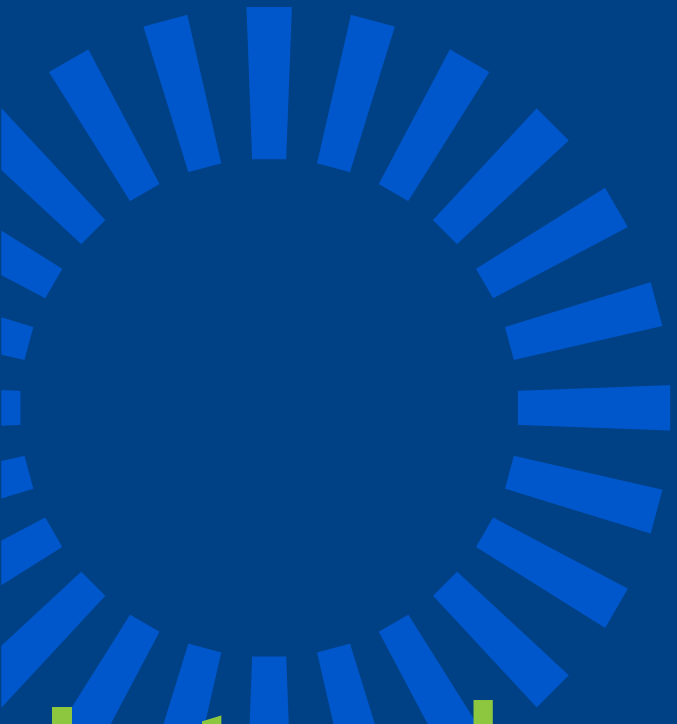


Microsoft

Introducing

Windows 8.1 for IT Professionals

Technical Overview

ED BOTT

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

Library of Congress Control Number: 2013949892
ISBN: 978-0-7356-8427-0

Acquisitions Editor: Anne Hamilton
Developmental Editor: Valerie Woolley
Project Editors: Valerie Woolley and Carol Dillingham
Editorial Production: Christian Holdener, S4Carlisle Publishing Services
Technical Reviewer: Randall Galloway
Copyeditor: Roger LeBlanc

Contents

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

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

microsoft.com/learning/booksurvey

Introduction

It's difficult to believe that Windows 8 was introduced only a year ago, and yet today its successor, Windows 8.1, is ready for widespread adoption. By Microsoft's standards, that is warp speed. And it is a tribute to the developers who designed and built Windows 8 and 8.1 that they have been able to sustain that pace and deliver such a polished product.

The Windows 8 product line represents a radical departure for Microsoft. A new user experience. A new app platform. New security features and new management tools. If you're an IT pro, you have the daunting job of helping your users adapt to the newness of Windows 8.1 while you try to stay at least one step ahead.

Although I've written in-depth guides to Windows in the past, this book is not one of those. Nor do I pretend to offer much in the way of opinions or review. Only you can decide whether and how and when to incorporate Windows 8.1 into your enterprise, based on your own organizational requirements.

My goal in this book is to help you on that upgrade path by presenting the facts and features about Windows 8.1 as clearly as I can. If you've been living in an environment built around a previous version of Windows, you have a lot to absorb in the transition to Windows 8.1. I've tried to lay out those facts in as neutral a fashion as possible, starting with an overview of the operating system, explaining the many changes to the user experience, and diving deep into deployment and management tools where it's necessary.

By design, this book focuses on things that are new, with a special emphasis on topics of interest to IT pros. So you might find fewer tips and tricks about the new user experience than your users want but more about management, deployment, and security—which ultimately is what matters to the long-term well-being of the company you work for.

This book is just an introduction, an overview. For more detailed information about the features and capabilities described in this book, I encourage you to become a regular visitor at the Springboard Series on TechNet: *http://www.microsoft.com/springboard*. Tell 'em Ed sent you.

Acknowledgments

I'd like to thank the many folks at Microsoft who contributed their in-depth knowledge of Windows technologies to this book: Craig Ashley, Roger Capriotti, Stella Chernyak, Adam Hall, Chris Hallum, Dustin Ingalls, Michael Niehaus,

and Fred Pullen. I'd also like to thank the good folks at Microsoft Press—Anne Hamilton, Martin DelRe, Carol Dillingham, and especially Valerie Woolley—for their efforts at making this project happen on very short notice.

About the author

Ed Bott is an award-winning technology journalist and author who has been writing about Microsoft technologies for more than two decades. He is the author of more than 25 books on Microsoft Windows and Office. You can find his most recent writing at The Ed Bott Report at ZDNet: *http://www.zdnet.com/blog/bott*.

Errata & book support

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed at:

http://aka.ms/IntroW8pt1/errata

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://aka.ms/tellpress

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

Stay in touch

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

CHAPTER 1

An overview of Windows 8.1

Windows 8.1, a free update to Windows 8 and Windows RT, arrives almost exactly a year after Windows 8's General Availability date. The final version was released to Microsoft's hardware partners in late August, ensuring that a new wave of hardware devices powered by Windows 8.1 would debut at the same time.

Historically, new versions of Windows have come out roughly every three years, with one or more service packs released in the interim to roll up security and reliability updates. So what's behind this sudden acceleration in the update process? Does the rapid-fire schedule and the incremental name change mean that Windows 8.1 is a minor update, equivalent to a service pack?

Not at all.

Windows 8.1 is, by any objective measure, a major release. It includes the historic changes that were introduced in Windows 8 and adds a very long list of improvements, refinements, and new features, big and small—more than enough to fill this book.

This faster update cycle isn't a one-time event—it's the new normal for Windows, a reflection of the modern, fast pace of change in the technologies that define our lives. There's no guarantee that future versions of Windows will arrive at the same annual pace, but it's certain that the every-three-years cycle of upgrades is history.

If you formed your initial opinions about Windows 8 a year ago and haven't been paying much attention lately, this release deserves your attention. Microsoft says it listened to feedback about Windows 8, from a wide range of sources. This update is an attempt to address the most important feedback items and move the platform forward.

In this chapter, I provide an overview of Windows 8.1 and its changes, with a special emphasis on features and capabilities of interest to IT pros.

What is Windows 8.1?

If you have any hands-on experience with Windows 8, you're already familiar with its basic underpinnings. The biggest, most obvious changes in the initial release of Windows 8 were a touch-enabled user experience designed for a new generation of mobile hardware and support for a new class of applications. But the initial release of Windows 8 included many changes under the hood as well, with significant gains in performance, reliability, security, and manageability over previous Windows versions.

In enterprise settings, the most important changes in Windows 8.1 involve features that might not be immediately obvious. Significant enhancements in security, for example, are important enough to warrant their own chapter (Chapter 4, "Security in Windows 8.1"). You'll also find improvements in management and virtualization features for client PCs, which are introduced in this overview and covered in more detail in later chapters.

To follow along with this book, I encourage you to get the Windows 8.1 Enterprise Evaluation, which is available as a free download from the Microsoft TechNet Evaluation Center (*http://technet.microsoft.com/en-US/evalcenter/*). The trial is good for 90 days, and it works on most modern hardware and in a virtual machine. It's the best way to get hands-on experience with the Windows 8.1 features and capabilities described in this book.

Support for new device types

Windows 8.1 has the same device requirements as Windows 8 and will run on most PC hardware that was originally designed for Windows Vista or Windows 7. That makes it possible to evaluate Windows 8.1 on a device that isn't currently in production use.

To see Windows 8.1 at its best, however, you really need to see it in action on a variety of devices, including modern hardware with touchscreens and processors and power-management subsystems engineered specifically to work with Windows 8.1. Widespread support for InstantGo, the new name for a feature previously called Connected Standby, for example, is just beginning to appear in the first wave of hardware for Windows 8.1.

The core design principles of Windows 8 are a direct response to a defining trend in modern technology: the movement to pervasive computing. Users are no longer tied to a desktop but instead can use multiple devices, choosing each device for its suitability to the task at hand. With proper management controls, these devices can switch easily between personal files, digital media, and enterprise resources. Combined with robust online services, the Windows 8 design allows people to remain productive regardless of where they are.

Windows 8 expanded the traditional definition of a Windows PC to include all sorts of mobile devices that are distinctly non-PC. These new device types include tablets that work with touch and stylus input as well as hybrid designs that include detachable keyboards to allow a single device to shift quickly between tablet and notebook form factors. Microsoft's original Surface Pro (Figure 1-1), with its integrated kickstand and click-on keyboard, is an excellent example of the latter category.

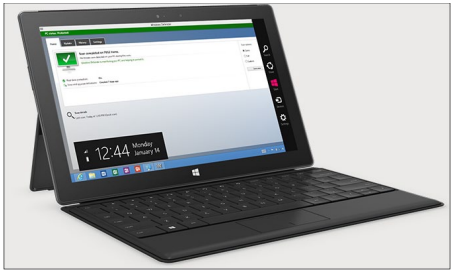


FIGURE 1-1 The Microsoft Surface Pro, released in 2013, was part of the first wave of hybrid devices released with Windows 8.

In Windows 8.1, the specifications for these devices, especially screen size and resolution, are relaxed, allowing an even wider array of mobile form factors. Previously, devices needed to support a minimum resolution of 1366 by 768 to be certified by Microsoft. In Windows 8.1, the minimum resolution drops to 1024 by 768. The revised specifications also allow new aspect ratios (4:3 and 16:10) that are more conducive to small devices used in portrait mode than the 16:9 ratio (typical in modern laptop and desktop displays) required for Windows 8.

The Acer Iconia W3-810, shown in Figure 1-2, was the first device available in this new category. Notice that the device in portrait orientation is more naturally suited to reading online content or ebooks.

Windows 8.1 adds built-in support for embedded wireless radio on mobile devices. This hardware configuration allows device makers to build thinner and lighter devices that should cost less than designs using external radios. It also provides power savings that translate into longer battery life. With mobile broadband enabled, you can use the built-in tethering feature to turn a Windows 8.1 PC or tablet into a personal Wi-Fi hotspot, allowing other devices to connect and access the Internet.

To work with mobile devices in an enterprise setting, you can take your choice of management tools, which are described in more detail in Chapter 11, "Managing mobile devices."

User experience

This new generation of hardware benefits greatly from the Windows 8 user experience. Touchscreens function as the primary form of input on a mobile device; on more traditional PC form factors, touch becomes an equal partner to the keyboard and mouse.

FIGURE 1-2 The Acer Iconia W3-810, with its 8.1-inch screen, was the first commercially available device designed for Windows 8.1.

Regardless of which input methods you use, the Windows 8.1 interface is consistent across devices. Windows 8.1 adds a variety of important changes to the Start screen and the desktop, including significant changes to support users who prefer a mouse and keyboard experience and who use desktop applications almost exclusively.

Here's a partial list of important changes in the Windows 8.1 user experience:

- Two new tile sizes on the Start screen are available, in addition to the two sizes used in Windows 8.
- Customizing the Start screen is much easier, and a new Apps view lets you quickly sort and arrange the list of installed apps and pinned websites.
- Enhancements to the Touch Keyboard make it possible to type faster and more accurately.

- A greatly expanded Search feature, accessible using the new keyboard shortcut Windows logo key+S, returns results from your device (programs, settings, and files) as well as from the Internet, via Bing. Figure 1-3 shows an example.

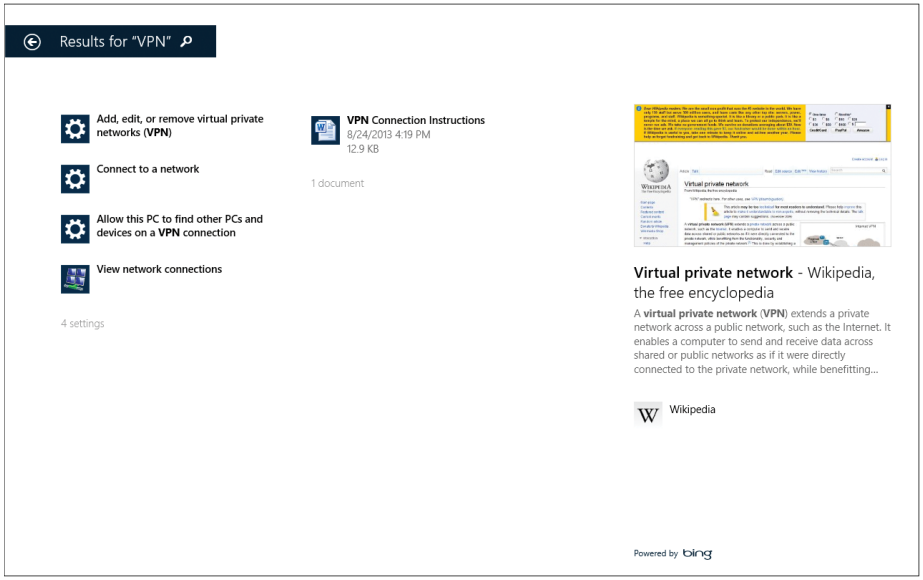


FIGURE 1-3 Integrated search, a new feature in Windows 8.1, returns settings, local documents, and webpages in a single scrolling results page.

- A new option allows you to configure Windows 8.1 to go directly to the desktop instead of the Start screen when you sign in.
- On the desktop, a Start hint appears on the taskbar, where the Windows 7 Start button is located.

You'll find more details about these and other user experience changes in Chapter 2, "The Windows 8.1 user experience."

User accounts and synchronization

One of the most significant changes in Windows 8 is support for a third user account type in addition to the familiar local and domain accounts. Signing in with a Microsoft account instead of a local account provides tightly integrated support for cloud-based file storage (every Microsoft account includes 7 GBs of free SkyDrive storage), along with easy synchronization of settings and apps between devices.

Windows 8.1 expands the list of settings that can be synchronized, including the layout of the Start screen, and it can automatically download and install Windows Store apps when you sign in with a Microsoft account on a new device. It also adds the ability to automatically back up settings that can't be synced. This feature makes it possible to roam easily between devices, with personal settings, apps, and browser tabs, history, and favorites available from

each device on which you sign in using a synced Microsoft account. One related feature: When you set up a new device, you're offered the option to clone the settings from a device you already own instead of using the default configuration.

On a device running Windows 8, synchronizing files to local storage from a SkyDrive account in the cloud requires the installation of a separate utility. In Windows 8.1, this feature is integrated into the operating system and for the first time is also compatible with Windows RT. The option to enable SkyDrive file synchronization is available when you first set up an account and can be toggled on or off through PC Settings. On a device with internet access, you can browse files and folders from SkyDrive (including live thumbnails for documents and images) without needing to download the full files.

In enterprise settings, you can link a Windows domain account with a Microsoft account to allow robust security and effective network management while still getting the benefits of synchronization with a Microsoft account, as shown in Figure 1-4.

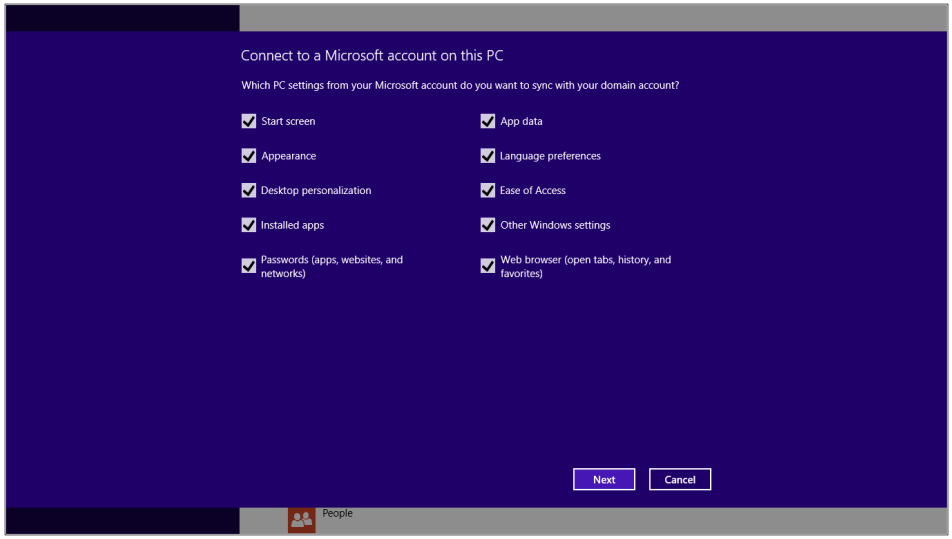


FIGURE 1-4 Connecting a domain account to a Microsoft account in Windows 8.1 allows fine-grained control over which settings sync between different devices.

New apps

Windows 8 includes support for virtually all desktop programs that are compatible with Windows 7. It also supports a new programming model designed for immersive, touch-enabled apps that are secure, reliable, and optimized for mobility. These apps are available through the Windows Store—a capability that can be extended in corporate environments to include your company's line-of-business apps.

