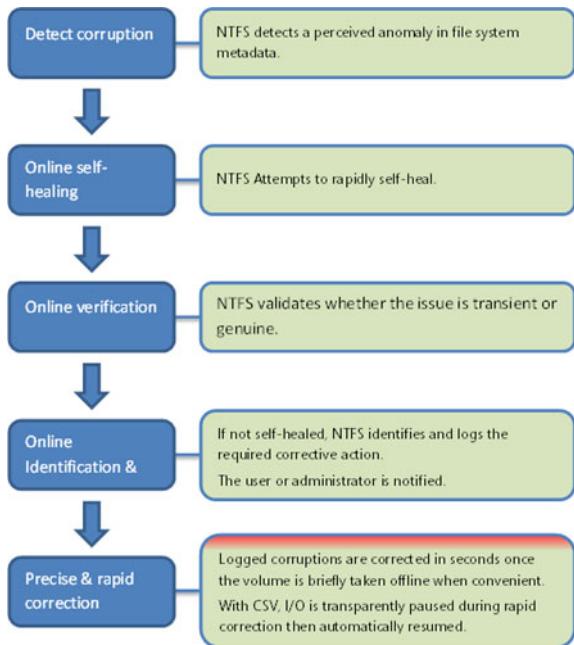


FIGURE 3-5 Windows 8 redesigned chkdsk.

New NTFS health model

Unlike the previous two-state model, the redesigned NTFS health model implements four health states. Some states are for informational purposes only, while some require action. The health states are:

- **Online and healthy** This state represents normal operation. In this state, there is no user action required and no corruptions are detected.
- **Online spot verification needed** The file system is briefly placed in a transient state after it detects a corruption that cannot be self-healed. The volume is placed in this state only until the spot verification service verifies the corruption. This state does not require any user action.
- **Online scan needed** After the spot verification service confirms the corruption, the file system is placed in this state. During the next maintenance window, an online scan is automatically performed. If more convenient, the online scan can also be run manually from the Action Center. During the online scan, all verified issues and corrective actions are logged for later execution.
- **Spot fix needed** The file system puts the corrupted volume in this state after the online scan is completed and will notify the user via the Action Center. Corrupted system volumes must be taken offline for corrections. Corruptions of removable media and other non-system volumes can be corrected without taking the system offline by selecting "Error checking" under the Tools tab of the volume's Properties menu. For Windows Server 2012 systems, spot fix corrections on data volumes can be scheduled during maintenance windows.

In the previous NTFS health model, a user might not know there is a problem until the chkdsk screen suddenly appeared when booting. To improve transparency and user awareness, Windows now exposes the current state of the file system and provides repair options via the Action Center, Explorer, Windows PowerShell "REPAIR-VOLUME" cmdlet, and Server Manager. These transparencies improve the user experience by providing full resolution control when it is most convenient.

Windows PowerShell 3.0

Windows PowerShell 3.0 is packed with new features and cmdlets that extend its use, improve its usability, and allow for more comprehensive control of Windows-based environments. Previously, users and administrators enjoyed the rights and permissions provided by PowerShell. With more than one thousand new cmdlets, Windows PowerShell 3.0 is now more powerful than ever.

NOTE Windows PowerShell 3.0 is backward compatible. No changes are required for scripts, modules, cmdlets, functions, snap-ins, and profiles designed for Windows PowerShell 2.0 to work in Windows PowerShell 3.0. This allows you to use all of your previous management scripts without converting them to a new format.

New features

PowerShell 3.0 has updated features for Windows 8, as well as Windows Server 2012. A few of the additional features specifically for Windows Server 2012 include BranchCache, Server Manager, and web cmdlets. The new features found in Table 3-2 are only a small portion of the new features available in Windows 8, but they are some of the most impactful.

Table 3-2 Windows PowerShell 3.0 New Features

FEATURE NAME	DESCRIPTION
Disconnected Sessions	In Windows PowerShell 3.0, you can now disconnect from a session without disrupting the commands that are running. Once a "PSSessions" is started, it does not rely on that current session to run. This feature allows users to disconnect and reconnect to the session later.
Windows PowerShell Workflow	Workflows are long-running tasks that affect multiple computers. These workflows can now be written and run in PowerShell just like cmdlets, and can be comprised of many different scripts.
Scheduled Jobs	Unlike in previous Windows versions, you can now schedule Windows PowerShell background jobs and manage them in PowerShell and Task Scheduler.

Updatable Help	Administrators can now download updated Help files for their module cmdlets. Simply type "Update-Help" in the PowerShell command window and the Help files will automatically be updated.
Windows PowerShell Web Access	This is a new feature in Windows Server 2012 that acts as a Windows PowerShell gateway, providing a web-based Windows PowerShell console that is targeted at a remote computer. You can run Windows PowerShell commands and scripts from a Windows PowerShell console in a web browser, with no Windows PowerShell, remote management software, or browser plug-in installation necessary on the client device.
Enhanced Online Help	Windows PowerShell online Help has been expanded and can now be accessed from the command line. To get help online for any PowerShell cmdlet, simply type "Get-Help <cmdlet name> - Online."

TIP Need help finding a specific PowerShell command? By using the "show-command" cmdlet, you are provided with a graphical list of all commands available in all installed modules. From this user interface, you can also run the cmdlets directly.

Integrated Scripting Environment (ISE)

Windows PowerShell ISE is a host application for Windows PowerShell. It allows you to run commands and write, test, and debug scripts in one graphical user interface. Windows PowerShell ISE introduces many new features in Windows PowerShell 3.0. A few notable new features are described in Table 3-3.

Table 3-3 Windows PowerShell ISE Features

FEATURE NAME	DESCRIPTION
New Command pane	The redesigned Command pane combines the features of the command and output panes from previous versions of Windows PowerShell ISE. Its visual similarities to the PowerShell console make transitioning back and forth seamless. In addition, new features such as color-coded text, brace-matching, error indicators, rich copy, and snippets have been introduced.
Show Command window	The Show Command window also simplifies script development by displaying all commands from installed PowerShell modules and it automatically imports a module when referenced.
IntelliSense	The new IntelliSense feature in Windows PowerShell 3.0 autocompletes valid commands and also displays cmdlets, functions, scripts, workflows, etc. in a similar manner to Windows Search.

Snippets	The Snippets feature allows you to copy saved text strings into the script and command panes. Snippets can be imported from modules and includes three basic cmdlets: New-IseSnippet, Get-IseSnippet, and Import-IseSnippet. To see inserted snippets, press Ctrl+J.
Editing and Debugging enhancements	Editing and debugging has never been easier in PowerShell. With customizable features such as brace-matching, outlining, expand-collapse, and error indicators, real-time error catching is simple.
Help window	The new Help window provides a pop-up window that contains information regarding available cmdlets. This is a huge improvement over the previous command line Help options found in Windows PowerShell 2.0.

Networking enhancements

Windows 8 and Windows Server 2012 provide new features and resources when deployed together. Many new features that IT pros love about Windows Server 2012 are optimized for use with Windows 8 clients. In fact, many of the new improved management features in Windows Server 2012 can also be used from a local console only available in Windows 8. Many redesigned features were available in Windows Server 2008 but have been reimaged for the modern, expanding business needs.

BranchCache

BranchCache was first introduced in Windows Server 2008 as a way of caching content from wide area network (WAN) web and file servers locally at branch offices. BranchCache greatly reduces network traffic by accessing reused files from the local cache instead of the WAN. BranchCache has been enhanced with new features in Windows Server 2012 and Windows 8 that far surpass its previous capabilities. Just some of its many improvements include:

- Removed requirement for individual Group Policy Objects for each branch.
- Automatically encrypted cached content.
- New management options in Windows PowerShell.
- New ability to preload content into cache before a client request.
- Increased scalability through multiple Hosted Cache servers and improved database performance.

BranchCache supports two cache modes: Distributed Cache mode and Hosted Cache mode. Figure 3-6 displays the fundamental differences of each.

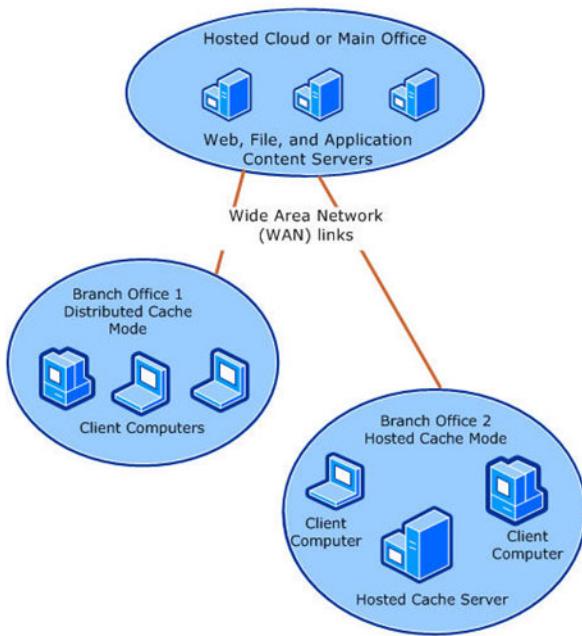


FIGURE 3-6 Distributed Cache mode (Left), Hosted Cache mode (Right).

In Hosted Cache mode, the hosted cache server is a central repository of data that is downloaded from the central office. This repository does not require a dedicated server but can be on an existing server at the local branch. In this model, when a file is requested, the central server is contacted as it would be without BranchCache. The central server then authenticates the request and sends the metadata for the file only. The client then searches the local hosted cache repository for the file. If it is not cached locally, the file is then taken from the central server and copied from the client to the local hosted cache.

In Distributed Cache mode, the cache is on the individual client machines. This quick deployment cache method is best suited for small offices with less than 50 users. It can also automatically self-configure as Hosted Cache mode once server infrastructure is implemented. In this model, when a file is requested, the central server is contacted as it would be without BranchCache. However, instead of pointing the client to a hosted cache repository, it provides the location of another client's cache repository. If the file is not cached on one of the local clients, it is retrieved from the central server and cached into the requesting client's cache repository.

NOTE In distributed cache mode, cache availability decreases as PCs go offline.

DirectAccess

Most IT pros are familiar with remotely connecting to their corporate network resources through a virtual private network (VPN). There are time-consuming redundancies associated with using VPN—such as the need to always log into a VPN service, run security scans, etc. Connection initiation and user authentication is

necessary every time VPN is reconnected. If users do not frequently reconnect, their PCs may not receive the latest updates or Group Policy pushes. DirectAccess allows remote users to securely access their organizations shares, websites, and applications every time they connect their DirectAccess-enabled portable device to the Internet. DirectAccess does not require frequent logins or access maintenance, and even allows remote computer management to administrators without an established VPN connection. This availability of constant connection minimizes frustration and improves efficiency in everyday "out-of-the-office" needs. Windows 8 and Windows Server 2012 make DirectAccess simpler to deploy and implement.

Mobile broadband support

Windows 8 offers a completely redesigned mobility experience to its users. Windows 8 was designed to work well on a variety of platforms including desktops, laptops, and tablets, so this feature was designed accordingly. Previously, if you wanted to use a mobile broadband device on a laptop, you had to retrieve the software and drivers from the manufacturer and carrier, install the correct one, and then troubleshoot any associated issues. In Windows 8, the management tool and driver is built in. There is no hassle associated with configuring mobile broadband in Windows 8.

Windows 8 includes a connection management API called Windows Connection Manager that provides functionality native to broadband devices currently in use. Additionally, Windows 8 comes with an integrated mobile broadband class driver. It works with virtually all devices and completely eliminates the frustration of locating the correct driver for your device. Windows 8 is optimized for all wireless connectivity and offers connection prioritization, among many other user customizations. Using the Windows Connection Manager, you can manage all wireless radios side-by-side.

Included with mobile broadband support are many other wireless enhancements for Windows 8. This optimized end-user experience includes metered connection awareness and efficient data usage as well as the ability to conserve bandwidth by delaying network heavy actions until an unmetered connection is made. Connection priority is learned by the operating system, which can then automatically choose the network for you. This feature can be overridden through user customization. When resuming from standby, Windows 8 can also reconnect much faster to your wireless network than previous versions—oftentimes before your display is refreshed. Due to substantial wireless improvements, Windows 8 is capable of connecting to a wireless network in less than two seconds. Previously, the process spanned nearly 12 seconds.

IPv6 Internet support

Most currently implemented networks have the ability to connect to the Internet via IPv4. However, IPv4 has address limitations that are beginning to show strain and cannot keep up with the quickly expanding Internet. Currently, network address translation (NAT) is used to share addresses in residences around the country. This technology allows each home to have one IP address but multiple devices connected to the Internet. With IPv4 addresses quickly depleting, NATs may be used on a broader scale, hindering location based services such as Bing and degrading the P2P application experience.

To remedy these issues, IPv6 was created with unimaginable scale, offering 3×10^{38} available IP addresses (enough for every person to have billions to themselves). In addition to offering an immense address range,

IPv6 also offers new security features such as IPsec, which provides security at the packet level. During the transition from IPv4 to IPv6, dual stack topologies will be implemented. This allows devices to be configured with both IPv6 and IPv4 addresses. In Windows 8, if an IPv6 address is present, it will automatically take connection priority over the IPv4 address. Also, not all applications will support IPv6 immediately. Windows will automatically select the correct connection for applications to properly communicate by using a method called *address sorting*. These advanced Windows features indicate that Windows 8 is fully capable of supporting the IPv6 Internet.

Remote Server Administration Tools

Remote Server Administration Tools (RSAT) for Windows 8 includes Server Manager, Microsoft Management Console (MMC) snap-ins, consoles, Windows PowerShell cmdlets and providers, and command-line tools for managing roles and features that run on Windows Server 2012. To fully use these tools, Windows Server 2012 is required.

NOTE To include these tools, and other administrative tools, on your Start screen: From the Start screen, open the Charm Bar (Windows key +C), select Settings, and select the Tiles option, then select Show Administrative Tools. You can also use the Windows Search feature to find a particular snap-in. Right-clicking it and selecting Pin To Start will pin only that one feature to your Start screen.

The new Windows Server Manager, found in RSAT for Windows 8 and Windows Server 2012, facilitates management of all remote servers running Windows Server 2012 from one centralized console. In some cases, these tools can be used to manage roles and features on running on Windows Server 2008. Remote management capabilities of Windows Management Instrumentation (WMI), Windows PowerShell, and Distributed Component Object model (DCOM) are used to manage the servers. Windows Server Manager removes the necessity to remote into each server to change roles or update policies and empowers administrators with these management tools on their desktop. Windows Server Manager also hosts links to nearly all other tools found in RSAT, including the MMC snap-ins.

Windows Server 2012

Windows Server 2012, formerly codenamed Windows Server 8, is the most recent release of the Windows Server operating system. Windows Server 2012 offers features unlike any Windows Server operating system before. It is optimized for use with Windows 8 clients. Windows Server 2012 shares features and management tools with Windows 8, such as Server Manager, which allow remote server management for IT administrators. These features depend on a Windows Server 2012 and Windows 8 environment to function. Additionally, Windows Server 2012 supports multiple installation options: Server Core, Full, and Minimal Server Interface, which is similar to a server with a GUI installation but does not include Internet Explorer 10, Windows Explorer, the Desktop, or the Start screen. . This customization allows administrators to pick and

customize their interface layout.

Virtualization

Virtualization offers many benefits to an organization. Some of these benefits include greater agility, improved cost efficiency, and expanded flexibility. To meet the changing demands of today's business environment, combining virtualization with the infrastructure and tools needed to provision a cloud environment is essential. Windows Server 2012 makes this expansion possible through integrated tools like Hyper-V. For more information on how virtualization can improve your environment, see Chapter 11, "Windows 8 virtualization."

ReFS

Resilient File System (ReFS) is a new file system available in Windows Server 2012 and Windows 8. ReFS is an improvement on NTFS that has major feature upgrades. Below is a quick description of the primary file system upgrades found in ReFS:

- **Robust disk capabilities** ReFS vastly raises the upper limits for the following: file size, volume size, number of files in a directory, and number of directories in a volume. The new available maximum file size is 16 Exabytes and the maximum volume size is 1 Yottabyte. These storage capabilities provide immense future scalability.
- **Resiliency to disk corruption** To minimize disk corruptions, ReFS has built-in features that minimize the need for tools such as chkdsk. ReFS metadata is check-summed and stored off page to allow real-time corruption, miswrite, and bit rot detection. This new option, known as *integrity streams*, ensures that preexisting data is not lost due to the new written data.
- **Compatibility with existing technology** ReFS supports many of the existing Windows and NTFS features such as BitLocker, Access Control Lists, junction points, mount points, etc. without requiring new system application programming interfaces (APIs). This makes ReFS easy to implement into existing data structures.
- **Storage Spaces** *Storage Spaces* is the new storage virtualization pool technology which offers the joining of different-sized storage drives into virtual drives. It also allows users to select parity and mirroring features on a folder-by-folder basis.

Summary

Windows 8 offers a wide variety of targeted improvements while keeping its standard usability and functionality derived from Windows 7. With reimagined system applications, simple configuration, vast customization options, a redesigned NTFS health model, and new features such as windows PowerShell 3.0, networking enhancements, and Client Hyper-V, Windows 8 is the most improved Windows operating system yet. Its design integrates the best of Windows 7 and improves specific applications and features that make your life as an IT pro easier.

Preparing for deployment

Deploying any new operating system requires careful planning, and Microsoft Windows 8 is no exception. Successful operating system deployment includes automation, application compatibility testing, user state migration, and hardware readiness. To that end, Microsoft deployment tools and technologies can help streamline operating system deployment, improve the user experience, and reduce support costs.

The good news is that IT pros comfortable with Windows 7 deployment will be just as comfortable with Windows 8 deployment. That is because Windows 8 deployment is based on the proven tools and technologies they used for Windows 7 deployment (see Chapter 5, "Deploying Windows 8"). While the tools are familiar, there are other elements of deployment that you need to consider when deploying Windows 8. This chapter describes those considerations. After introducing you to the stock keeping units (SKUs) available for deployment, it provides guidance for evaluating application compatibility, migrating user state, and choosing a deployment strategy.

Windows 8 SKUs

Not only did Microsoft reimagine the Windows 8 user interface, but it also reimagined the available SKUs to make choosing the right one simpler. Of course, all of the SKUs offer the same fluid experience—on a variety of devices—using touch, a keyboard, or a mouse.

For PCs and tablets powered by x86 or x64 processors, Microsoft offers two editions: Windows 8 and Windows 8 Pro. For consumers, Windows 8 is often the best choice. On the other hand, Windows 8 Pro edition is the best choice for enthusiasts, technology professionals, and businesses. It includes everything in Windows 8 plus a broader set of technologies, such as encryption, virtualization, management, and domain connectivity.

As with previous Windows versions, Windows 8 Enterprise edition is available to Software Assurance customers. It includes all of the features in Windows 8 Pro plus management, deployment, security, virtualization, and mobility features that IT organizations need to enable new computing scenarios.

Windows To Go, DirectAccess, BranchCache, AppLocker, VDI enhancements, and Windows 8 App deployment are features unique to Windows 8 Enterprise. (Windows 8 Enterprise is already preconfigured to support app sideloading, as long as the PC is joined to the domain.) This is the SKU with which most IT pros will work.

Windows RT edition (previously known as Windows on ARM or WOA) is a new addition to the Windows family. Windows RT is only available pre-installed on PCs and tablets powered by ARM processors. Windows RT helps enable thin and lightweight devices with remarkable battery life. The main focus for Windows RT is running cloud-enabled, touch-enabled, web-connected apps based on the new Windows runtime (WinRT).

However, it includes touch-optimized desktop versions of Microsoft Word, Excel, PowerPoint, and OneNote. For more information about Windows RT, see Chapter 1, "Overview."

Table 5-1 lists the key features available in each SKU.

TABLE 5-1 Windows 8 SKUs

FEATURE NAME	WINDOWS 8	WINDOWS 8 PROFESSIONAL	WINDOWS 8 ENTERPRISE	WINDOWS RT
Upgrades from Windows 7 Starter, Home Basic, Home Premium	x	x	x	
Upgrades from Windows 7 Professional, Ultimate		x	x	
Start screen, Semantic Zoom, Live Tiles	x	x	x	x
Windows Store	x	x	x	x
Apps (Mail, Calendar, People, Messaging, Photos, SkyDrive, Reader, Music, Video)	x	x	x	x
Microsoft Office (Word, Excel, PowerPoint, OneNote)				x
Internet Explorer 10	x	x	x	x
Device encryption				x
Connected standby	x	x	x	x
Microsoft account	x	x	x	x
Desktop	x	x	x	x
Installation of x86/64 and desktop software	x	x	x	
Updated Windows Explorer	x	x	x	x
Windows Defender	x	x	x	x
SmartScreen	x	x	x	x
Windows Update	x	x	x	x
Enhanced Task Manager	x	x	x	x
Switch languages on the fly (Language Packs)	x	x	x	x
Better multiple monitor support	x	x	x	x
Storage Spaces	x	x	x	
Windows Media Player	x	x	x	
Exchange ActiveSync	x	x	x	x
File history	x	x	x	x
ISO / VHD mount	x	x	x	x
Mobile broadband features	x	x	x	x

Picture password	x	x	x	x
Play To	x	x	x	x
Remote Desktop (client)	x	x	x	x
Reset and refresh your PC	x	x	x	x
Snap	x	x	x	x
Touch and Thumb keyboard	x	x	x	x
Trusted boot	x	x	x	x
VPN client	x	x	x	x
BitLocker and BitLocker To Go		x	x	
Boot from VHD		x	x	
Client Hyper-V		x	x	
Domain Join		x	x	
Encrypting File System		x	x	
Group Policy		x	x	
Remote Desktop (host)		x	x	
Windows To Go			x	
DirectAccess			x	
BranchCache			x	
AppLocker			x	
VDI enhancements			x	
Windows 8 app deployment			x	

Application compatibility

The overall compatibility of Windows 8 with existing apps is very high. However, some compatibility issues are possible because of innovative new features, tightened security, and improved operating system reliability.

IT pros planning for application compatibility should consider the "Windows 8 Release Preview and Windows Server 2012 RC Compatibility Cookbook" available from the Microsoft Download Center at <http://www.microsoft.com/en-us/download/details.aspx?id=27416> to be essential reading. This document describes changes in Windows 8 and Microsoft Windows Server 2012 that could break an application, how those problems manifest themselves, and how to mitigate those problems. While this document is targeted primarily at developers working on the compatibility of their apps, it offers a glimpse into potential compatibility issues. (The large size of the document does not necessarily mean that there will be numerous problems.)

While the compatibility cookbook is theoretical, you will need empirical data from your environment to assess and mitigate your applications. The Application Compatibility Toolkit (ACT) helps you inventory and

test applications, devices, and PCs for compatibility with Windows 8. You can get compatibility information from Microsoft and independent software vendors (ISVs), identify compatibility issues in your environment, and share compatibility data with other ACT users. ACT provides tools that can help you analyze and mitigate the compatibility issues that you discover in your organization.

Application compatibility resources for IT pros include:

- Application Compatibility TechCenter on TechNet at <http://technet.microsoft.com/en-us/windows/aa905066>.
- Compatibility Center for Windows 8 Release Preview at <http://www.microsoft.com/en-us/windows/compatibility/en-US/CompatCenter/Home>.
- Windows 8 Release Preview and Windows Server 2012 RC Compatibility Cookbook available from the Microsoft Download Center at <http://www.microsoft.com/en-us/download/details.aspx?id=27416>.

ACT 6.0 improvements

ACT 6.0, the most recent version of the toolkit, adds support for Windows 8. The following list describes ACT:

- **Support for Windows 8** ACT 6.0 adds support for Windows 8.
- **Runtime-analysis package** The runtime-analysis package gathers compatibility information. You install it on PCs running Windows 8 for compatibility testing. Data from the runtime-analysis package replaces data from issue detectors that attempt to forecast compatibility issues by running on a previous version of Windows.
- **Streamlined inventory collection** Limiting the inventory-collector package to inventory collection reduces data collection overhead. The redesigned inventory-collector package does not cause application conflicts because it does not interact with applications, so you do not have to schedule the inventory-collector package to avoid conflicts.
- **Application grouping** The application reports in Application Compatibility Manager (ACM) group multiple versions of an application together under a single parent entry.
- **Restructured ACT documentation** ACT 6.0 includes streamlined documentation to help you find information more quickly and conveniently.
- **Windows Assessment and Deployment Kit (Windows ADK) integration** ACT is now part of the Windows ADK. The Windows ADK (see Chapter 5, "Deploying Windows 8") consolidates the assessment and deployment tools in one place.
- **Focus on Operating System Deployment** ACT 6.0 focuses on operating system deployment. It no longer includes update compatibility.

Common compatibility problems

The following list describes common sources of compatibility issues for Windows 8, particularly when using an application originally designed for Windows XP.

- **User Account Control (UAC)** In Windows 8, by default, all interactive users, including members

of the Administrators group, run as standard users. UAC is the mechanism through which users can elevate applications to full administrator privileges. Because of UAC, applications that require administrator rights or check for administrator privileges behave differently in Windows 8, even when run by a user as administrator.

NOTE Windows 8 apps require UAC. If you disable UAC, Windows 8 apps will not run.

- **Windows Resource Protection (WRP)** WRP is designed to protect the system in a read-only state to increase system stability, predictability, and reliability. This will affect specific files, folders, and registry keys. Updates to protected resources are restricted to the operating-system trusted installers (TrustedInstaller group), such as Windows Servicing. This helps to protect components and applications that ship with the operating system from any impact of other applications and administrators. This can be an issue for custom installations not detected as set up by Windows 8 when they try to replace WRP files and registry settings and check for specific versions and values.
- **Internet Explorer Protected Mode (IEPM)** In Windows 8, Microsoft Internet Explorer 10 processes run in IEPM with greatly restricted privileges to help protect users from attack. IEPM significantly reduces the ability of an attack to write, alter, or destroy data on the user's computer, or to install malicious code. This could affect ActiveX controls and other script code that tries to modify higher integrity level objects.
- **Deprecation** Any application that uses .dll files, executable (.exe) files, COM objects, registry keys, application programming interfaces (APIs), or other files that are deprecated in Windows 8 might break.
- **Graphical Identification and Authentication (GINA) dynamic-link library (DLL)** Prior to the release of Windows Vista, ISVs were able to modify authentication by installing a GINA DLL. The GINA DLL performed the user identification and authentication. The current authentication model does not require the GINA DLL and ignores all previous GINA DLLs. This change affects any application or hardware component that attempts to log on by using customized logon applications, including biometric devices (fingerprint readers), customized user interfaces, and virtual private network (VPN) solutions for remote users with customized logon user interfaces.
- **Session 0 isolation** Running services and user applications together in Session 0 poses a security risk because services run at an elevated privilege and therefore are targets for malicious agents looking for a means to elevate their own privilege level. In earlier versions of the Windows operating system, services and applications ran in the same session as the first user who logged on to the console (Session 0). To help protect against malicious agents in Windows 8, Session 0 has been isolated from other sessions. This could impact services that communicate with applications using window messages.
- **Windows Filtering Platform (WFP)** WFP is an API that enables developers to create code that interacts with the filtering at several layers in the networking stack and throughout the operating system. With previous versions of the WFP API, you might experience failures when running network scanning, antivirus, or firewall applications.

- **Operating system and Internet Explorer versioning** Many applications check the version of the operating system and behave differently or fail to run when an unexpected version number is detected. You can resolve this issue by setting appropriate compatibility modes or applying versioning shims (application compatibility fixes).
- **Windows 64-bit** 64-bit versions of Windows use the Windows on Windows 64 (WOW64) emulator. This emulator enables the 64-bit operating system to run 32-bit applications and can cause an application or a component that uses 16-bit programs or installers, or 32-bit kernel drivers, to break.
- **New folder locations** User folders, My Documents folders, and folders with localization have changed since Windows XP. Applications with hard-coded paths might fail. You can mitigate this by using directory junctions or by replacing hard-coded paths with appropriate API calls to get folder locations.

User state migration

Operating system deployment always involves user state migration—the process of migrating users' documents and settings from one operating system to another. Even when you don't migrate user state during deployment, users can spend countless hours trying to restore their preferences (such as desktop backgrounds, screensavers, and themes). Because this manual process reduces user productivity and usually increases support calls, you might choose to migrate some portion of user state to Windows 8 as you deploy it.