For Windows 8.1, the Windows Store has been completely redesigned, with the goal of making it easier to discover useful apps. Windows 8.1 also includes a handful of new

"first party" (Microsoft-authored) apps as well as a complete refresh of the apps included with a default installation of Windows 8. (For more details on these apps and on the changes to the Windows Store, see Chapter 6, "Delivering Windows apps.")

Apps written for Windows 8.1 can access new capabilities, most notably more options for arranging apps side by side, on a single screen or multiple monitors. And a crucial addition in Windows 8.1 allows Windows 8 apps to download and install updates automatically, without requiring manual intervention or approval.

What's new for IT pros?

As an IT pro, your first concern is probably your users. How much training will they need? Which of your business applications will run problem-free, and which will require modification or replacement? How much effort will a wide-scale deployment require? And most important of all, can you keep your business data and your networks safe and available when they're needed?

Those questions become even more important to ask when users bring in personal devices—smartphones, tablets, and PCs—and expect those devices to shift between business apps and personal tasks with as little friction as possible. That flexibility has become so common in the modern era that the phenomenon has a name, "consumerization of IT." To users, the strategy is known by a more colorful name: Bring Your Own Device (BYOD).

Microsoft's approach to the consumerization of IT is to try to satisfy users and IT pros. For users, the goal is to provide familiar experiences on old and new devices. IT pros can choose from a corresponding assortment of enterprise-grade solutions to manage and secure those devices when they access a corporate network.

Security enhancements

The cat-and-mouse game between online criminals and computer security experts affects every popular software product. Microsoft's commitment to securing Windows is substantial, and it includes some groundbreaking advanced features. As part of the ongoing effort to make computing safer, Windows 8 introduced major new security features, and Windows 8.1 adds still more improvements.

One group of Windows 8 features leverages modern hardware to ensure that the boot process isn't compromised by rootkits and other aggressive types of malware. On devices equipped with the Unified Extensible Firmware Interface (UEFI), the Secure Boot process validates and ensures that startup files, including the OS loader, are trusted and properly signed, preventing the system from starting with an untrusted operating system. After the OS loader hands over control to Windows 8, two additional security features are available:

- **Trusted boot** This 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. Early Launch Antimalware (ELAM) drivers are initialized

before other third-party applications and kernel-mode drivers are allowed to start. This configuration prevents antimalware software from being tampered with and allows the operating system to identify and block attempts to tamper with the boot process.

- **Measured boot** On devices that include a Trusted Platform Module (TPM), Windows 8 can perform comprehensive chain-of-integrity measurements during the boot process and store those results securely in the TPM. On subsequent startups, the system measures the operating-system kernel components and all boot drivers, including third-party drivers. This information can be evaluated by a remote service to confirm that those key components have not been improperly modified and to further validate a computer's integrity before granting it access to resources, a process called *remote attestation*.

To block malicious software after the boot process is complete, Windows 8 includes two signature features:

- **Windows Defender** Previous Windows versions included a limited antispyware feature called Windows Defender. In Windows 8, the same name describes a full-featured antimalware program that is the successor to Microsoft Security Essentials. Windows Defender is unobtrusive in everyday use, has minimal impact on system resources, and updates both its signatures and the antimalware engine regularly. In Windows 8.1, for the first time Windows Defender includes network behavior monitoring. If you install a different antimalware solution, Windows Defender disables its real-time protection but remains available.
- **Windows SmartScreen** Windows SmartScreen is a safety feature that uses application reputation-based technologies to help protect Windows 8 users from malicious software. This browser-independent technology checks any new application before installation, blocking potentially high-risk applications that have not yet established a reputation. 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 user names, passwords, and billing data.

Windows 8.1 adds significant new security capabilities to that already robust feature list:

- **Improved Biometrics** All Windows 8.1 editions include end-to-end biometric capabilities that enable authenticating with your biometric identity anywhere in Windows (Windows sign-in, remote access, User Account Control, and so on). Windows 8.1 is optimized for fingerprint-based biometrics and includes a common fingerprint enrollment experience that works with various touch-based readers (an improvement over the previous generation of devices that often required multiple swipes to work properly). The new biometric framework includes *liveliness detection*, a feature that prevents spoofing of biometric data. Purchases in the Windows Store and Xbox Music and Video apps, as well as access to Windows Store apps and to functions within those apps, can be managed using biometric identity information.

- **Remote Business Data Removal (RBDR)** In Windows 8.1, administrators can mark and encrypt corporate content to distinguish it from ordinary user data. When the relationship between the organization and the user ends, the encrypted corporate data can be wiped on command using Exchange ActiveSync or management systems that support RBDR, such as Windows Intune. (This feature uses the OMA-DM protocol, support for which is new in Windows 8.1.) This capability requires implementation in the client application (Mail, for example) and in the server application (Exchange Server). The client application determines if the wipe simply makes the data inaccessible or actually deletes it.
- **Pervasive Device Encryption** Device encryption (previously available on Windows RT and Windows Phone 8 devices that use ARM processors) is now available in all editions of Windows. It is enabled out of the box and can be configured with additional BitLocker protection and management capability on the Pro and Enterprise editions. Devices that support the InstantGo feature (formerly known as Connected Standby) are automatically encrypted and protected when using a Microsoft account.

Organizations that need to manage encryption can easily add additional BitLocker protection options and manageability to these devices. On unmanaged Windows 8.1 devices, BitLocker Drive Encryption can be turned on by the user, with the recovery key saved to a Microsoft account, as shown in Figure 1-5.

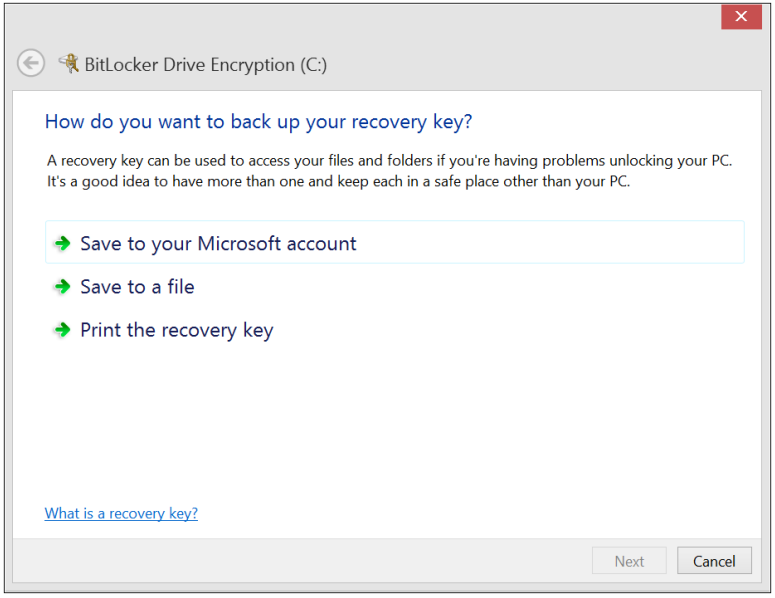


FIGURE 1-5 In previous Windows versions, provisioning BitLocker Drive Encryption required time and IT expertise. In Windows 8.1, the process is quick and streamlined so that an end user can do it.

BitLocker in Windows 8 supports encrypted drives, which are hard drives that come pre-encrypted from the manufacturer. On this type of storage device, 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 than in previous versions. BitLocker allows you to choose to encrypt only the used space on a disk instead of the entire disk. In this configuration, free space is encrypted when it's first used. This results in a faster, less disruptive encryption process so that enterprises can provision BitLocker quickly without an extended time commitment. In addition, the user experience is improved by allowing a standard user, one without administrative privileges, to reset the BitLocker PIN.

Chapter 4 provides more information about these security features.

Deployment and migration

Deploying Windows 8.1 in an organization is faster and easier than in 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). Note that this tool in Windows 8.1 does not support migrating user data from Windows XP or Windows Vista installations—with Windows XP reaching its end-of-support date in April 2014, you'll need to take this limitation into account.

For more information about planning and carrying out a Windows 8.1 deployment, see Chapter 3, "Deploying Windows 8.1."

On unmanaged devices, the Refresh Your PC and Reset Your PC options help streamline the recovery process. The refresh and reset options allow users to restore a damaged Windows 8 installation without having to make an appointment with the help desk. 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. Reset Your PC includes data-wiping options that make it possible for a user to transfer a device to another person without worrying about sensitive data.

The File History feature saves copies of data files to external storage at regular intervals, allowing users to recover quickly from inadvertent deletions or even wholesale drive corruption. This capability replaces the Previous Versions feature found in some prior editions of Windows.

For more information about Refresh Your PC and Reset Your PC, see Chapter 7, "Recovery options in Windows 8.1." That chapter also describes the Microsoft Diagnostics And Recovery Toolset, which provides more advanced troubleshooting and recovery tools that can be incorporated into Windows 8.1.

Manageability

This section describes the most important manageability features in Windows 8 and 8.1.

It's fitting to start with *Windows PowerShell 4.0*, which is an upgrade in Windows 8.1. This task-based, command-line environment and scripting language allows IT pros and network administrators to control and automate common Windows management tasks, on a local or remote PC or server. The Windows PowerShell Integrated Scripting Environment (ISE) makes it possible to author clear, maintainable, production-ready automation scripts. Some 1,200 built-in commands, called *cmdlets*, allow you to work (interactively or using scripts) with the file system, Windows Management Interface, and registry. The `Get-File hash` cmdlet, for example, is new in Windows PowerShell 4.0 and allows you to calculate a hash for any file. A key new feature in Windows 8.1 is Windows PowerShell Desired State Configuration, which enables the deployment and management of configuration data for software services and the environment in which these services run.

Other management tools available in Windows 8.1 include the following:

- **AppLocker** Available as part of Windows 8.1 Enterprise edition, this tool is a simple and flexible mechanism that allows you to specify exactly which apps are allowed to run on users' PCs. Using AppLocker, an administrator creates security policies through Group Policy that prevent apps from running unless they're on an approved list. The effect is to block potentially harmful apps. 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 you can more effectively control apps with less management.
- **Claim-based access control** This feature enables you to set up and manage usage policies for files, folders, and shared resources.

With Windows 8.1 and Windows Server 2012 R2, you can dynamically allow users access to the data they need based on the user's role in the company. Unlike security groups, which are defined statically, claim-based access control allows administrators 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.

Virtualization

Windows 8 is the first desktop version of Windows to include a robust, built-in virtualization platform. Client Hyper-V uses the same hypervisor found in Windows Server, allowing you to create virtual machines (VMs) capable of running 32-bit and 64-bit versions of Windows client and server operating systems. IT pros and developers can create robust test beds for evaluating and debugging software and services without adversely affecting a production environment.

Client Hyper-V leverages the security enhancements in Windows 8 and can be managed easily by existing IT tools, such as System Center. VMs can be migrated easily between a desktop PC running Windows 8 or 8.1 and a Hyper-V environment on Windows Server. Client Hyper-V requires Windows 8.1 Pro or Windows 8.1 Enterprise; it also requires that specific hardware features be available on the host device. For more details about the capabilities of Client Hyper-V, see Chapter 10, "Virtualization in Windows 8.1. "

In conjunction with Windows Server 2012, Windows 8.1 also supports an alternative form of virtualization: Virtual Desktop Infrastructure (VDI). Setting up a VDI environment is straightforward, thanks to a simple setup wizard. Managing a VDI environment is simple with administration, intelligent patching, and unified management capabilities.

The Remote Desktop client in Windows 8.1 allows users to connect to a virtual desktop across any type of network, either a local area network (LAN) or wide area network (WAN). Microsoft RemoteFX provides users with a rich desktop experience that compares favorably with a local desktop, including the ability to play multimedia, display 3D graphics, use USB peripherals, and provide input on touch-enabled devices. Features such as user-profile disks and Fair Share ensure high performance and flexibility, with support for lower-cost storage and sessions helping to reduce the cost of VDI. All these benefits are available across different types of VDI desktops (personal VM, pooled VM, or session-based desktops).

For more information about both of these features, see Chapter 10.

Under the hood

Some of the most valuable improvements in Windows 8 and 8.1 are those you can't see. Startup times are considerably faster than earlier Windows versions on identical hardware, for example, thanks to improvements in the operating system's fundamentals.

But there are some system-level changes you can see.

In addition to the Start screen and other prominent new features, some familiar and essential system applications get a major overhaul in Windows 8. These additions, which are included "in the box" with Windows 8.1, include Internet Explorer 11 (which gets its turn in the spotlight in Chapter 5). In addition, there's a significantly updated File Explorer (with the addition of the ribbon introduced in Microsoft Office) and an enhanced Task Manager, shown in Figure 1-6.

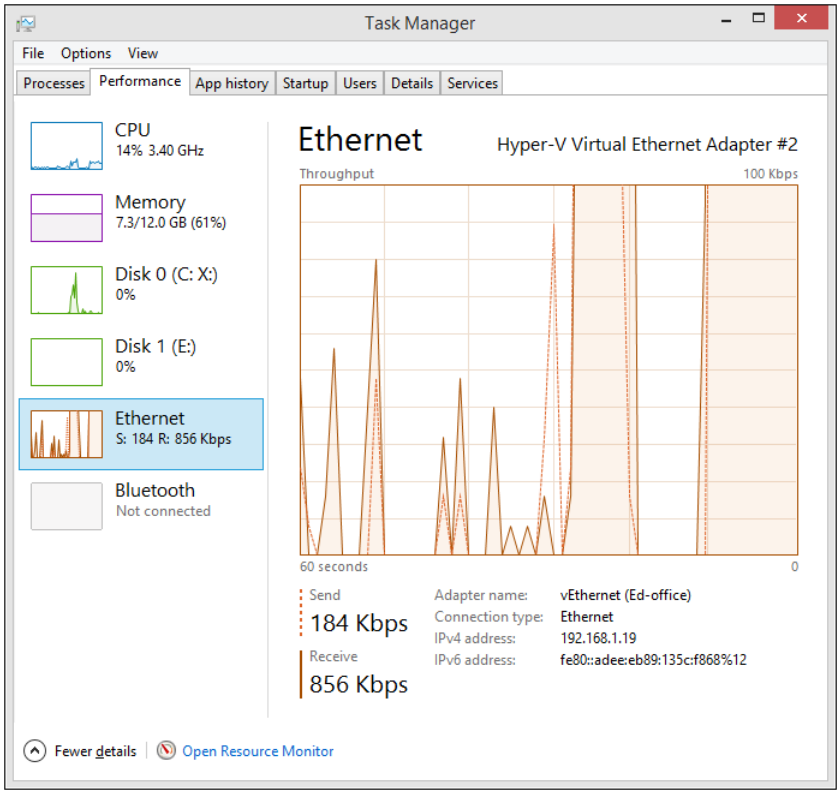


FIGURE 1-6 The enhanced Task Manager, introduced in Windows 8, displays real-time performance information and also offers tools for managing startup programs.

Windows 8.1 installation and upgrade options

Windows 8.1 shares the same hardware recommendations as those for Windows 8 (and for that matter, Windows 7). Table 1-1 and the following text list the hardware recommendations for Windows 8.1.

Table 1-1 Windows 8.1 hardware recommendations

Component	Recommendation
Processor	1 GHz or faster
Memory	32-bit PCs: 1 GB 64-bit PCs: 2 GBs
Hard disk space	32-bit PCs: 16 GBs 64-bit PCs: 20 GBs
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 multitouch.
- To access the Windows Store to download and run apps, you need an active Internet connection and a screen resolution of at least 1024 by 768.
- To snap apps, you need a screen resolution of at least 1024 by 768. Note that this resolution is lower than the requirement for Windows 8.

You have multiple options for installing Windows 8.1. Which of the following options you choose depends on your current environment and your deployment needs:

- **Update via the Windows Store** For most consumers, this is the preferred option. The update appears as an option in the Windows Store, which downloads in the background and installs relatively quickly.
- **Enterprise deployment tools** On enterprise networks, software distribution tools such as Configuration Manager can easily be employed to push Windows 8.1 out to users who need the update. I discuss these options in more detail in Chapter 3.
- **Integrated installation media** For devices that do not include an operating system, or where the goal is to completely replace the existing operating system, it's possible to install Windows 8.1 directly, using installation media that incorporates the update without requiring a separate upgrade. This installation media is available for download by Volume License customers from the Microsoft Volume Licensing Service Center. This media is also available on a subscribers-only basis for members of the Microsoft Developer Network (MSDN) and the Microsoft Partner Network.

CHAPTER 2

The Windows 8.1 user experience

Windows 8 introduced a completely new user experience that exists alongside the familiar Windows desktop. As feedback to Microsoft in the first year after the release of Windows 8 made clear, the transition to this new user experience caused some frustration. If you worked with the initial release of Windows 8, you probably experienced some of those issues firsthand.

In response to that feedback, Microsoft made three important changes in Windows 8.1:

- The Start screen is significantly refined, with a long list of enhancements that affect its appearance, functionality, and customizability.
- More parts of the operating system, especially PC Settings, are available in the new user experience. This lessens the need for potentially confusing transitions between traditional desktop controls and the new, touch-friendly experience.
- Windows 8.1 adds options to ease the transition between the Start screen and the desktop. These options include a setting to boot straight to the desktop without stopping at the Start screen, and the inclusion of a Start button at the left of the taskbar.

Even with these refinements, Windows 8.1 represents a big change from its predecessors, one that requires a thoughtful and thorough plan for training and orienting new users. This chapter describes what you need to know about the changes in the Windows 8.1 user experience so that you can make those plans intelligently. It also points to new customization options that IT pros might want to deploy to make the experience more comfortable for users who work primarily in a desktop environment.

Introducing the Windows 8.1 user experience

Windows 8 represents the most significant change to the Windows user experience in two decades, and Windows 8.1 adds another large helping of change. As an IT pro, you need to understand the core elements of the Windows 8.1 user experience so that you can effectively train and support users (and, of course, be more productive yourself). Armed with that knowledge, you can also decide how and where to deploy custom settings to keep those users productive with the apps they use most often.

The most important building block of the Windows 8.1 user experience is the Start screen, which appears by default after you sign in to a device running Windows 8.1. Figure 2-1 shows a customized Start screen containing multiple tiles in all four sizes supported in Windows 8.1.

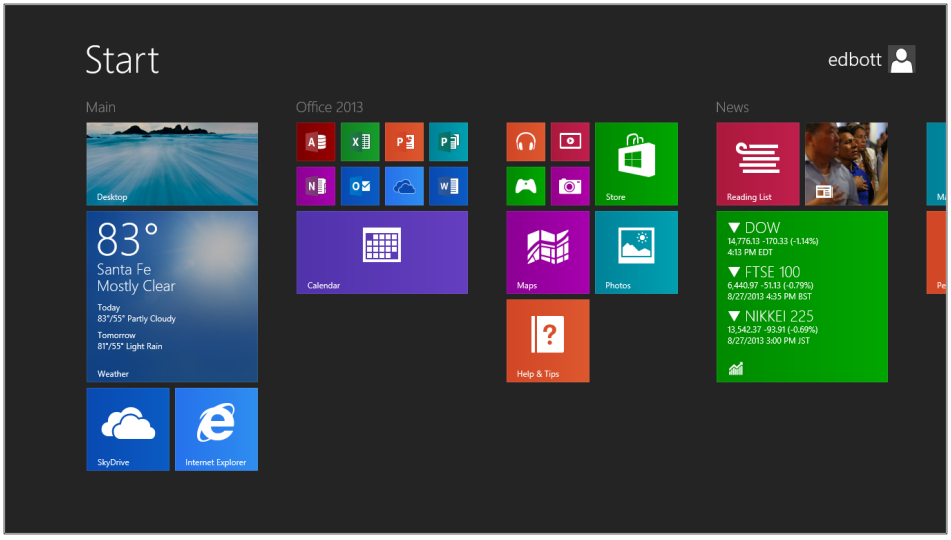


FIGURE 2-1 This Start screen has been customized, with a neutral background and tiles arranged into groups, some of them with names.

Each tile on the Start screen is a shortcut to an app, website, or location in File Explorer. Some are live tiles, with content that refreshes continuously to reflect underlying data for that app. The new Large tile size, shown in the Weather and Finance apps in Figure 2-1, allows for more information to appear in a live tile. Shortcuts for desktop programs, such as the eight small Office 2013 tiles shown in Figure 2-1, now pick up the dominant color of the program icon, just as they do in shortcuts on the taskbar.

When you're using a mouse or trackpad in a single-monitor configuration, each of the display's four corners has a specific function. The charms menu, which appears when you move the mouse pointer to the top or bottom corner on the right side, is essentially unchanged from Windows 8. (You'll notice one small usability change if you use Windows 8.1 on a large, high-resolution monitor—in that configuration, the charms appear close to the corner you activated, unlike in Windows 8, where the charms are always centered vertically.)

Tapping the Search charm (at the top of the charms menu) or pressing Windows logo key + S opens a search box, with the Everywhere scope selected by default.

In Windows 8.1, the Touch Keyboard supports swipe gestures you can use to enter a character without changing keyboard layouts. In the example shown in Figure 2-2, swiping up on any of the keys in the top row enters the number shown in gray on that key. (This feature is especially handy for entering passwords that mix letters and numbers.)

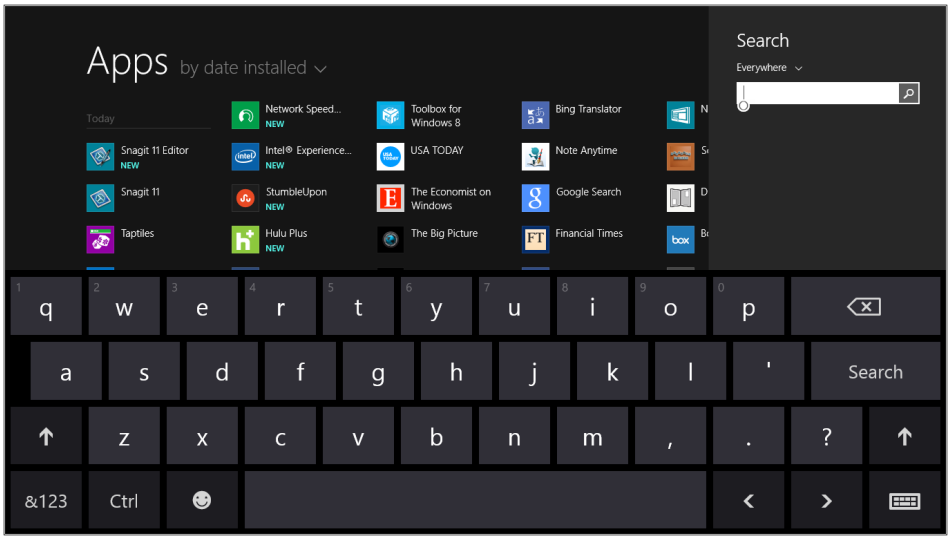


FIGURE 2-2 The gray characters in the top row of the Windows 8.1 Touch Keyboard indicate that you can swipe up to enter that character without changing layouts.

Apps view in Windows 8.1 is significantly more usable than its predecessor in Windows 8 (which was called All Apps), especially on PCs that lack a touchscreen.

To get to Apps view from Start on a touchscreen device, swipe up from the bottom. On a conventional PC, move the mouse toward the lower-left corner of the Start screen, where a down arrow conveniently appears in response to the mouse movement. (By contrast, Windows 8 requires that you right-click the Start screen and then click All Apps on the Command bar.)

Apps view includes entries for all installed Windows 8 apps and desktop programs. In a significant change from Windows 8, new programs are no longer pinned to Start as part of the installation process. Instead, they appear as entries here, with each app able to use additional metadata to indicate its category and when it was installed.

In Windows 8.1, you can sort Apps view using any of four options, as shown in Figure 2-3.

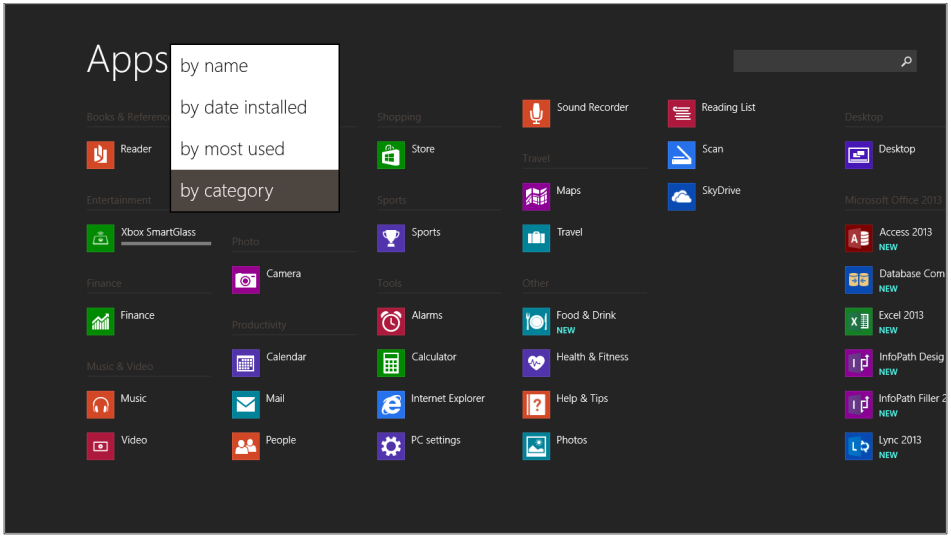


FIGURE 2-3 In Windows 8.1, you can choose one of four sort orders for Apps view. Notice the Search box in the upper-right corner.

In Windows 8, the touch-friendly PC Settings included a limited number of options. In Windows 8.1, the number of options is expanded tremendously, duplicating virtually all the options you would otherwise have to adjust using the desktop Control Panel. For example, Windows 8.1 includes the full range of settings for adjusting display resolution on a single-monitor or multi-monitor configuration, options that required a trip to the desktop Control Panel in Windows 8.

These usability improvements make it much easier to adjust settings on a touchscreen device, such as a tablet. Figure 2-4 shows the controls for the Quiet Hours feature, new in Windows 8.1, which you use to mute notifications during your normal sleeping time. It's especially useful for mobile devices like tablets that are kept on a nightstand or on a hotel room desk, in close proximity to sleeping quarters.

In enterprise settings, you're likely to manage updates centrally using Windows Server Update Services, Windows Intune, or a similar service. On unmanaged devices, Windows 8.1 offers a much more complete implementation of Windows Update in PC Settings, meaning there's no need to visit the desktop to install Optional Updates.

Another subtle usability improvement in Windows 8.1: Apps view includes a PC Settings shortcut that can be pinned to Start, eliminating the need to click a link at the bottom of the charms menu.

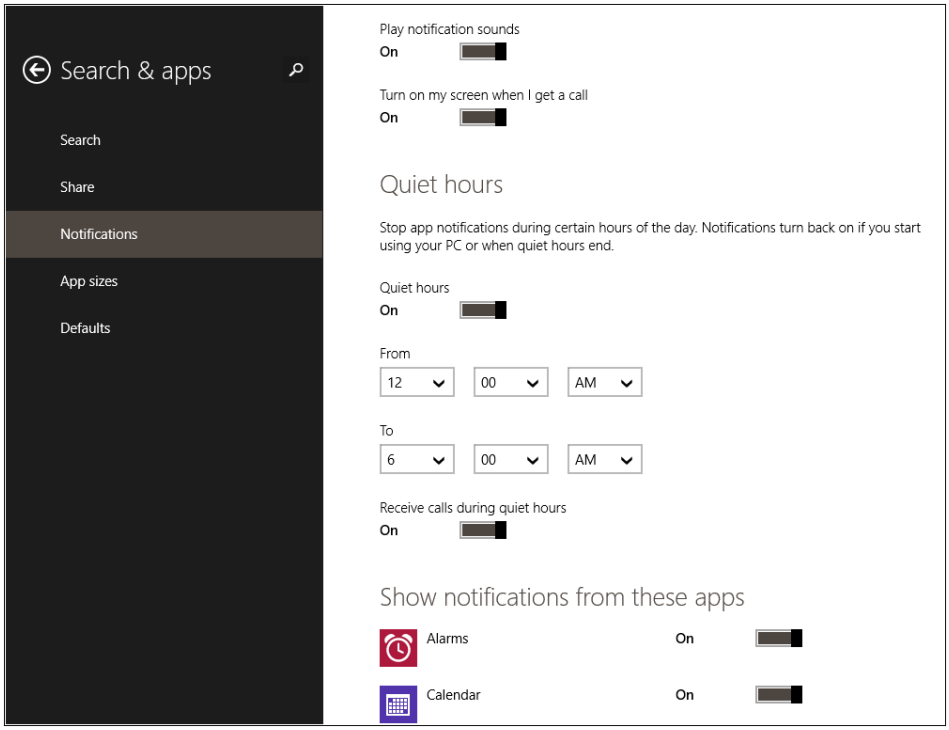


FIGURE 2-4 In Windows 8.1, the number of options available in PC Settings is greatly expanded, including most Control Panel options and new features like this fine-grained control over notifications.

Windows 8.1 includes significant improvements in multiple-monitor support. Most noteworthy is the new capability to run each display at a scaling that's appropriate to its size and resolution. In Windows 8 and earlier versions, the same scaling is used for all monitors, making for desktop apps that are too large or too small to work with comfortably. This difference is especially noticeable with the new breed of high-resolution mobile devices, such as touchscreen Ultrabooks with 13-inch displays running at full HD resolution, 1920 by 1080. If you connect that mobile display to a 24-inch full HD desktop monitor, Windows 8.1 automatically adjusts the scaling factors individually.

The capabilities of Windows 8 apps are both covered in Chapter 6, "Delivering Windows apps."

The Windows 8.1 desktop

Most of the elements that make up the desktop in Windows 8.1 should be familiar to anyone who has used Windows in the past decade. The taskbar and notification area work very much like their Windows 7 counterparts. Desktop programs work just as they did in Windows 7. Control Panel and File Explorer look a little different but essentially work the same as their

predecessors. The techniques for moving, arranging, and managing program windows on the desktop are the same.

The single difference is in the lower-left corner of the desktop, where Windows 8.1 displays the same Windows flag icon that occupies the center spot in the charms menu. That's a change from Windows 8, where a thumbnail of the Start screen appeared only when you moved the mouse to the lower-left corner. Figure 2-5 shows the differences between the Start hints in Windows 8.1 (left) and Windows 8 (right).

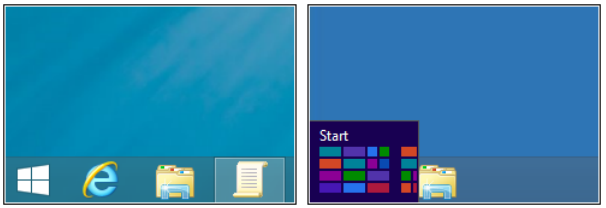


FIGURE 2-5 The Windows logo in Windows 8.1 (shown on the left) is always visible at the left edge of the taskbar; the corresponding element in Windows 8 is shown on the right.

Although this new element occupies the same spot as the Start button in Windows 7, it doesn't lead to a Start menu. Instead, it leads to the Start screen and Apps view.

For experienced users, it's worth pointing out that many of the Start menu's functions are available from the power menu shown in Figure 2-6, which appears when you right-click the Start hint. You can also summon this menu by pressing Windows key+X. (Even if you don't use that keyboard shortcut, it's worth remembering so that you can find this menu's Group Policy settings under the WinX heading.)

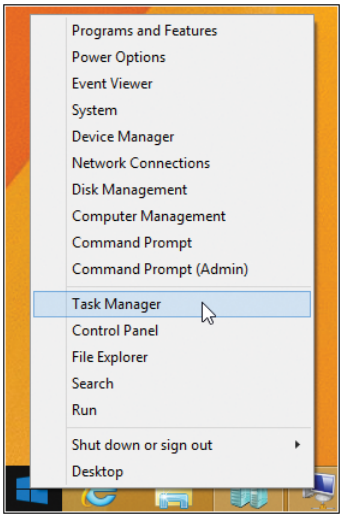


FIGURE 2-6 This power menu offers many options found on the Start menu in previous Windows versions. The Shut Down option near the bottom is new in Windows 8.1.

One common request in the feedback box for Windows 8 came from workers who want the system-level benefits of Windows but spend all their time in desktop apps and prefer to optimize the system for desktop usage.

Windows 8.1 addresses this feedback by adding a new Navigation tab in what was previously the Taskbar Properties dialog box. These new options are shown in Figure 2-7.

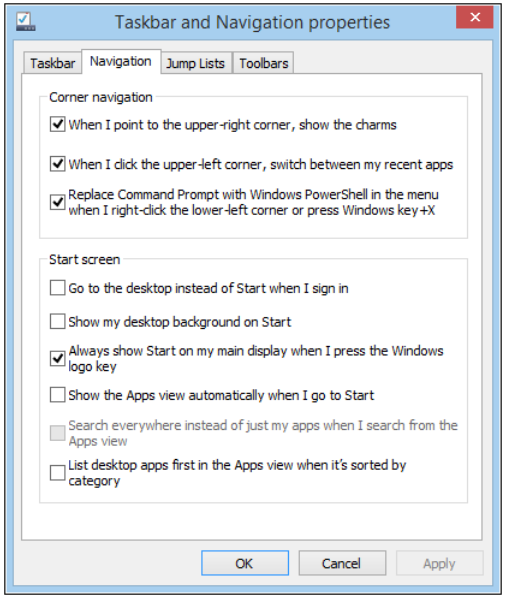


FIGURE 2-7 All the options on this tab are new in Windows 8.1 and are aimed at users who intend to use the desktop for most tasks.