User satisfaction is another reason to elevate the importance of user state migration in your project. Users are simply more satisfied and feel less overwhelmed when they sit down in front of a new operating system and they don't have to recover their preferences. Unsatisfied users can have negative consequences for future deployment projects.

The primary tool you use to migrate user state during a high-volume Windows 8 deployment is the User State Migration Tool (USMT). Version 5.0 is the most recent version of USMT supporting Windows 8 migrations. USMT is part of the Windows ADK (see Chapter 5, "Deploying Windows 8"). USMT can perform complex, repeatable migrations of user state data between earlier Windows versions and Windows 8.

There are a few different ways to use USMT:

- Script USMT.
- Run it as part of a Microsoft Deployment Toolkit (MDT) 2012 Update 1 Lite Touch Installation (LTI).
- Run it as part of a System Center 2012 Configuration Manager Zero Touch Installation (ZTI).
- Run it directly at the command prompt.

NOTE Although USMT will generally be used in most enterprise environments, some businesses may find Windows Easy Transfer a simple and useful alternative to using USMT. It is particularly useful in one-off scenarios for individual users. Windows Easy Transfer can move user accounts, files and folders, program settings, Internet settings and favorites, and e-mail settings from a computer

running earlier versions of Windows to Windows 8. However, you cannot customize what it transfers to the extent that you can customize USMT.

Running USMT in MDT 2012 Update 1 or Configuration Manager task sequences is probably the simplest way to use USMT. (System Center 2012 Configuration Manager with Service Pack 1 is required for Windows 8.) Both include built-in support for running USMT pre-deployment (to gather user state) and post-deployment (to restore user state). This ability allows you to focus on planning for and customizing the USMT to migrate the data and settings required in your organization.

NOTE An alternative to using USMT to migrate user state is to implement user state virtualization prior to Windows 8 deployment. Part of the Microsoft Desktop Optimization Pack for Software Assurance customers, User Experience Virtualization (UE-V) synchronizes Windows and application settings in a settings store (a simple but secure file share). Folder Redirection moves users' documents off the endpoint to a central location on the network. Implementing user state virtualization enables replaceable PC scenarios, where you can install Windows 8 on the users' PCs and user state virtualization restores their experience and their documents. For more information about user state virtualization, see the Microsoft Desktop Virtualization website at <http://www.microsoft.com/dv>.

Deployment strategies

Microsoft recommends a few targeted strategies for deploying Windows 8. These strategies range from manually configuring Windows 8 on a few computers to using automation tools and technologies to deploy the operating system to thousands of computers.

The following list describes the four recommended deployment strategies:

- **High Touch with retail media** This is a hands-on, manual deployment, where you install Windows 8 on each client PC by using the retail installation media, and then you manually configure each PC. Microsoft recommends this strategy if your organization does not have dedicated IT staff, and it has a small, unmanaged network with fewer than 100 client computers.
- **High Touch with standard image** This strategy is similar to the High Touch with retail media strategy, but it uses an operating system image that includes your customizations and application configurations. Microsoft recommends this strategy if your organization has at least one IT pro (with or without prior deployment experience) on staff, and a small or distributed network with 100–200 client PCs.
- **Lite Touch, high-volume deployment** This strategy requires limited interaction during deployment. Interaction occurs at the beginning of the installation, but the remainder of the process is automated. Microsoft recommends this strategy if your organization has a dedicated IT staff, and it has a managed network with 200–500 client computers. Prior deployment experience is not required, but it is beneficial for using this strategy.
- **Zero Touch, high-volume deployment** This strategy requires no interaction during deployment.

The process is fully automated by using Configuration Manager. Microsoft recommends this strategy if your IT organization has experts in deployment, networking, and Configuration Manager, and it has a managed network with 500 or more client computers.

Table 5-2 shows guidelines for choosing a strategy based on many factors, including:

- The skill level of your organization's IT staff members.
- Your organization's license agreement.
- The number of client computers.
- Your infrastructure.

To use the table, choose the column that best matches your organization's network scenario. In cases where you identify with multiple columns, start with the leftmost column. As you move to the right, the solutions require more skills and investment to implement, and they provide for quicker, more thorough and more automated deployments.

As you plan to deploy more computers, consider improving your scenario to enable you to move to the right in the table. For example, if the only thing preventing you from performing a Lite Touch, high-volume deployment is that you are using retail media, consider purchasing a volume license.

TABLE 5-2 Choosing a Deployment Strategy

	HIGH TOUCH WITH RETAIL MEDIA	HIGH TOUCH WITH STANDARD IMAGE	LITE TOUCH, HIGH- VOLUME DEPLOYMENT	ZERO TOUCH, HIGH- VOLUME DEPLOYMENT
IT SKILL LEVEL	IT generalist	IT pro with optional deployment experience	IT pro with deployment experience recommended	IT pro with deployment and Configuration Manager
WINDOWS LICENSE AGREEMENT	Retail	Retail or Software Assurance	Software Assurance	Enterprise Agreement
NUMBER OF CLIENT COMPUTERS	<100	100–200	200–500	>500
INFRASTRUCTURE	Distributed locations Small, unmanaged networks Manual client computer configuration	Distributed locations Small networks Standardized configurations, including applications	Managed network At least one office with more than 25 users Windows Server products Configuration Manager (optional)	Managed network At least one office with more than 25 users Windows Server products Configuration Manager

APPLICATION SUPPORT	Manually installed commercial applications	Manually installed commercial or line-of-business (LOB) applications	Automatically installed commercial or LOB applications	Automatically installed commercial or LOB applications
USER INTERACTION	Manual, hands-on deployment	Manual, hands-on deployment	Limited interaction at the beginning of installation	Fully automated deployment
WINDOWS 8 TOOLS	Retail media	Retail or volume-licensed (VL) media	VL media	VL media
	Windows ADK	Windows ADK MDT 2012	Windows ADK MDT 2012 Windows Deployment Services	Windows ADK MDT 2012 Windows Deployment Services Configuration Manager

New deployment scenarios

The deployment strategies that the previous section describes are traditional. You install an operating system on a physical PC. However, desktop virtualization enables new deployment scenarios that can streamline and simplify Windows 8 deployment.

Windows To Go

Windows To Go offers a new alternative to traditional operating system deployment. Windows To Go is a Windows 8 Enterprise feature that enables users to boot and run Windows 8 from a USB drive. It provides a flexible way for workers to access their personal desktop on any PC. The article "Windows To Go: Feature Overview" at <http://technet.microsoft.com/en-us/library/hh831833.aspx> provides additional information about Windows to Go as well as step-by-step instructions for preparing, securing, and managing Windows To Go devices.

Virtual Desktop Infrastructure

Microsoft Virtual Desktop Infrastructure (VDI) is an alternative desktop delivery model that gives users secure access to centrally managed desktops running in the datacenter. VDI is powered by Remote Desktop Services (RDS), which is a server role in Windows Server 2012. It provides a single platform to deliver any type of hosted desktop, and RemoteFX provides a consistently rich user experience. RDS enables organizations to choose the deployment method that works best for them—all by using a single platform.

- **Session-based desktops** Session-based desktops provide users access to applications, data, and shared desktops centralized in the datacenter from a webpage, through a SharePoint portal, on a local desktop, or over the Internet.

- **Pooled virtual machines (VMs)** Pooled VMs give users access to high-performance desktops from any connected device. VDI assigns VMs on demand from an existing pool to users. When they log off a VM, VDI returns it to the pool for use by another user.
- **Personal VMs** Personal VMs give users access to a personal, high-performance desktop over which they have full administrative control.

With all three VDI deployment methods, user state virtualization maintains users' data and settings across physical and virtual sessions. VDI empowers enterprises with unified management of centralized desktops and corporate data by using System Center 2012. IT can extend existing management tools and processes to the VDI environment.

Partner technology, such as Citrix XenDesktop, adds value to VDI by offering additional scale and flexibility to enterprises. With Citrix technologies, users can access their Windows environment even from non-Windows devices.

Chapter 11, "Windows 8 virtualization," provides more information about Windows 8 and VDI. You can also learn more on the Desktop Virtualization website at <http://www.microsoft.com/dv>.

Client Hyper-V

On PCs running Windows 8, Client Hyper-V provides a robust virtual platform for developers and IT pros. It supports a broad range of devices and leverages the driver ecosystem of Windows 8 to run on the broadest range of 64-bit PCs. Client Hyper-V provides a rich user experience, including multimedia, touch, and USB support. Because Client Hyper-V is a core part of Windows 8, it leverages all of that operating system's security and management features.

Client Hyper-V requires:

- A 64-bit system
- 4 GB of RAM is required
- Support for Second Level Address Translation (SLAT)

SLAT unloads from the processor the process of mapping physical memory to virtual memory. For intensive graphics, it provides significant performance improvements. It is required for Hyper-V on Windows 8, because most systems have extensive graphics capabilities. It's only required for Windows 8 Server when enabling the RemoteFX role service.

For more information, see the article "Client Hyper-V" at <http://technet.microsoft.com/en-us/library/hh857623.aspx>.

Summary

Important considerations when preparing to deploy Windows 8 include automation, application compatibility testing, and user state migration. The Windows ADK provides the ACT for compatibility testing and USMT for user state migration. Additionally, Microsoft offers MDT 2012 to automate Windows 8 deployment in Lite Touch and Zero Touch installations. Organizations with a Configuration Manager

infrastructure can use the tools they already use to manage their PCs to deploy Windows 8. Chapter 5, "Deploying Windows 8," describes these tools in more detail and provides step-by-step instructions for using them to deploy Windows 8. Chapter 5, "Deploying Windows 8" and Chapter 11, "Windows 8 virtualization," describe powerful alternatives to deploying Windows 8 by using traditional means.

CHAPTER 5

Deploying Windows 8

Operating system deployment can be challenging--not only for Windows 8 but for all operating systems. Managing deployment content (operating system, device driver, package, and application source files) takes a lot of time and effort. The result is often out-of-date operating system images or a larger than necessary number of images to maintain. Preserving user settings and files represents a deployment risk for existing users. Additionally, configuration drift that occurs when users make changes that deviate from the standard configuration can cause devices to become unstable or even unusable.

Automation and wizard-guided user interfaces reduce the effort and risk of deploying and managing operating systems and applications, however. It helps prevent configuration errors by reducing manual steps, avoiding human error. Automation also provides a repeatable process that can drive consistency, and help you get more done with less time and effort. Also, wizard-guided user interfaces help users customize configurations with less error, and centralized administration helps drive consistency and reduce configuration drift.

To that end, Microsoft provides tools that can help you deploy Windows 8, and applications along with it, using less effort and with more success. If you're already familiar with Windows 7 deployment, you'll be happy to know that the learning curve for Windows 8 is almost nothing. The Windows 8 deployment tools and technologies are based on the same tools and technologies that you used for Windows 7. The only differences account for new and improved Windows 8 features, like Windows 8 apps, Windows To Go, and so on. This chapter will focus primarily on the differences from Windows 7.

Windows Assessment and Deployment Kit

One of the first things you'll notice is that the Windows Automated Installation Kit (Windows AIK) is now part of the Windows Assessment and Deployment Kit (Windows ADK). The Windows ADK also consolidates deployment tools that were once separate (e.g., User State Migration Tool). You will use the same tools to customize and automate high-volume Windows 8 deployment that you used to deploy Windows 7—only, you get them all from once place.

The following sections describe the tools in the Windows ADK. You can download the Windows ADK from <http://go.microsoft.com/fwlink/?LinkId=232339>.

Deployment and Imaging

The Deployment and Imaging component of the Windows ADK contains the tools that you need to customize, deploy, and service Windows images. These tools can stand alone but are recommended to be used with the Microsoft Deployment Toolkit 2012 Update 1 (MDT 2012) and System Center 2012

Configuration Manager. The tools in the Deployment and Imaging component of the Windows ADK are required by both.

The Deployment and Imaging component includes:

- **Deployment Image Servicing and Management (DISM).** DISM is a command-line tool that mounts and services Windows images before deployment. You can use DISM image-management commands to mount, and get information about, Windows image (.wim) files or virtual hard disks (VHD) and to capture, split, and otherwise manage .wim files. DISM replaces the ImageX tool for image management.
- **System Preparation (Sysprep) tool.** Sysprep prepares a computer for delivery by configuring it to create a new computer security identifier (SID) when the computer is restarted. In addition, the Sysprep tool removes user-specific and computer-specific settings and data that must not be copied to a destination computer.
- **Windows System Image Manager (Windows SIM).** Windows SIM creates unattended Windows Setup answer files. You can create an answer file by using information from a .wim file and a catalog (.clg) file. Component settings are added to appropriate configuration settings in the answer file. You can also add packages to be installed during Windows Setup.
- **Windows Recovery Environment (Windows RE).** Windows RE is a recovery environment that can repair common causes of unbootable operating systems.

The Deployment and Imaging tools include many other command-line tools that assist in the deployment and imaging of Windows, boot configuration, and Windows PE configuration.

Windows Preinstallation Environment

The Windows Preinstallation Environment (Windows PE) is a minimal operating system designed to prepare a computer for Windows installation by starting a computer that has no operating system. During Windows deployment, you can use Windows PE to partition and format hard drives, copy disk images to a computer, and start Windows Setup from a network share.

Windows PE 4.0 is based on the Windows 8 operating system, and it is available as a standalone product to customers who have the appropriate licensing agreement, and is an integrated component of many Windows technologies, including Windows Setup and Windows Deployment Services. Both MDT 2012 and Configuration Manager rely on it.

Customized Windows PE images can be created using the tools provided with Windows PE. MDT 2012 and Configuration Manager can also create customized Windows PE images.

User State Migration Tool

The User State Migration Tool (USMT) migrates user profiles and files from existing Windows operating systems to Windows 8. It captures the user state from the existing operating system and restores the user state to Windows 8.

The USMT includes three command-line tools:

- **ScanState.exe.** The ScanState.exe tool captures user state from the existing operating system (such

as Windows XP, Window Vista, Windows 7, or Windows 8). You can store the captured user state, on a removable drive, or on a network shared folder. The ScanState.exe tool can also estimate the amount of disk storage required by the migrated user state.

- **LoadState.exe.** The LoadState.exe tool restores the captured user state from the location where it is stored by the ScanState.exe tool.
- **UsmtUtils.exe.** The UsmtUtils.exe tool performs user state migration-related functions, such as extracting files from a compressed migration store or removing hard-link stores that cannot be otherwise deleted due to a sharing lock.

USMT includes three .xml files that configure the user state capture and restore process (MigApp.xml, MigDocs.xml, and MigUser.xml). In addition, the Config.xml file specifies files or configuration settings to exclude from the migration. You can create custom .xml files to support specialized migration needs.

Both MDT 2012 and Configuration Manager rely on USMT to migrate user state. At the appropriate time during the deployment process, the ScanState.exe and LoadState.exe command-line tools automatically run to migrate user state. You can customize the process in both deployment tools.

Volume Activation Management Tool

The Volume Activation Management Tool (VAMT) enables network you to automate and centrally manage the volume and retail-activation processes of Windows, Microsoft Office, and select other Microsoft products. The VAMT can manage volume activation using MAKs or KMS and is typically deployed in enterprise environments. The VAMT is a standard Microsoft Management Console (MMC) snap-in that requires MMC 3.0. You can install it on any computer running Windows 8, Windows 7, Windows Server 2012, or Windows Server 2008 R2.

Windows Performance Toolkit

The Windows Performance Toolkit (WPT) contains performance monitoring tools that produce in-depth performance profiles of Windows operating systems and applications. It is a powerful recording tool that creates Event Tracing for Windows (ETW) recordings. You can run the WPT from the WPT user interface or from the command line. It provides built-in profiles that you can use to select the events that are to be recorded. Alternatively, you can author custom profiles in XML. The WPT is a powerful analysis tool that combines a very flexible user interface with extensive graphing capabilities and data tables that can be pivoted and that have full text search capabilities. It allows you to explore the root cause of any identified performance issues.

Windows Assessment Toolkit

Another component in the Windows ADK is the Windows Assessment Toolkit. The Windows Assessment Toolkit helps you determine the quality of a running operating system or a set of components with regard to performance, reliability, and functionality. The toolkit includes the tools that you need to assess a local computer, review the results, diagnose problems, and determine how to make improvements. Assessments can be performed using the Windows Assessment Console or command-line tools.

Windows Assessment Services

The final component in the Windows ADK is the Windows Assessment Services component. Windows Assessment Services is a test framework used to automate running assessments that measure performance, reliability and functionality on multiple computers in a lab environment. It helps you eliminate fragmented, error-prone, expensive, pre-deployment test processes, and enables you to replace multiple steps and inconsistent tools with just one tool.

Windows ASC is the graphical user interface that interacts with Windows Assessment Services. This enables you to manage settings and assets, such as which lab computers to test, which images should be applied to those computers, and which assessments should be run on the test computers. You can use Windows ASC to monitor the progress of a running job and to view and compare the results that were produced. Additional benefits include the ability to import results into a central database for consolidated report generation.

Deployment Options

The Windows ADK is the fundamental collection of tools for configuring and deploying Windows 8. You use these tools individually or directly infrequently, however. Instead, Microsoft provides a variety of deployment options that are built on top of the Windows ADK.

MDT 2012 is one of the most popular toolsets built on top of the Windows ADK. It's more of a deployment framework. MDT 2012 helps manage deployment content in preparation for deployment, and then collects and applies deployment information through wizards at the time of deployment. MDT 2012 allows you to control the level of information required at deployment time. MDT 2012 also allows you to perform fully automated deployments that require no deployment information at the time of deployment.

MDT 2012 can be used by itself or in conjunction with Configuration Manager. While Configuration Manager is very capable of deploying Windows 8 without using MDT 2012, Microsoft recommends that you use MDT 2012 with Configuration Manager to extend its capabilities with a deployment framework based on years of real-world experience. Essentially, MDT 2012 is like having dozens of deployment experts writing custom code to support your Windows 8 deployment.

Microsoft Deployment Toolkit 2012 Update 1

MDT 2012 (Figure 5-1) helps automate the deployment of and ongoing management of Windows 8 deployment content. It leverages and automates the tools in the Windows ADK to deploy Windows 8 and applications along with it. MDT 2012 provides wizards that help in the initial creation of deployment content.

FIGURE 5-1. THE MICROSOFT DEPLOYMENT TOOLKIT 2012 UPDATE 1

MDT 2012 also reduces the effort and complexity of performing deployments. It performs highly automated deployments that allow you to control the type of information that you wish to provide at the time of deployment. It provides different deployment methods:

- **Lite Touch Installation (LTI).** LTI can perform partially and fully automated deployments for environments without Configuration Manager. This allows you to determine the deployment

configuration settings that you wish to provide prior to deployment and at the time of deployment.

- **User-Driven Installation (UDI).** UDI can perform partially and fully automated deployments for environments with Configuration Manager. This also allows you to determine the type of deployment configuration settings you wish to provide prior to deployment and at the time of deployment.
- **Zero Touch Installation (ZTI).** ZTI performs fully automated deployments for environments with Configuration Manager. This allows you to provide all the configuration settings in advance and eliminate the need for any user or deployment technician interaction at the time of deployment.

The deployment process and guidance provided by MDT 2012 are based on industry best-practice recommendations for operating system and application deployment. This helps ensure that deployments are performed efficiently and with minimal risk.

As a whole, if you're already familiar with MDT 2010, you will feel very comfortable with MDT 2012. It adds support for the Windows ADK, Windows 8, and new features like UDI. However, the basic tasks like stocking deployment shares with applications, operating systems, packages, and device drivers; creating task sequences, and running the Windows Deployment Wizard are largely the same. You can learn more about MDT 2012 on TechNet at <http://www.microsoft.com/deployment>.

System Center 2012 Configuration Manager with SP1

Just like MDT 2012, if you're familiar with operating system deployment in System Center Configuration Manager 2007, you will be comfortable with System Center 2012 Configuration Manager (Figure 5-2). The original release adds support for user device affinity by allowing you to associate a user with the computer where the operating system is deployed. You can use the Install Application task sequence step to install applications during operating system deployment. There are other enhancements of course.

FIGURE 5-2. OPERATING SYSTEM DEPLOYMENT IN CONFIGURATION MANAGER

System Center 2012 Configuration Manager Service Pack 1 (SP1) is the latest version of Configuration Manager, and it adds support for Windows 8. The following list summarizes the changes in SP (see <http://technet.microsoft.com/en-us/library/gg682108.aspx> for a complete list of changes in Configuration Manager SP1):

- Configuration Manager SP1 uses the Windows ADK instead of the Windows AIK to deploy an operating system. Before running setup, you must download and install Windows ADK on the site server and the provider computer.
- Configuration Manager SP1 modifies the default task sequences to optimize the deployment of operating systems starting with Windows 7. Additionally, they offer support for computers in the Unified Extensible Firmware Interface (UEFI) mode. Task sequences in SP1 include other enhancements for Windows 8.
- Configuration Manager SP1 changes how you create prestaged media. For example, you can specify applications, packages, and driver packages to deploy with the operating system. You can add or remove content for prestaged media.
- Configuration Manager SP1 improves support for BitLocker Drive Encryption. Use the Pre-provision

BitLocker task sequence step to encrypt the disk drive from Windows PE and only encrypt the space used by data for much faster encryption times. TPM and PIN is now available as one of the key management options for the current operating system drive in the Enable BitLocker task sequence step.

- Configuration Manager SP1 adds a handful of new task sequence variables. For example, the variable _SMSTSWTG indicates if the computer is running as a Windows To Go device.
- Configuration Manager SP1 can provision Windows To Go. You can provision the Windows To Go drive much like you provision other operating system deployments.
- Configuration Manager SP1 provides better monitoring and status for task sequence content and task sequence deployments.

As previously mentioned, Configuration Manager is more than capable of deploying Windows 8 without using MDT 2012. However, MDT 2012 adds an additional framework to Configuration Manager that helps you build a more flexible and more intelligent deployment process for your organization.

Learn more about operating system deployment with Configuration Manager on TechNet at <http://technet.microsoft.com/en-us/library/gg682018.aspx>.

Desktop Virtualization

Desktop virtualization isn't really a deployment tool as it is an alternative way to deliver desktop environments to users. It enables you to provide a work desktop to users that they can access from any device. The result is that you can more easily and more responsibly adopt Bring Your Own Device programs in your company. The topic is significant enough that it gets its own chapter in this book. See Chapter 11, "Windows 8 Virtualization," to learn more.

Windows To Go

Windows To Go is an innovative feature found in the enterprise version of Windows 8 that enables the creation of a portable Windows 8 workspace, hosted on a flash drive. By simply placing a configured bootable Windows To Go USB drive into a computer and booting to it, a user can access their personal Windows 8 desktop; regardless of the operating system that is installed on the PC. The bootable Windows To Go workspace can also use the same Windows 8 images that are used on desktops or laptops in the enterprise. This allows you to use an existing when provisioning Windows To Go.

The portability and flexibility provided by Windows To Go standardizes the same user-experience wherever users go. This allows for greater efficiency in offsite productivity and overall familiarity of Windows 8 to the user. For Example, if a person uses Windows 8 at work and other operating systems at home, placement of settings and applications can get very confusing. Windows To Go remedies this situation and many others by providing the exact same layout on any computer that a user inserts their USB drive. Windows To Go is also not as volatile as you would think an operating system booted from a USB drive would be. If the drive is suddenly disconnected, there is a 60 second window for the drive to be put back in

and resume functionality, exactly where it left off. Features like this make Windows To Go a user friendly way to unify the work and work at home environments.

Preparation and Requirements

Properly preparing for a deployment such as Windows To Go increases its overall success. There are few preliminary requirements for Windows To Go, since it is intended to seamlessly integrate with existing hardware. Aside from a few exceptions, the Windows To Go workspace operates exactly like any other Windows platform. These exceptions are:

- **Offline internal disks.** When booted into a Windows To Go workspace, internal hard disks are disabled by default. The Windows To Go workspace completely disassociates itself from the other drives in a machine. This minimizes the risk of unwanted manipulation of either device and data leakage.
- **Absence of Trusted Platform Module (TPM).** Traditionally, BitLocker is implemented using the TPM integrated hardware. Since the TPM is linked with a specific computer, it cannot be used with Windows To Go because it can be used on multiple computers. To replace TPM, for a Windows To Go workspace, a pre operating system boot password is used for security.
- **Disabled hibernation.** Hibernation has been disabled by default to maximize a workspace's versatility to move between machines. If a machine is in hibernate, a user might remove the USB media, thinking the computer is turned off.
- **Removed Windows Recovery Environment.** In a Windows To Go workspace, the Windows recovery environment is not available. In the event that a recovery is needed, re-image the drive.
- **Disabled Push Button Reset.** This feature was disabled due to the nonsensical nature of resetting to the manufacturer's standard for a computer while running Windows To Go.
- **Disabled Microsoft Store.** The Windows store uses hardware identification for licensing purposes. For this reason, the Windows Store is disabled on Windows To Go. If the Windows To Go workspaces will not be moving to multiple computers, the store can be re-enabled.
- **Absence of Multiple Activation Key (MAK) method.** The MAK activation method is not supported for Windows To Go. This is because each host PC would require a separate activation.

Preliminary Considerations

Deciding whether or not to use Windows To Go needs to be based on preliminary consideration for which scenarios Windows To Go will benefit your organization. Additionally, some great questions to ask before implementing Windows To Go are:

- How and where will data be stored and synchronized?
- Are all of the required applications compatible with Windows To Go?
- What architecture should the image be (32bit/64bit)?
- What management software is going to be used for Windows To Go?
- How will users connect to the enterprise network (VPN/DirectAccess)?

- Are the intended host machines known? If so, install the drivers for them before deployment to ensure full hardware functionality.

Windows To Go can be provisioned using standard enterprise deployment methods such as System Center 2012 Configuration Manager and the Deployment Image Servicing and Management (DISM) tool. Additional consideration should be given to the Windows To Go deployment method that works best for your organization.

Note: To provision Windows To Go, use tools provided for Windows 8. Using previous versions of deployment tools to provision Windows To Go is not supported.

Hardware Requirements

Windows To Go does not require any software to be installed on the host machine to run. However, the host machine does have to meet several basic hardware requirements. Either Windows 7 or Windows 8 certified hardware works well with Windows To Go. Table 5-1 describes the basic hardware requirements for Windows To Go.

NOTE: Windows To Go is not supported when booting from a Mac computer or Windows RT device.

TABLE 5-1. HARDWARE REQUIREMENTS FOR WINDOWS TO GO

ITEM REQUIRED	DESCRIPTION
USB PORT	Must have a USB 2.0 port or greater Note: External USB hubs are not supported, the Windows To Go USB drive must be directly inserted into the host machine.
USB BOOT	Must be capable of booting from a USB drive. Ensure that USB booting is enabled in the BIOS
RAM	2 GB or greater is required
PROCESSOR	1 Ghz or faster is required
GRAPHICS	DirectX 9 compatible device with Windows Display Driver Model (WDDM) 1.2 or greater

NOTE: USB drives must be certified for use with Windows To Go. If a USB drive is not certified, it is not supported.

In addition to the requirements listed in Table 5-1, corresponding Windows To Go architectures must be matched with the Host PC firmware type and processor architecture. Table 5-2 describes the requirements for each.

TABLE 5-2 BIOS COMPATIBILITY

HOST PC FIRMWARE	HOST PC ARCHITECTURE	COMPATABLE WINDOWS TO GO ARCHITECTURE
Legacy BIOS	32-bit	32-bit only
Legacy BIOS	64-bit	32-bit or 64-bit
UEFI BIOS	32-bit	32-bit only
UEFI BIOS	64-bit	64-bit only

Implementation Scenarios

Windows To Go is not suited for every organization and user. Choosing whether or not to provide your employees with Windows To Go should be based on your organization's needs. Some example scenarios in which using Windows To Go could benefit an organization are listed below.

- **Continuance of operations (COO).** Continuance of operations employees often require work desktop environments at home. In this scenario, you provide selected COO employees with a Windows To Go USB drive. This drive can be preconfigured with their Group Policies and be provisioned using standard provisioning tools such as Configuration Manager. For users requiring network access, Windows To Go supports virtual private network (VPN) and DirectAccess.
- **Temporary workers.** If temporary workers require specific programs or just a work environment, you could provide a Windows To Go workspace. This would allow the user to have access to company programs while not requiring company hardware. The device can then be returned at the end of the specified contract or assignment. With Windows To Go, no software installation is ever required on the host machine so it remains completely unaffected.
- **Ability to travel lighter.** This situation involves employees who frequently travel or move from site-to-site. Instead of requiring a laptop, those employees can simply take their Windows To Go USB drive and boot to it from any PC at the new location.
- **Telecommuting.** Many professionals either fully or partially telecommute. In this scenario, Windows To Go drives can be provisioned using standard tools then provided to employees. The initial boot to Windows To Go will need to be on-site in order for it to cache the employee's credentials for later access. Once on their home computer, employees can access their Windows To Go drive with or without enterprise network connectivity.
- **Free seating.** This scenario includes organizations that provide temporary offices for off-site or roaming employees. Providing a Windows To Go drive to these roaming employees allows them to maintain the same user experience at whatever site they are currently located.