The first two options under the Corner Navigation heading allow you to enable or disable the hot corners at the top of the display. These options are useful for users who want to avoid accidentally triggering the charms menu or the app-switching bar. If you clear one or both check boxes, the bottom corners continue to work, but moving the mouse pointer into one of the top corners has no effect. The third option, also enabled by default, sets Windows PowerShell as the default command-line environment on the Windows key+X menu. Clear this check box if you prefer to use the traditional Command Prompt (Cmd.exe) instead.

Options under the Start Screen heading allow you to configure the system so that it bypasses the Start screen for most common actions:

- **Go to the desktop instead of Start when I sign in** Select this option, which is cleared by default, to bypass the Start screen after signing in and go directly to the desktop.
- **Show my desktop background on Start** This setting replaces the normal background colors and patterns for the Start screen and uses the same background as the desktop. Changing the desktop background in Personalization options changes the background for the Start screen as well.

- **Always show Start on my main display when I press the Windows logo key** This option is useful on systems with multiple monitors.

The final three options in this section allow you to set up Apps view to match your preferences:

- **Show the Apps view automatically when I go to Start** With this option selected, clicking the Start hint on the taskbar or tapping the Windows logo key takes you to the Apps view, bypassing the Start screen and its tiles.
- **Search everywhere instead of just my apps when I search from the Apps view** This option is available only if the previous option is selected and changes the default search scope to Everywhere when you start typing from the Apps view.
- **List desktop apps first in the Apps view when it's sorted by category** This option flips the order of the two groups of apps in the Apps view, showing desktop apps on the left, with Windows Store apps arranged to the right of desktop apps. Again, this option is most useful for users who prefer desktop programs and want to see a comprehensive list of those apps instead of Windows Store apps.

Many options described in this section can be set by an administrator using Group Policy settings listed at the end of this chapter.

In Windows 8.1, as in Windows 8, there is no direct equivalent to the Start menu found in Windows 7 and previous versions. Its functions have been distributed to other parts of the user experience, and it's not possible to flip a switch or edit the registry to make such an option appear. In this area, one of the fundamental strengths of the Windows platform—its openness to extensions and add-ons—has prevailed. Various third-party utilities take advantage of the extensibility features in Windows and are available for those who want to re-create the Start menu in Windows 8.1. An Internet search for *Windows 8.1 start menu replacements* should turn up suitable candidates.

Customizing the Start screen

Creating a standard Windows 8.1 image for deployment involves the same set of actions as customizing an individual user experience. For a worker who primarily uses desktop apps, you might want to uninstall most of the Windows 8 apps included with a default installation and pin shortcuts to those desktop apps as tiles on the standard Start screen. That creates a clean, uncluttered experience where all available actions involve familiar program names.

To switch into customization mode, go to the Start screen or Apps view, swipe up from the bottom (or right-click), and then click Customize on the command bar. Even simpler, right-click a tile on the Start screen or an app in Apps view, or on a touchscreen press and hold a tile or app. That action selects the tile or app and switches into customization mode, where you can continue selecting apps and tiles. Figure 2-8 shows the Start screen in customization mode.

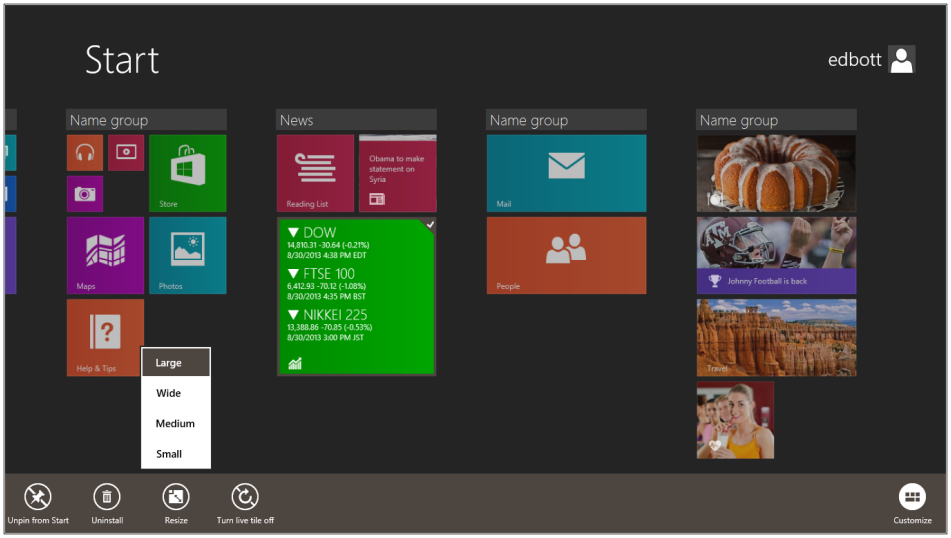


FIGURE 2-8 A check mark in the upper-right corner of a tile indicates that the tile has been selected for customization, with options available from the command bar at the bottom of the display.

Windows 8.1 allows you to perform most of the following actions on multiple selections, provided that the action you want to take applies:

- **Move tiles** In Windows 8.1, you can select multiple tiles and drag them to a new location on the Start screen.
- **Arrange tiles into groups, with or without names** Windows 8.1 uses the same basic procedure as Windows 8 for grouping tiles on the Start screen, with two improvements. First, you can select multiple tiles and move them at once, and second, you can name a group from the basic customization screen instead of having to zoom out.
- **Pin and unpin tiles for Windows apps** Any entry on the list of Windows 8 apps and desktop programs in Apps view can be pinned to the Start screen. To unpin one or more tiles, make a selection and then click Unpin From Start on the app bar at the bottom of the display.
- **Pin and unpin tiles for Internet Explorer shortcuts and File Explorer shortcuts** You can pin any website to Start from Internet Explorer.
- **Change the size of tiles on the Start screen** Windows 8.1 supports a total of four tile sizes. The Medium and Wide sizes were introduced in Windows 8 and remain unchanged. Windows 8.1 adds a new Small size, which allows eight Small tiles to fit in the same space as one Wide tile. The new Large tile, which is twice the height of a Wide tile, is available only for apps that are written to support it.
- **Turn live tiles on and off** For Windows apps that support the feature, you can click Turn Live Tile Off to disable automatic updates on the Start screen. Click Turn Live Tile On to re-enable the feature.

- **Uninstall Windows Store apps** You can uninstall most Microsoft-authored apps that are included with a default installation of Windows 8.1. A handful of items can't be uninstalled and must remain in Apps view, although they can be unpinned from Start; PC Settings, SkyDrive, Desktop, and Store are all in this group. Note that Windows desktop apps can be uninstalled only by using a desktop uninstaller, typically reached through the Programs And Features option in the desktop Control Panel.

Managing the user experience

Windows 8.1 includes a collection of new Group Policy options you can use to control the desktop experience in a standard configuration. These policy settings are found under the following two Group Policy paths:

- User Configuration\Administrative Templates\Windows Components\Edge UI
  - **Search, Share, Start, Devices, and Settings don't appear when the mouse is pointing to the upper-right corner of the screen** If you enable this policy setting, the charms (Search, Share, Start, Devices, and Settings) no longer appear when the mouse pointer is in the upper-right corner. They are available if the mouse is pointing to the lower-right corner.
  - **Do not show recent apps when the mouse is pointing to the upper-left corner of the screen** If you enable this policy setting, the user is no longer able to switch to recent apps using the thumbnails of the last app and currently running apps that appear in response to this mouse gesture. Touch gestures, keyboard shortcuts, and the Start screen still work for app-switching purposes.
  - **Prevent users from replacing the Command Prompt with Windows PowerShell in the menu they see when they right-click the lower-left corner or press the Windows logo key+X** This policy setting allows you to prevent users from replacing the Command Prompt with Windows PowerShell in the menu they see when they right-click the lower-left corner or press Windows logo key+X. If you enable this policy setting, the Command Prompt will always be listed in that menu, and users won't be able to replace it with Windows PowerShell. Users will still be able to access Windows PowerShell using other methods—from Apps view or from a shortcut, for example.
- User Configuration\Administrative Templates\Start Menu and Taskbar
  - **Go to the desktop instead of Start when signing in** If you enable this policy setting, users will always go to the desktop instead of the Start screen when they sign in.
  - **Show the Apps view automatically when the user goes to Start** If this policy is enabled, Apps view appears whenever the user goes to Start. Users are still able to switch between the Apps view and the Start screen.

- **Search just apps from the Apps view** This policy setting prevents the user from searching apps, files, and settings (and the Web if enabled) when searching from Apps view. This policy setting is ignored unless Apps view is set as the default view for Start.
- **List desktop apps first in the Apps view** With this policy setting enabled, desktop apps are listed first in the Apps view when apps are sorted by category. Other sorting options are available, and the user can choose to change their default sorting options.
- **Show Start on the display the user is using when they press the Windows logo key** This policy setting applies only when using multiple displays. With this policy setting enabled, the Start screen appears on the display the user is using when she presses the Windows logo key.

CHAPTER 3

Deploying Windows 8.1

Diving headfirst into a wide-scale deployment of Windows 8.1 without preparation isn't a recipe for success. On the contrary, deploying a new operating system requires careful planning and testing for application compatibility and hardware readiness.

The good news is that IT pros who've mastered the Windows 7 deployment tools have a head start on Windows 8.1, which uses the most recent generation of those proven tools and technologies. Automation and wizard-guided user interfaces reduce the effort and risk of deploying and managing operating systems and applications. This deployment 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.

This chapter focuses on the most recent updates to those deployment tools and technologies, updated for Windows 8.1. The biggest differences from their Windows 7 predecessors are support for features introduced in Windows 8, including Windows Store apps, changes in security models, and Windows To Go.

Windows 8.1 editions at a glance

With Windows 8, Microsoft simplified the number of editions available to consumers and businesses. Windows 8.1 continues that lineup, with no changes.

On mainstream PCs sold in the retail market to consumers, Windows 8.1 is commonly preinstalled. This edition includes all the core features of Windows 8.1, including the new touch-friendly user experience, improvements in security and reliability, and support for apps delivered through the Windows Store.

For deployment in enterprise environments, you'll want to choose one of the two Windows editions designed expressly for business use. In this book, I assume you deployed one of these editions. Here's what you'll find in each one:

- **Windows 8.1 Pro** This edition is available preinstalled on new PCs, as a retail package, and as an upgrade direct from Microsoft. It is also available via volume licensing.
- **Windows 8.1 Enterprise** This edition is available only to enterprise customers who purchase Software Assurance for Windows as part of a volume-license agreement.

Table 3-1 lists features that are not available in the consumer edition of Windows 8.1. Note that Windows 8.1 Enterprise edition is a complete superset of Windows 8.1 Pro.

TABLE 3-1 Features found only in Windows 8.1 business editions

Feature	Windows 8.1 Pro	Windows 8.1 Enterprise
BitLocker and BitLocker To Go	X	X
Encrypting File System	X	X
Boot from VHD	X	X
Client Hyper-V	X	X
Domain Join	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 8.1 app deployment		X
Start Screen Control		X

NOTE **The newest member of the Windows 8 family is Windows RT. It has a unique place in the product lineup and defies easy categorization. For a full discussion of what Windows RT can and can't do, especially in an enterprise setting, see Chapter 10, "Windows RT."**

Assessing compatibility

The most important step in planning a Windows 8.1 enterprise deployment is testing your business apps for compatibility with the new operating system. That can be a daunting task, because even a well-managed enterprise typically has several thousand apps that need to be tested for compatibility.

In general, you can expect most apps that ran properly under Windows 7 to work under Windows 8 and 8.1. However, some compatibility issues are possible because of changes to the Windows 8.1 feature set and tightened security.

IT pros planning for application-compatibility testing should at least glance through the "Windows and Windows Server Compatibility Cookbook," which is available from the Microsoft Download Center at *http://www.microsoft.com/en-us/download/details.aspx?id=27416*. This document, originally created while Windows 8 was available as a preview, is updated regularly and now covers changes in Windows 8.1 that could cause an application to break. Although this document is targeted primarily at developers working on the compatibility of their apps, it offers a glimpse into potential compatibility issues and mitigation strategies.

You will need empirical data from your environment to assess and mitigate applications that are currently in use. The Application Compatibility Toolkit (ACT) is included with the Windows Assessment and Deployment Kit, which is described later in this chapter. Using the most recent version of the toolkit, ACT 6.3, you can inventory and test applications, devices, and PCs for compatibility with Windows 8.1. 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 you discover in your organization.

Additional application-compatibility resources for IT pros include the following:

- Application Compatibility TechCenter on TechNet at *http://technet.microsoft.com/en-us/windows/aa905066*.
- Windows Compatibility Center at *http://www.microsoft.com/en-us/windows/compatibility/en-US/CompatCenter/Home*.

The following list describes common sources of compatibility issues for Windows 8 and 8.1, particularly when using an application originally designed for Windows XP:

- **User Account Control (UAC)** In Windows 8 and 8.1, 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 and 8.1, even when run by a user as administrator.

NOTE **Windows Store apps require that the User Account Control (UAC) feature be enabled. If you disable UAC, those apps will not run properly.**

- **Windows Resource Protection (WRP)** WRP is designed to protect key system files, folders, and registry keys from being modified or replaced by unauthorized applications or users, potentially affecting the stability of components and applications that ship with the operating system. Updates to protected resources are restricted to trusted installers (members of the TrustedInstaller group), such as Windows Servicing. Custom installations that try to replace files and registry settings covered by WRP will fail.
- **Internet Explorer Enhanced Protected Mode** In Windows 8.1, Internet Explorer 11 processes run in Enhanced Protected Mode, with greatly restricted privileges. This feature significantly reduces the ability of an attack to write, alter, or destroy data on the user's computer, or to install malicious code. This security feature can interfere with ActiveX controls and other script code that tries to modify objects running at a higher integrity level.
- **Deprecation** Any application that uses dynamic-link library (DLL) files, executable files, Component Object Model (COM) objects, registry keys, application programming interfaces (APIs), or other files that are deprecated in Windows 8 and Windows 8.1 might break.
- **Graphical Identification and Authentication (GINA) DLL** Prior to the release of Windows Vista, ISVs were able to modify authentication by installing a GINA DLL. The GINA DLL performed user identification and authentication functions. The authentication model used in Windows 8 and 8.1 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 and Windows 8.1 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. Windows 8.1 changes this behavior so that calls for a specific version will return the Windows 8 version number (6.2) rather than the Windows 8.1 version number (6.3). For applications that fail, 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 that use hard-coded paths based on those older paths might fail. You can mitigate these failures by using directory junctions or by replacing hard-coded paths with appropriate API calls to get folder locations.

Choosing a deployment strategy

Microsoft recommends a few targeted strategies for deploying Windows 8.1. These strategies range from manually configuring Windows 8.1 on a few computers to using automation tools and technologies to deploy the operating system to thousands of computers.

For client PCs that are already running Windows 8, an in-place upgrade is the fastest, simplest, and most reliable alternative, accomplished either by installing the Windows 8.1 update package or by refreshing the operating system. In either case, there's little worry about drivers or update states. Although this upgrade path requires some app compatibility testing, it should be a significantly more manageable project than a traditional operating system deployment.

For enterprises that want to deploy Windows 8.1 on new or existing hardware that isn't already running Windows 8, 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 8.1 on each client PC by using retail installation media and then manually configure each PC. This strategy is most appropriate for organizations with fewer than 100 client computers, no dedicated IT staff, and a small, unmanaged network.
- **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. Organizations that choose this strategy should have 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 for organizations that have a dedicated IT staff (ideally with prior deployment experience) and a managed network with 200–500 client computers.
- **Zero Touch, high-volume deployment** This strategy requires no interaction during deployment. The process is fully automated by using System Center Configuration Manager. Microsoft recommends this strategy if your IT organization includes experts in deployment, networking, and System Center Configuration Manager, and it has a managed network with 500 or more client computers.

Table 3-2 shows guidelines for choosing a strategy based on many factors, including the following:

- 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 3-2 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 experience
Windows license agreement	Retail	Retail or Software Assurance	Software Assurance	Enterprise Agreement
Number of client computers	<100	100–200	200–500	>500

	High Touch with Retail Media	High Touch with Standard Image	Lite Touch, High-Volume Deployment	Zero Touch, High-Volume Deployment
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 8.1 Tools	Retail media Windows Assessment And Deployment Kit (ADK)	Retail or volume-licensed (VL) media Windows ADK Microsoft Deployment Toolkit (MDT) 2013	VL media Windows ADK MDT 2013 Windows Deployment Services	VL media Windows ADK MDT 2013 Windows Deployment Services Configuration Manager

NOTE **The deployment strategies described involve traditional installations on a physical PC. An attractive alternative for some scenarios is desktop virtualization, which provides a way to deliver a working environment that users can access from any device. Desktop virtualization is powered by Remote Desktop Services (RDS), which is a server role in Windows Server 2012 and later. It provides a single platform to deliver any type of hosted desktop, and RemoteFX provides a consistently rich user experience. You can read more about these options in Chapter 9, "Virtualization in Windows 8.1."**

Windows Assessment and Deployment Kit

The Windows Assessment and Deployment Kit (Windows ADK) is a comprehensive collection of tools designed for use by original equipment manufacturers (OEMs) and IT pros. Depending on the task at hand, you can mix and match tools to accomplish specific goals ranging from identifying potential hardware and software issues to customizing and automating a large-scale Windows deployment.

The Windows ADK includes deployment tools that were previously available in the OEM Preinstallation Kit (OPK) and the Windows Automated Installation Kit (AIK). It also consolidates deployment tools that were previously available as separate downloads, such as the User State Migration Tool. You can download the Windows ADK from *http://www.microsoft.com/en-us/download/details.aspx?id=39982*.

In the remainder of this section, I discuss the individual tools that are part of the Windows ADK.

Application Compatibility Toolkit (ACT)

ACT 6.3, the most recent version of the toolkit, adds support for Windows 8.1 and is otherwise essentially unchanged from its predecessor, ACT 6.0. Its purpose is to provide compatibility information for deployment scenarios; unlike previous versions, ACT 6.x does not provide update information. The only way to get the most recent ACT version is to install it as part of the Windows ADK.

The runtime-analysis package gathers compatibility information. You install it on PCs running Windows 8.1 for compatibility testing. Application reports appear in Application Compatibility Manager (ACM). If multiple versions of an application are detected, the reports for that application are grouped together under a single parent entry.

Deployment and Imaging

The Deployment and Imaging component of the Windows ADK contains the tools you need to customize, deploy, and service Windows images. These tools can stand alone but are recommended for use with the Microsoft Deployment Toolkit 2013 and System Center Configuration Manager 2012 R2. The tools in the Deployment and Imaging component of the Windows ADK are required by both.

The Deployment and Imaging component includes the following components:

- **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 and PowerShell cmdlets to mount, and get information about, Windows image (.wim) files or virtual hard disk (VHD) files and to capture, split, and otherwise manage .wim files. DISM replaces the ImageX tool for image management.
- **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.

Two tools that were previously part of this group are now included in the operating system: The System Preparation (Sysprep) tool prepares a computer for delivery by configuring it to create a new computer security identifier (SID) when the computer is

restarted, removing user-specific and computer-specific settings and data that must not be copied to a destination computer. Windows Recovery Environment (Windows RE) is a recovery environment that can repair common causes of unbootable operating systems and is discussed in more detail in Chapter 7, "Recovery options in Windows 8.1."

The Deployment and Imaging tools include many other command-line tools that assist in the deployment and imaging of Windows, boot configuration, and Windows Preinstallation Environment 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 5.0 is based on the Windows 8.1 operating system, and it is available as a standalone product to customers who have the appropriate licensing agreement. It is an integrated component of many Windows technologies, including Windows Setup and Windows Deployment Services. Both MDT 2013 and System Center Configuration Manager rely on it.

Customized Windows PE images can be created using the tools provided with Windows PE. MDT 2013 and System Center 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 8.1. It captures the user state from the existing operating system and restores the user state to Windows 8.1. USMT can perform complex, repeatable migrations of user state data between a source and target installation of Windows. USMT is flexible enough to support migrations from a 32-bit Windows source to a 64-bit target. (The opposite path, from 64-bit to 32-bit, is not supported.)

If you're planning to use USMT as part of a Windows 8.1 deployment, you should be aware of one significant change. Earlier versions of USMT supported migrations with Windows 8 as the target and Windows XP or later running on the source computer. USMT version 6.3, which is included in the Windows ADK and is required for Windows 8.1 migrations, supports only Windows 7, 8, and 8.1 as both target and host operating systems. Windows XP and Windows Vista are not supported. As a workaround, Microsoft recommends using USMT version 5 to capture the user state from Windows XP and Vista; that state can then be restored to Windows 8.1 using USMT 6.3.

NOTE **An alternative to using USMT to migrate user state, especially if moving from Windows XP or Windows Vista to Windows 8.1, is to implement user state virtualization prior to deployment of the new operating system. Part of the Microsoft Desktop Optimization Pack (MDOP) for Software Assurance customers, User Experience Virtualization (UE-V) synchronizes Windows and application settings in a settings store (a simple but secure file share). The most recent version of UE-V 2 for Windows 8.1 allows storage of settings for Windows Store apps—a major change from the corresponding feature in Windows 8, which supported only desktop programs. Folder Redirection moves users' documents off the endpoint to a central location on the network. The combination of the two features allows users to move between devices while maintaining access to all apps and documents. For more information about user state virtualization, see the Microsoft Desktop Virtualization website at *http://www.microsoft.com/dv*.**

The USMT includes three command-line tools:

- **ScanState.exe** The ScanState.exe tool captures user state from the existing operating system (Windows 7, 8, or 8.1). You can store the captured user state on a removable drive or on a network shared folder. The ScanState.exe tool also can 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 was saved by the ScanState.exe tool.
- **UsmtUtils.exe** The UsmtUtils.exe tool performs functions related to user-state migration, such as extracting files from a compressed migration store or removing hard-link stores that cannot be otherwise deleted because of 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 2013 and SCCM rely on USMT to migrate user states. 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.

NOTE **Although USMT is the most appropriate choice for enterprise migrations, some businesses might opt for the simpler alternative of Windows Easy Transfer, a feature of Windows 8.1. 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 email settings between computers running Windows 7, 8, or 8.1. Note that the version of Windows Easy Transfer in Windows 8.1 does not support migrations from Windows XP or Windows Vista.**

Volume Activation Management Tool

The Volume Activation Management Tool (VAMT) enables 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 Multiple Activation Keys (MAKs) or Key Management Service (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 7, 8, or 8.1; Windows Server 2012; Windows Server 2012 R2; 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 you can use to select the events 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

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 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 ASC). 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 it 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.

Microsoft Deployment Toolkit

As described in the previous section, the Windows ADK is the fundamental collection of tools for configuring and deploying Windows 8.1. For the most part, these tools are rarely used directly on an individual basis. Instead, Microsoft provides various deployment options that are built on top of the Windows ADK.

The Microsoft Deployment Toolkit 2013 (MDT 2013) is the most recent version of one of the most popular toolsets built on top of the Windows ADK. It's more of a deployment framework. MDT 2013 helps manage deployment content in preparation for deployment, and then it collects and applies deployment information through wizards at the time of deployment. You can use MDT 2013 to control the level of information required at deployment time. You also can use MDT 2013 to perform fully automated deployments that require no deployment information at the time of deployment.

You can use MDT 2013 by itself or in conjunction with Configuration Manager. Although Configuration Manager is capable of deploying Windows 8.1 without using MDT 2013, Microsoft recommends that you use MDT 2013 with Configuration Manager to extend its capabilities with a well-tested deployment framework built to simplify this otherwise complicated set of tasks.

Microsoft Deployment Toolkit 2013

MDT 2013 helps automate the deployment and ongoing management of Windows 8.1 deployment content. It leverages and automates the tools in the Windows ADK to deploy Windows 8.1 and applications along with it. MDT 2013 provides wizards that help in the initial creation of deployment content.

MDT 2013 also reduces the effort and complexity of performing deployments. It performs highly automated deployments that allow you to control the type of information you want 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 you want 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 want 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 2013 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.

On the whole, if you're already familiar with previous MDT versions, you should feel comfortable with MDT 2013. It adds support for the Windows ADK, Windows 8.1, and new features like UDI. Basic tasks remain largely unchanged, however, including stocking deployment shares with applications, operating systems, packages, and device drivers; creating task sequences; and running the Windows Deployment Wizard. You can learn more about MDT 2013 on TechNet at *http://www.microsoft.com/deployment*.

System Center 2012 R2 Configuration Manager

As with MDT 2013, if you're familiar with operating-system deployment in earlier versions of System Center Configuration Manager, you should be comfortable with System Center 2012 R2 Configuration Manager. This release adds support for deploying and managing Windows 8.1 and Windows Server 2012 R2. It also adds the capability to create prestaged content files for task sequence content as well as virtual hard-disk management. See *http://technet.microsoft.com/en-us/library/gg682108.aspx#BKMK_OSDIntroWhatsNewR2* for a complete list of changes in this release.

As previously mentioned, Configuration Manager is more than capable of deploying Windows 8.1 without using MDT 2013. However, MDT 2013 adds an additional framework to Configuration Manager that helps you build a more flexible and intelligent deployment process for your organization. (With the latest updates, System 2012 Configuration Manager SP1 will also be able to deploy Windows 8.1, by using a Windows PE 5.0 boot image for deployment.)

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

Windows To Go

What if you could sit down at any PC, plug in a USB flash drive, and access a secure version of your desktop, complete with apps and files? That's the idea behind Windows To Go, a feature first made available with Windows 8 Enterprise. In Windows 8.1, it allows an administrator to create a portable Windows 8.1 Enterprise workspace on a high-performance flash drive. You can slip that bootable Windows To Go USB drive into your pocket and boot to it from any PC, completely bypassing the operating system installed on that PC. What you see when you sign in is your personal Windows account, exactly as you left it.

When creating the bootable Windows To Go workspace, you can use the default Windows 8.1 Enterprise image, or you can choose one of the custom images you created for deployment on desktops and laptops in the enterprise. The most important new Windows To Go feature in Windows 8.1 is support for the Windows Store, which allows you to roam to any number of machines, access the Windows Store, and use Windows Store apps in a Windows To Go workspace.

You're expected to shut down a Windows To Go session completely before removing the USB drive. If the drive is inadvertently disconnected, though, don't panic: You have a 60-second window to reinsert the drive and resume where you left off.

Who should use Windows To Go

Windows To Go is not suited for every organization and user. Choosing whether and when to provide users with Windows To Go workspaces should be based on your organization's needs. Following are some sample scenarios in which using Windows To Go could benefit an organization:

- **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 provisioned using standard provisioning tools, such as Configuration Manager. For users requiring network access, Windows To Go supports 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 gives the user access to company programs while not requiring the user to have company hardware. The device then can 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 between remote offices. Instead of requiring those employees to have a laptop, they 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 and then provided to employees. The initial boot to Windows To Go needs to be on-site for it to cache the employee's credentials for later access. After they are 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 minimizes the risk of the drive's deletion from Active Directory and retains its access privileges.**

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, because it is intended to seamlessly integrate with existing hardware. Aside from the following few exceptions, the Windows To Go workspace operates exactly like any other Windows platform:

- **Offline internal disks** When a user boots 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, as well as data leakage.
- **Absence of Trusted Platform Module (TPM)** Traditionally, BitLocker is implemented using the TPM-integrated hardware. Because the TPM is linked with a specific computer, it cannot be used with Windows To Go. This is because Windows To Go can be used on multiple computers. To replace TPM for a Windows To Go workspace, a preoperating-system boot password is used for security.
- **Disabled hibernation** Hibernation is disabled by default to maximize a workspace's ability to move between machines. If a machine is in hibernation, 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 is disabled because of the nonsensical nature of resetting to the manufacturer's standard for a computer while running Windows To Go.
- **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.

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. In general, hardware that is certified for use with Windows 7 or Windows 8.1 works well with Windows To Go. Table 3-3 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 3-3 Hardware requirements for Windows To Go

Item Required	Description
USB port	Must have a USB 2.0 port or greater. A USB 3.0 port offers improved performance. ***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 GBs 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 3-3, corresponding Windows To Go architectures must be matched with the host PC firmware type and processor architecture. Table 3-3 describes the requirements for each.

TABLE 3-4 BIOS compatibility for Windows To Go

Host PC Firmware	Host PC Architecture	CompatIble 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

Management and security

Because a Windows To Go workspace, from a user aspect, is identical to a standard Windows 8.1 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 8.1, 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 8.1. The following features describe the profile data-management options for user profiles and data files 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 it is 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 requires DirectAccess to be enabled.
- **Offline Files** Makes network files available to users when DirectAccess is not configured or the enterprise network is not accessible. After 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 VPN. Windows To Go allows users to take advantage of these advanced Windows 8.1 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 9.

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 joined easily to a domain in 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 "Offline Domain Join (Djoin.exe) Step-by-Step Guide" at *http://technet.microsoft.com/en-us/library/jj574150.aspx*.**

Group Policy management

Group Policy management of Windows To Go is nearly identical to what is available for typical machine installations of Windows 8.1. In addition to the Windows 8.1 policies, there is added functionality specifically for Windows To Go. The unique Windows To Go Group Policy settings can be found in \Computer Configuration\Policies\Administrative Templates\ Windows Components\Portable Operating System\ in the Group Policy Management Editor.

Enabling BitLocker security

Because most Windows To Go users will be using their USB drives 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 if the drive is lost or stolen. Unlike the BitLocker available on standard devices that 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 or Windows PowerShell, or you can encrypt it later by using the BitLocker user interface.

Windows To Go workspace creation

When creating a Windows To Go workspace, you can use any existing Windows 8.1 installation image, including the generic image available with volume-licensed media or a custom image that has been generalized using the Sysprep tool and is in Windows Imaging Format (WIM). If an image does not exist, one needs to be created before a Windows To Go drive can be created. After a WIM file is created, a Windows To Go workspace can be provisioned two ways:

- **Windows To Go Creator Wizard** The Windows To Go Creator Wizard (shown in Figure 3-1) is a GUI application that provisions a Windows To Go drive. Available only in Windows 8.1 Enterprise, this wizard automates most of the creation process by prompting only for a few pieces of information. To access the Windows To Go Creator wizard, press Windows key+W and type **Windows To Go** in the search box.
- **PowerShell** You can automate the creation of a Windows To Go workspace by using Windows PowerShell. PowerShell must be run with administrative privileges in order to create a Windows To Go drive.

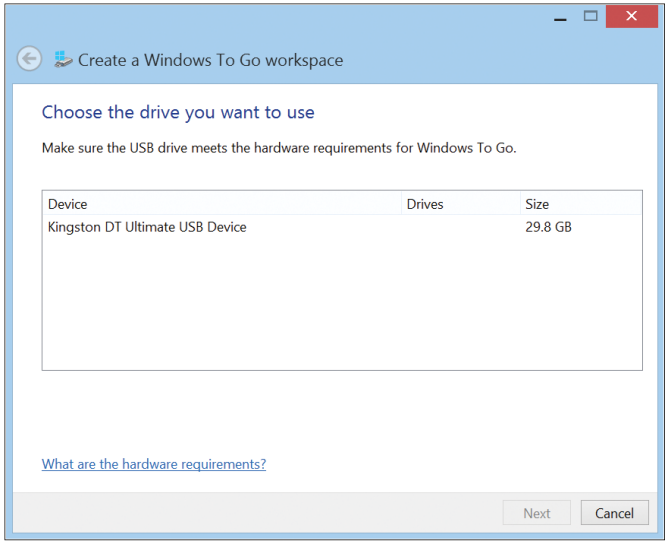


FIGURE 3-1 Windows To Go Creator Wizard.

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 approach 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 run.**

After the Windows To Go workspace is created and configured, you are ready to boot from the USB drive on any computer that meets the minimum hardware requirements. A computer can be enabled to always boot from the USB, to allow but not prioritize USB boots, or to set boot options in Windows 7 or later.

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

CHAPTER 4

Security in Windows 8.1

Computer security is a cat-and-mouse game, with occasionally expensive and even deadly stakes. The players include criminals and spies and the computer scientists tasked with fighting them. At Microsoft, security is a top priority, and it has been a core principle since the Trustworthy Computing initiative began formally in 2002. Since then, each new version of Windows has been progressively more effective at protecting users from common and not-so-common threats.

Windows 8 introduced significant security enhancements, and Windows 8.1 raises the bar still higher.

How effective are these changes? Microsoft's security researchers have found that Windows 8 is significantly more effective than its predecessors at preventing malware infections. With Windows 7, they say, you're several times more likely to experience a malware attack compared to the same system running Windows 8. Using Windows XP you are even more likely to be a malware victim as you are with Windows 8, according to those researchers. The security improvements in Windows 8.1 should make these advantages even more pronounced. (For a detailed report containing up-to-date statistics, see the most recent Microsoft Security Intelligence Report at *http://www.microsoft.com/security/sir/*.)

Because of the ever-changing threat landscape, security is best thought of as a process, in which Windows 8.1 is one layer among several. Most casual observers see the obvious manifestations of security, in the form of features that have a visible set of controls, such as Windows Defender and the Windows Firewall. Windows 8.1 also enables crucial features in other security layers that you can't see, specifically hardware-based protection, which operates before Windows loads, and network-based security capabilities that can be defined and enforced by administrators using Group Policy and management tools.