Note: If DirectAccess is not enabled, employees using Windows To Go should connect to the enterprise network frequently using VPN. This will minimize the risk of the drive's deletion from Active Directory and retain its access privileges.

Management and Security

Since a Windows To Go workspace, from a user aspect, is identical to a standard Windows 8 installation, there are many security and management features available. Windows To Go provides a standard user interface regardless of which PC a user decides to use while still providing the same access management and security as a physical machine. Using advanced features found in Windows 8, that standardization can be taken a step further. An example of this is Microsoft User Experience Virtualization (UE-V) which can be used to cache user settings and implement them on physical systems as well as Windows To Go.

User State Virtualization

Windows To Go offers the same user state virtualization opportunities as a traditional installation of Windows 8. The features below describe the profile data management options for user's files and profiles when using Windows To Go:

- **Folder redirection** enables you to redirect the known path of a folder to a new location. Even though the folder is being redirected, from a user's perspective, the folder is still local. Implementing folder redirection also allows users to access their files from anywhere on the network whether on their Windows To Go drive or a local machine. For example, Windows To Go users would save to their documents folder while the path would be redirected to a file server on the enterprise network. This scenario would require DirectAccess to be enabled.
- **Offline Files** make network files available to users when DirectAccess is not configured or the enterprise network is not accessible. Once computers using the Offline Files feature are reconnected to the enterprise network, they are automatically synced with the file server.
- **User Experience Virtualization (UE-V)** allows administrators to provide an optimum user experience by saving user settings for specified programs. This can be used in conjunction with Windows To Go configured with DirectAccess.

These user state virtualization features can be easily implemented with either DirectAccess or a virtual private network (VPN). Windows To Go allows users to take advantage of these advanced Windows 8 features on any machine booting their Windows To Go drive. Consider your organization's available bandwidth and resources before implementing these advanced features. For more information, see chapter 11, "Windows 8 virtualization".

Active Directory Integration

Just like a standard Windows installation, Windows To Go will not be joined to your domain upon creation. However, Windows To Go can be easily joined to a domain one of two ways:

- **Traditional Method.** The traditional way to join a computer to the domain is through the computer properties.

- **Offline Domain Join.** Offline domain join is a process that allows Windows To Go to join a domain without contacting a domain controller. This makes it possible to join computers to a domain in locations where there is no connection to the network.

Note: For more information about offline domain join, see the article titled "Offline Domain Join (Djoin.exe) Step-by-Step Guide" at [http://technet.microsoft.com/en-us/library/offline-domain-join-djoin-step-by-step\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/offline-domain-join-djoin-step-by-step(v=WS.10).aspx).

Group Policy Management

Group Policy management of Windows To Go is nearly identical to what is available for typical machine installations of Windows 8. In addition to the Windows 8 policies, there is added functionality specifically for Windows To Go. The unique Windows To Go Group Policy settings can be found in \Computer Configuration\Administrative Templates\Windows Components\Portable Operating System\ in the Group Policy Management Editor.

A few specific policies that should be noted when considering a Windows To Go deployment are:

- **Allow hibernate (S4) when starting from a Windows To Go workspace.** Hibernation is disabled by default in Windows To Go in order to minimize data loss and user frustration. When a Windows To Go drive is put into hibernate, it must resume from hibernation on that host PC and in the same USB port. Enabling this policy turns the hibernation feature on.
- **Windows To Go Default Startup Options.** This policy automatically configures selected Windows 8 machines to boot from Windows To Go drives at startup. Enabling this policy makes USB booting #1 priority on all host PCs. This poses a potential security risk if someone wanted to boot from a USB other than Windows To Go.
- **Disallow standby sleep states (S1-S3) when starting from a Windows To Go workspace.** Standby sleep states are enabled by default in a Windows To Go workspace. Enabling this policy disables the use of these states. It is very hard to tell that a Windows To Go drive is in standby mode. It is a common mistake to pull the drive from the machine thinking that it is turned off. This mistake can cause data loss, system crashes, and ultimately a corrupt unusable drive.
- **Allow Store to install apps on Windows To Go workspaces.** The Windows Store is disabled on Windows To Go workspaces by default. This is because software obtained through it is tied to a specific host PC. If a user wanted to download and use software from the store on different machines, they would have to re-activate it with a different key every time they changed machines. This policy can be found in \Computer Configuration\Administrative Templates\Windows Components\Store\ in the Group Policy Management Editor.

Enabling BitLocker Security

Since most Windows To Go users will be using their USB drive off-premises, it is recommended to secure them using BitLocker. Enabling BitLocker security on a Windows To Go drive ensures the safety of your organization's programs, network resources, and user data in the event that the drive is lost or stolen. Unlike

BitLocker available on standard devices which provide the Trusted Platform Module (TPM), BitLocker for Windows To Go is secured with a boot password to unlock the drive and boot into Windows. The password requirements for BitLocker can be defined by your domain controller. You can encrypt a Windows To Go workspace when you create it by using the Windows To Go Creator wizard, by using Windows PowerShell, or later by using the BitLocker user interface.

Windows To Go Workspace Creation

Before creating a Windows To Go workspace, it is recommended that you see the previous sections of this chapter referring to preliminary considerations. It is simple to implement. As long as the host computer meets the hardware requirements shown in the previous section, "Hardware Requirements", little else is required.

When creating a Windows To Go workspace, an existing Windows 8 image can be used as long as the image has been generalized using the Sysprep tool and is in Windows Imaging Format (WIM). If an image does not exist, one will need to be created before a Windows To Go drive can be created. Once a WIM file has been created, a Windows To Go workspace can be provisioned two different ways:

- **Windows To Go Creator wizard.** Only available on Windows 8 Enterprise, the Windows To Go Creator wizard (Figure 5-3) is a GUI application that provisions a Windows To Go drive. The creator wizard automates most of the creation process by only prompting for a few pieces of information. To access the Windows To Go Creator wizard, simply press **Window key + W** and type **Windows To Go** in the search box.
- **PowerShell.** You can automate Windows To Go workspace creation by using Windows PowerShell. PowerShell must be run with administrative privileges in order to create a Windows to Go drive.

FIGURE 5-3. WINDOWS TO GO CREATOR WIZARD

Note: For detailed step-by-step instructions for creating a Windows To Go workspace by using either method, see <http://social.technet.microsoft.com/wiki/contents/articles/6991.windows-to-go-step-by-step.aspx>

Note: The initial boot of Windows To Go should be on a work machine. This allows the drive to join the domain, download any security policies, and enable BitLocker Security. If the drive cannot be booted first from work, an offline domain join can be executed.

Once the Windows To Go workspace has been created and configured, you are now ready to boot from the USB drive on any computer that meets the minimum hardware requirements. Enabling a computer to boot from the drive is simple and can be achieved three ways as shown below:

- **Always boot from USB.** To set the BIOS to always boot from USB, power on the computer and select the hotkey that the computer manufacturer has mapped to the BIOS. From there, navigate to the "Boot Order" or "Boot Priority" option found under the "Boot", "System Configuration", or

"Storage" tab, depending on the manufacturer. From here, enable USB booting and move it up the list to the top. Finally, save changes and exit. The machine will now boot into a USB drive by default, if one is present.

Tip: Not sure which "F" Key gets you into the BIOS Utility or Boot Menu? For a list of hotkeys by manufacturer visit <http://social.technet.microsoft.com/wiki/contents/articles/12911.tips-for-configuring-your-bios-settings-to-work-with-windows-to-go.aspx>

- **Select to boot from USB.** To enable USB booting but not prioritize it, perform the same steps as in "Always boot from USB" without the moving it up the list step. To select USB booting, upon power up, press the Boot Menu "F" Key and choose "boot from USB".
- **Set boot option in Windows 8.** Windows 8 allows users to edit Windows To Go startup options within the operating system rather than restarting the machine and entering the BIOS. To edit this option in Windows 8, press Window key + W, and search for "Windows To Go startup options". After clicking on the "Change Windows To Go startup options" Tile, click **Yes** when prompted.

Note: Prioritizing USB booting to #1 can be a potential security risk. Once you have the option set, USB drives will always have priority over the internal hard drive.

TIP: Group Policy can be used to enable Windows To Go booting on a domain level for Windows 8 machines.

Summary

MDT 2012 can help reduce the effort and complexity of performing Windows 8 deployments. MDT 2012 can also help deploy applications that are specifically designed to be deployed as though they were part of the operating system image.

MDT 2012 helps reduce deployment risk by providing highly automated deployment processes and wizard-driven user interfaces. The highly automated processes are based on best-practice recommendations and help eliminate any configuration errors that might be introduced through manual configuration methods. The wizard-driven user interfaces help you know exactly the right information you need to provide to successfully complete Windows 8 and corresponding application deployment.

MDT 2012 can be used by organizations of any size. For organizations without Configuration Manager, the LTI deployment method allows you to leverage all the benefits of MDT 2012. For organizations with Configuration Manager, the UDI and ZTI deployment methods allow you to leverage your existing investment and streamline Windows 8 and application deployment.

Microsoft offers exciting alternatives to traditional operating system deployment to physical PCs. These alternatives support a BYOD programs and an increasingly mobile workforce. First, Microsoft Desktop

Virtualization helps you more easily deploy a virtual desktop infrastructure (VDI) to give users access to a Windows workspace from almost any device and any location. Second, Windows To Go provides users a portable Windows workspace that they can use with multiple PCs.

Delivering Windows apps

Windows apps are an integrated application experience for Windows 8 that are available from the Windows Store. In addition, organizations can make their own custom line-of-business (LOB) apps available to users inside their organization. This process is called sideloading.

In addition to creating and deploying apps, an IT department can also control the use of apps using Group Policy. This applies to sideloaded apps and any other apps, including those that are built-in to Windows 8. For example, an organization may choose to remove or not allow the Weather app to run.

This chapter looks at the delivery and control of Windows apps, whether through sideloading or controlled through Group Policy.

A look at Windows apps

Windows apps extend the "app" experience to Windows 8. This experience has become popular over the last several years with the increased use of mobile computing with seamless application delivery and installation. Windows apps are built using Microsoft Visual Studio and are delivered through the Windows Store, in much the same way that other platforms have their own application delivery stores.

Windows apps have certain features and characteristics that make them distinct from traditional applications. Windows apps:

- May be launched primarily through an application tile, which can update dynamically.
- May be placed in the background and communicate with other apps.
- Exists through a full-screen, chromeless interface.
- Can be viewed and used in multiple display types and views.
- Support touch, pen input, and gestures as some of the primary means of user interaction.

Windows apps display in the Windows 8 user interface (UI) shown in Figure 6-1.

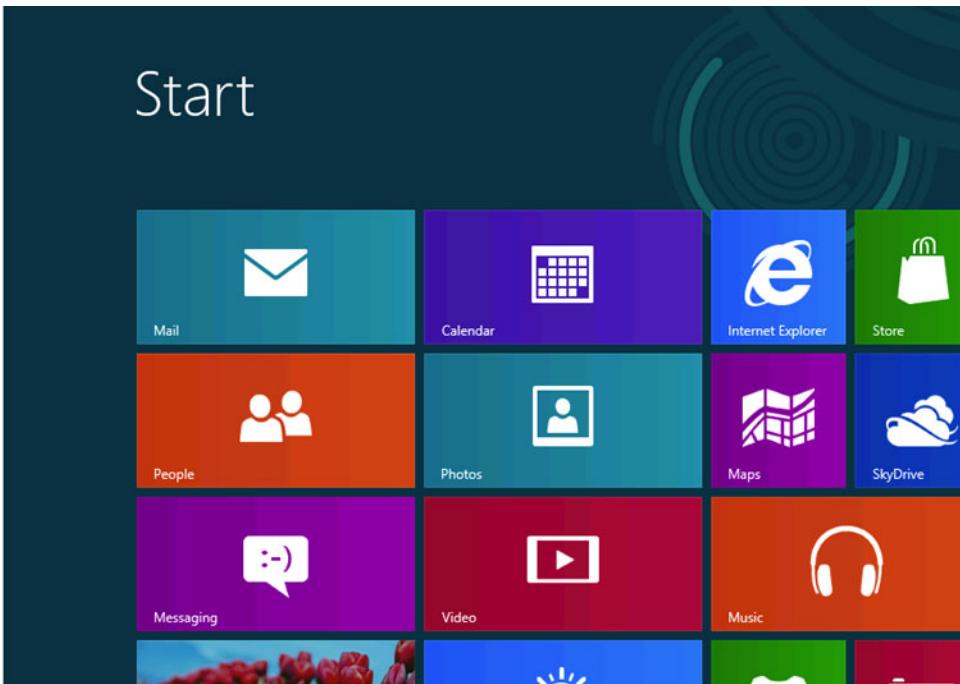


FIGURE 6-1 The Windows 8 Start UI with tiled applications.

As described in the next section, Windows apps are built using Visual Studio 2012. Apps can be built using several programming languages but all use the same Windows Runtime Application Programming Interface (API) to access the standard Windows app library and other application functions.

Apps, more formally known as App Packages (with the extension .appx), can be distributed within an organization or made available through the Windows Store. Distributing through the Windows Store has its own set of rules, as described later in this chapter. Once distributed in the Windows Store, the app is available to the public. Apps distributed within an enterprise don't need to be certified by Microsoft but do need to be signed with a trusted certificate.

Windows app lifecycle

Apps have a specific lifecycle, from the time they are removed to their removal. During an app's lifecycle, it can go through any of the following stages:

- App launch
- App activation
- App suspend
- App resume
- App close
- App crash

Additionally, there are two other special states: App Visibility and App Removal.

MORE INFO You can find more information on the app lifecycle at <http://msdn.microsoft.com/library/windows/apps/hh464925.aspx>.

Building a Windows app

Any edition of Visual Studio can be used to build apps for Windows. Though most organizations will use the Professional, Premium, or Ultimate version of Visual Studio, the Express edition for Windows also includes the necessary Software Development Kit (SDK) for developing Windows apps.

When an App is built, it becomes an App Package. The App Package contains the files for the App along with the package manifest. The package manifest contains information about the App, including how it interacts with the computer or device, what resources it needs, and so on.

Organizations can continue to use their language of choice for developing Windows apps. For example, an organization standardized around Visual C# development with the requisite in-house expertise can continue to use Visual C# for Windows App development. One of the most powerful features of Windows apps is that they can be built using several languages:

- JavaScript
- Visual Basic
- Visual C#
- Visual C++

Among these languages, Visual Basic, Visual C#, and Visual C++ are traditional client-side languages that can be used to build server-side web applications. However, the addition of JavaScript is noteworthy for Windows app development. The inclusion of JavaScript in the available languages for Windows app development means that organizations with expertise in HTML, CSS, and JavaScript can build fully functional Windows apps that have the same capabilities as apps developed in the other languages.

Visual Studio includes five templates customized for each of the available Windows App development languages. The templates help with the development process and show common design patterns and layouts for Windows apps. Some of the templates are shown in Figure 6-2.

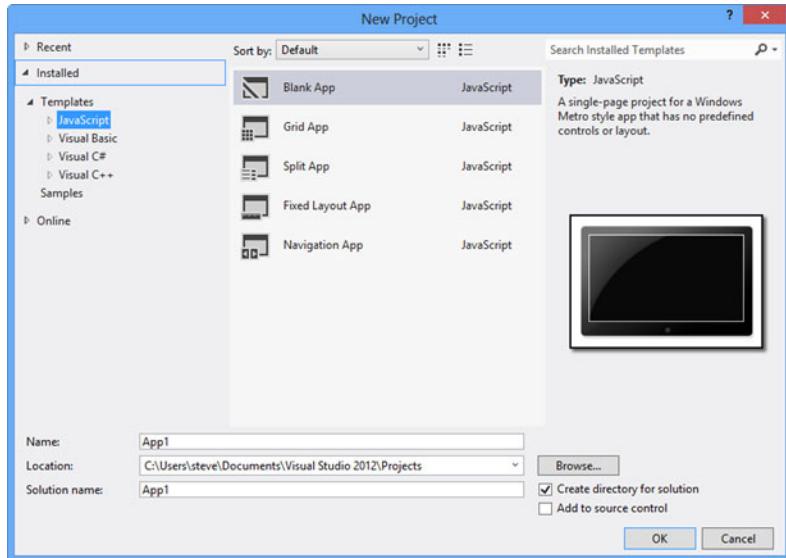


FIGURE 6-2 App templates in Visual Studio 2012 Express for Windows.

The five templates provide a good sampling of the design patterns needed for many types of apps. The type of information and user interaction expected for the app drives the choice of template. For example, an app that needs to display more than one item might choose a Grid App template, such as the one shown in Figure 6-3.

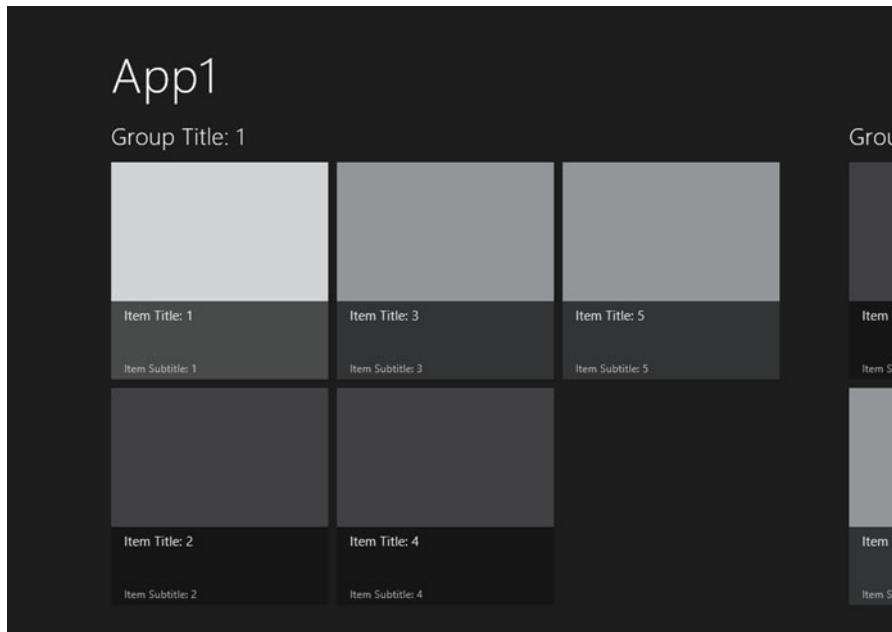


FIGURE 6-3 A Grid App template style.

An app that needs to enable drill-down for detailed information might choose a Split App template, such as the one shown in Figure 6-4.

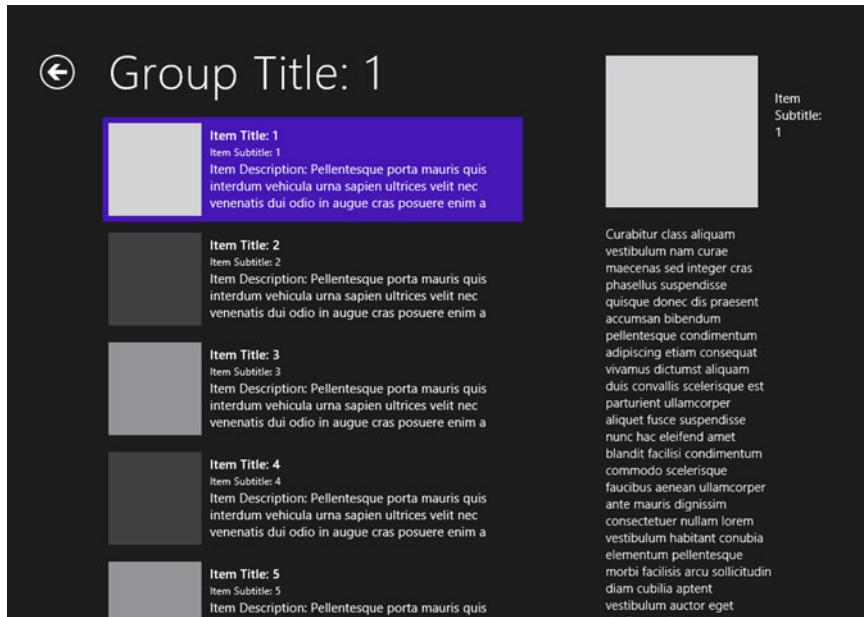


FIGURE 6-4 A Split App in Windows 8.

If one of the available templates isn't appropriate, the developer can use Blend to design the layout for the app.

Using Visual Studio to build a Windows app

This section demonstrates how easy it is to build a Windows App. The demonstration shown here will use Visual Studio 2012 Express edition for Windows to build an App. This example builds a simple app that shows a list of the files inside of the Documents library on the computer and enables the user to select a file.

The first step in building a Windows app is to choose a programming language and an appropriate template. We'll use JavaScript with the Blank App template for this example. This is shown in Figure 6-5.

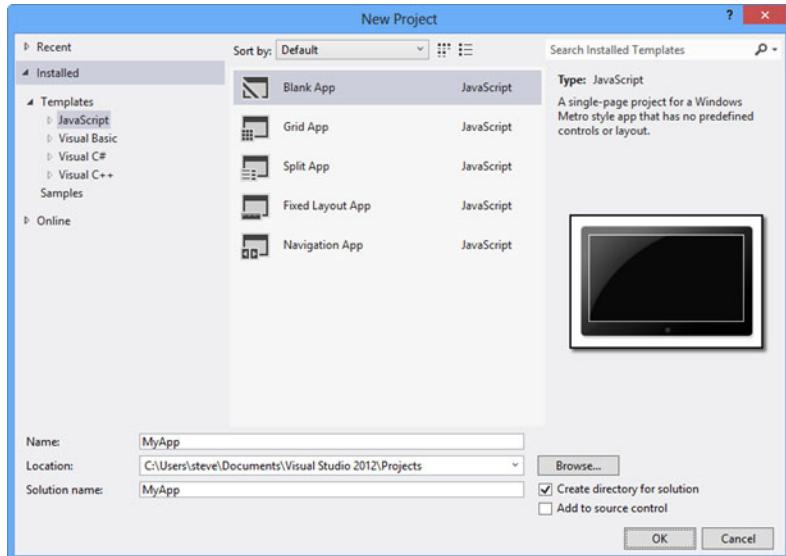


FIGURE 6-5 Beginning the app development process by choosing a template.

Once a template is chosen, Visual Studio opens the code for the chosen template. In this case, the code is shown in Figure 6-6.

The screenshot shows the Microsoft Visual Studio Express 2012 RC for Windows 8 interface. The main window has a title bar 'MyApp - Microsoft Visual Studio Express 2012 RC for Windows 8'. The menu bar includes FILE, EDIT, VIEW, PROJECT, BUILD, DEBUG, TEAM, TOOLS, STORE, TEST, WINDOW, and HELP. Below the menu is a toolbar with various icons. The code editor window on the left contains 'default.js' with the following code:

```
// For an introduction to the Blank template, see the following documentation:  
// http://go.microsoft.com/fwlink/?LinkId=232509  
function () {  
    "use strict";  
  
    var app = WinJS.Application;  
    var activation = Windows.ApplicationModel.Activation;  
    WinJS.strictProcessing();  
  
    app.onactivated = function (args) {  
        if (args.detail.kind === activation.ActivationKind.launch) {  
            if (args.detail.previousExecutionState !== activation.ApplicationExecutionState.Todo)  
                // TODO: This application has been newly launched. Initialize  
                // your application here.  
            } else {  
                // TODO: This application has been reactivated from suspension.  
                // Restore application state here.  
            }  
            args.setPromise(WinJS.UI.processAll());  
        }  
    };  
  
    app.oncheckpoint = function (args) {  
    };  
};
```

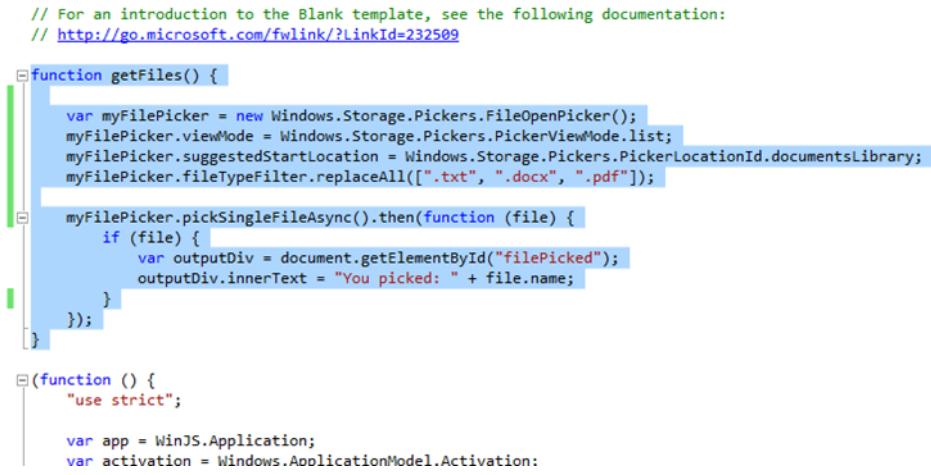
The Solution Explorer window on the right shows a single project 'MyApp' with files: References, css, images, js, default.html, MyApp.TemporaryKey.pfx, and package.appxmanifest. The Properties window is also visible on the right. The status bar at the bottom shows 'Creating project 'MyApp'... project creation successful.' and other status indicators like 'Ln 1', 'Col 1', 'Ch 1', and 'INS'.

FIGURE 6-6 Beginning code for building a Windows app with the Blank App template.

Visual Studio takes care of all of the behind-the-scenes setup and configuration for the app based on the chosen template. This means that you could compile and run the project as-is and it would display. In the case of the Blank App template, a blank screen with a simple "Content goes here" note is displayed.

Creating an app using one of the templates requires using the helper functions (created automatically by the template), and then customizing and adding to them to produce the app. In this example, we'll add a single function to access some built-in functions that create a File Picker.

The code gets added to default.js, though it's likely in a real-world scenario you'd create one or more separate JavaScript files and include those in your project. The code (highlighted) and its position in default.js is shown in Figure 6-7.



```
// For an introduction to the Blank template, see the following documentation:  
// http://go.microsoft.com/fwlink/?LinkId=232509  
  
function getFiles() {  
    var myFilePicker = new Windows.Storage.Pickers.FileOpenPicker();  
    myFilePicker.viewMode = Windows.Storage.Pickers.PickerViewMode.list;  
    myFilePicker.suggestedStartLocation = Windows.Storage.Pickers.PickerLocationId.documentsLibrary;  
    myFilePicker.fileTypeFilter.replaceAll([".txt", ".docx", ".pdf"]);  
  
    myFilePicker.pickSingleFileAsync().then(function (file) {  
        if (file) {  
            var outputDiv = document.getElementById("filePicked");  
            outputDiv.innerText = "You picked: " + file.name;  
        }  
    });  
}  
  
(function () {  
    "use strict";  
  
    var app = WinJS.Application;  
    var activation = Windows.ApplicationModel.Activation:
```

FIGURE 6-7 Adding a function to create a file listing.

With that code in place, the next area of customization needed is within the HTML file. The Blank App template includes a default HTML file. The file, aptly titled default.html, contains basic HTML and also the links to include CSS and JavaScript for the app. This file is shown when the app is loaded, though this can be changed to start with any file that is appropriate for your app.

For the example here, we'll customize default.html for our needs. Specifically, we'll add some HTML, JavaScript, and also some CSS to the file. Like the JavaScript example, in a real-world scenario where you're building a more complex app, it's likely that the CSS would be in a separate file and that the JavaScript would as well.

The bottom portion of default.html is shown in Figure 6-8, with the new items highlighted (the code above this in default.html is not changed).

```

<script src="/js/default.js"></script>
<style type="text/css">
  div {
    font-size: 1.5em;
    margin-left: 50px;
  }
  p {
    font-size: 1.5em;
    margin-left: 50px;
    border: 2px solid white;
    display: inline;
    padding: 5px;
  }
</style>
</head>
<body>
  <h1>My App!</h1>
  <br />
  <br />
  <p id="getList">Get Files List</p>
  <br />
  <br />
  <div id="filePicked"></div>
  <script type="text/javascript">
    var listH1 = document.getElementById("getList");
    getList.addEventListener("click", getFiles, false);
  </script>
</body>
</html>

```

FIGURE 6-8 Changing default.HTML for the App.

With default.html saved, the app can be run, typically by pressing F5. The app's splash screen is shown and then the app is loaded. The output of the initial screen is shown in Figure 6-9.

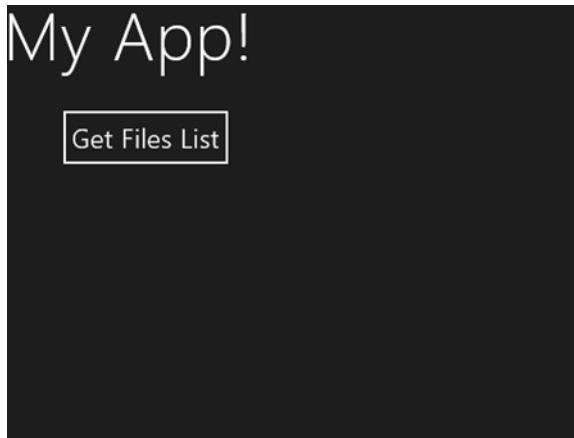


FIGURE 6-9 The default screen of the App.

Clicking or tapping the "Get Files List" button reveals the File Picker screen, shown in Figure 6-10.

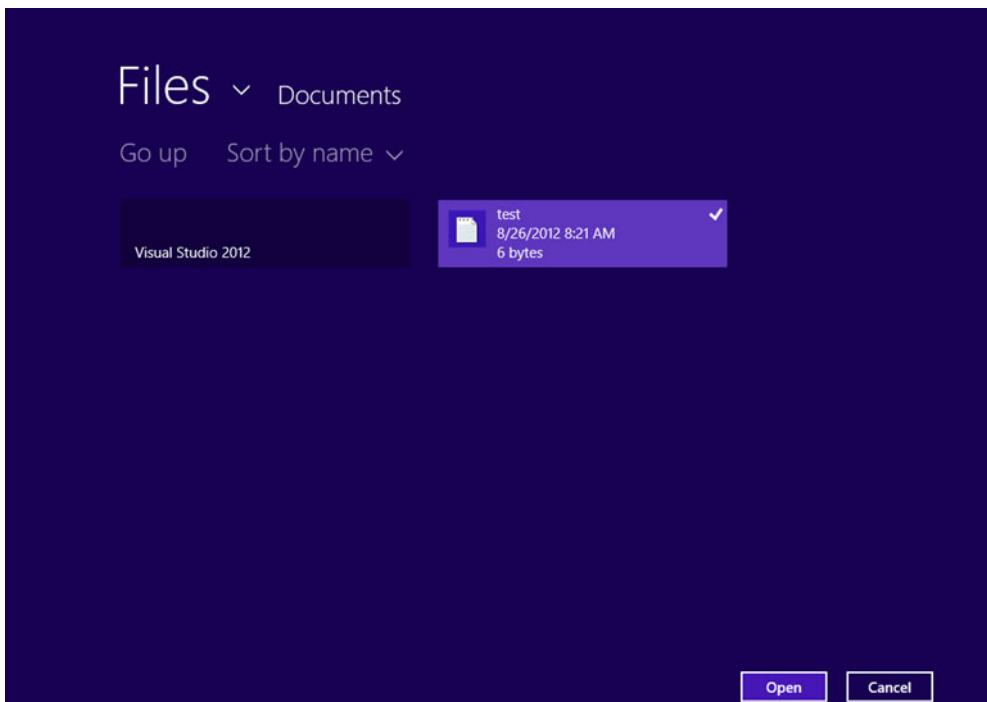


FIGURE 6-10 Choosing a file.

The File Picker screen is built and its interface is set up primarily by the built-in functions available as part of the Windows app library. This provides a consistent interface for the user when choosing files on the Windows 8 platform. Once a file has been chosen it receives a checkmark (like the one shown in Figure 6-10). Clicking or tapping Open then hands processing to your app, where you can perform the appropriate action for the file. In this case, we merely output the name of the file back to the original screen, as shown in Figure 6-11.

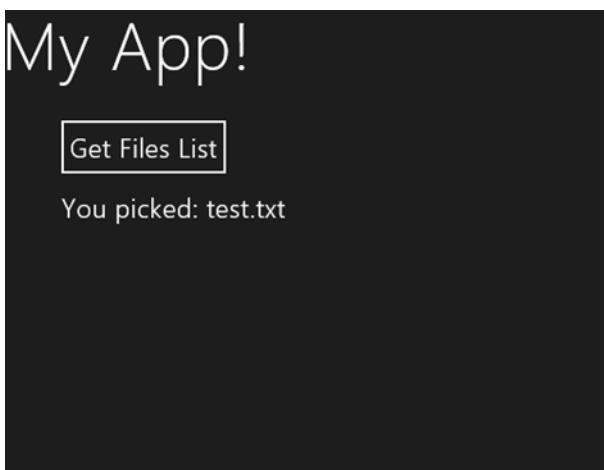


FIGURE 6-11 The file has been chosen in the App.

This demonstration shows how easy it is to create a Windows app. In just a few lines of JavaScript, HTML, and CSS, an app was created to choose files from the Documents library of a computer.

Once an app is created, it needs to be distributed. App distribution is accomplished either by making the app available in the Windows Store or by loading it for internal-use only through a process called sideloading. Both of these distribution methods are the focus of the next two sections.

Distributing in the Windows Store

Distributing an app through the Windows Store involves several steps, including creating a developer account, accepting various terms of service agreements, submitting the app for approval, and setting its terms, among other things.

As described in the "Windows 8 app certification requirements" (<http://msdn.microsoft.com/library/windows/apps/hh694083.aspx>) Microsoft has several requirements for Windows apps:

- The app must provide value.
- The app must provide more functionality than a simple website.
- The app must behave predictably.
- The app must adhere to privacy and security practices.
- The app's content and subject matter must be appropriate for many audiences.
- The app must be identified easily with a unique name and other information.

MORE INFO See <http://msdn.microsoft.com/library/windows/apps/hh868181.aspx> for more information on the requirements for Windows app developers.

The certification process

The certification process to distribute an app through the Windows Store is a multistep process. In the first step of the process, the app package is uploaded to Microsoft where it's checked for compliance with various app certification requirements.

Among the tests that Microsoft performs are:

13. Security tests, which are fairly basic malware-type scans.
14. Technical compliance tests. The Windows App Certification Kit is used to test the app for compliance. The Windows App Certification Kit can also be used by the developer prior to submission in order to perform the same tests and help ensure a successful test when performed by Microsoft.
15. Content compliance tests. The final test prior to release, the content compliance test is a manual process performed by someone at Microsoft.

When an app is approved, Microsoft performs digital signing of the app to prevent tampering, and then publishes the app to the Windows Store. However, you can set the release date and other aspects of the app, as described in the next section.

MORE INFO See <http://msdn.microsoft.com/library/windows/apps/hh923026.aspx> for more information on the certification process and see <http://msdn.microsoft.com/library/windows/apps/hh694062.aspx> for an App submission checklist that can be helpful when preparing an App for submission.

The app purchase experience

When potential customers find your app through the Windows Store, it's your chance to entice them to install or purchase your app. You do this by setting up a page on the Windows Store for your app. Your app's page contains at least one screenshot (though more are encouraged) and other details about your app, such as its description, purchase price, rating, and other details pertinent for the potential customer to know.

You choose the pricing model and structure for app distribution. You can offer the app for free, provide a time-limited trial, a feature-limited trial, or set a price for the app that must be paid prior to download. You can also set up in-app purchases to sell additional features to customers. A frequent model for apps is ad-supported, whereby the app is offered for free but then advertisements are displayed within the app. You can use any ad platform that meets Microsoft's certification requirements—which offers great flexibility to obtain the highest revenue for an ad-supported app.

MORE INFO See <http://msdn.microsoft.com/library/windows/apps/jj193596.aspx> for more information on marketing apps, including information specific to the purchase experience.

Distributing within an Enterprise

Distributing an app within an enterprise requires the Enterprise edition of Windows 8. As you might expect, the process for distributing within an enterprise is different than distributing through the Windows Store. A typical scenario would have a LOB app developed and then automatically pushed out to computers within the organization. Aside from the edition of Windows 8 being used, there are three primary requirements for sideloading apps:

- The target computer must be joined to the domain.
- Group Policy must be set to "Allow all trusted apps to install."
- The app must be signed by a Certificate Authority (CA) that is trusted by the target computer.

The Group Policy setting is found within the Windows Components\App Package Deployment hierarchy, as shown in Figure 6-12.

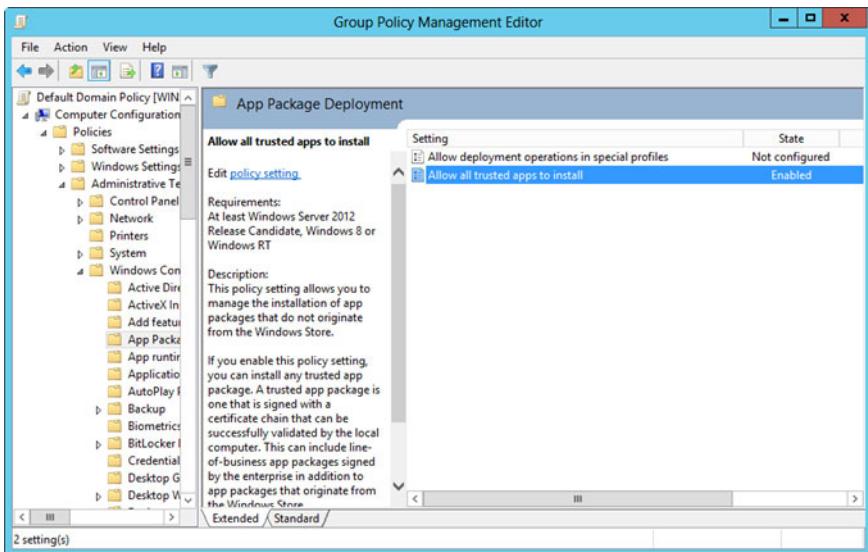


FIGURE 6-12 Configuring the Allow all trusted apps to install setting in Group Policy.

NOTE You can also deploy a sideloading product key instead of having the computer joined to the domain, though doing so is beyond the scope of this chapter. See <http://msdn.microsoft.com/library/windows/apps/hh975356.aspx> and <http://technet.microsoft.com/library/hh852635.aspx> for more information.

Sideload an app

To create an app package for distribution through sideloading, you must run the Windows App Certification Kit. The Windows App Certification Kit is part of the Windows 8 Software Development Kit (SDK) but is also included with Visual Studio 2012. For example, in the Express edition of Visual Studio 2012, selecting Create App Package from the Store menu starts the Create App Package wizard.

The first step of the wizard is where you choose whether or not the package will be distributed through the Windows Store. Selecting No, as shown in Figure 6-13, displays the requirements and limitations for this type of distribution.

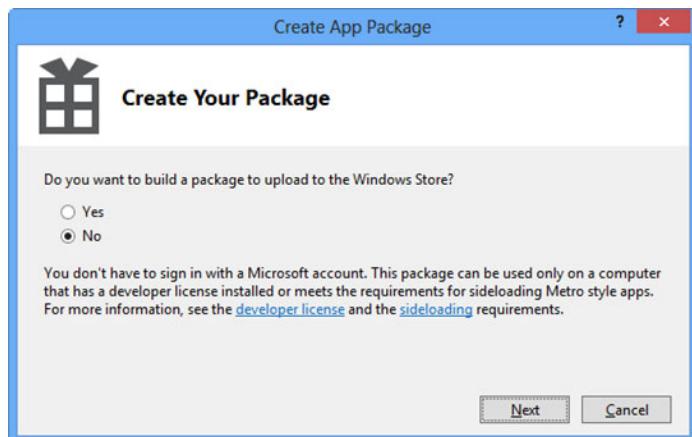


FIGURE 6-13 Creating an App Package in Visual Studio.

The package settings are configured next, as shown in Figure 6-14.

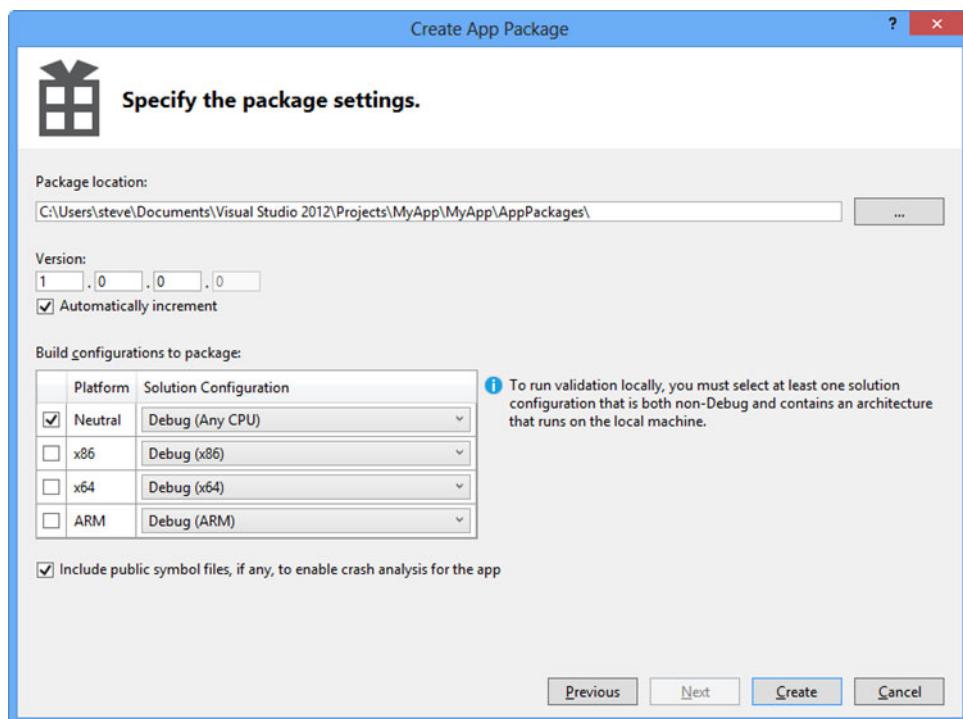


FIGURE 6-14 Configuring package settings.

The next phase begins the Windows App Certification Kit, shown in Figure 6-15.

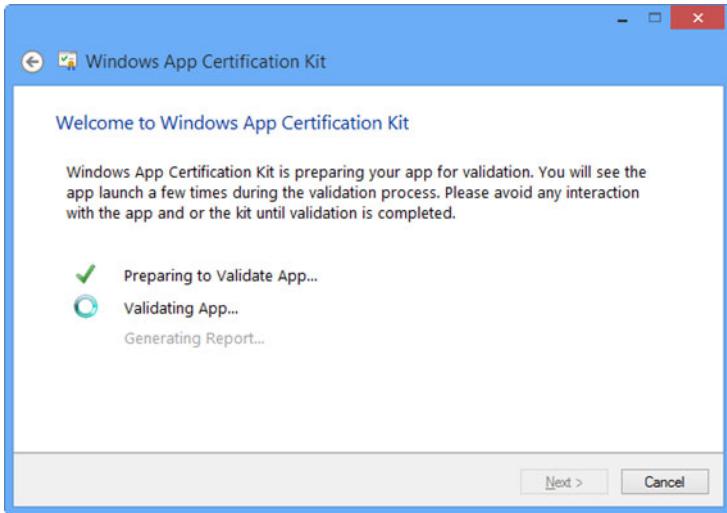


FIGURE 6-15 Running the Windows App Certification Kit.

The Windows App Certification Kit will run various tests and then display the results, as shown in Figure 6-16.

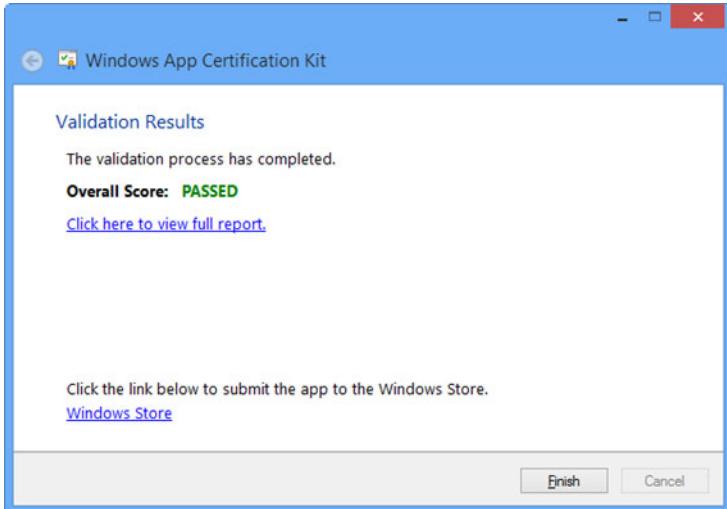


FIGURE 6-16 Results of the Windows App Certification Kit.

MORE INFO See <http://msdn.microsoft.com/library/windows/apps/hh694081.aspx> for more information on the Windows App Certification Kit.

Once it's created, the app packaging process creates a file with a .appx file extension, typically located in the AppPackages folder within the Visual Studio hierarchy in the Documents library. The app package also

contains dependencies, if there are any, for the app. For example, Figure 6-17 shows the hierarchy created for the test app created earlier in this chapter.

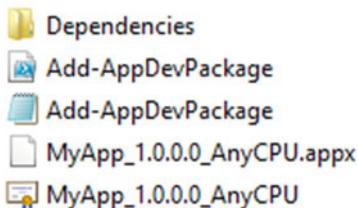


FIGURE 6-17 The app hierarchy created for an App ready for distribution.

Assuming that the certificate is installed and trusted on the target computer, and that Group Policy has been set accordingly, the app package can be installed using the add-appxpackage PowerShell command, as shown in this example, which would install the app created earlier in the chapter:

```
add-appxpackage .\MyApp_1.0.0.0_AnyCPU.appx -DependencyPath .\Dependencies\Microsoft.WinJS.1.0.RC.appx
```

The command would be run from the local computer on which the App is being installed, therefore it would be expected to be scripted in an enterprise scenario.

MORE INFO See <http://technet.microsoft.com/library/hh856045.aspx> for a listing of all of the related installation cmdlets in PowerShell for Windows apps.

Aside from this process, up to 24 apps can also be provisioned within a Windows image so that they're deployed right with the image when a new computer is set up. The Deployment Image Servicing and Management (DISM) tool has been updated to enable this feature. See <http://technet.microsoft.com/library/hh852635.aspx> for more information.

Managing Windows apps

Certain aspects of Windows apps can be managed through Group Policy. The previous section detailed the Group Policy setting to enable LOB Apps to be installed. Other settings are configured using AppLocker.

NOTE This chapter assumes that you're familiar with AppLocker and therefore doesn't give an overview of its capabilities. For more information on AppLocker, see <http://technet.microsoft.com/library/hh831440.aspx>.

AppLocker is managed through Group Policy Management Editor, as shown in Figure 6-18.

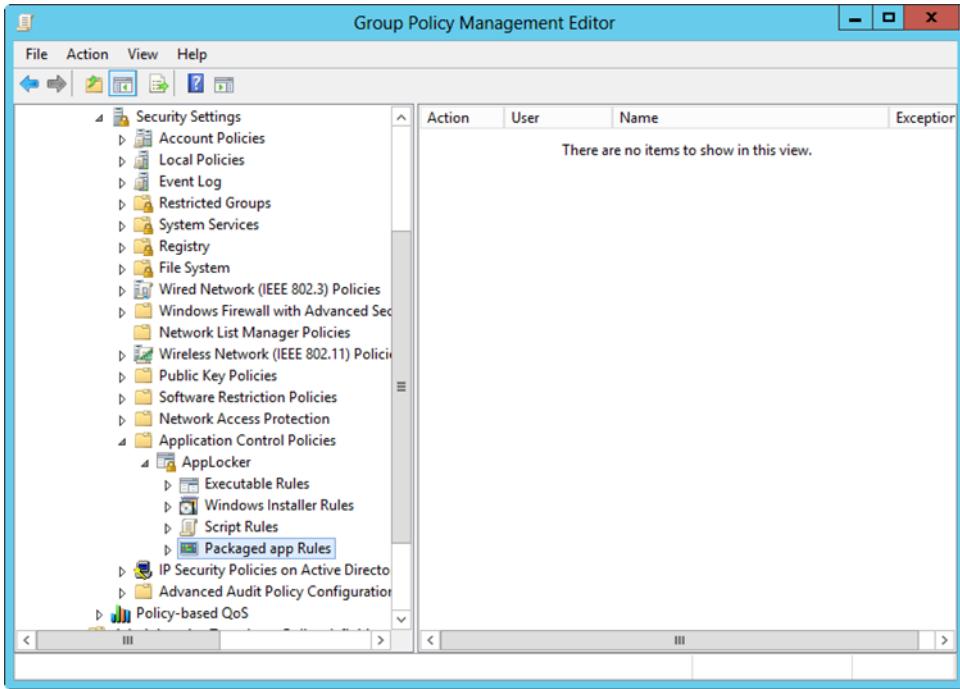


FIGURE 6-18 AppLocker managed through Group Policy Management Editor.

Creating the rules for Windows apps involves configuring rules within the "Packaged app Rules" section. You can either configure rules manually, use the Automatically Generate Rules option, or Create Default Rules from the context menu. Choosing to Create Default Rules automatically generates a rule to allow everyone to run all signed apps, as shown in Figure 6-19.

Action	User	Name	Exception
<input checked="" type="checkbox"/> Allow	Everyone	(Default Rule) All signed packaged apps	

FIGURE 6-19 A default rule to allow everyone to run signed apps.

However, a default rule to allow everyone to run all signed packaged apps may not be a likely (or very secure) policy for most organizations. Therefore, you can change this policy to Deny within its Properties dialog, as shown in Figure 6-20.

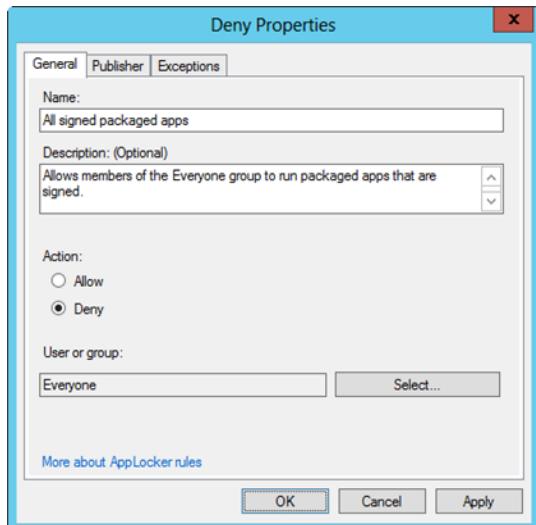


FIGURE 6-20 Changing the default rule to Deny.

Once the rule has been changed to a default Deny policy, you can then add exceptions for apps that will be allowed to run. This is accomplished through the Exceptions tab. Within the Exceptions tab, shown in Figure 6-21, you can manage the current exceptions.

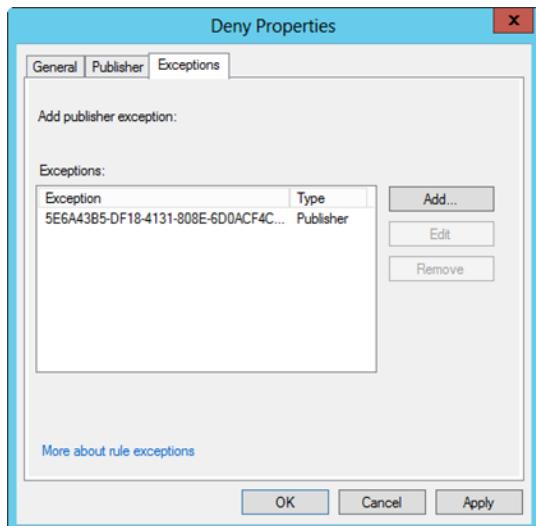


FIGURE 6-21 Managing app exceptions.

Adding an exception is accomplished by clicking Add, which reveals the Add Exception dialog. Figure 6-22 shows the Add Exception dialog used to configure an exception for the app developed earlier in this chapter.

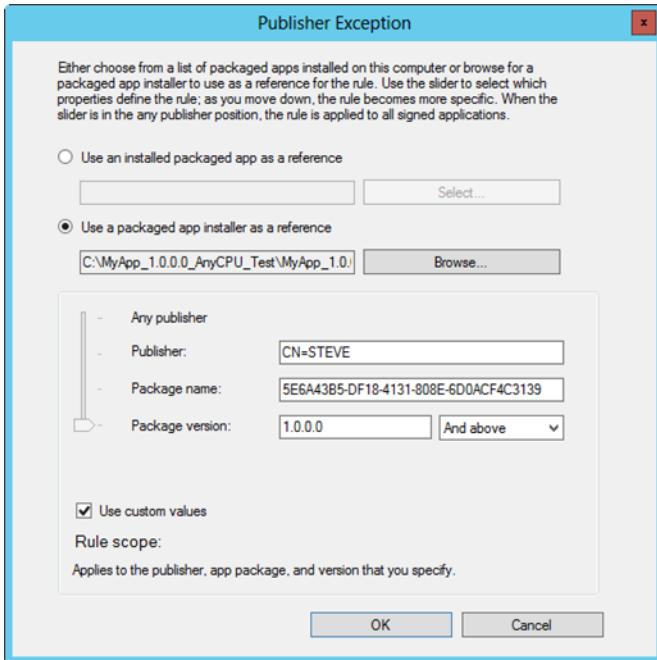


FIGURE 6-22 Configuring an exception for an app.

In addition to configuring exceptions for individual apps using their app package, you can also choose to add exceptions using an installed package. In order for this to work, the app has to be installed on the computer from which you're using AppLocker. In the case of Figure 6-23, AppLocker was run from a Windows 8 Enterprise computer, therefore exceptions can be granted for any of the apps installed there.

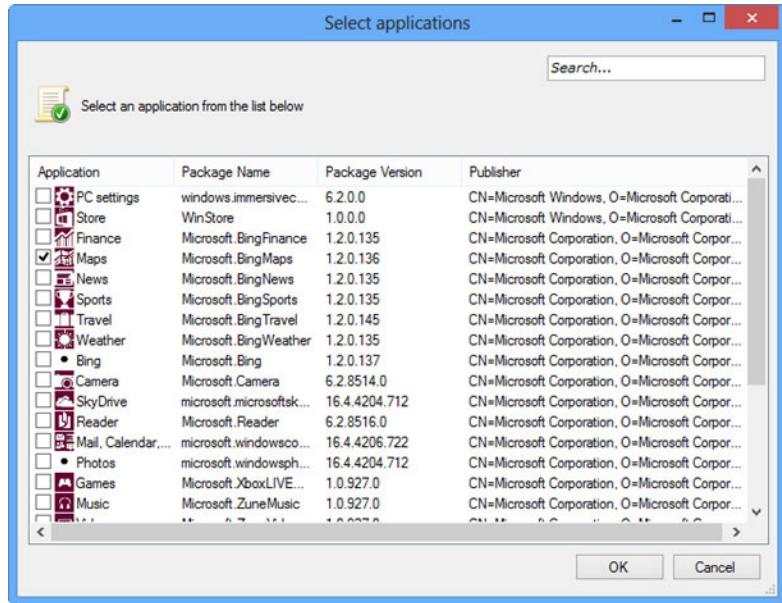


FIGURE 6-23 Configuring an exception using installed Apps in Windows 8.

The enterprise scenario here is to configure exceptions for apps that are allowed, while disallowing apps that an organization doesn't want its users to run. It's worth noting that exceptions can be configured based on Active Directory group membership, so certain groups could be allowed to run the Finance or Travel app.

Summary

Windows 8 app development reflects the importance of the new UI in Windows 8 and the importance of the app experience for tablet and mobile computing. Windows 8 apps are developed using Visual Studio, along with the Windows 8 App SDK. You can build apps using several programming languages, which enables organizations to leverage in-house expertise for app building. Visual Studio includes several templates to help speed up the application development process.

Once built, apps can be distributed to the public through the Windows Store or within the organization. When distributed within the organization, the process of installing apps on computers is called sideloading. There are a few requirements for sideloading.