Assessing the threat landscape

In the movies and in popular fiction, computer security topics usually focus on flashy viruses and hackers who can break into any system in minutes. Here in the real world, the threat landscape certainly includes malware and intrusions, but it also includes data breaches, unauthorized access to local and network resources, and physical theft.

The threat landscape and attacker motivations have evolved over the past two decades. In the past, hackers were motivated by personal fame and bragging rights. Today, cyber attacks have become big business, ranging from malware and phishing attacks that cast a wide net to targeted attacks that aim to exploit weaknesses in a specific company or government agency. And, of course, just about every nation on earth is developing cyber-espionage capabilities.

In general, attacks can occur at any layer of the stack. Malicious agents can lurk in software, in seemingly innocent web pages, or in packets on a network. They can target vulnerabilities in the operating system or in popular applications. Some of the most successful attacks in recent years have come through so-called *social engineering*, where a would-be attacker pretends to be something he isn't—forging the sender's name on an email message to convince its recipient to open a booby-trapped attachment, for example.

New hardware, new security capabilities

The first layer of protection for a Windows 8.1 device starts with the hardware itself, with three key features. Although Windows 8.1 security doesn't depend on these features, you'll get best results when they are present:

- **Unified Extensible Firmware Interface (UEFI)** After 30 years, the PC BIOS has finally been retired. Its replacement is UEFI, a firmware interface that takes over the functions traditionally performed by the BIOS. UEFI plays a critical role in security with Windows 8.1. It offers the Secure Boot capability and support for self-encrypted drives, for example. (I'll say more about both those features later in this chapter.) Although Windows 8.1 can run on systems that use a legacy BIOS, many of its new security features require UEFI. You're likely to find a wide selection of UEFI-equipped devices, because UEFI is a requirement for an original equipment manufacturer (OEM) to certify a system or hardware device for Windows 8 or 8.1 under the Windows Hardware Certification Program (formerly known as the Windows Logo program).
- **Trusted Platform Module (TPM)** A TPM is a hardware chip (sometimes included as part of another component, such as a network card) that supports high-grade encryption and prevents tampering with or unauthorized export of certificates and encryption keys. The TPM can perform cryptographic operations and store keys for BitLocker volumes and virtual smartcards. A TPM can also digitally sign data, using a private key that software can't access. The presence of a TPM enables several key Windows 8.1 features, including BitLocker drive encryption, virtual smartcards, and Measured Boot. I discuss all these features later in this chapter.

- **Improved support for biometric devices** The capability to identify yourself to a device or a network using biometric information such as a fingerprint is a proven way to overcome the inherent flaws of passwords. Windows has had biometrics support since Windows XP; Windows 8.1 significantly improves the experience of setting up and using a fingerprint reader. The biometric technology in Windows 8.1 is designed to be extremely effective at resisting attempts to spoof its protection, unlike simpler technology found in some popular consumer-focused devices.

Securing the boot process

The most aggressive forms of malware try to insert themselves into the boot process as early as possible so that they can take control of the system early and prevent antimalware software from doing its job. This type of malicious code is often called a *rootkit* (or *bootkit*). The best way to avoid having to deal with it is to secure the boot process so that it's protected from the very start.

Windows 8.1 supports multiple layers of boot protection, some of which are available only if specific types of hardware are installed. Figure 4-1 shows how these features are integrated into the boot process.

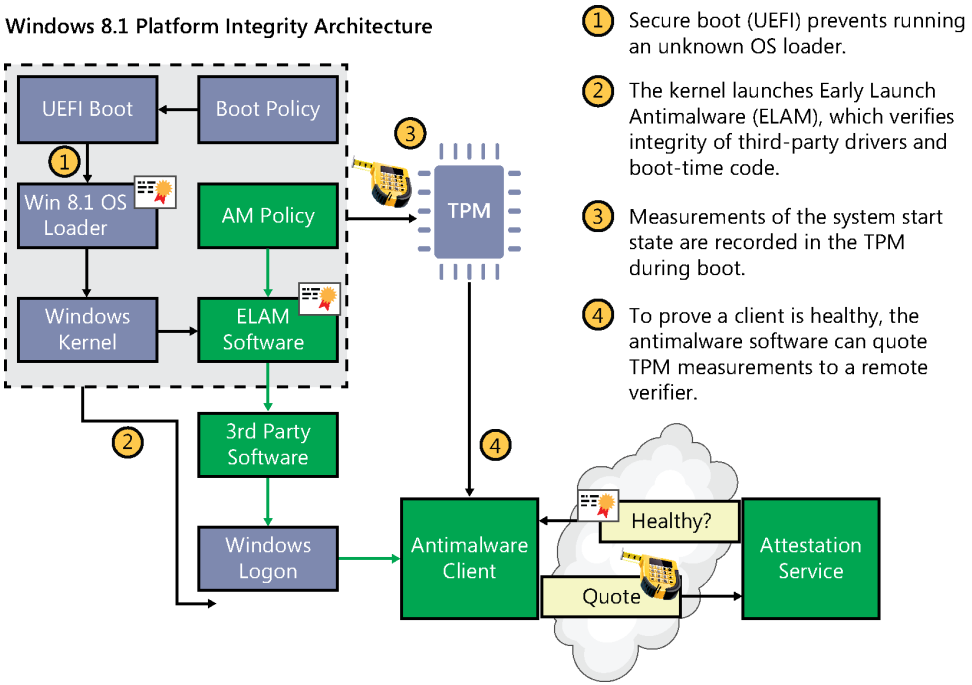


FIGURE 4-1 New security features in Windows 8.1 and compatible hardware help prevent malicious software from tampering with the boot process.

Here is a description of the elements shown in Figure 4-1:

- **Secure Boot** The most basic protection is the Secure Boot feature, which is a standard part of the UEFI architecture. (It's defined in Chapter 27 of the UEFI 2.3.1 specification.) On a PC with a conventional BIOS, anyone who can take control of the boot process can boot using an alternative OS loader, potentially gaining access to system resources. When Secure Boot is enabled, you can boot using only an OS loader that's signed using a certificate stored in the UEFI firmware. Naturally, the Microsoft certificate used to digitally sign the Windows 8.1 OS loader is in that store, allowing the UEFI firmware to validate the certificate as part of its security policy. All devices that are certified for Windows 8.1 under the Windows Hardware Certification Program.
- **Early Launch Antimalware (ELAM)** Antimalware software that's compatible with the advanced security features in Windows 8 and 8.1 can be certified and signed by Microsoft. Windows Defender, the antimalware software that is included with Windows 8.1, supports this feature; it can be replaced with a third-party solution if that's what your organization prefers. These signed drivers are loaded before any other third-party drivers or applications, allowing the antimalware software to detect and block any attempts to tamper with the boot process by trying to load unsigned or untrusted code.
- **Trusted Boot** This feature verifies that all Windows boot components have integrity and can be trusted. The bootloader verifies the digital signature of the kernel before loading it. The kernel, in turn, verifies every other component of the Windows startup process, including the boot drivers, startup files, and the ELAM component.
- **Measured Boot** This feature requires the presence of a TPM on the Windows 8.1 device. This feature takes measurements of the UEFI firmware and each of the Windows and antimalware components as they load during the boot process. When these measurements are complete, their values are digitally signed and stored securely in the TPM and cannot be changed unless the system is reset. During each subsequent boot, the same components are measured, allowing the current values to be compared with those in the TPM.

For additional security, the values recorded during Measured Boot can be signed and transmitted to a remote server, which can then perform the comparison. This process, called *remote attestation*, allows the server to verify that the Windows client is secure. After this analysis is complete, the server can issue a signed Claim ticket, which can then be used to determine whether that device should be granted access to a resource such as a corporate server.

The most common use of Claim tickets is in the Windows 8 and Windows 8.1 Dynamic Access Control (DAC) feature, which uses the claims-based infrastructure to control access to File Server and SharePoint resources.

Securing the sign-in process

Passwords are, to put it mildly, notoriously ineffective at protecting devices and data. They're too easily stolen: on the client by keylogging software or phishing attempts, and on the server by data breaches that give intruders access to large sets of user names and passwords. And because humans frequently reuse those passwords, a breach on one site can lead to intrusions on other sites that use the same credentials.

That's why, increasingly, enterprises insist on a second, physical factor for authentication. Windows 8.1 adds significant support for two forms of hardware-based authentication.

The first is biometric authentication—specifically, using a fingerprint reader as a form of authentication. Windows offered support for fingerprint readers in previous versions, but the overall experience for crucial activities like enrolling fingerprints has historically required third-party software with its own user experience. Windows 8.1, for the first time, manages the fingerprint-authentication process end to end, with a consistent enrollment process. Figure 4-2 shows the modern fingerprint enrollment experience.

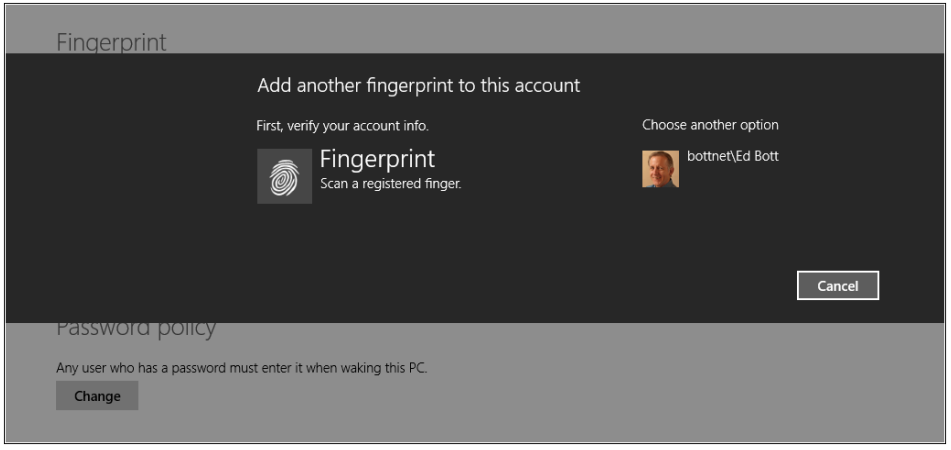


FIGURE 4-2 Windows 8.1 offers end-to-end functionality for fingerprint authentication, with drivers and an enrollment experience that is consistent with the rest of the operating system.

If you've used fingerprint readers in the past, you might not recognize the new generation that should begin appearing on devices with Windows 8.1. Although the traditional swipe-style devices are still supported, new devices allow you to touch a sensor, which can identify your unique fingerprint with startling accuracy.

Fingerprint authentication isn't just for signing in to Windows, either. Fingerprint access is possible when you're accessing network resources, signing in to a website, or making a purchase. And it works in domain and nondomain environments.

Another built-in, hardware-based authentication option, the virtual smart card (VSC), was introduced in Windows 8 and gets some improvements in Windows 8.1. The idea behind a VSC is to require two-factor authentication, with an authorized device and a PIN (or biometric authentication) to access specific resources, such as your corporate virtual private network (VPN). Historically, this has been done with dedicated hardware devices that read physical smartcards. Adding a card reader to a notebook PC or tablet isn't practical. But what if there's another way to securely identify the device you're using and in essence turn it into a smartcard? That's a VSC.

This feature requires that a device be equipped with a TPM; enrolling the device creates a certificate that is stored securely in the TPM and allows the device to authoritatively identify itself to a remote server. An attacker who learns your user name and password won't be able to impersonate you and gain access to that resource because he won't have the second, crucial piece of ID: the virtual smart card.

Windows 8.1 adds APIs that simplify the VSC enrollment process. This enrollment process works on multiple hardware types, including ARM-based devices, and it doesn't require that the device be domain joined making this feature especially useful in BYOD scenarios.

Blocking malware

Successfully resisting malware and phishing attacks starts with some fundamental security features that have protected the core of the operating system for several years. The first two features are designed to protect against exploits that use vulnerabilities such as buffer overruns in the operating system and in applications:

- **Address Space Layout Randomization (ASLR)** This feature randomizes how and where important data is stored in memory, making it more likely that attacks that try to write directly to system memory will fail because the malware can't find the specific location it needs to attack. Windows 8.1 increases the level of entropy significantly, making it more difficult for most exploits to succeed. In addition, ASLR is unique across devices, making it more difficult for an exploit that works on one device to also work on another.
- **Data Execution Prevention (DEP)** This feature substantially reduces the range of memory that code (including malicious code) can run in. Windows 8 and 8.1 require hardware-based DEP support and will not install on a device that lacks this feature. DEP uses the Never eXecute (NX) bit on supported CPUs to mark blocks of memory so that they can store data but never run code. Therefore, even if malicious users succeed in loading malicious code into memory, they are unable to run it.

Windows 8.1 improves the process of automatically providing security updates through Windows Update or a corresponding enterprise tool. A system that is regularly updated is far less likely to be susceptible to malware.

In addition, the security status and configuration tool in Windows Action Center provides a complete picture of the system's current status, identifying problems in the Windows Firewall, for example, and flagging virus protection that's out of date.

Windows Defender

Windows 8 was the first version of Windows to ship antimalware software in the box, and Windows 8.1 continues this configuration. In previous Windows versions, Windows Defender was the name of a limited antispyware solution. In Windows 8 and 8.1, this is a full-featured solution (the successor to Microsoft Security Essentials) capable of detecting all sorts of malicious software. Because it supports the ELAM feature, it also prevents rootkits that try to infect third-party boot drivers. In Windows 8.1, Windows Defender for the first time includes network behavior monitoring.

Windows Defender is designed to be unobtrusive, updating automatically and providing messages only when required to do so. It is intended primarily for use in unmanaged PCs. In enterprise settings, you'll probably want to use an alternative antimalware solution. Microsoft's System Center 2012 Endpoint Protection, which uses the same engine as Windows Defender and also includes support for ELAM, is designed for use with enterprise-management tools. A number of third-party solutions that meet those same criteria are also available.

Internet Explorer 11

Windows 8.1 includes Internet Explorer 11 as part of a default installation. The new version, which replaces Internet Explorer 10 in an upgrade to Windows 8, includes a plethora of new features that are covered in Chapter 5, "Internet Explorer 11." This section focuses exclusively on security-related changes. (And no, you can't replace Internet Explorer 11 with an earlier version—at least, not without using a virtual machine.)

The most notable change in Internet Explorer 11 is that Enhanced Protected Mode (EPM) is enabled in the desktop browser by default. This feature was available in Internet Explorer 10 in Windows 8 but was disabled by default. You can control this option using Group Policy or on an individual basis, using a setting on the Advanced tab of the Internet Options dialog box, as shown in Figure 4-3.

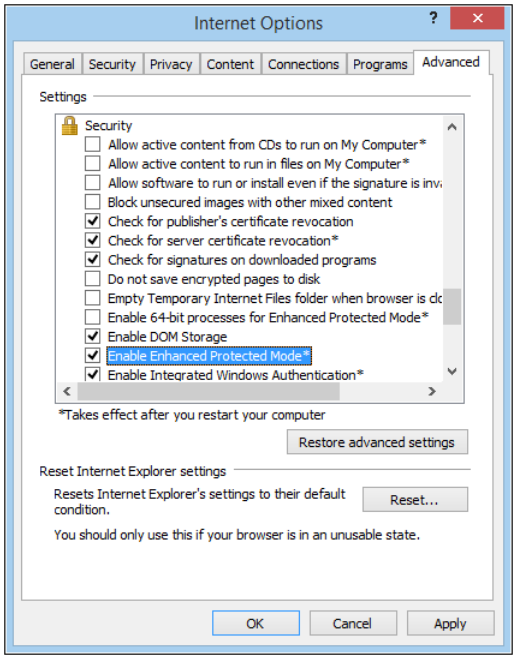


FIGURE 4-3 In Internet Explorer 11 on Windows 8.1, Enhanced Protected Mode is enabled by default. Note that 64-bit EPM processes are not enabled by default.

EPM restricts the ability of browser processes and plugins to perform potentially dangerous actions in the following ways:

- On devices running 64-bit Windows 8.1, EPM is capable of using 64-bit processes. This feature increases the effectiveness of memory-protection features such as ASLR by giving them a larger space in which to work.
- Internet Explorer is restricted from accessing personal information such as files unless the user explicitly grants permission. Access is managed by a broker process that works seamlessly in the background, using standard dialog boxes without any potentially confusing additional security prompts.
- On corporate networks, tab processes in the Internet zone (which load untrusted pages) do not have access to a user's domain credentials. In addition, those processes cannot act as web servers or make connections to intranet servers. The net effect is to protect corporate network resources from unauthorized access.

Enhanced Protected Mode also requires that browser add-ons be rewritten for compatibility. Incompatible add-ons won't load in EPM-enabled browser processes at all.

The Adobe Flash add-on that is included with Internet Explorer 11 is compatible with EPM. Administrators who want to restrict the ability of Flash content to run can control it using ActiveX Filtering or Group Policy.