This chapter demonstrated the process of building an app and showed the overall process for sideloading. In addition to sideloading apps, another common task for IT staff will be controlling how apps are run. This is accomplished using AppLocker. Exceptions can be set for individual apps or based on installed apps.

Windows 8 recovery

Microsoft Windows 8 features greatly enhanced recovery options for users and IT professionals alike. There are options to refresh and reset the PC, and there are advanced options, down to the command-line level, as well. Windows 8 features its own Recovery Environment that can be customized for your organization, and the Diagnostic and Recovery Tool (DaRT) has been updated for this release.

This chapter examines recovery for Windows 8, including an overview of the recovery options, the advanced recovery boot options startup menus, customization of the Windows RE, and a look at DaRT.

The Windows Recovery Environment

Windows recovery options have evolved throughout the history of the operating system. In previous versions of Windows, you could access Safe Mode and other recovery options by pressing F8 on the keyboard prior to the operating system boot process. However, due to the ultra-fast boot of Windows 8, accessing that console would be difficult. Windows 8 implements a Recovery Environment (Windows RE) that provides the tools necessary to recover a Windows 8 computer.

The Windows RE is shown automatically if Windows detects a problem with booting the computer (after two successive failed boots). This can be triggered for various reasons, not the least of which is the user powering the computer off during boot. Therefore, the user may end up in the Windows RE even though there's no real problem with the operating system. The following four scenarios invoke the Windows RE:

- A BitLocker error
- Two successive failed boots of Windows
- Two successive unexpected shutdowns or crashes within two minutes of boot
- A Secure Boot error

When the Windows RE is invoked through this process, an automatic repair is attempted. In the event that the Windows RE isn't available on the user's computer a Windows RE CD or DVD can be used to begin recovery.

Another way to access Windows RE is by pressing (and holding) the Shift key when shutting down or restarting the computer. By doing so, Windows automatically boots into the Boot Options menu of Windows RE, shown in Figure 7-1.

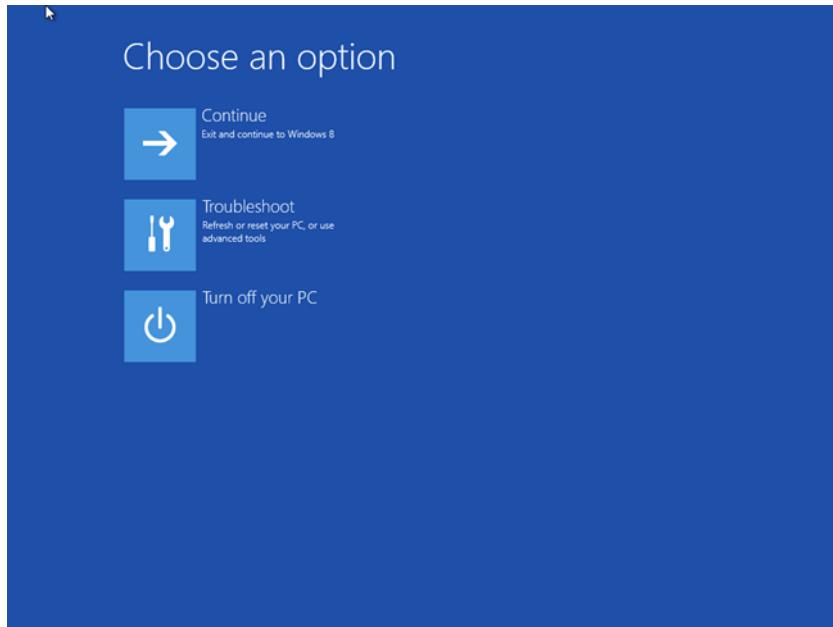


FIGURE 7-1 The Boot Options menu in Windows 8.

TIP Another method for entering the Windows RE is using the command "shutdown /r /o" from a command prompt.

On a computer without Universal Extensible Firmware Interface (UEFI), the Boot Options menu provides three options: Continue, Troubleshoot, and Turn off your PC, as shown in Figure 7-1. On a UEFI-based computer, two additional options are shown: Use a device and Access firmware. The Boot Options menu may also display a Tile to enable the choice of another operating system if multiple operating systems are installed on the computer.

In the Boot Options menu, the Continue Tile enables the user to simply continue booting into Windows 8 in case the screen is displayed when there's not really a problem. The Troubleshoot Tile opens the Troubleshoot screen, which displays three options, shown in Figure 7-2:

- Refresh your PC
- Reset your PC
- Advanced options

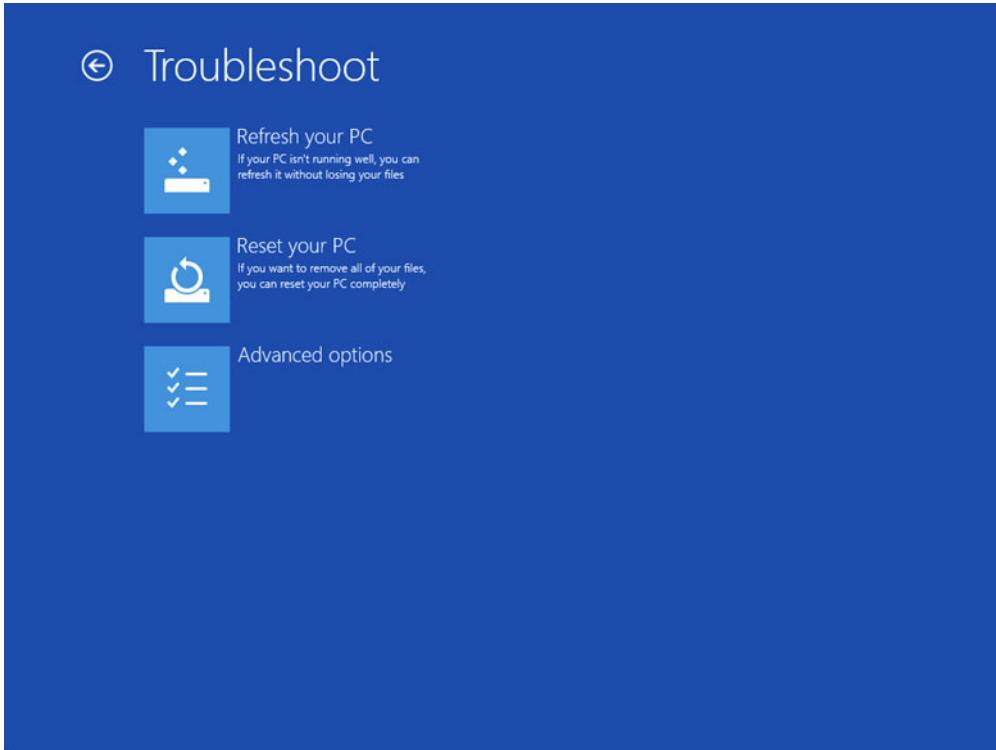


FIGURE 7-2 The Troubleshoot options as part of Windows 8.

The Refresh your PC and Reset your PC options will be discussed later in this chapter.

MORE INFO See <http://technet.microsoft.com/en-us/library/hh825173.aspx> for an overview of the Windows RE.

Advanced options

In the Windows RE, the Advanced options Tile reveals several more ways to repair and troubleshoot a computer, as described in Table 7-1. These options should look familiar to those who have used previous Windows recovery tools.

Table 7-1 Advanced Options for Recovery

OPTION	DESCRIPTION
System Restore	Restore a computer to a previous state. A Restore Point needs to have been created for this option to work.
System Image Recovery	Replaces everything on the computer with a system image.

Automatic Repair	Windows will attempt to diagnose and correct common boot problems.
Command Prompt	Enables you to use a command prompt.
Startup Settings	Changes the boot process so that you can alter other options.

Automatic Repair is the method used when Windows RE is automatically invoked. Automatic Repair can also be invoked manually through this screen. System Image Recovery requires an image from an external device.

MORE INFO See <http://technet.microsoft.com/en-us/library/hh824837> for more information on Automatic Repair and System Image Recovery.

The Startup Settings option displays several additional items that can be selected to help troubleshoot or correct a problem. This includes items like:

- Safe Mode (including with Networking and Command Prompt)
- Debugging
- Low-resolution video
- Boot logging
- Disabling driver signature enforcement, early-launch anti-malware protection, and automatic restart on failure.

The Startup Settings screen is shown in Figure 7-3.

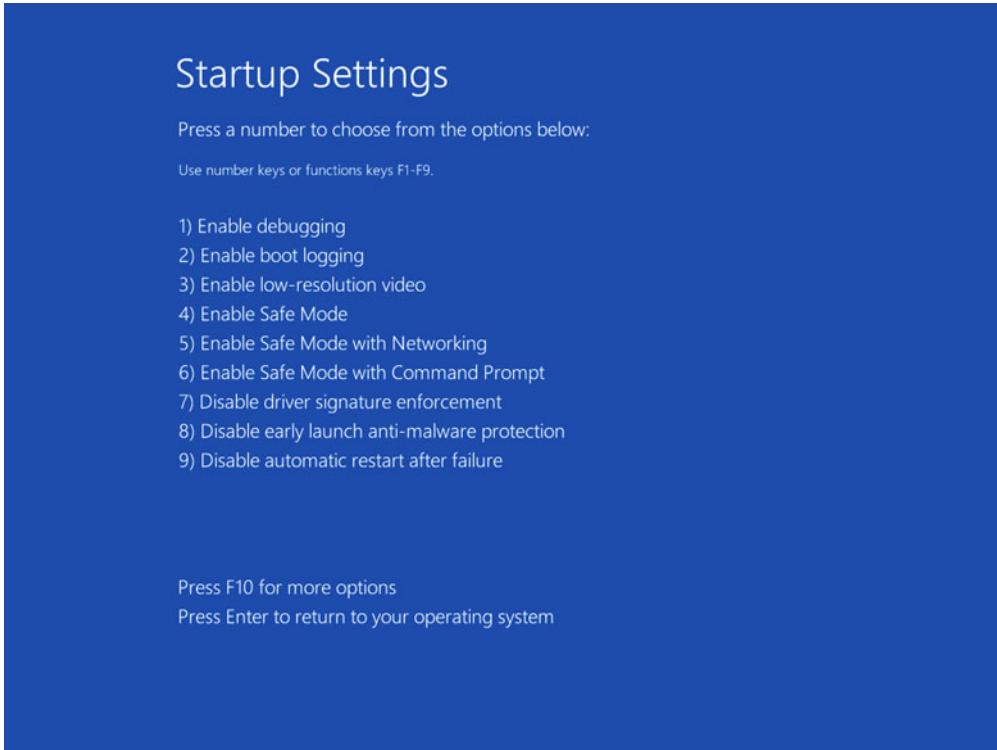


FIGURE 7-3 Startup Settings in Windows 8.

There is also a command-line tool, **REAgentC.exe**, that enables the administrator to perform recovery operations. See <http://technet.microsoft.com/library/hh825204> for more information on this tool.

Refresh and reset

Within the Troubleshoot screen (shown in Figure 7-2) there are two options for an IT pro looking to recover or restore a system quickly: Refresh your PC and Reset your PC. The option you choose depends on the goal of your recovery.

When a computer has repeated problems, many organizations choose to wipe the computer and restore it from their standard build image. Sometimes that's not a viable option—especially if the user has vital company information stored on the computer. In such an instance, recovering the computer will need to be attempted, and refreshing your PC may be an option.

Windows 8 also enables a push-button reset option. This option completely resets the computer and erases all data on the hard drive, so it should be used with care. Note that users may not be aware of the ramifications of performing this procedure.

Refresh your PC

The Refresh your PC option changes settings back to their defaults while retaining personalization settings and apps purchased from the Windows Store. Apps downloaded from the web and apps installed from other media are removed. The initial Refresh your PC screen is shown in Figure 7-4.

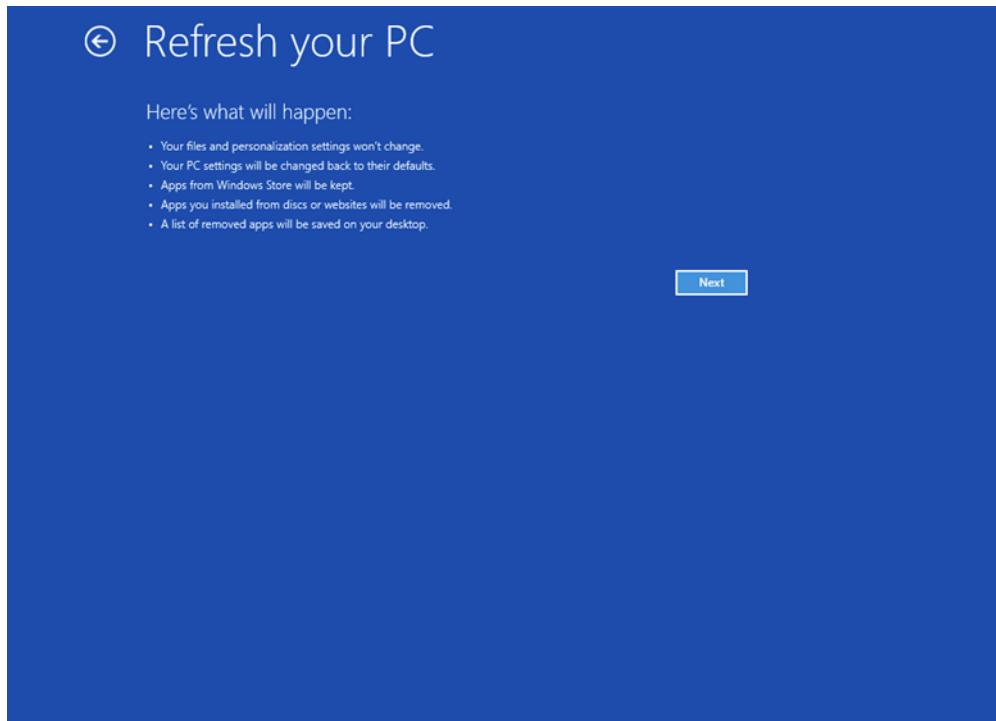


FIGURE 7-4 Beginning the Refresh your PC process.

Once invoked, the Refresh your PC option will automatically restore settings to their defaults as appropriate. This process can take several minutes to complete.

This process first scans the disk for data and other settings considered "personalizations." Once those are gathered, they're put into a special location on the disk and a new copy of Windows is installed. The personal data is then replaced and the new environment is started for the user.

The initial image to which the PC is refreshed can be customized. This enables the organization to include applications and other customizations so that after a refresh is performed, the basic environment will already be established.

Reset your PC

Unlike the Refresh your PC option that keeps apps from the Windows Store and also retains personalization settings, the Reset your PC option removes all apps and removes any personalization settings. The initial screen for the Reset your PC process is shown in Figure 7-5.

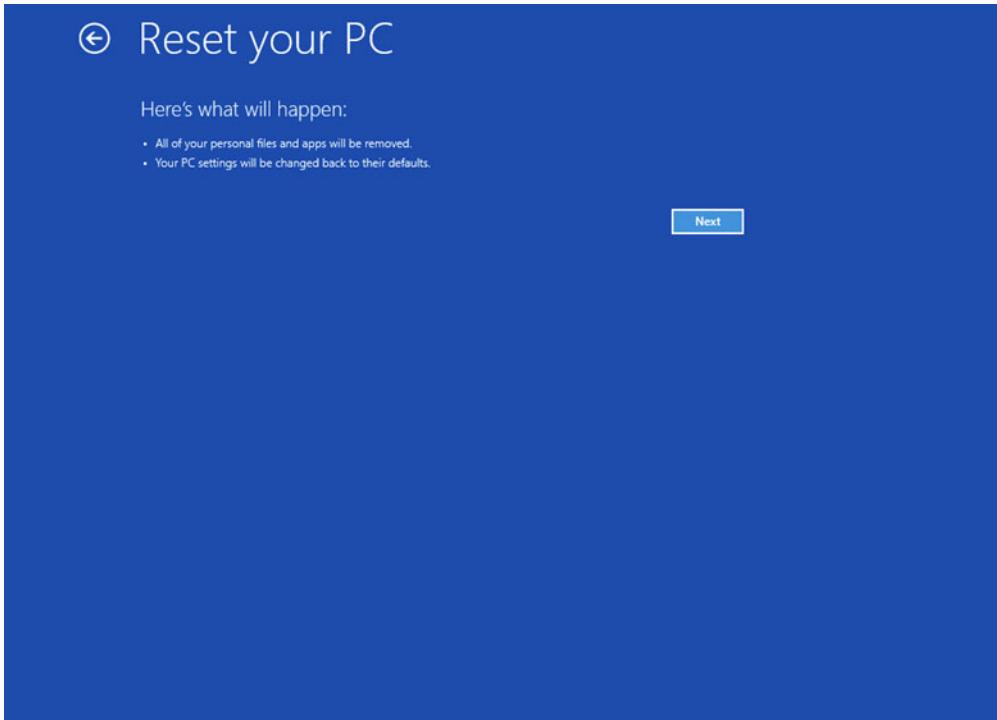


FIGURE 7-5 Beginning the Reset your PC process.

During a reset all settings, applications, and customizations are removed. The reset process begins by erasing and formatting the Windows partition. The process continues by reinstalling Windows and then booting into the newly reset operating system.

Customizing the Windows Recovery Environment

Many organizations develop custom recovery tools to help troubleshoot, manage, and fix computer issues quickly. The Windows RE can be configured to add a company's own tool or other customizations to the Boot Options menu.

Building a customized Windows RE

The Windows RE is based on the Windows Preinstallation Environment (PE). This means that the optional components available in Windows PE are also available to be added to a Windows RE image. Customizing the Windows RE image requires the Windows Assessment and Deployment Kit (ADK).

NOTE Working with Windows PE and installing the ADK is beyond the scope of this chapter. See <http://technet.microsoft.com/en-us/library/hh825109> for more information on creating a Windows PE.

Prior to customizing the Windows RE, you need to set up the environment. This involves several steps described in Table 7-2. These steps assume that you have the ADK running on a Windows 8 computer and that you have the Windows product DVD available.

The overall process for customizing Windows RE is:

1. Mount a Windows image.
2. Locate the Windows RE image inside of that Windows image.
3. Mount and customize the Windows RE image.

Table 7-2 Steps to Begin Customizing Windows RE

STEP	DESCRIPTION
Run the Deployment and Imaging Tools Environment	Open a command prompt with the ADK's Deployment and Imaging Tools available. You must run this as administrator.
Copy a Windows image to the computer	Use xcopy to copy a Windows image from the Windows product DVD to your computer. Any of the valid images on the DVD can be used.
Mount the Windows image	Use the DISM tool to mount the Windows image that you just copied in the previous step.
Mount the Windows RE image	Mount the Windows RE image on the computer so that it can be edited.

Once the initial steps are complete, the Windows RE image is ready to be customized. The customization process is dependent on the needs of your organization but frequently includes some or all of the items described in Table 7-3.

Table 7-3 Typical Customization Points for Windows RE

CUSTOMIZATION	DESCRIPTION
Add drivers	You can include device and other drivers that are critical to booting the computer. This is accomplished with the DISM tool.
Add a Boot Option tool	You can add a tool that shows up within the Boot Options screen. See http://technet.microsoft.com/library/jj126994.aspx for more information specific to this process.
Add language packs	You can add language support, but it needs to be added to both the Windows RE image and each of the optional components included in the Windows PE image.
Add Windows PE optional components	There are several optional components available with Windows PE and you can add them to the image. See http://technet.microsoft.com/library/hh824858.aspx and http://technet.microsoft.com/library/hh824926.aspx for more information

on this process.

Once the image has been customized, the next step is to unmount the image and its corresponding Windows image, and then deploy the image. Deployment of a Windows RE image involves updating computers that have a Windows RE partition and updating any other recovery media used in your organization.

MORE INFO See <http://technet.microsoft.com/library/hh825221.aspx> for more information on deploying a Windows RE image.

Enhanced recovery with DaRT

The Diagnostics and Recovery Toolkit (DaRT) has been updated for Windows 8. In version 8, DaRT enables more advanced images to be created and provides extended recovery and repair options beyond those provided in the Windows RE. DaRT supports UEFI boot and can now create Windows Imaging Format (WIM) or ISO images that can be deployed with USB media. DaRT also now features scripting more prominently to make it easier for those new to scripting to get up to speed quickly.

Using DaRT, an organization can also allow remote connections within the recovery partition, thus enabling support staff to reach a computer for recovery without having to be physically present at the computer.

DaRT includes a Recovery Image wizard, shown in Figure 7-6, that can be used to create an advanced recovery tool for IT professionals.

Windows 8 Media

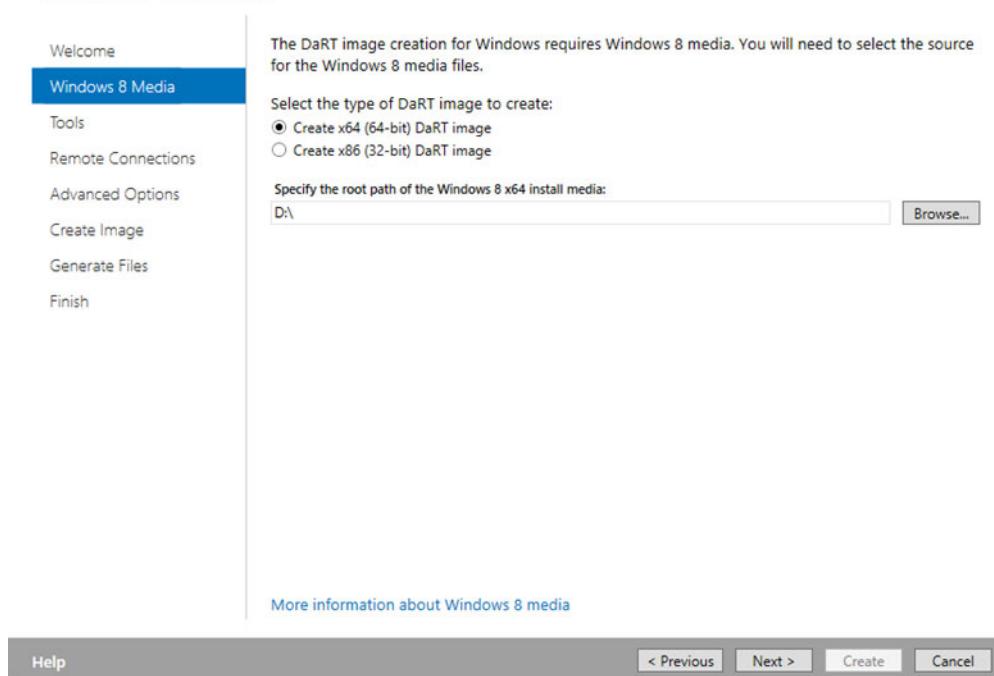


FIGURE 7-6 The DaRT Recovery Image wizard.

Like the Windows RE, a DaRT image can be customized to add drivers and other items necessary to aid in the recovery of a computer. During the Create Image phase, you can choose to edit the image. This mounts the DaRT image and enables the administrator to make the necessary changes for the image.

Once an image has been created, it can be deployed in a number of ways:

- Manual boot with removable media such as CD or USB.
- Manual installation as a recovery partition on the computer's hard drive.
- Automated installation as a recovery partition using System Center 2012 Configuration Manager or Microsoft Deployment Toolkit (MDT) 2012.
- As a network service delivered from Windows Deployment Services.

Many organizations will choose to deploy DaRT as its own recovery partition as part of new builds. Doing so makes the recovery tools available at all times and eliminates the need for bootable removable media.

When booted with a DaRT-created image, the Troubleshoot screen displays an additional menu item to invoke DaRT, as shown in Figure 7-7.

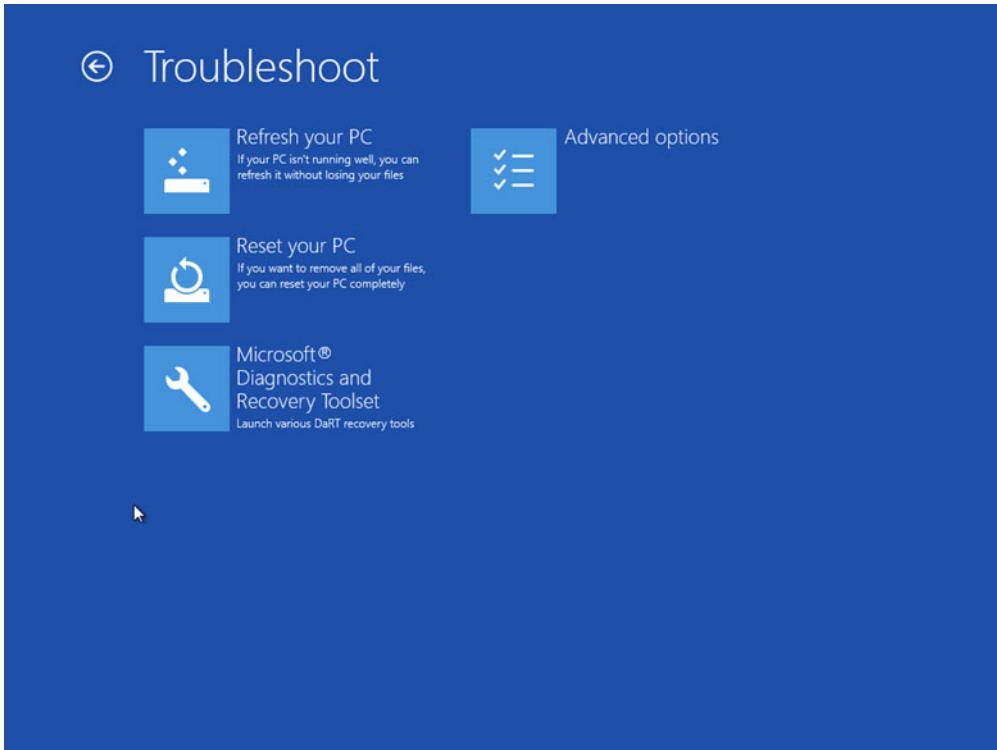


FIGURE 7-7 Booting with a DaRT image enables an additional recovery option.

Clicking the Microsoft Diagnostic and Recovery Toolset option displays the DaRT toolset, shown in Figure 7-8.

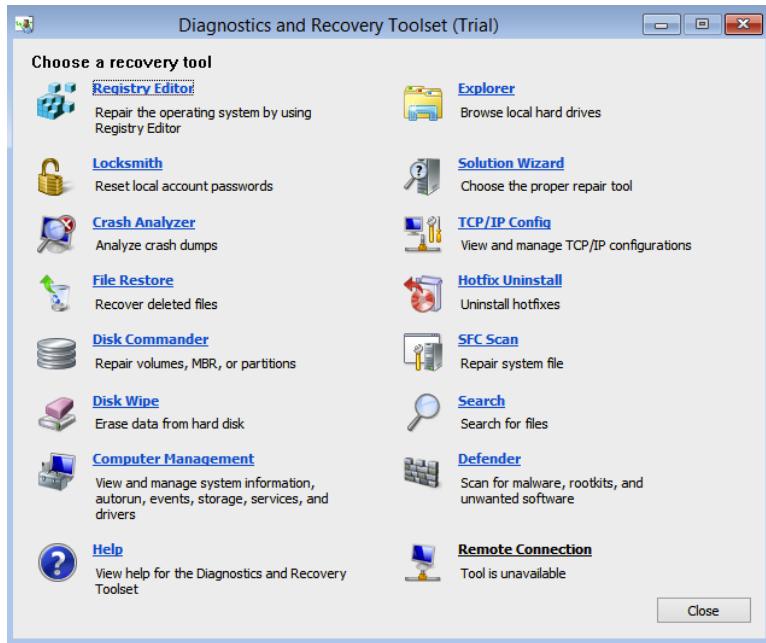


FIGURE 7-8 The DaRT toolset.

By using DaRT, the administrator has a full toolset available to recover the computer using advanced and granular tools like Disk Commander, Registry Editor, and others.

DaRT recovery images work alongside BitLocker. Microsoft recommends deploying the DaRT recovery image prior to enabling BitLocker, otherwise the disk may go into BitLocker recovery mode when the disk partitioning changes. Manual intervention is required to deploy a DaRT recovery image to a computer with BitLocker already enabled.

MORE INFO See <http://technet.microsoft.com/en-us/windows/hh826071.aspx> for more information on DaRT.

Summary

The Windows 8 RE is a significant step forward for helping IT organizations manage and maintain computers. When problems are encountered, Windows 8 attempts to automatically recover. If automatic recovery isn't possible, support personnel can use the advanced tools available through the Windows RE to attempt recovery.

Windows 8 provides several recovery options for both users and IT staff that can be used to refresh or reset a computer. When IT staff become involved, the traditional image recovery and system restore options are available. Safe Mode and the command prompt can also be used.

The Windows RE can be fully customized so that an IT organization can speed up the recovery process. Windows RE is based on Windows PE, and any of the optional components for Windows PE can be installed in a Windows RE image. The Windows RE image can be deployed to its own partition on a computer or it can be made available through other media.

The Diagnostic and Recovery Toolset (DaRT) extends the capabilities of the Windows RE, and provides even more granular tools for the administrator to use when recovering a computer. DaRT images can be customized as well, and when used with Windows 8 they provide an additional recovery option on the Troubleshoot options screen.

CHAPTER 8

Windows 8 management

Windows 8 embraces and improves on the core foundation that Windows 7 provided. It integrates into almost any existing Windows management infrastructure—from Microsoft System Center 2012 Configuration Manager to Windows Intune—to help streamline and simplify systems management and security. Windows PowerShell 3.0 provides management capabilities for nearly all graphical management tools. This diversity greatly enhances the remote management capabilities in Windows 8 and Windows Server 2012.

You can manage Windows 8 by using a variety of new and improved Microsoft tools and technologies. This chapter describes some of the various management options available for Windows 8 systems and offers an overview of their capabilities. Everything from Group Policy to Windows PowerShell has been revamped and reimagined for simplicity and maximum performance, in order to make your life as an administrator easier.

NOTE This chapter describes several Windows PowerShell cmdlets to showcase its enhanced functionality in Windows 8. Whenever this chapter mentions a new module, you see the actual importable module name in parentheses. To import these modules, simply type “**Import-Module**” followed by the module name.

NOTE Alongside advanced management tools and enhanced remote management abilities, Windows 8 offers many security improvements—such as enhancements to BitLocker Drive Encryption, Trusted Boot, and so on. For more information on security improvements in Windows 8, see Chapter 9, “Windows 8 security.”

IT Pros perform a variety of tasks on a daily basis. These tasks often include management tasks such as managing Group Policy objects (GPOs) or repairing a PC. Many of the management improvements in Windows 8 simplify these daily tasks. Table 10-1 describes where resources can be found in this book and online for some of the common management tasks performed by IT Pros.

TABLE 10-1 Common Management Tasks

MANAGEMENT TASK	RESOURCE IN BOOK	ONLINE RESOURCES
Using Windows PowerShell	Chapter 3, “Windows 8 for IT Pros,” section “Windows PowerShell 3.0” Chapter 8, “Windows 8 management,” section “Windows PowerShell”	http://technet.microsoft.com/en-us/library/hh857339.aspx http://technet.microsoft.com/en-us/scriptcenter/bb410849.aspx

Managing GPOs	Chapter 8, "Windows 8 management," section "Group Policy improvements"	http://technet.microsoft.com/en-us/library/ee461027.aspx http://technet.microsoft.com/en-us/library/dd759177.aspx http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx
Remote server management	Chapter 3, "Windows 8 for IT Pros," section "Remote Server Administration Tools"	http://technet.microsoft.com/en-us/library/hh831501.aspx
Implementing desktop, application, and user experience virtualization	Chapter 11, "Windows 8 virtualization"	http://technet.microsoft.com/en-us/appvirtualization/bb508934.aspx http://technet.microsoft.com/en-us/windows/hh943107.aspx
Managing system security	Chapter 9, "Windows 8 security"	http://technet.microsoft.com/en-us/windows/explore-windows-8.aspx
Software management	Chapter 8, "Windows 8 management," sections "System Center 2012 Configuration Manager" and "Windows Intune"	http://www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012.aspx http://www.microsoft.com/windows/intune
Operating system deployment	Chapter 4, "Preparing for deployment" Chapter 5, "Deploying Windows 8"	http://blogs.technet.com/b/inside_osd/ http://technet.microsoft.com/en-us/library/ee376932.aspx http://technet.microsoft.com/en-us/library/hh831833.aspx

Windows Backup

File History is the new file archiving feature in Windows 8. It replaces Windows Backup, which has been deprecated, and allows users to select which files to back up and where to save them. File History is not a backup utility that updates every few days; it syncs every hour unless configured otherwise, and can be mapped to cloud or USB storage. It also has an integrated recovery feature that simplifies recovery of accidentally removed or changed files. File History is disabled by default. To enable it, use the File History app in the Windows 8 Control Panel. You can still run Windows Backup, however, in cases where you need to restore files from backup sets created in Windows 7. On the Start screen, type **file recovery**, select Settings, and then click Windows 7 File Recovery.

Windows PowerShell

Windows Script Host (WSH) has been available since the days of Windows 95 and was the primary scripting host on Windows platforms until Windows 7, when Windows PowerShell took over that role. Today, Windows PowerShell 3.0 is the latest version of Windows PowerShell from Microsoft and is the preferred scripting host for Windows 8 systems. It enhances Windows scripting by implementing new, more powerful commands while requiring much less code for tasks than WSH. Providing cmdlet modules from Group Policy management to remote server tools, Windows PowerShell 3.0 has more functionality on Windows 8 than any other scripting language available. In addition, most Windows 8 add-ons, such as those in the Microsoft Desktop Optimization pack, extend Windows PowerShell with new modules.

Windows PowerShell 3.0 is also optimized for maximum human readability. Many syntax requirements that previously required curly braces now do not. These and many other confusing syntax requirements are now implied by the system.

TIP To get help on the required syntax for a cmdlet, use the "get-help" command followed by the cmdlet that you would like help with. For example, if you need help with the "Show-Eventlog" cmdlet, type **get-help Show-Eventlog**. Also remember that PowerShell 3.0 has IntelliSense capabilities. This allows you to auto-complete commands by pressing the Tab key.

The newest version of Windows PowerShell includes new remote management functionality. Several improvements were made to remote PowerShell Sessions (PSSession). Once a session is started, an administrator is no longer limited by firewalls or remote credential verification. Also, command history has been optimized for use when a new PSSession is initiated.

For example: An administrator needs to remotely administer a command to many computers. Instead of connecting to each one and pasting the same content into the command window, the administrator can simply press the Up-arrow key to retrieve the last command.

Table 10-2 offers a few examples of the new management features found in Windows PowerShell 3.0. For more information regarding important new features in Windows PowerShell, see "Windows PowerShell 3.0" in Chapter 3, "Windows 8 for IT Pros."

TIP For PowerShell 3.0 and Server Manager quick reference guides, see <http://www.microsoft.com/en-us/download/details.aspx?id=30002>. Also, another comprehensive Windows PowerShell resource is the Script Center on Microsoft TechNet at <http://www.microsoft.com/technet/scriptcenter/>.

TABLE 10-2 Management in PowerShell 3.0

FEATURE	DESCRIPTION
Windows feature management	The Deployment Image Servicing and Management (DISM) module " Get-WindowsOptionalFeature –Online " cmdlet allow administrators to remotely view the installed windows features on a machine. By using

this feature with the "**Add-WindowsFeature**" and "**Remove-WindowsFeature**" cmdlets found in the Server Manager module (ServerManager), an administrator can remotely manage Windows features in PowerShell.

Disconnected Sessions

Remote Windows PowerShell connections are not easily severed. Unlike previous versions of PowerShell, which dropped connection at the first signs of trouble, Windows PowerShell 3.0 PSSessions stay connected for a few seconds when network connectivity is lost. Also, if a computer is shut down or the connection is completely lost, an administrator can reconnect from a different computer.

Windows PowerShell Workflow

Workflows are like scripting checklists. They are implemented for long-running, complex activities to keep tasks moving. They are repeatable, interruptible, recoverable, and can run in parallel with other workflows.

Scheduled Jobs

There are 16 cmdlets found in the task scheduler module (PSScheduledJob) for Windows PowerShell 3.0. This new module provides all the basic functionality of the graphical utility, Task Scheduler. Remote task management allows administrators to implement aggressive energy saving tasks and much more.

TIP Having trouble starting on a script? <http://gallery.technet.microsoft.com/scriptcenter> is where IT Professionals share scripts from all different scripting languages and is an excellent starting point for implementing new scripts. To filter the scripts, simply search for "PowerShell 3.0" for Windows 8 specific scripts.

Nearly every graphical management utility found in Windows 8 and Windows Server 2012 is provided in the form of cmdlet modules in Windows PowerShell 3.0. The previous Windows Management Instrumentation (WMI) cmdlets that were available in Windows PowerShell 2.0 are still available in Windows PowerShell 3.0. In addition, previously available cmdlets are included alongside a new set of cmdlets for the Common Information Model (CIM). Both sets of cmdlets provide advanced system functionality to administrators through Windows PowerShell.

Windows Firewall is a great example of an advanced system feature that is available using these modules. PowerShell 3.0 provides cmdlets for creating firewall rules, caching Group Policy, modifying existing rules, and deleting rules. In addition to all of the basic functionality, it also provides advanced security administration. In Windows PowerShell 3.0, administrators can also remotely manage firewall settings by simply initiating a remote session to a client and providing the desired cmdlets. By using PowerShell scripting for managing firewall rules instead of netsh, you improve readability and reduce the amount of code

required for task execution. Listing 10-1 shows an example of how to add a basic firewall rule to block outbound traffic from local port 22 to a Group Policy object.

Listing 10-1 Configuring firewall rules with Windows PowerShell.

```
New-NetFirewallRule -DisplayName "Block Outbound Telnet" -Direction Outbound -Program  
%SystemRoot%\System32\tlntsvr.exe -Protocol TCP -LocalPort 22 -Action Block -PolicyStore  
domain.microsoft.com\gpo_name
```

NOTE Windows PowerShell automatically imports an entire module when you use just one cmdlet found in that module. This reduces the need for the Import-Module cmdlet.

Group Policy improvements

Group Policy is the primary way that system administrators quickly configure and enforce settings on large numbers of computers in their environment. You can learn more about Group Policy at <http://www.microsoft.com/grouppolicy>.

You manage domain-based Group Policy objects by using the Group Policy Management Console (GPMC). The GPMC is available for Windows 8 as part of the Remote Server Administration Tools (RSAT) pack for Windows 8.

Download RSAT from <http://www.microsoft.com/en-us/download/details.aspx?id=28972>.

Several new Group Policy features were introduced in Windows 8 and Windows Server 2012. In this chapter, the section titled "New functionality" describes many of these new features. Additionally, there are many new and changed Group Policy settings for Windows 8.

NOTE For a complete list of all group policy settings available in Windows 8, see <http://www.microsoft.com/en-us/download/details.aspx?id=25250>.

PowerShell GPO management

The Windows PowerShell 3.0 Group Policy module (`grouppolicy`) provides administrators with powerful Group Policy management cmdlets. You can run these locally on the server or remotely to drastically expand previous GPO functionality and availability. This new GPO PowerShell module includes commands for making, removing, changing, and backing up GPOs—and much more. For a full list of all cmdlets found in the GPO module for Windows PowerShell 3.0, see <http://technet.microsoft.com/en-us/library/hh857339.aspx> on Microsoft TechNet. Listings 10-2 and 10-3 are examples of commonly performed Group Policy tasks implemented in Windows PowerShell.

NOTE To implement Windows PowerShell Group Policy cmdlets, you must first download and install the RSAT pack for Windows 8, and then import the Group Policy module by using the "**Import-Module grouppolicy**" command.

Listing 10-2 shows an example of a PowerShell 3.0 command that creates a GPO called "Test," links it to the "Engineering" OU in the contoso.com domain, and provides GPO edit permissions to the "Engineering Admins" security group:

Listing 10-2 PowerShell GPO creation example.

```
new-gpo -name Test | new-gplink -target "ou=Engineering,dc=contoso,dc=com" | set-gppermisions  
-permissionlevel gpoedit -targetname "Engineering Admins" -targettype group
```

Listing 10-3 shows an example of a PowerShell 3.0 command that removes a GPO specified by the GUID 60cd9e46-0c18-46dc-9f3d-adf092bc531c from the contoso.com domain:

Listing 10-3 PowerShell GPO removal.

```
Remove-GPO -guid 60cd9e46-0c18-46dc-9f3d-adf092bc531c -Domain contoso.com
```

Along with these commands, there are twenty six cmdlets available in the Windows PowerShell 3.0 Group Policy module (grouppolicy). In addition to this new module, Windows 8 administrators can now use PowerShell for logon and logoff scripts in Group Policy. This allows new commands to run that were not available in any other scripting environment. There is now a PowerShell Scripts tab when you edit the Logon and Logoff properties in the Group Policy Management Editor.

TIP To get more information on a specific cmdlet, use the "Get-Help" command. For information regarding all of the commands available in Windows PowerShell, filtered by module, use the "Show-Command" command.

New functionality

Windows 8 and Windows Server 2012 Group Policy include a few new features that provide faster execution times and expand reporting capabilities. These innovative features provide IT Pros with improved functionality for quicker access to more accurate information. Table 10-3 outlines some of the notable new Group Policy features found in Windows 8 and Windows Server 2012.

TABLE 10-3 Group Policy Features

FEATURE	DESCRIPTION
Remote update	Remote Group Policy update allows administrators to remotely schedule a policy update for an individual or group of computers. This feature provides the most accurate information possible by using these precise updates. Previously, to force an unscheduled policy update, someone would have to remote into each machine and manually run gpupdate.exe.
Infrastructure status	This new feature is vital to an IT Pro implementing Group Policy on a domain level. It provides critical information that aids in monitoring and diagnosing policy replication issues. Potential

differences that are available using infrastructure status are SYSVOL and Active Directory (AD) security descriptor, each domain controller's number of policies listed in SYSVOL and AD, and GPO version details. Similar functionality to this integrated utility was previously acquired using separate tools such as GPOTool.

Improved results reporting	This feature can be used in conjunction with infrastructure status. Once a machine or group is found to have a replication or other type of issue, this feature displays information regarding the discrepancy. This feature has been improved in Windows Server 2012 to include more detailed information to help remedy Group Policy deployment issues.
Internet Explorer 10 support	Group Policy settings, preferences, and administrative templates are available for Internet Explorer 10. For more information on Group Policy settings for Internet Explorer 10, see Chapter 10, "Internet Explorer 10."

AppLocker

AppLocker is a simple yet powerful feature in Windows 8. It allows IT administrators to control exactly which programs specific users or groups can access. Implemented through Group Policy, AppLocker in Windows 8 is very similar to Windows 7. However, AppLocker in Windows 8 includes support for Windows 8 apps.

An example use of AppLocker as a management tool is to help manage restricted software. AppLocker can minimize the need for multiple images due to these restrictions. For example, imagine you have several tiers of developers that use different programs. Instead of having different images containing only the software that each tier can use, by using AppLocker all of the software can be on one image and user access can be specified for each tier.

For more information regarding AppLocker and how it can streamline management and security in your Windows 8 environment, see Chapter 9, "Windows 8 security."

System Center 2012 Configuration Manager

System Center 2012 Configuration Manager provides specialized and comprehensive management tools for your Windows systems and Windows mobile devices. Previously, multiple tools were required for managing multiple devices. Today, with System Center 2012 Configuration Manager, those multiple tools are no longer required. Configuration Manager is now a centralized management tool that can manage all of your organization's physical, mobile, and virtual devices (as well as employees' personal devices). This new unified management functionality improves the overall work environment by allowing implementation of the "bring your own device (BYOD) philosophy.

Unlike previous versions of System Center Configuration Manager, System Center 2012 Configuration Manager is designed around a user-centric asset management model by interfacing with an organization's Active Directory. This means that it associates hardware assets with specific users, allowing fine-tuned management of exactly which software and features are available to users. This new ability perfectly complements the new Group Policy and other features found in Windows 8. System Center 2012 Configuration Manager provides IT Pros with a comprehensive reporting platform that provides enhanced security and a user-centric focus for software management, integrated with full featured deployment and update options that they require for daily use.

One unique feature found in System Center 2012 Configuration Manager is the Software Center and Application Catalog. This catalog contains configurable settings for the Configuration Manager client, and also allows users to access downloadable content. This software-on-demand theme is common throughout the 2012 product lineup, including Windows Intune and the Windows RT management client. This exclusive "App Store" model allows users to download content provided by their IT department.

Redesigned management console

The redesigned management console available in System Center 2012 Configuration Manager incorporates several previously separate consoles into one. For example, within the Configuration Manager console, you can manage:

- applications
- operating system deployment
- application virtualization
- virtual desktop environments
- endpoint protection

It provides a simplified management console for greater efficiency.

Management options for software distributions have also been drastically improved. A new "purpose" role for each application has been implemented to coincide with an application's entire lifecycle. Also, you can now set the deployment type to custom, Windows Installer(MSI), script, Microsoft App-V, or Windows mobile (Windows 8 app deployment will be available in Service Pack 1). In addition, new requirement rules now native to package deployment minimize the necessity for using complex queries before deployment.

Infrastructure improvements

Microsoft System Center 2012 Configuration Manager has implemented a flatter structure that requires fewer site servers. While distribution points can still remain on their current versions of Windows server, the site server requires Windows Server 2008 and is best on Windows Server 2012. System Center 2012 also now offers bandwidth control amongst distribution points. This means that one distribution point needing to push large amounts of updates can use the bandwidth from other, less active distribution points.

The client agent settings, previously defined at the site level, are now defined by collection. This streamlined implementation allows clients to receive settings from multiple collections at once. Another

intuitive feature in Configuration Manager is the ability to implement client cache for distribution points. Similar to BranchCache, this feature uses client cached packages for future deployments.

Expanded reporting options

System Center 2012 Configuration Manager provides new reporting functionality to administrators. New report subscriptions allow administrators to schedule automatic reporting delivered through email or to a file share location. Also, there is a dual interface for running reports—either through the web via Report Manager, or from the Configuration Manager console via Report Viewer. Report Builder 2.0 is the new authoring and editing tool found in Microsoft SQL Server that is used for System Center 2012 reports. It is automatically installed when the first report is modified.

Mobile device support

System Center 2012 Configuration Manager fully integrates the BYOD methodology. There are two types of mobile device management for these devices: Light and Depth. Light provides services via the Exchange connector and provides data such as what mobile devices are on the network, Exchange policy summary, and a single view for all enterprise assets. Primarily, Light management transfers the mobile device administrator role from Microsoft Exchange to Configuration Manager.

Depth management provides enhanced features for mobile device software distribution. This includes client content monitoring, reporting, application installations, and application uninstallations—just like on x86 and x64 Windows 8 consoles.

System Center 2012 Endpoint Protection

Microsoft System Center 2012 Endpoint Protection (formerly known as Forefront Endpoint Protection 2010), when integrated with Configuration Manager, provides a consolidated view of compliance and security on all systems in an organization. This simplified view improves system protection by making it easier to quickly identify and correct security vulnerabilities. The key new features of Microsoft Endpoint Protection include:

- Single management and security console
- Centralized policy creation
- Enhanced scalability
- Accurate, efficient, and adaptive intrusion detection
- Windows Firewall management

App-V Simplifies Management

Microsoft Application Virtualization (App-V) enables enterprises to improve remote productivity and accelerate the application deployment process by hosting applications virtually. Virtual applications are never installed on a client, do not conflict with other applications, and can be simpler to manage. Importantly, virtual applications help ensure that users have access to the applications that they need, even when they change devices.

Instead of having IT Pros manage thousands of program updates while restricting access to all of them, why not have only one update on a virtual application that everyone uses and restrict access to that one instance? Using App-V, businesses can provide rich, full featured applications to its employees with low risk and high reliability. Additionally, App-V minimizes conflicts between applications and increases an organization's agility by providing quick application deployment. For more information on how Microsoft Application Virtualization can simplify your organization's application management, see Chapter 11, "Windows 8 virtualization."

Windows Intune

Windows Intune uses a unified web-based administration console to provide cloud-based device management features, software deployment capabilities, and security capabilities. Windows Intune is well-suited to businesses that require IT services but lack an existing infrastructure. This is because Windows Intune does not require any established infrastructure at all, only Internet connectivity and (for the Administrator) a web browser that is compatible with Microsoft Silverlight. Windows Intune 3.0 has a very intuitive layout and design similar to the previous version, making it easy to navigate.

In addition to all of the management features available in Windows Intune, it also provides an upgrade license to the latest version of Windows so that your organization can standardize the operating system on managed devices. Its flexibility to synchronize with Active Directory combined with its security and usability features makes Windows Intune a low-cost, enterprise-grade IT service for businesses.

Cloud management

Windows Intune is a cloud-based management console and does not require a virtual private network (VPN) connection to your local domain. This allows administrators to access it from anywhere that they have an Internet connection. Equally, clients have access to updates and software outside of your corporate environment. This functionality is great for small businesses considering IT consolidation into one centralized location rather than multiple sites, and it is perfect for providing IT services to remote employees.

Company portal

One of the unique features found in Windows Intune is its customizable company portal. The company portal is an interface customized with downloadable applications that your IT administrators have made available for your organization. The company portal also allows users to directly contact IT and request remote assistance.

In addition to remote application and service features, implementing the company portal feature in Windows Intune is a valuable security feature. If a managed mobile device is ever lost, there is a remote security wipe utility available which immediately clears all personal and corporate data from it whenever the device is connected to the Internet.

Summary

Windows 8 and PowerShell 3.0 introduce many new management features and improve existing Windows management features for IT Pros. Group Policy has new capabilities and many new policy settings, and you can use System Center 2012 Configuration Manager and Windows Intune to manage Windows 8 devices in your environment.

The key takeaway is that you can use the same management tools and technologies that you used to manage Windows 7 to manage Windows 8. While Microsoft has improved them for Windows 8, they look and feel mostly the same so the learning curve is very small.

Windows 8 security

Microsoft Windows 8 builds on the security features of Windows 7. It enables the enterprise to provide a secure and stable computing platform from which users can accomplish their tasks. Three primary areas are the focus of the Microsoft security approach. Those areas are:

1. Protect the client against threats.
2. Protect sensitive data.
3. Secure access to resources.

To help protect a client against threats, Windows 8 offers several enhancements such as Trusted Boot, Internet Explorer SmartScreen Application Reputation, and app sandboxing.

The changes made to BitLocker in Windows 8 highlight the efforts to protect sensitive data. Securing access to resources centers on Virtual Smart cards and Dynamic Access Control.

This chapter looks at some of the enhancements to security available with Windows 8.

Protecting the client against threats

Windows 8 includes numerous enhancements that reflect Microsoft's focus on protecting the computer against threats. This section looks at some of those enhancements.

Boot options for security

The Universal Extensible Firmware Interface (UEFI) offers several key advantages over traditional computer BIOS, such as the ability to initialize devices like the mouse prior to handing off control to the operating system. UEFI also provides security enhancements such as network unlock and self-encrypting drives for BitLocker. This section looks at two boot options: Secure Boot and Measured Boot.

Secure Boot

After the normal Power On Self Test (POST) activities, a computer hands the boot process off to a boot loader. With traditional BIOS, the boot process could be handed off to malware just as easily as a legitimate operating system. Secure Boot helps to prevent this attack vector by using databases containing pre-approved signatures and images that can be used for the computer.

NOTE Secure Boot requires UEFI 2.3.1 but does not require a Trusted Platform Module (TPM).

Secure Boot uses three databases. The first database, known as the signature database (db), contains signatures and hashes of images for things like UEFI applications and operating system loaders. The second database, known as the revoked signatures database (dbx), contains images that have been revoked or are otherwise marked as untrusted. The final database used in Secure Boot is the Key Enrollment Key database (KEK), which contains keys that can be used to sign updates to the signature and revoked signatures databases.

The firmware non-volatile RAM (NVRAM) is populated with these databases when the computer is manufactured. Further changes to the firmware are prevented unless the change is signed with the correct signature. A platform key, which can be used to turn off Secure Boot, is generated once the firmware has been locked.

The boot sequence for Trusted Boot is as follows. This includes the steps for the UEFI Secure Boot feature as well as the Trusted Boot process in Windows 8.

16. The platform key is queried in the signature databases.
17. If untrusted firmware is encountered, the UEFI firmware initiates recovery (specific to the computer manufacturer) to remediate the issue.
18. At this point, the UEFI Secure Boot process is complete and the Windows Boot Manager takes over. If there's a problem with the Windows Boot Manager, a backup copy of the Windows Boot Manager is used. If the backup copy has problems, recovery is initiated specific to the computer manufacturer.
19. Once the Windows Boot Manager takes over, if a problem is noticed with vital Windows drivers or the kernel, the Windows Recovery Environment (RE) is started.
20. Early Launch Antimalware (ELAM) compliant software is loaded.
21. The remaining drivers and user processes are started.

Windows 8 can be deployed to devices that support UEFI's Secure Boot capability using the same tools that you already use to deploy Windows.

MORE INFO See <http://technet.microsoft.com/en-us/library/hh824987.aspx> for more information on Secure Boot.

Measured Boot

Measured Boot aims to improve network health by ensuring that clients meet a certain health status before being granted access to resources. The specific scenario protected with Measured Boot surrounds the boot process itself. For example, a file server might ask the client to prove that its boot process was healthy. The client can then pass its health data to the Remote Attestation service from which a Client Health Claim will be obtained and passed to the file server in order to obtain access.

Measured Boot works in conjunction with the Trusted Platform Module (TPM) to provide the measurements through Platform Configuration Registers (PCR). Included in the Measured Boot measurements is a log of all kernel components and boot-related drivers that have been loaded.

MORE INFO See <http://msdn.microsoft.com/en-us/library/windows/hardware/br259097.aspx> for more information on secure and measured boot.

SmartScreen

Windows SmartScreen is a reputation system for downloaded software. SmartScreen Application Reputation was originally included in Microsoft Internet Explorer 9 but was moved into the core Windows 8 operating system to offer broader protection.

When Windows SmartScreen is activated, an application downloaded from the Internet is compared to the SmartScreen database. If the application is found to have a bad reputation or doesn't yet have a reputation established, the user is notified about the status of the software. That way, the user can choose whether the software should be allowed to run. This process is called the Application Reputation check.

Built on the same concept, but separate from Windows SmartScreen, is the Internet Explorer SmartScreen Filter. SmartScreen Filter runs in the background to notify users of suspicious websites. SmartScreen Filter supports Group Policy which can be used to enable or disable the filter or to prevent users from disabling the filter or overriding its warnings. The SmartScreen Filter is enabled within the Internet Options of Internet Explorer, within the Security tab.

In an enterprise scenario, there are privacy implications for using the SmartScreen Filter. Certain information is sent to the URL Reputation Web Service. Table 9-1 describes this information.

Table 9-1 Information Sent as Part of the SmartScreen Filter Process

DATA POINT	DESCRIPTION
Anonymous statistics	For example, how often a query is made and how often a warning is generated.
Language and locale	The browser's language and locale settings.
Operating system version	The version of Windows being used.
Software version	The version of the browser being used, along with the version of the SmartScreen Filter and the version of the "high traffic site" list.
URL	The URL being requested by the user.

MORE INFO See <http://technet.microsoft.com/library/jj618329.aspx> for more information on the SmartScreen Filter.

Vulnerability mitigation and sandboxing

Windows 8 has improved Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP)—both of which make exploiting vulnerabilities more difficult. DEP prevents data from being executed while ASLR ensures that the address space of a process is randomized, thus making it more difficult to predict

the location of code within memory. The combination of DEP and ASLR in Windows 8 increase the amount of effort required by an attacker to develop and be successful with an exploit.

Apps in Windows 8 execute in an app container sandbox which, like other sandboxing techniques, helps to limit the amount of access that an app has to things outside its sandbox.

The vulnerability mitigation through both ASLR and DEP and app container help to keep Windows 8 computers protected.

Protecting sensitive data

Another area of focus for Windows 8 security is on protecting sensitive data. This section examines the enhancements to BitLocker.

BitLocker

BitLocker provides volume-level encryption for Windows 8 computers to help prevent unauthorized access to data on encrypted volumes. In Windows 8, BitLocker offers several enhancements over previous versions. Among some of the key enhancements are:

- Network unlock
- PIN and password changes by Standard User accounts
- TPM provisioning enhancements
- Used Disk Space Only encryption
- Encrypted hard drive support

Authentication to decrypt a BitLocker-enabled volume occurs prior to boot and can be done in a number of ways, including manual input of a PIN or password, through a USB device, network unlock, or through a TPM, depending on the methods available.