SmartScreen and phishing protection

Windows 8.1 includes two separate but related features that share a common name: *SmartScreen*. The basic security principle is simple: It's much more effective to stop malicious code from running in the first place than to remove it after it's already secured a foothold on the system.

Independently of the browser, SmartScreen checks any executable file when it's run. If the file is marked as being from an online source, a web service checks a hash of the file against Microsoft's application-reputation database. Files that have established a positive reputation and are thus presumed to be safe are allowed to run. Files with a negative reputation that are presumed to be malicious are blocked.

Windows SmartScreen technology is particularly effective at preventing untrained users from running files of unknown provenance that have a greater-than-normal chance of being malicious. When SmartScreen identifies a file that has not yet established a reputation, it blocks execution and displays a warning message like the one shown in Figure 4-4.

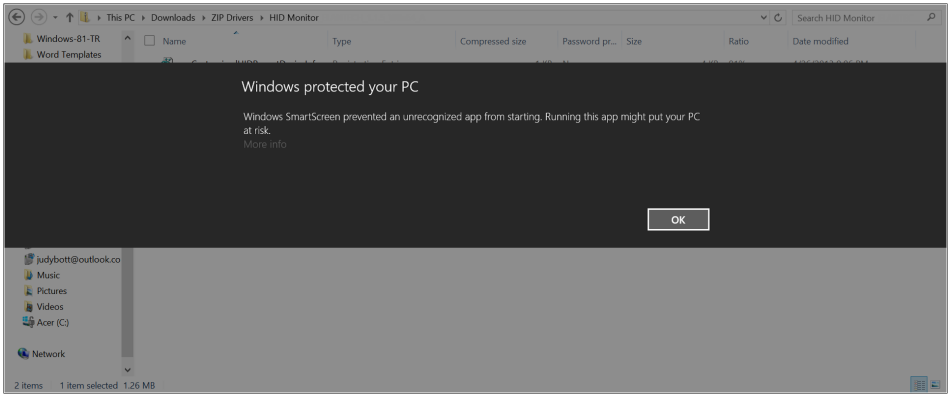


FIGURE 4-4 If a Windows 8.1 user attempts to run an unrecognized app, Windows SmartScreen blocks the app's execution. Administrators can override this behavior.

Local administrators can override the block shown in Figure 4-4 by clicking the More Info link and then clicking Run Anyway. If you want to disable the SmartScreen technology or adjust its behavior (for example, to prevent users from overriding SmartScreen actions), you can use Group Policy.

Securing data

Watch enough movies and read enough pulp fiction, and you'll be forgiven for assuming that the greatest threat to your data is from a mad genius cybercriminal in a far-off land like Freedonia. In reality, your data is more likely to be stolen by an old-fashioned thief, with no technical skills required. As we increasingly rely on mobile devices, those risks increase.

If someone walks away with a laptop or tablet stuffed with confidential corporate information, you'll be able to sleep better if you made sure the data on that device is encrypted and protected by a strong password. You'll get an even better night's sleep if you're able to wipe the confidential data clean from an administrative console.

In certain regulated industries, having a comprehensive and effective data-protection plan isn't just a good idea, it's mandated by law and backed by threats of fines and jail time.

As a direct response to those realities, Windows 8.1 incorporates robust data-encryption options that encompass a full range of devices. Device encryption is now a standard feature in all editions of Windows. That's a significant change from previous editions, which traditionally reserved that feature for business/enterprise editions. Encryption can be enabled out of the box on Windows 8.1 and can be configured with additional BitLocker protection and management capability on the Pro and Enterprise editions.

Device encryption

On any device that supports the InstantGo (formerly Connected Standby) standard and is running Windows 8.1, data is encrypted by default. On a device that clears those two hurdles, even one intended for casual use by consumers, encryption is automatically enabled for the operating-system volume during setup.

This encryption initially uses a clear key, allowing access to the volume until a local administrator signs in with a Microsoft account and, by so doing, automatically turns on encryption. The recovery key is automatically stored in the user's SkyDrive storage in case an administrator needs to recover the encrypted data later (if a password is lost, for example, or an employee leaves the company and management needs to access encrypted files on a company-owned device). If you need to reinstall the operating system or move the drive to a new PC, you can unlock the drive with the recovery key (which is stored at *http://skydrive.com/recoverykey*) and re-seal the drive with a key from your new machine.

BitLocker Drive Encryption

From a technological standpoint, Device Encryption and BitLocker are identical. Both device encryption and BitLocker default to 128-bit Advanced Encryption Standard (AES), but BitLocker can be configured to use AES-256.

The most important advantages for BitLocker in enterprise scenarios involve control and manageability. BitLocker comes with a long list of features that are appropriate for enterprise-class data protection, including the capability to use a TPM plus a PIN for encryption as well as Network Unlock, which allows management of BitLocker-enabled devices in a domain environment by providing automatic unlocking of operating-system volumes at system reboot when connected to a trusted wired corporate network.

Normally, BitLocker uses software-based encryption to protect the contents of Windows operating-system and data volumes. On devices without hardware encryption, BitLocker encrypts data more quickly than in previous versions. With BitLocker, you can choose to encrypt only the used space on a disk instead of the entire disk. In this configuration, free space is encrypted when it's first used. This results in a faster, less disruptive encryption process so that enterprises can provision BitLocker quickly without an extended time commitment.

An administrator can use Group Policy settings to require that either Used Disk Space Only or Full Encryption is used when BitLocker Drive Encryption is enabled. The following Group Policy settings are located under the \Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption path of the Local Group Policy Editor:

- Fixed Data Drives\Enforce drive encryption type on fixed data drives
- Operating System Drives\Enforce drive encryption type on operating system drives
- Removable Data Drives\Enforce drive encryption type on removable data drives

For each of these policies, you can also require a specific type of encryption for each drive type. In addition, the user experience is improved by allowing a standard user, one without administrative privileges, to reset the BitLocker PIN.

In Windows 8 and 8.1, BitLocker supports a new type of storage device, the Encrypted Hard Drive, which includes a storage controller that uses hardware to perform encryption operations more efficiently. Encrypted Hard Drives offer Full Disk Encryption (FDE), which means encryption occurs on each block of the physical drive rather than data being encrypted on a per-volume basis.

Windows 8.1 is able to identify an Encrypted Hard Drive device, and its disk-management tools can activate, create, and map volumes as needed. Windows 8.1 also provides API support for applications to manage Encrypted Hard Drives independently of BitLocker Drive Encryption. The BitLocker Control Panel allows users to manage Encrypted Hard Drives using the same tools as on a standard hard drive.

Remote business data removal

In Windows 8.1, administrators can mark and encrypt corporate content to distinguish it from ordinary user data. When the relationship between the organization and the user ends, the encrypted corporate data can be wiped on command using Exchange ActiveSync (with or without the OMA-DM protocol). This capability requires implementation in the client application (Mail, for example) and in the server application (Exchange Server). The client application determines whether the wipe simply makes the data inaccessible or actually deletes it. This feature includes support for an API that allows third-party apps to adopt the remote-wipe capability.

CHAPTER 5

Internet Explorer 11

For nearly two decades, each new version of Microsoft Windows has been accompanied by a new version of Internet Explorer. Windows 8.1 carries on that tradition, including Internet Explorer 11 as part of a standard installation.

Internet Explorer 11 is a significant upgrade from its predecessor, Internet Explorer 10, which debuted with Windows 8. It includes an assortment of important security enhancements, comprehensive support for modern web standards, and excellent performance, especially on touchscreen devices. Collectively, these improvements make Internet Explorer 11 a sound choice for enterprise networks.

Microsoft has released Internet Explorer 11 as an upgrade for Windows 7, making it possible to standardize on this version even in mixed computing environments. Several of the most significant changes in Internet Explorer 11 are available only with Windows 8.1, however. IT pros looking for detailed information on deploying Internet Explorer can find useful resources at *http://technet.microsoft.com/en-US/ie*.

The two faces of Internet Explorer in Windows 8.1

In Windows 8.1, Internet Explorer 11 uses a single engine with two distinctly different user experiences, depending on your starting point.

Clicking the Internet Explorer tile on the Start screen (or tapping a pinned tile on the Start screen) launches the immersive Internet Explorer 11 user experience, which incorporates the same user-interface conventions found in apps available from the Windows Store. By contrast, opening Internet Explorer on the desktop uses the familiar multitabbed interface in a desktop window that can be maximized, minimized, and resized like any other desktop program.

Figure 5-1 shows the immersive browsing experience.

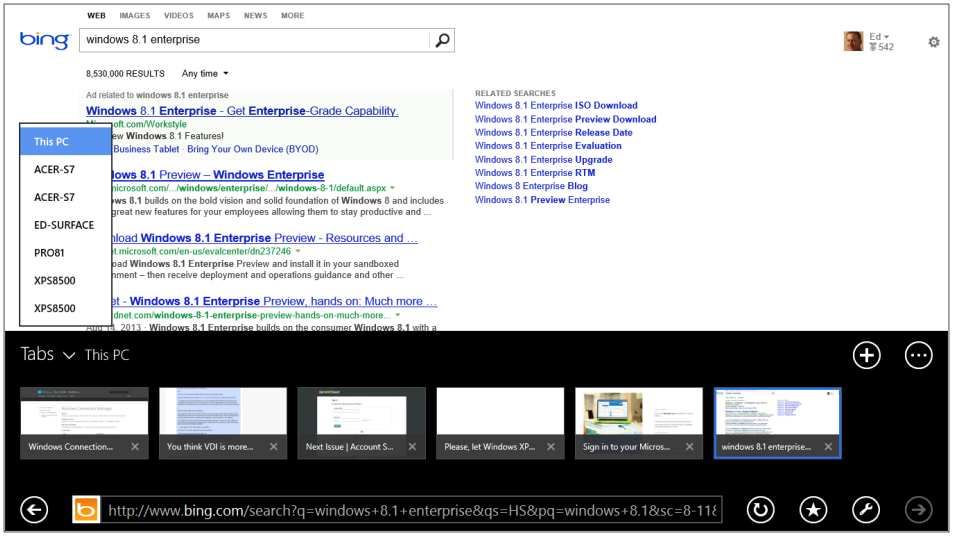


FIGURE 5-1 The user experience for tabbed browsing in Internet Explorer 11 moves the tab thumbnails along the bottom and adds support for up to 100 tabs per session.

Compared with its predecessor, the immersive Internet Explorer 11 includes a broad set of usability enhancements that improve the everyday browsing experience significantly. This list includes the following features:

- **Tabs** Internet Explorer 11 supports up to 100 tabs per window. (By contrast, Internet Explorer 10 supports only 10 tabs per session.) Tabs can be suspended for efficient use of memory and battery, and switching between tabs is faster. The tabs bar appears at the bottom of the Internet Explorer screen, and tab thumbnails scroll left and right if more tabs are open than will fit in the screen width at one time.
- **Side-by-side browsing** In the immersive Internet Explorer experience, opening a link in a new window opens a second browser window alongside the original window, with each taking up half the screen.
- **Address bar** In another response by Microsoft to feedback from users, Internet Explorer 11 includes a new option to always show the tabs and address bar instead of keeping them hidden.
- **Favorites** Internet Explorer 11 significantly improves the experience of saving and managing Favorites when using the immersive browser. By clicking the star button in the command bar to save a Favorite, you can select a custom thumbnail image and a location for the saved favorite, using the same group of folders available from the desktop user experience, as shown in Figure 5-2.

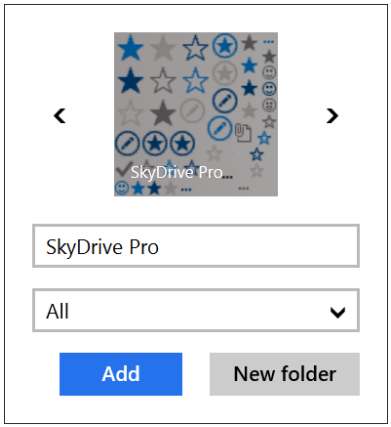


FIGURE 5-2 Arrows along the top of the Save Favorite dialog box let you pick a thumbnail for the favorite. You can also choose a location, using the same folders as Internet Explorer on the desktop.

If you want to customize an individual Windows 8.1 installation so that shortcuts to saved webpages always open in Internet Explorer on the desktop, you can do so by using the Opening Internet Explorer section at the top of the Programs tab in the Internet Options dialog box. This section contains three options, as shown in Figure 5-3.

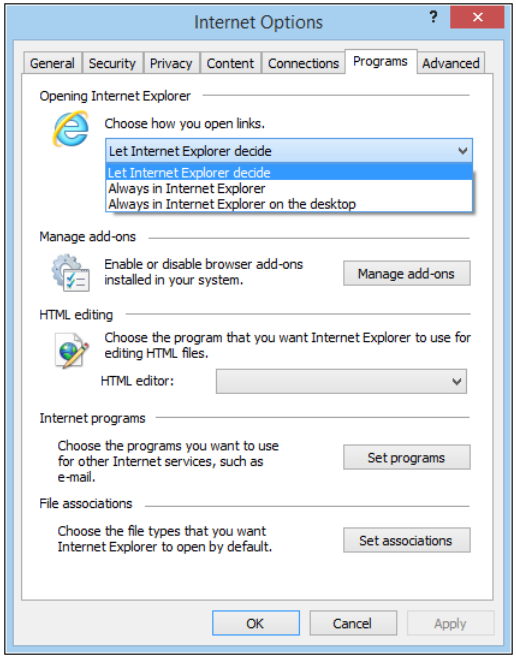


FIGURE 5-3 The three options at the top of the Internet Options dialog box allow you to specify which user experience Internet Explorer uses when you click a link.

The default option, Let Internet Explorer Decide, generally uses the immersive browser if you open or switch to Internet Explorer from a pinned shortcut on the Start screen, and it uses the desktop browser when your navigation begins on the desktop. The other two options make the immersive browser or desktop browser the default for all actions, regardless of their starting point.

When browsing a page in the immersive browser, you can open that page in the desktop browser by using the Page Tools menu in the command bar. (It looks like a wrench.) To perform the reverse operation—opening the current page in the immersive browser when starting from the desktop—right-click an open tab and then click Open In Immersive Browser.

Note that Internet Explorer must be set as the default browser to use the immersive experience. If another browser is set as the default, tapping or clicking the Internet Explorer tile on the Start screen opens the desktop browser only.

What's new in Internet Explorer

Internet Explorer 10, which debuted in Windows 8, included a long list of new features. Internet Explorer 11 expands that list significantly. Many of the changes in both iterations are under the hood, with significant improvements in performance and reliability as well as better support for interactions on touchscreen devices. Here are some of the highlights for features you and your users are likely to see:

- **Adobe Flash as a platform feature** Adobe Flash is included by default, automatically updated via Windows Update and available even in the immersive Internet Explorer 11, which does not allow the installation of any browser plug-ins. The ability to play back Flash content can be disabled via the Internet Options dialog box or using Group Policy.
- **Do Not Track (DNT)** The DNT header is enabled as part of the Express setup option to enhance privacy online. This feature sends a DNT=1 signal with every page request, enabling users to express their preference about whether their browsing history should be collected and used for targeted ads, content, and other purposes. Additionally, third-party Tracking Protection Lists can block or allow content from specific sites, further protecting users' privacy. These features are controllable through Group Policy, as discussed at the end of this chapter.
- **Enhanced Protected Mode** Enhanced Protected Mode provides additional security compared with the Protected Mode that was first introduced in Internet Explorer 7. Enhanced Protected Mode enforces additional restrictions on the browser's capabilities, preventing many common exploit scenarios and also limiting the information that the browser can provide to untrusted sites. In Internet Explorer 11, Enhanced Protected Mode is enabled by default.

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 added support for several additional CSS features, including CSS3 regions; flexible box, grid, and multicolumn layout; device adaptation; 3-D transforms; fonts; animations; gradients; and transitions.

  HTML5 features supported for the first time in Internet Explorer 10 include 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. Internet Explorer 11 enhances flexible box support and adds support for drag and drop touch, Mutation Observers, and Pointer Events.

MORE INFO **See the Developer Guide for Internet Explorer 11 at *http://msdn.microsoft.com/en-us/library/bg182636(v=vs.85).aspx* for more information about additional web standards.**

- **Support for Web Graphics Library (WebGL)** The WebGL standard does for web applications what OpenGL does for desktop applications. Internet Explorer 11 is the first version to support WebGL, which enables developers of web applications to deliver smooth animations and 3-D graphics.
- **Flip Ahead** Internet Explorer 11 uses the Flip Ahead feature (configurable through privacy 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 navigate backward using a swipe gesture as well. This is especially useful when browsing search results and multipage news articles.
- **Sync** Internet Explorer 10 included the capability to automatically sync history and typed URLs, Favorites/Bookmarks, and home-page settings. Internet Explorer 11 expands sync capabilities to include recently opened browser tabs, saved website passwords, and a broader range of settings and preferences. The list of saved tabs appears on the New Tab on other devices where the user signs in with the same Microsoft account.
- **F12 Developer Tools** This toolbar, which is normally hidden, is designed primarily for web developers to debug code, fix compatibility issues, improve performance, and resolve problems with the display of webpages. This toolbar appears when you press the F12 shortcut key (naturally); it's also available from Internet Explorer's Tools menu. The F12 Tools pane is normally docked to the bottom of a browser window but can be dragged out and positioned separately for maximum visibility, as shown in Figure 5-4.