When a user self-provisions BitLocker encryption to a device, the user is prompted for how unlock information will be provided, as shown in Figure 9-1. In an enterprise scenario, the IT organization will set the available method and the user will use one of the previously described mechanisms as set by the organization's policy. See the section titled "BitLocker in the enterprise" later in this chapter for more information.



FIGURE 9-1 Choosing how to unlock a BitLocker-encrypted drive.

The BitLocker boot sequence is described in Table 9-2.

Table 9-2 BitLocker Boot Sequence

STEP	DESCRIPTION
Boot integrity check	When TPM is present and used as a protector, the TPM Platform Configuration Registers (PCR) measurements are reviewed to determine whether the system boot process has integrity and has not been tampered with.
Bootmgr started	Bootmgr starts the boot process.
Authentication	The user provides authentication information to unlock the BitLocker-enabled drive.
BitLocker unsealing	Encryption keys for BitLocker are unsealed.
Unlock volume	If unsealing was successful, the volume is unlocked and boot of the operating system begins.
Launch Windows Recovery Environment if failure	Windows RE is launched if BitLocker encryption keys are unable to be unsealed.

BitLocker in Windows 8 enables the ability to store recovery keys in Microsoft SkyDrive in addition to the traditional recovery methods supported in Windows 7. BitLocker's performance has been improved with

Windows 8 as well. Encrypted Hard Drives can be used to offload the processing required for encryption, thus saving power.

BitLocker can be used without a TPM by selecting protector options such as StartUp Key from the "Require additional authentication at startup" policy found in Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives. BitLocker can then be used on the computer.

BitLocker protection mechanisms

BitLocker protection mechanisms vary depending on the hardware scenario under which BitLocker is deployed. When protecting an operating system, BitLocker can use TPM or TPM+PIN if a TPM is available on the device. If not, a startup key, password, or Data Recovery Agent (DRA) can be used. When protecting a removable drive or fixed data drive, a password or smart card will be used. Additionally, a fixed data drive can also use automatic unlock as well.

BitLocker in the enterprise

Windows 8 enables the use of Active Directory account- or group-based unlocking. Designed specifically for Windows Server clusters, this feature unlocks a protected volume when an authorized user or machine account accesses it. Finally, when computers are connected to the corporate network with a wired connection, this Network Protector enables a device to boot without a PIN or password, which makes automated patching easier.

Group Policy has been enhanced for BitLocker as well. New settings include the ability to set whether BitLocker will use Full Encryption or Used Disk Space Only for encryption. This setting can be enabled separately for fixed data drives, operating system drives, and removable data drives.

BitLocker can store recovery keys in Active Directory Domain Services (AD DS). This helps support personnel working with computers to address issues. BitLocker supports removable media through BitLocker To Go.

When provisioning new computers, BitLocker can be pre-provisioned prior to a Windows installation using the Windows Preinstallation Environment (Windows PE). When the provisioning method is the Used Disk Space Only, the pre-provisioning process is very fast.

NOTE BitLocker works with TPM v1.2 and v2.0.

Storage Area Networks (SANs) are supported with BitLocker as well. BitLocker can encrypt iSCSI and Fibre Channel-based volumes, and even large volumes are encrypted quickly because of the Used Disk Space Only encryption method. In addition, BitLocker supports Microsoft Windows Server 2012 clustered shared volumes.

Microsoft has also worked with OEMs to ensure that devices such as tablets don't have ports with Direct Memory Access (DMA). This helps to ensure that the BitLocker process can't be bypassed by an attacker.

Advanced administration of BitLocker with MBAM

Microsoft BitLocker Administration and Monitoring (MBAM), part of the Microsoft Desktop Optimization Pack (MDOP), is the next level in BitLocker administration. As its name suggests, MBAM provides administration and monitoring of BitLocker services. MBAM enables the recovery and hardware data to be stored in a database and has several audit and compliance reports.

MBAM runs with a client/server architecture, with a central server running on Windows Server 2008 or 2012 and clients running on each Windows 8 computer. MBAM uses Microsoft SQL Server for providing database services. Table 9-3 describes the components involved in MBAM.

Table 9-3 MBAM Architectural Components

COMPONENT	DESCRIPTION
Administration and Monitoring server	The main server used to perform all data collection and act as the management console for MBAM.
Database server	SQL server that hosts: The Recovery and Hardware database The Compliance and Audit database The Compliance and Audit reports. This can be a single server or you can use a server for each of the three data and reporting components.
Management Workstation	The computer from which administrators connect to and use the management console for MBAM.

The deployment of MBAM uses a client which is installed on client computers. The MBAM client is contained in a standard Windows Installer Package file (.MSI), and can be deployed through any electronic software distribution (ESD) method. The settings related to MBAM are configured through Group Policy, which is discussed in the next section.

You can manage MBAM and access reports using the management console. The management console can be accessed using a web browser, which means that IT staff can use their own workstations to manage MBAM. The MBAM management console is shown in Figure 9-2.

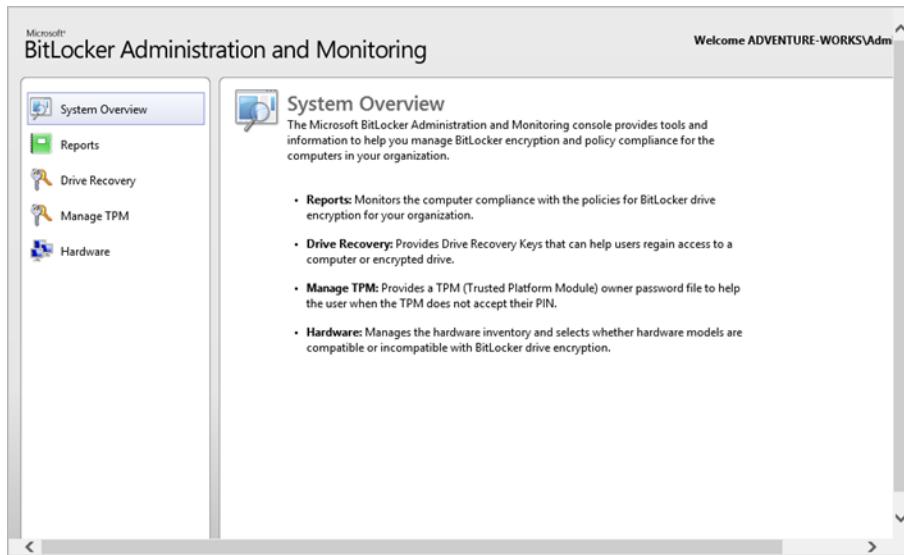


FIGURE 9-2 The MBAM management console.

Administration and support tasks for MBAM are managed at the group level using Active Directory. This means that an IT organization can delegate certain tasks—such as the ability to view reports—to certain staff, while others can use help desk features. Table 9-4 shows the roles available with MBAM.

Table 9-4 Administrative Roles with MBAM

ROLE	DESCRIPTION
MBAM Advanced Helpdesk Users	Provide additional help desk tasks beyond those provided by the MBAM Helpdesk Users group.
MBAM Hardware Users	Manage hardware compatibility.
MBAM Helpdesk Users	Perform help desk related activities in support of MBAM clients.
MBAM Report Users	View compliance and audit reports.
MBAM System Administrators	Access all features of MBAM.

For example, members of the MBAM Helpdesk Users group can perform Drive Recovery tasks in the MBAM management console, shown in Figure 9-3.

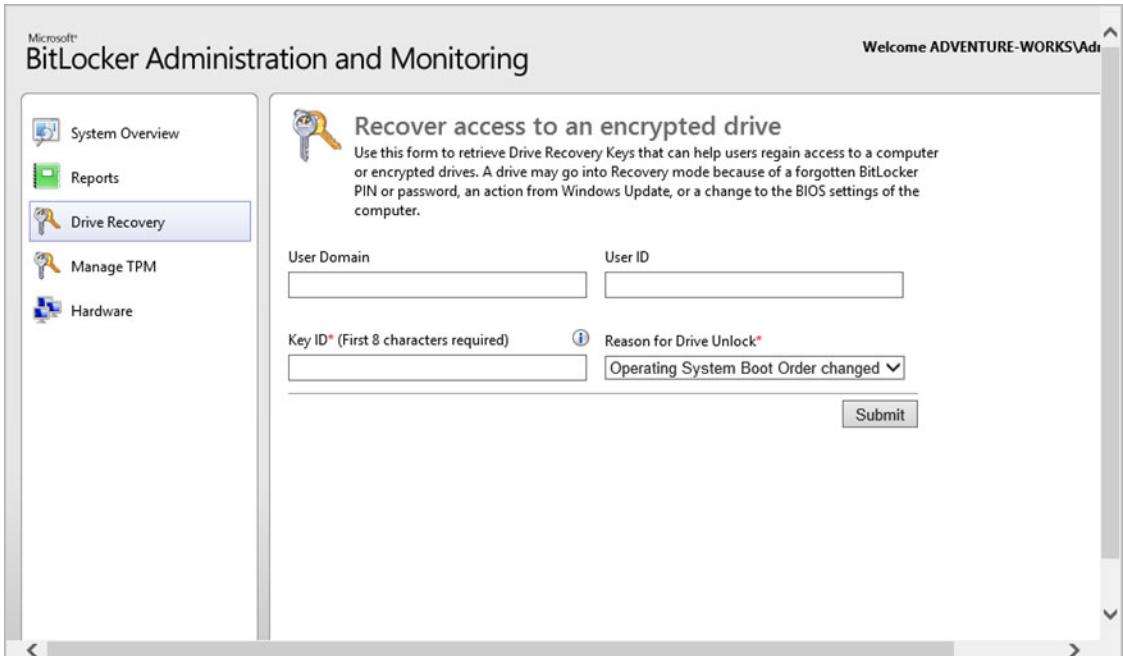


FIGURE 9-3 Using Drive Recovery in MBAM.

MBAM and Group Policy

MBAM policies are distributed through Group Policy. The settings for MBAM are found in:

- Computer Configuration\Policies\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management)
- User Configuration\Policies\Administrative Templates\Windows Components\MDOP MBAM (BitLocker Management)

The available Group Policy settings are described in Table 9-5.

Table 9-5 Group Policy Settings for MBAM

SETTING	DESCRIPTION
Client Management	Settings to configure MBAM services, user exemption, and hardware compatibility.
Fixed Drive	Encryption settings for fixed data drives.
Global Settings	Overall settings such as encryption method and cipher strength, the organization's unique identifier, and related settings.
Operating System Drive	Encryption settings related to the operating system disk drive.
Removable Drive	Settings related to how BitLocker is used on

	removable drives, including the denial of write access to drives that aren't protected by BitLocker.
--	--

MBAM includes administrative templates for Group Policy, available in %SYSTEMROOT%\PolicyDefinitions. The files BitLockerManagement.admx and BitLockerUserManagement.admx define policy settings for both the Computer Configuration and User Configuration folders.

Secure access to resources

Remote access to resources is more important than ever. Microsoft has enhanced and unified the remote access experience. With DirectAccess, security and software patching has been improved so that updates can be delivered whenever the client is connected to the Internet. This reduces the amount of update traffic that travels over the VPN connection.

DirectAccess features several authentication models and methods for data encryption. For example, a DirectAccess client can use end-to-end encryption or end-to-edge encryption depending on the needs of the organization or the data involved. DirectAccess can use several different methods for authentication including TPM virtual smart cards, two-factor authentication, or Active Directory credentials.

Virtual smart cards

Virtual smart cards enable two-factor authentication in a cost-effective manner. Rather than needing to deploy a complex infrastructure, virtual smart cards help reduce the chances of unauthorized access. Virtual smart cards work in conjunction with the TPM as a convenient and secure solution to access control.

MORE INFO See <http://technet.microsoft.com/en-us/library/hh831433.aspx> for more information on virtual smart cards.

Dynamic Access Control

Dynamic Access Control enables granular and complex resource protection throughout an enterprise. With Dynamic Access Control, the organization can apply permissions and restrictions on access to resources based on the resource's sensitivity, the user, or the device being used to access that resource. For example, a user is allowed to access a document from a trusted connection in the office but when travelling they can't access the document due to its access restrictions.

Dynamic Access Control works with the concept of central access rules and central access policies along with claims. Claims are unique data points about users, devices, or resources that can be used for rules and policies.

MORE INFO See <http://technet.microsoft.com/library/jj134043.aspx> for more information on Dynamic Access Control.

Summary

Windows 8 builds on the security features from previous versions of Windows. Windows 8 concentrates security around protecting the client against threats, protecting sensitive data, and securing access to resources.

Windows 8 implements Trusted Boot and Measured Boot to provide trusted computing environments. Trusted Boot works in conjunction with UEFI's Secure Boot feature and its signature database that exists in the computer's firmware in order to ensure that boot loaders are trusted. From here, Trusted Boot protects the remaining Windows boot process and ELAM compliant antimalware solutions.

Windows SmartScreen uses a reputation-based system for helping to determine whether software being run on the system is trusted. The primary scenario for Windows SmartScreen surrounds files downloaded from the Internet. Using the file's name and a hash signature, a warning may be displayed to the user if the software has a bad reputation or is otherwise unknown. Windows SmartScreen is different from—but uses the same concept as—the Internet Explorer SmartScreen Filter, which also uses a reputation-based system to provide feedback on sites that a user visits.

ASLR and DEP along with app container sandboxing provide further protection for Windows 8. The security enhancements to Windows 8 also reflect the importance of centralized management within an organization. Improvements have been made in BitLocker to enable its use with today's computers and to make provisioning easier. Advanced management of BitLocker in an organization is achieved with the Microsoft BitLocker Administration and Management (MBAM) tool, part of the Microsoft Desktop Optimization Pack (MDOP). MBAM provides a single location for administration and support of a BitLocker implementation. Compliance and audit reports are available with MBAM, and the use of MBAM's management features can be delegated through role-based administration.

Access control through virtual smart cards and Dynamic Access Control enable new ways to protect and secure access to resources with Windows 8.

Internet Explorer 10

New for Microsoft Windows 8, Internet Explorer 10 provides a fast and fluid browsing experience perfect for the touch interface. Internet Explorer 10 continues the advancement of web standards, with support for many HTML5 and CSS3 features. Internet Explorer 10 presents two different experiences to the user.

The desktop experience provides the browsing capabilities that users have come to expect from Internet Explorer, with a tabbed interface. As a Windows 8 app, Internet Explorer provides an immersive, full-screen browser optimized for a touch interface. This enhances the user experience of sites so that they perform more like apps.

When used as a Windows 8 app, Internet Explorer 10 is known simply as Internet Explorer. When used through the desktop, Internet Explorer 10 is known as Internet Explorer for the desktop.

This chapter looks first at the two modes found in Internet Explorer 10. The chapter continues into new settings in Internet Explorer 10, and then wraps up with a look at the management of Internet Explorer 10 through Group Policy.

Using Internet Explorer for the desktop

Internet Explorer for the desktop provides the traditional browsing experience that users are familiar with. The browser operates and has a traditional look and feel (with tabs and menus) similar to those seen in previous versions of Internet Explorer. Figure 10-1 shows Internet Explorer for the desktop.

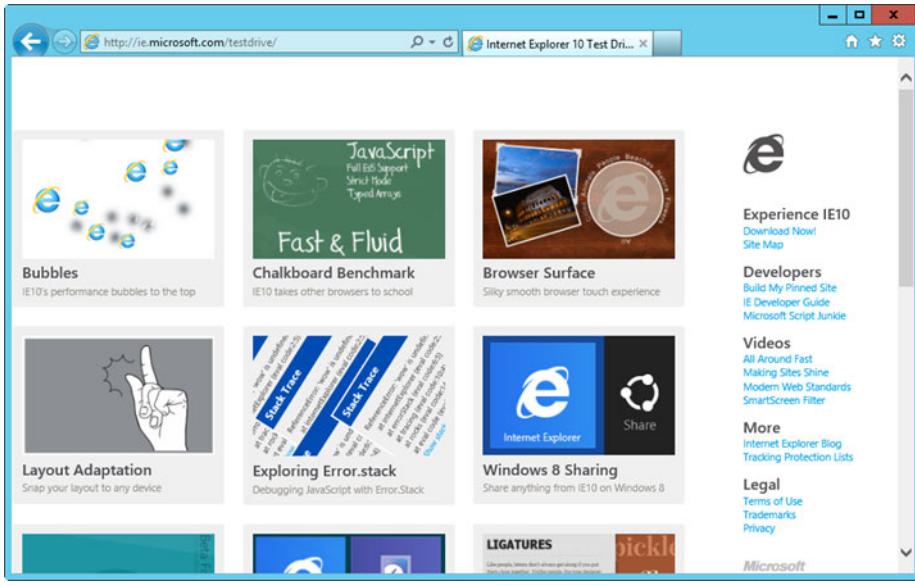


FIGURE 10-1 Internet Explorer for the desktop.

Internet Explorer for the desktop is invoked from the desktop but can be set as the default handler for links. This and numerous other settings are configurable through Group Policy—discussed later in this chapter.

Internet Explorer for the desktop uses the same rendering engine as Internet Explorer when used as a Windows 8 app. This makes supporting and troubleshooting much easier.

Using Internet Explorer

Internet Explorer, used as a Windows 8 app, presents a different browsing experience than traditional desktop browsing. The Internet Explorer experience is a touch-first interface but can be used with a mouse and keyboard. Internet Explorer is a full-screen browser with tabs and controls moved out of the way yet able to appear again at the swipe of a finger. Internet Explorer in the Modern UI is shown in Figure 10-2.

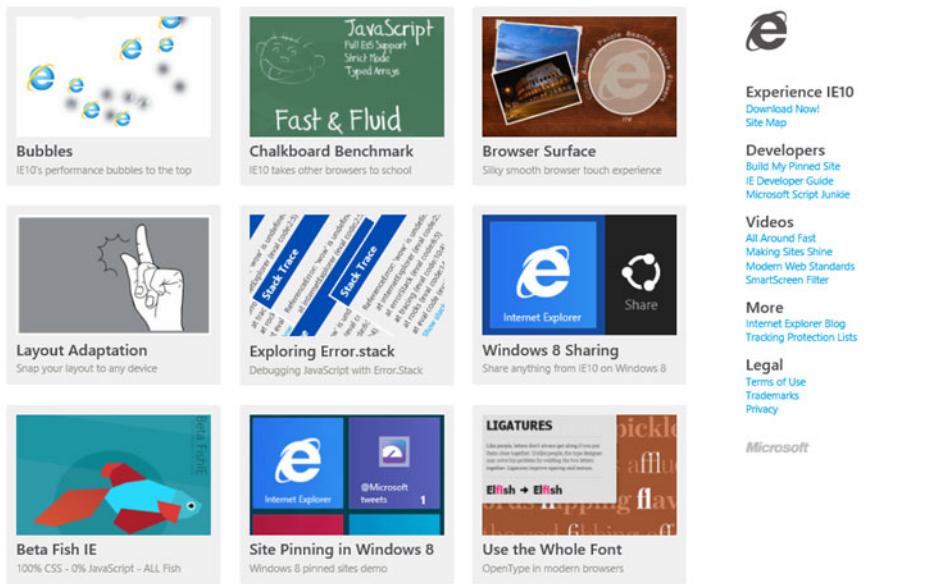


FIGURE 10-2 Internet Explorer in Windows 8.

New interface and new usage patterns

With the new touch-first interface of Internet Explorer comes new ways to accomplish browsing tasks. Internet Explorer uses hot spots to provide input and interaction with the webpages and with the browser itself. For example, you can bring up both the current URL and any other open tiles, as shown in Figure 10-3.

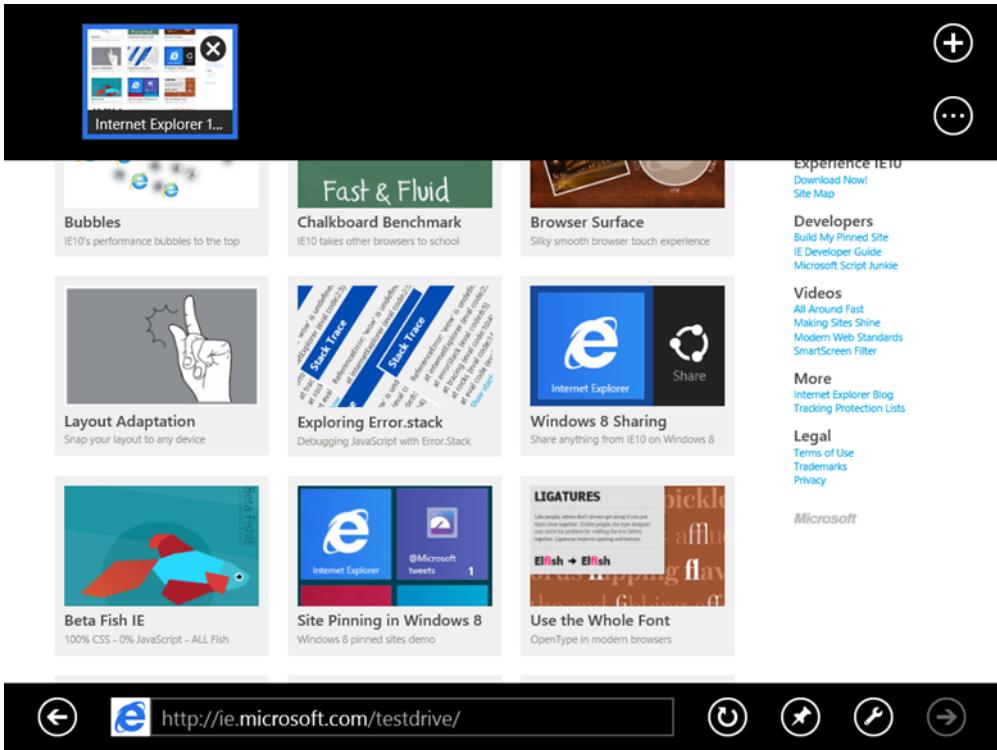


FIGURE 10-3 Viewing additional tiles and the current address in Internet Explorer.

With Internet Explorer you can pin sites for easy access by tapping the pin icon. Doing so reveals the dialog shown in Figure 10-4 that allows you to name the pin.

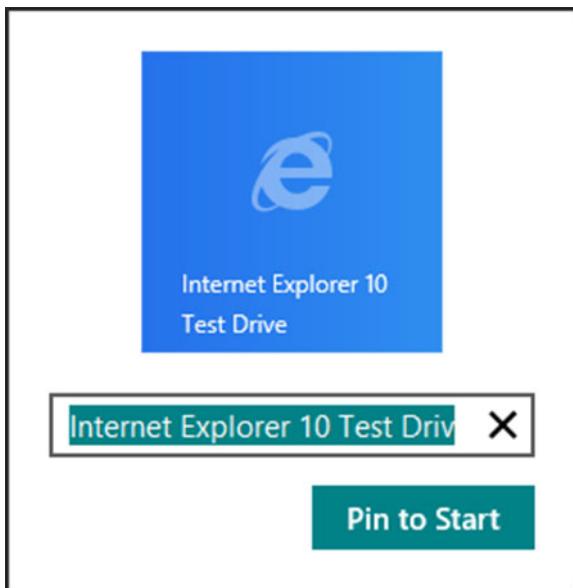


FIGURE 10-4 Pinning a site to Start in Windows 8.

Pinned sites remain on the Start screen, much like a bookmark in a traditional browser experience. Figure 10-5 shows an example of a site that has been pinned using the dialog from Figure 10-4.

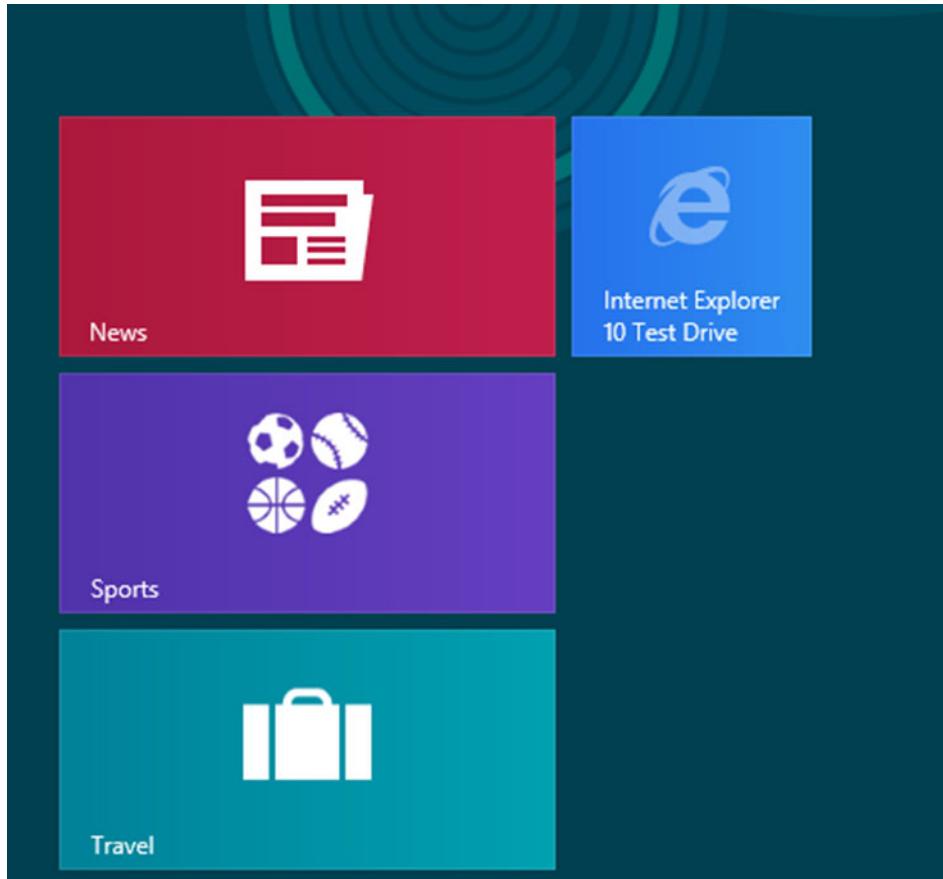


FIGURE 10-5 A pinned site Tile on the Start screen in Windows 8.

The address bar in Internet Explorer also acts as a quick search box with automatic site suggestions, and the controls provide easy access to recently visited and pinned sites from right within the browser.

Under the hood, Internet Explorer uses the same rendering engine as Internet Explorer for the desktop and can apply the same Group Policy settings, where appropriate. Aside from the built-in Flash support, however, toolbars and other add-ons will not work in the immersive Windows 8 app-style browser; this was designed to provide a modern, plug-in-free browsing experience.

The Windows 8 app-style interface for Internet Explorer is available only if Internet Explorer 10 is the default browser for Windows 8. If another default browser is used, double-clicking the Internet Explorer icon will start Internet Explorer for the desktop. To restore access to the Windows 8 app-style browser, select Internet Explorer 10 as the default browser.

New Features in Internet Explorer 10

Internet Explorer 10 has many new features, enhancements, and additional support for web standards.

Among the highlights of the new features are:

- **Adobe Flash included** Adobe Flash is included as a platform feature free of plug-ins in Internet Explorer 10.
- **Do Not Track (DNT)** The DNT header is now available to enhance privacy online. This feature enables users to express their preference about whether their browsing history should be collected and used for targeted ads, content, and other purposes. This feature is controllable through Group Policy, as discussed in the next section.
- **Enhanced Protected Mode** The new Enhanced Protected Mode provides additional protection over the Protected Mode that was first introduced in Internet Explorer 7. Enhanced Protected Mode reduces the browser's capabilities and the information that it provides to untrusted sites. With Enhanced Protected Mode, Internet Explorer 10 cannot access protected locations that contain personal information. Internet Explorer 10 with Enhanced Protected Mode also cannot access domain credentials unless allowed to do so.

MORE INFO See <http://blogs.msdn.com/b/ie/archive/2012/03/14/enhanced-protected-mode.aspx> for more information on Enhanced Protected Mode.

- **Support for CSS3 and HTML5** Internet Explorer 10 supports several additional CSS features such as CSS3 regions, flexible box, grid, and multicolumn layout, device adaptation, 3D transforms, fonts, animations, gradients, transitions, and more.

Additional HTML5 support that has been added to Internet Explorer 10 includes: history, Web Workers, WebSockets, Scalable Vector Graphics (SVG), asynchronous script execution, and several application programming interfaces (APIs) like AppCache, File, and Drag-and-Drop, among other features.

MORE INFO See the Developer Guide for Internet Explorer 10 at <http://msdn.microsoft.com/library/hh673549> for more information on additional web standards.

- **Flip Ahead** Internet Explorer uses a new Flip Ahead feature (configurable through settings and in Group Policy) that makes navigating sites through the touch interface easy. Users can "flip" to the next page with a swipe and can navigate backwards using a swipe gesture as well. This is especially useful when browsing search results and multi-page news articles.

Group Policy in Internet Explorer 10

With the new features in Internet Explorer 10 come new Group Policy objects (GPOs). These new objects enable further control of the behavior of Internet Explorer and Internet Explorer for the desktop. Some Group Policy settings have changed with Windows 8 as well. In total, there are almost 1,500 settings that can be changed in Group Policy for Internet Explorer 10.

This section highlights some of the Group Policy settings for Internet Explorer 10.

MORE INFO You can find a comprehensive list of all Group Policy settings at <http://technet.microsoft.com/en-us/library/hh846775>.

New Group Policies

There are numerous settings that can be applied through Group Policy for Internet Explorer 10. Some of them configure how the new features in Internet Explorer 10 will behave. Table 10-1 shows some of the highlights of the new Group Policy settings for Internet Explorer 10.

Table 10-1 New Group Policy Settings for Internet Explorer 10

SETTING	DESCRIPTION
Turn on Enhanced Protected Mode	Enables Enhanced Protected Mode for any zone that uses Protected Mode. Enhanced Protected Mode cannot be disabled by users.
Start Internet Explorer with tabs from last browsing session	When enabled, Internet Explorer will begin with the same tabs from the previous session. This cannot be overridden by users so that they can begin with a home page.
Turn off URL Suggestions	When enabled, URL Suggestions in the address bar will be disabled.
Open Internet Explorer Tiles on the desktop	When Tiles are opened, they are opened using Internet Explorer for the desktop.
Set how links are opened in Internet Explorer	When links are opened, such as when clicked from an email, this setting configures whether they will be opened in Internet Explorer or Internet Explorer for the desktop.
Install new versions of Internet Explorer automatically	Configures whether Internet Explorer will be automatically upgraded when a new version is available.
Always send Do Not Track header	Sends the DNT: 1 header on requests. If disabled, the header is sent when a Tracking Protection List is enabled or when an InPrivate browsing session is

	used.
Notify users if Internet Explorer is not the default web browser	Users will be notified that Internet Explorer is not the default web browser. If this policy isn't set, users will be able to choose whether to be notified.
Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects	This setting disables Flash within Internet Explorer.
Turn off Flip Ahead feature	Disables Flip Ahead for Internet Explorer. Doesn't apply to Internet Explorer for the desktop which doesn't have Flip Ahead.

Other Group Policy settings exist for configuring the behavior of HTML5 features such as WebSockets—including the maximum number of connections, and whether the WebSocket object is enabled. Other HTML5-related settings include configuration for the behavior and storage of indexed databases, AppCache, and websites in general.

Changed Group Policies

Some Group Policy settings applied to earlier versions of Internet Explorer but have changed with Windows 8. Table 10-2 highlights some of the changes.

Table 10-2 Changed Group Policies for Internet Explorer 10 and Windows 8

SETTING	DESCRIPTION
Prevent changing default browser check	This setting now applies to Internet Explorer 5.0 through 9.0. Internet Explorer 10 uses the "Notify users if Internet Explorer is not the default web browser" setting for this purpose.
Enforce full-screen mode	This setting makes Internet Explorer remain in full-screen mode. For Windows 8, this setting applies only to Internet Explorer for the desktop.
Turn off Print menu	When enabled in Windows 8, the Print flyout will not be available for Internet Explorer and printers won't be available under the Devices charm. This setting operates the same for Internet Explorer for the desktop as it did in previous versions.

Summary

Internet Explorer 10 for Windows 8 operates in two different modes. When running as a Windows 8 app, Internet Explorer 10 is known simply as Internet Explorer. When operated on the desktop, Internet Explorer 10 is called Internet Explorer for the desktop.

Internet Explorer for the desktop is a traditional browsing experience with a tabbed interface and the look and feel that users are familiar with from a desktop browser. When used as a Windows 8 app, Internet Explorer provides an interface designed with touch in mind. Users can interact with webpages just as they would an application by using features such as Flip Ahead.

Underneath the interface, Internet Explorer 10 uses a single rendering engine supporting many of the new web standards through CSS3 and HTML5. Internet Explorer 10 provides Adobe Flash within the platform and includes numerous new Group Policy settings to enable customization that IT pros need.

Windows 8 virtualization

"Consumerization of IT" is a growing term—one that many IT pros find frightening. They believe that it means putting the consumer in control of the devices they use at work and giving up the ability to manage and secure those devices. However, consumerization of IT really means that people want similar advantages at work that they have at home. In their personal lives, they have tremendous technologies available to them, and they want to use similar technologies at work to get more done in less time with increasing mobility. Of course, Microsoft believes that IT pros can embrace this trend while securing company resources and managing a work desktop environment.

Bring Your Own Device, or more simply BYOD, is a related idea that can help here. As IT organizations world-wide are optimizing their current infrastructure investments, they are considering how to enable support for BYOD. Once again, Microsoft believes that IT pros can embrace BYOD responsibly, and the company provides multiple tools and technologies that you can use to design just the right solution to fit users' unique requirements.

This chapter describes how Windows 8, Windows Server 2012, and the Microsoft Desktop Optimization Pack (MDOP) provide virtualization solutions that can enable BYOD. Windows Server 2012 enables you to more easily create a Virtual Desktop Infrastructure (VDI). Within MDOP, Microsoft Application Virtualization (App-V) and User Experience Virtualization (UE-V) help you provide users the same experience as they roam PCs. Of course, we provide multiple solutions for managing all of this, and you learned about those in Chapter 8, "Windows 8 management."

Virtual Desktop Infrastructure

VDI is an alternative desktop delivery model that can help you embrace BYOD. It gives users secure access to centrally managed desktops running in the data center. Using their personal devices, users can access their hosted desktops for work, while keeping their work and personal environments separate.

However, this only makes sense if you can host a full fidelity desktop experience and keep the corporate environment secure at the same time. Windows 8 supports this scenario, similar to Windows 7, by providing capabilities like a rich user experience, centralized management of apps and data, and enhanced security and compliance. But Windows 8 goes even further than Windows 7 did. For example, by tapping the remote access icon on employees' Windows 8 tablets, they can login and open a VDI session running in the data center with all their data, applications, and settings—as if they were working right in the office. Windows 8 can give them a high-fidelity experience by using RemoteFX, including:

- Touch
- 3D graphics

- Full multimedia experience
- USB device redirection

Microsoft VDI is powered by Windows Server 2012 Remote Desktop Services (RDS). It provides a single platform to deliver any type of hosted desktop, while RemoteFX provides a consistently rich user experience:

- **Rich experience** As previously mentioned, RemoteFX provides a rich multimedia experience by using a built-in software graphics processing unit (GPU) or hardware GPU on the server. Users can use tablets and most USB devices, because it offers true USB and multi-touch redirection. Users get a consistently rich performance over high latency, low bandwidth networks, including wide area networks (WANs).
- **Lower cost** FairShare ensures high system performance by distributing system resources dynamically. User profile disks provide the flexibility to deploy lower cost pooled- and session-based desktops while enabling users to personalize their experience. Last, it supports lower cost disk storage like Direct Attached Storage.
- **Streamlined management** A simplified wizard makes setting up VDI easier with automatic configuration of virtual machines (VMs). The included management console provides powerful administration of users, VMs, and sessions, without requiring additional tools. VMs and sessions can be intelligently patched through randomization and throttling of tasks, ensuring high system performance.

Installing and configuring RDS in Windows Server 2012 is very quick and easy by using the Add Roles and Features Wizard (Figure 11-1). In a lab environment, starting with a bare-metal server-class computer, you can install Windows Server 2012, install RDS, and deploy session- and VM-based desktops in less than an hour. You can find good lab guides instructions for various scenarios on TechNet in the article titled "Remote Desktop Services Overview" at <http://technet.microsoft.com/en-us/library/hh831447.aspx>. Another good resource for learning more about RDS in Windows Server 2012 is the book titled "Introducing Windows Server 2012," which you can download from <http://go.microsoft.com/fwlink/?LinkId=251464>.

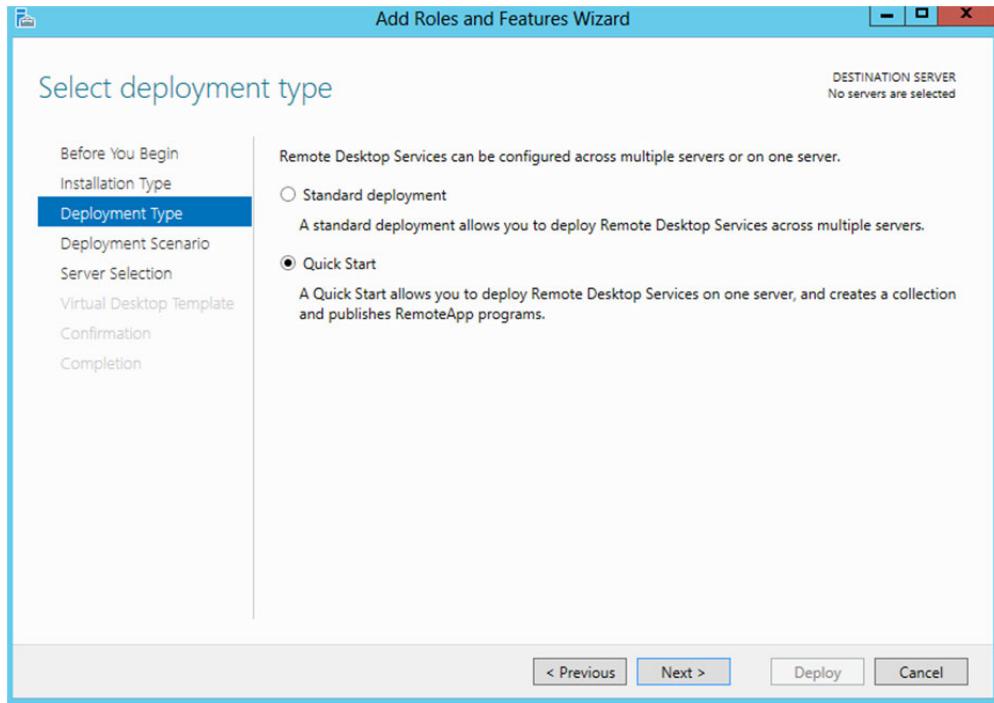


FIGURE 11-1. INSTALLING REMOTE DESKTOP SERVICES

Choosing the right VDI deployment

As this chapter already mentioned, RDS provides one platform to deliver desktops by using multiple methods, including:

- **Personal VMs** Personal VMs give users access to a dedicated, high-performance desktop over which they have full administrative control.
- **Pooled VMs** Pooled VMs give users access to high-performance desktops from connected devices. RDS assigns VMs on-demand from an existing pool to users. When they log off a VM, RDS returns the VM to the pool for another user.
- **Session-based desktops** Session-based desktops provide access to applications, data, and shared desktops that are centralized in the data center. This is the typical terminal services approach to virtualization a desktop.

NOTE With pooled VMs and session-based desktops, users can still personalize their experiences considerably. (Although they still cannot install applications.) Roaming user profiles and folder redirection are still available, but RDS adds support for user profile disks. With user profile disks enabled, RDS mounts a virtual hard disk containing the user's settings and data to their user profile folder

(C:\Users\Username). User profile disks persist between sessions. A great thing about user profile disks is that they are very simple to set up and manage.

RDS powers all three Microsoft VDI deployment methods, and they all have common benefits. They provide powerful administration features through the built-in management console (Figure 11-2). They offer a powerful and scalable virtualization platform, regardless of whether you are deploying session-based desktops, pooled VMs, or personal VMs. Lastly, they give users a consistently rich experience across LAN and WAN.

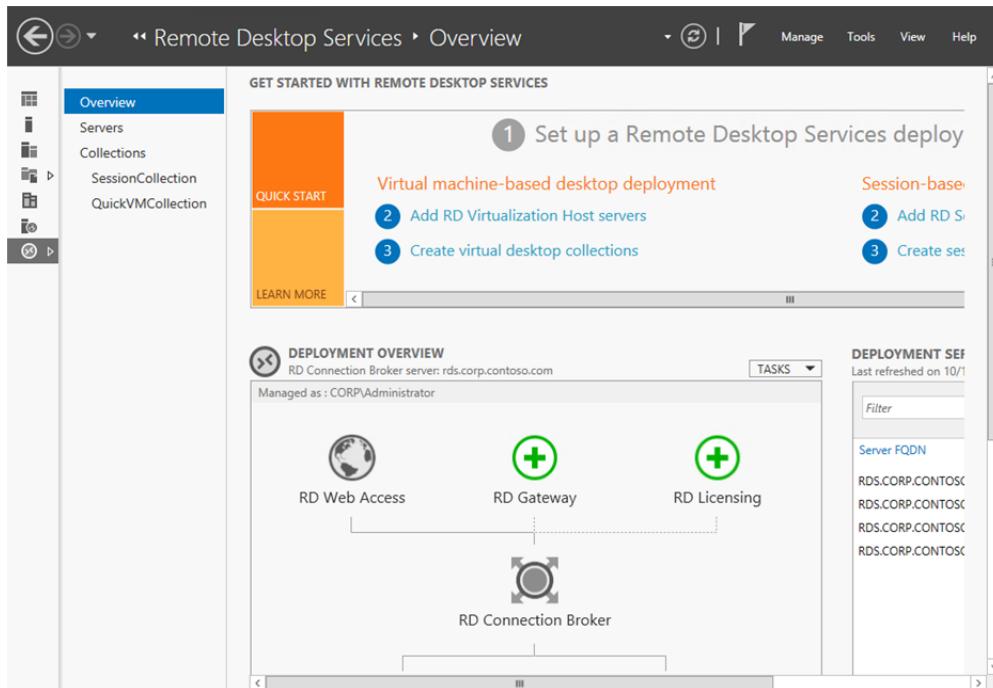


FIGURE 11-2. REMOTE DESKTOP SERVICES MANAGEMENT CONSOLE

Regardless of their common benefits, your choice depends on the following points, and Table 11-1 summarizes them for easy comparison:

- **Personalization** Do users need the ability to customize their desktops? If so, what level of customization do they need? With session-based desktops and pooled VMs, users have limited personalization capability with user profile disks (i.e., the ability to persist their data across different logins). However, they cannot keep their user-installed applications across logins. On personal VMs with administrator access, users can change any aspect of their desktop, including installing applications that persist across multiple logins.
- **Application compatibility** Session-based desktops share a common server operating system; therefore, any applications that are to be installed need to be compatible with Windows Server 2012. In both VM scenarios, however, Windows 8 is running in the VM. So application compatibility

is always higher for VMs. With personal VMs, users can install their own applications, but you decide what applications to install on pooled VMs. As a result, personal VMs provide the highest level of application compatibility across all three deployment methods.

- **User density** Because session-based desktops share a single server operating system, the number of users that a single server can accommodate is always going to be higher than either VM scenario. With pooled VMs, since user data is not stored locally (but can be stored on a separate user profile disk), the sizes are typically smaller than personal VMs. As a result, pooled VMs have slightly higher density. You can improve the density of pooled and personal VMs by using user state virtualization and application virtualization technologies on the VM, but they will always have a lower density than session-based desktops.
- **Image count** If maintaining a single image is important, the best way to achieve that goal is through session-based desktops or by deploying pooled VMs. In a session-based desktop, all users share a single server image. With pooled VMs, all users use a cloned copy of a single master image. Single image configurations are easier to manage and have lower costs in comparison to personal VMs, in which each user uses an individual image.
- **Cost** Because session-based VDI offers the highest densities and a single image, it is usually easier to manage, so it offers the lowest cost. Pooled VMs have the single image and management benefits of session-based VDI, but reduced densities and increased management effort means that they are more expensive to deploy. Personal VMs have the lowest density and highest management efforts, making them the most expensive deployment method. However, Windows Server 2012 helps organizations reduce overall costs for VDI with support for lower-cost storage (e.g., SMB and DAS), application virtualization, dynamic memory, and user profile disks.

Table 11-1 Choosing the Right VDI Deployment

	SESSION-BASED DESKTOP	POOLED VMS	PERSONAL VMS
Personalization	**	**	***
Application compatibility	**	***	***
Ease of management	***	**	*
Cost effectiveness	***	**	*

Complete desktop virtualization

Microsoft VDI can provide users a work desktop environment on multiple devices, but what about their applications, settings, and data? Microsoft has elegant solutions for both problems that work across all VDI deployment methods:

- **Application virtualization** Microsoft offers two technologies for providing users access to their applications across devices: RemoteApp and App-V. Each solves the problem in a different way and has different strengths.

- **User state virtualization** User state virtualization maintains users' data and settings across physical and virtual sessions. User state virtualization is not a new concept. You might have known it as IntelliMirror back in the Windows 2000 era. Modern technologies in the Windows 8 era provide many new exciting possibilities for virtualizing users' data and settings, however.

Application virtualization

Microsoft offers two solutions for application virtualization. The first is RemoteApp. RemoteApp is a Windows Server 2012 feature that is based on session virtualization. It enables you to provision applications remotely through RDS. Applications run on IT-managed hardware in the data center. By moving them from the endpoint to the data center, you can better manage the security and continuity of confidential data.

Users can easily access their remote applications from a variety of clients—through a webpage or an RDS client. Additionally, remote applications run side-by-side with local applications. For example, they run in their own resizable windows, can be dragged between multiple monitors, and have their own icons on the Start screen or taskbar.

The second solution is App-V. It enables you to meet user and IT needs by allowing users to work productively almost anywhere and by accelerating application deployment. Users can access their applications dynamically from almost anywhere on any authorized PC without first installing them or rebooting their PCs.

Virtual applications run in their own self-contained virtual environments on users' PCs. This eliminates application conflicts and allows you to reduce application-compatibility testing time, resulting in faster application deployment and updates. Virtual applications and user settings are preserved whether users are online or offline. Combined with user state virtualization, App-V provides a consistent experience and reliable access to applications and business data, regardless of users' locations or the PCs they are using.

You can deploy virtual application packages by using App-V servers, which stream virtual applications on demand to users' PCs and cache them locally so that they can be used offline. Another option is to use Configuration Manager to deploy, upgrade, and track usage of both physical and virtual applications in a single management experience. As a result, you can use existing processes, workflows, and infrastructures to deliver virtual applications to users.

App-V 5.0 offers a number of exciting enhancements over earlier versions, including:

- A new, easy-to-use web-based management interface that makes it easier to discover and use its features (see Figure 11-3). Also, it offers support for Windows PowerShell that enables you to script complex or repetitive tasks.
- Dynamic Configuration enables you to deliver a single virtual application package to users or PCs in a variety of configurations. Rather than creating separate packages for Marketing, Sales, Engineering, and so on; you can deploy and customize one package to all of the departments.
- Virtual Application Connection is a huge enhancement for App-V 5.0. With previous versions of App-V, you packaged applications and their dependencies together. When you had to update an add-in, though, you had to repackage the whole thing. Now you can package applications and add-ins separately, and connect them together when they need to interact. Updating individual

components is easier.

- Virtual Application Extension helps virtual applications to work like locally installed applications, so users don't run into unexpected user interface or functional changes due to virtualization. In fact, users might not even realize they are using virtual apps.

The screenshot shows the Microsoft Application Virtualization web-based management console. The left sidebar has tabs for 'PACKAGES' (which is selected), 'CONNECTION GROUPS', and other icons. The main area is titled 'PACKAGES' and shows a list of 25 applications in 6 packages. A search bar and a dropdown for filtering are at the top of the list. The list includes items like '7zip', 'adobe reader', 'notepad2', and several Microsoft Office components. One item, 'microsoft office 15 proplusvolume_visioprovolume_proj', is highlighted. Below the list, a detailed view for this package is shown, including its version (v0.0.0.0), a 'Package Description' field, and sections for 'APPLICATIONS' (listing Microsoft Excel, SkyDrive Pro Preview, InfoPath 15, Lync, Access, and Publisher), 'AD ACCESS' (CORP\Domain Computers), and 'CONNECTION GROUPS' (with an 'EDIT' button).

FIGURE 11-3. THE NEW APP-V 5.0 WEB-BASED MANAGEMENT CONSOLE

User state virtualization

With user state virtualization, user data and settings are centralized in the data center, eliminating the constraints of local storage and giving users the ability to access their data and settings from any PC. It makes backing up, securing, and managing the availability of users' data and settings easier for IT.

First, UE-V is a new part of MDOP that can roam users Windows and application experiences across devices—no matter how you deliver desktops or applications to them. It addresses challenges that users might face when logging onto multiple desktops at the same time, and it can roam experiences across physical PCs and session-based desktops. (It even roams settings between Windows 7 and Windows 8.) For example, UE-V can roam users' experience between a desktop PC running Windows 7, a tablet PC running Windows 8, and a session-based desktop running either operating system. They will have the same Windows and application experiences each time they log onto their desktop environments.

Additionally, UE-V synchronizes experiences intelligently. When users log onto their PCs, UE-V synchronizes only the settings required to get them to their desktop, instead of synchronizing an entire

profile. It also synchronizes Windows settings when users lock or unlock their PC. It synchronizes application settings when users open or close the application, and not during logon. The result of smart synchronization is that it makes logons faster when compared with roaming user profiles.

UE-V is also very flexible. It uses settings location templates to define the paths of settings and files that it should roam. Settings location templates help UE-V quickly and precisely identify settings instead of grabbing the entire profile. You can create custom settings location templates very easily for applications that UE-V doesn't support natively by using the UE-V Generator (Figure 11-4). For example, you can create custom settings location templates for the line-of-business (LOB) that your company deploys. All you do is run the UE-V Generator, launch the application for which you want to create a custom settings location template, and then close the application. UE-V will automatically discover where the application stores its settings, but you can refine the template by editing it in the UE-V Generator.

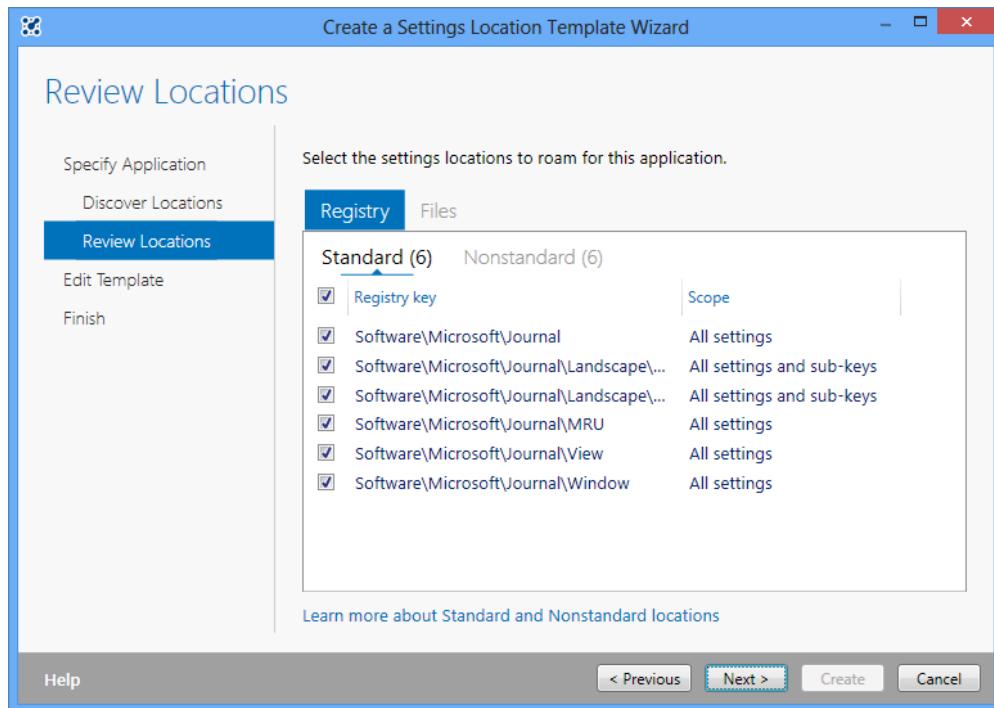


FIGURE 11-4. USER EXPERIENCE VIRTUALIZATION GENERATOR

For such a powerful and useful tool, it can be incredibly simple to deploy:

22. Create and share a folder to store users' experiences (i.e., settings store).
23. Install the UE-V agent on the desktops where you want to synchronize settings.
24. Configure the location of the settings store. You can do this on the installation command line, by configuring a home folder in Active Directory, or by using Group Policy. Group Policy is usually the most flexible way. (You can optionally configure the location of your custom settings location templates [that is, settings catalog]).

UE-V also supports Windows PowerShell. For example, you can rollback a single application's settings for a specific user by using Windows PowerShell.

You can learn more about UE-V at <http://www.microsoft.com/technet/mdop>.

While UE-V roams users settings, Folder Redirection compliments UE-V by centralizing user data folders (e.g., Documents, Pictures, and Videos) in the data center, making these folders accessible to users from any PC they log on to by using their domain credentials. Folder Redirection in Windows 8 works largely the same as it did in Windows 7. Folder Redirection is not new, but it's an essential part of Microsoft's user state virtualization story. Users have full-time access to their documents, pictures, videos, and other files from any PC.

For both technologies, Offline Files in Windows 8 helps ensure that users have access to their files even if they aren't connected to the network. To do so, Offline Files caches copies of the files and folders locally, then synchronizes changes the next time a connection is available. It works with UE-V and Folder Redirection to give users a consistent experience even when they are offline.

Client Hyper-V

On PCs running Windows 8, Client Hyper-V provides a robust virtual platform for developers and IT pros. It leverages the security, scale, and manageability of Windows 8 and Server Hyper-V platforms, providing developers with a robust development platform and IT pros with a convenient lab and test environment. Client Hyper-V uses the same VHD format as Hyper-V on the server.

Client Hyper-V in Windows 8 supports 32-bit and 64-bit operating systems in extremely large VM configurations (i.e., 32 virtual processors and 512GB of memory). It supports multiple forms of storage, including IDE, iSCSI, SMB, and USB flash drives. Also, Client Hyper-V takes advantage of the security and management enhancements of Windows 8, such as BitLocker Drive Encryption, Secure Boot, and so on.

You can install Client Hyper-V on each 64-bit device that has Second Level Address Translation (SLAT) enabled. Most modern PCs have support for SLAT. It supports as many as 12 monitors, most USB devices, wireless networks, and sleep and hibernate states. It also offers a full fidelity experience, including 3D, audio, multi-touch, and so on.

In short, Client Hyper-V can help you work more efficiently. It's not really a feature intended for user virtualization. Instead, it can help you avoid buying new hardware to setup lab and test environments. You can easily transfer VMs between Client and Server Hyper-V environments. Most IT pros will have a zero learning curve for using Client Hyper-V, because it is almost identical to Server Hyper-V.

Summary

Windows 8, Windows Server 2012, and MDOP are ushering in a new era for desktop virtualization. To take advantage of desktop virtualization, you should start by identifying the business problems you're trying to solve and then understanding how different desktop virtualization solutions can address your specific needs.

Microsoft recommends VDI for scenarios where the primary business requirements are giving users flexible access to their desktop environments from multiple managed or unmanaged devices, enhancing business security and compliance, and centralizing desktop management. VDI based on Windows Server 2012 and Windows 8 offers you one platform with a single experience based on RemoteFX, and three deployment choices: session-based desktops, pooled VMs, or personal VMs. Session-based VDI and pooled VMs are better suited to providing users access to centrally hosted LOB applications with high degrees of scalability. Personal VMs are more beneficial when users need a high level of personalization, operating-system isolation, and application compatibility.

NOTE When considering VDI, take into account potential investments required to expand the data center, as well as the network bandwidth required to give users rich, uninterrupted access to hosted virtual desktops. While most companies can benefit from VDI, not every desktop is a good candidate for it.

While VDI provides flexible access to a desktop environment, user state virtualization provides users a consistent experience across physical and virtual desktops. Microsoft's user state virtualization solution comprises UE-V, Folder Redirection, and Offline Files.

For more information, see the Microsoft Desktop Virtualization website at <http://www.microsoft.com/dv>.

What do you think of this book?

We want to hear from you!

To participate in a brief online survey, please visit:

microsoft.com/learning/booksurvey

Tell us how well this book meets your needs—what works effectively, and what we can do better. Your feedback will help us continually improve our books and learning resources for you.

Thank you in advance for your input!

Microsoft®
Press