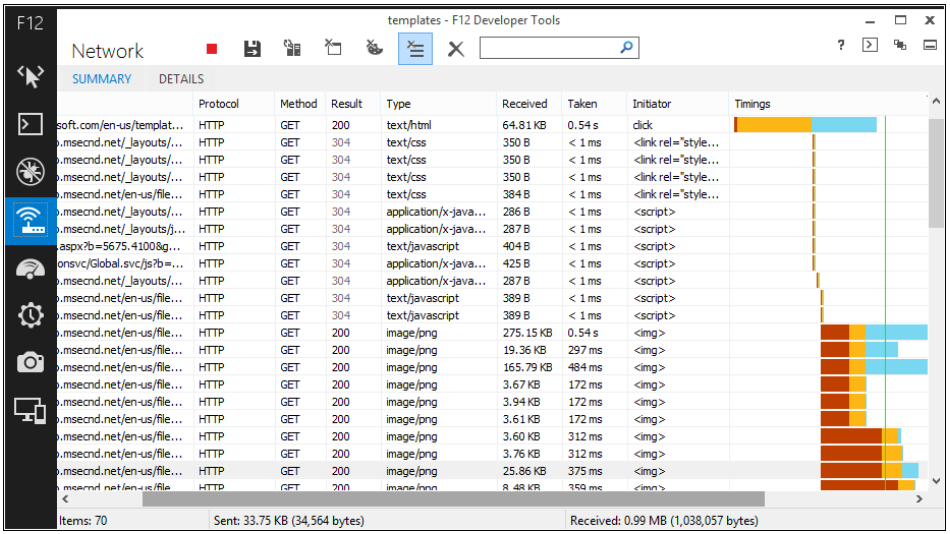


FIGURE 5-4 Each of the icons along the left side of the F12 Developer Tools leads to advanced features suitable for web developers and website administrators, like this profile of network performance for a target page.

Deploying and managing Internet Explorer 11

A determined user can adjust hundreds of settings for Internet Explorer 11. In an enterprise environment, the most common way to ensure that these settings are uniform across an organization is to use the Internet Explorer Administration Kit (IEAK). Using the IEAK, you can customize, brand, and distribute Internet Explorer in any supported language across your organization. (In some Windows versions, the Internet Explorer executable files are included with the IEAK package; this isn't necessary in Windows 8.1, because Internet Explorer is installed with the operating system.)

Settings you can adjust with the help of the IEAK Wizard include the following feature groups:

- Language Selection
- Feature Selection
- Corporate Install
- User Experience
- Browser User Interface
- Search Providers
- Important URLs - Home page and Support
- Accelerators
- Favorites, Favorites Bar, and Feeds

- Browsing Options
- Connection Settings
- Automatic Configuration
- Proxy Settings
- Security and Privacy Settings

The most recent version of IEAK is available from *http://ieak.microsoft.com*.

Use the IEAK to configure initial settings; use Group Policy objects (GPOs) to enforce those settings and control the behavior of Internet Explorer in its immersive mode and on the desktop. In total, there are almost 1,500 settings that can be changed in Group Policy for Internet Explorer 10 and 11.

> ***MORE INFO*** **You can find a comprehensive list of all new Group Policy settings for Internet Explorer 10 at *http://technet.microsoft.com/en-us/library/hh846775*. Most of them apply to Internet Explorer 11 as well. A corresponding document listing new Group Policy settings exclusive to Internet Explorer 11 is available at *http://technet.microsoft.com/en-US/library/dn321453.aspx*.**

Table 5-1 highlights the most interesting of the new Group Policy settings for Internet Explorer 11.

TABLE 5-1 Useful Group Policy settings for Internet Explorer 11

Setting	Description
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.
Turn off loading websites and content in the background to optimize performance	Prevents Internet Explorer from preemptively loading websites and content in the background, a default setting that speeds up performance when the user clicks a hyperlink.
Allow Microsoft services to provide enhanced suggestions as the user types in the Address bar	Allows Internet Explorer to send the user's keystrokes to a Microsoft service that provides enhanced suggestions as the user types in the Address bar.
Allow Internet Explorer to use the SPDY/3 network protocol	Determines whether Internet Explorer can use the SPDY/3 network protocol, which optimizes the latency of HTTP requests through compression, multiplexing, and prioritization; this feature is enabled on a per-zone basis.
Don't run antimalware programs against ActiveX controls	When enabled, this setting blocks Internet Explorer from checking with your antimalware program to see if it's safe to create an instance of the ActiveX control.

Setting	Description
Turn on Enhanced Protected Mode	Enables Enhanced Protected Mode for any zone that uses Protected Mode and prevents users from disabling Enhanced Protected Mode.
Turn on 64-bit tab processes when running in Enhanced Protected Mode on 64-bit versions of Windows	Determines whether Internet Explorer 11 uses 64-bit processes (for greater security) or 32-bit processes (for greater compatibility) when running in Enhanced Protected Mode on 64-bit versions of Windows.
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 phone number detection	Disables the feature that recognizes phone numbers in webpages and turns them into hyperlinks, which can be used to invoke the default phone application on the system (Skype or Lync, for example).
Turn off the flip ahead with page prediction feature	Disables background loading of pages in Internet Explorer when using the swipe gesture or Forward button. Doesn't apply to Internet Explorer for the desktop.
Prevent deleting ActiveX Filtering, Tracking Protection and Do Not Track data	When enabled, this setting prevents users from deleting this data for visited websites.
Always send Do Not Track header	When this setting is enabled, Internet Explorer sends a DNT:1 header with all HTTP and HTTPS requests; when it's disabled, a DNT header is sent only if a Tracking Protection List is enabled or inPrivate Browsing mode is used.
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.
Install new versions of Internet Explorer automatically	Administrators might want to disable this setting to prevent Internet Explorer from being automatically upgraded when a new version is available.
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. This setting replaces the Prevent Changing Default Browser Check setting from previous Internet Explorer versions.

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.

Internet Explorer 11 no longer supports the following Group Policy settings:

- Turn on Internet Explorer 7 Standards Mode
- Turn off Compatibility View button
- Turn off Quick Tabs functionality
- Turn off the quick pick menu
- Use large icons for command buttons

Compatibility changes in Internet Explorer 11

In recent versions of Internet Explorer, Microsoft has used Compatibility View to help deal with sites that display incorrectly when viewed in Internet Explorer. The most frustrating display problems arise when the user visits a site that should work correctly with Internet Explorer 11 but is forced into rendering improperly because the site tries to use code designed for an older version of Internet Explorer.

In Internet Explorer 11, Microsoft has changed the user-agent string that the browser sends to websites when it visits. The new user-agent string is

```
Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
```

Compared with earlier versions of Internet Explorer, this user-agent string includes the following changes:

- The compatible ("compatible") and browser ("MSIE") tokens have been removed.
- The "like Gecko" token has been added for consistency with other browsers. (Gecko is the name of the rendering engine used by Mozilla Firefox.)
- The version of the browser is now reported by a new revision ("rv") token.

On well-written pages, these changes should prevent Internet Explorer 11 from being detected as an out-of-date browser. For pages that incorrectly detect the browser, Microsoft uses a Compatibility View list, which is downloaded automatically as part of default Windows 8.1 installation. You can add sites individually to this list by using the Compatibility View dialog box on the Tools menu. (Tap Alt or F10 to make this menu visible.)

Resources that can help developers build sites that work properly with Internet Explorer 11 include the following:

- **modern.IE** A set of tools to help developers updates sites using modern standards, incorporating best practices from MSDN documentation including the Compatibility Cookbook. An intranet scanner is available for download, for use on corporate networks. It's available at *http://modern.ie*.
- **Compat Inspector** A JavaScript-based testing tool to help sites migrating to modern standards. It's available at *http://ie.microsoft.com/testdrive/HTML5/CompatInspector/*.
- **Compatibility Cookbook** Documentation on changes to features, general tools, and guidance for sites updating to recent versions of Internet Explorer. It's available at *http://msdn.microsoft.com/library/ie/dn384059*.

CHAPTER 6

Delivering Windows Store apps

Devices designed and built for Windows 8 and its successors can do something their predecessors in the Windows family never could. These modern machines can run a new class of modern apps, built using the new Windows Runtime (WinRT) platform, with a clean user experience that takes full advantage of touch-enabled devices.

Windows 8.1 includes a large selection of Microsoft-authored apps in this category, all of them included as part of a default Windows 8.1 installation. Additional apps are available through the Windows Store, whose distinctive green tile can be found on the Windows 8.1 Start screen. In addition, enterprises running Windows 8.1 can make custom line-of-business (LOB) apps available to users inside their organization. These apps can be deployed using enterprise app stores or through a process called *sideloading*.

In addition to creating and deploying apps, administrators can also use Group Policy to control the use of all apps, including those that are built in to Windows 8.1. For example, an organization might choose to remove the Sports app or prohibit it from running.

If you read enough technical material for developers and administrators, you'll find this class of apps referred to variously as *Windows Store apps*, *WinRT apps*, *modern apps*, and *immersive apps*. You might also find occasional references to *Metro*, a code name used in prerelease documents for Windows 8 and still used by some writers today. In this book, I use the term *Windows Store apps*.

This chapter looks at the ways you can deliver and control Windows apps. But first, let's take a closer look at what these apps are and what they do.

What is a Windows Store app?

Unlike every previous Windows version, Windows 8 (and its successor, Windows 8.1) can run apps built on two separate platforms. Virtually any desktop program that runs under Windows 7 will also run on Windows 8.1. The new WinRT apps run only on Windows 8 and Windows 8.1.

> ***NOTE*** **Devices powered by Windows RT 8.1 can run most Windows Store apps but are unable to run desktop programs, including installers and browser add-ons. For a more detailed discussion of what makes this edition different, see Chapter 10, "Windows RT 8.1."**

To build apps for Windows 8.1, you must use Microsoft Visual Studio 2013 running on Windows 8.1. If you run these development tools on Windows 8, or if you use Visual Studio 2012 on any supported Windows version, you can target apps for Windows 8, but not for Windows 8.1.

Three Visual Studio 2013 editions—Professional, Premium, and Ultimate—are intended for professional developers. A fourth edition, Visual Studio Test Professional 2013, consists of an integrated test toolset that allows collaboration between developers and testers. The most common way to acquire these tools is with an MSDN subscription. Visual Studio Express 2013, the free member of the family, includes the same core tools as its paid brethren as well as the Software Development Kit (SDK) for developing Windows apps.

> ***NOTE*** **More information about Visual Studio features and pricing is available from *http://www.microsoft.com/visualstudio*.**

Within the Visual Studio 2013 environment, you can take your choice of multiple programming languages 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# to develop LOB Windows apps. Other organizations might choose Microsoft Visual Basic or Visual C++, both of which are traditional client-side languages that can be used to build server-side web applications.

Notably, you can also use JavaScript, HTML, and cascading style sheets (CSS) for Windows app development. This capability allows you to build fully functional Windows apps that leverage modern web technologies that might already be in use within your organization.

Regardless of the language you choose, the resulting apps all use the same Windows Runtime application programming interface (API) to access the standard Windows app library and other application functions. The end product is an *app package* (with the extension .appx), which contains a manifest and the files that make up the app. The manifest is used by Windows 8.1 when it installs or removes the associated app.

The package manifest also specifies the app's capabilities. For enterprise apps you create using a company account (described later in this chapter), you can apply special-use capabilities that determine whether the app requires enterprise authentication and programmatic access to protected resources or connected devices.

MORE INFO **For a full discussion of app capabilities with an emphasis on enterprise app development, see the MSDN Dev Center article "App capability declarations (Windows Store apps)," at *http://msdn.microsoft.com/en-US/library/windows/apps/hh464936.aspx*.**

How Windows Store apps work

Windows Store apps are designed and built first and foremost for use with touchscreen-equipped devices. Touch is not a requirement, however; these apps also work well on conventional PCs and notebooks, where every action can be accomplished with a mouse and keyboard or other pointing device.

Windows Store apps have the following common characteristics:

- Apps are installed on a per-user basis, using a simple installation mechanism that does not require local administrative rights.
- Every app has an application tile, which can be programmed to update dynamically, making it a *live tile*. (Hint: In enterprise apps, live tiles can draw from your business data, making the Windows 8.1 Start screen a dashboard where employees can get at-a-glance status updates and messages.)
- Apps must adhere to a strict set of APIs that prevent them from directly accessing system resources. That limits an app's ability to perform many functions that are commonplace for desktop apps. The trade—off is those limitations help ensure the security and reliability of the underlying operating system by blocking the most common attack vectors.
- The default user experience is immersive, using the full screen with a *chromeless* design that eschews menus and borders. Although a limited number of app commands are visible, most are available in a normally hidden app bar at the top and bottom of the screen, which appears in response to a swipe gesture or a right-click. Figure 6-1 shows the Weather app (included in Windows 8.1) with its app bar visible.

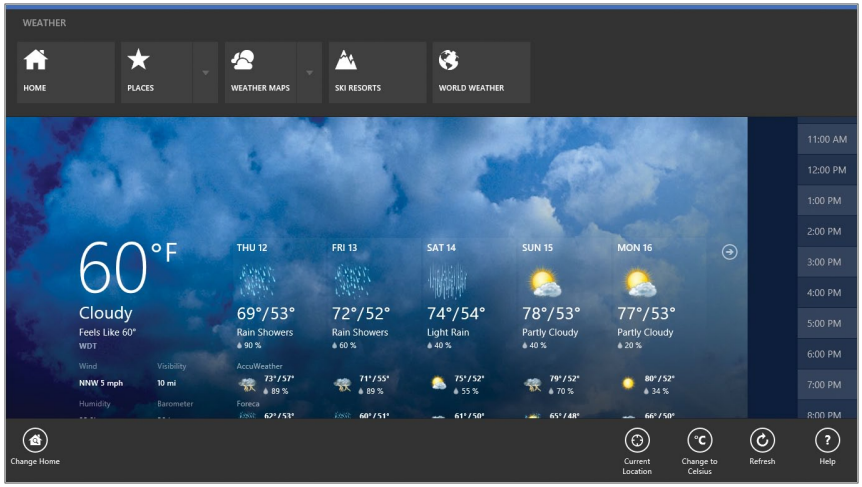


FIGURE 6-1 Swiping from the bottom edge on a tablet (or right-clicking on a conventional PC) reveals the commands on the app bar in a Windows Store app.

- All apps share a common group of user-interface conventions and gestures designed for use with touch, pen, traditional pointing devices, and keyboards.
- The width (but not the height) of a Windows Store app can be adjusted, allowing two or more apps to be arranged side by side on one or more displays. In this arrangement, the Windows desktop functions like an app and can be snapped alongside a Windows Store app. Windows 8.1 significantly improves this capability compared to Windows 8, which allowed only a single app to snap into a slim bar alongside another app or the Windows desktop. Figure 6-2 shows the new capabilities in action.

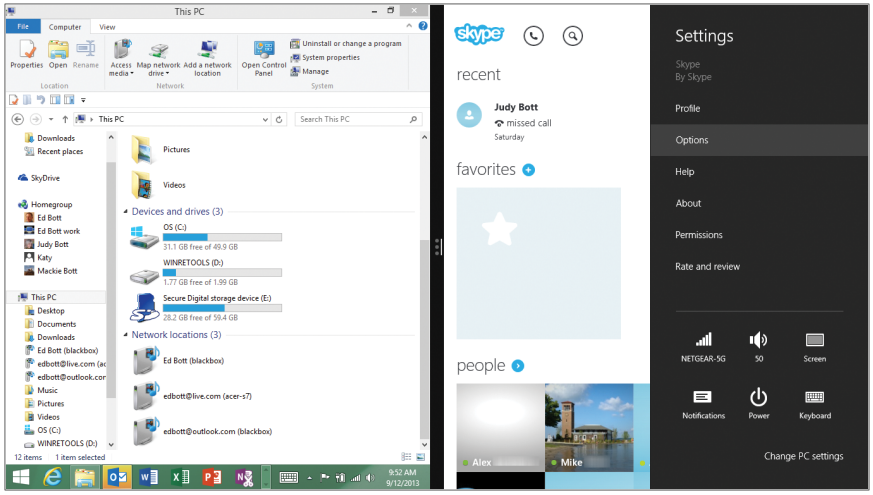


FIGURE 6-2 Windows 8.1 allows Windows Store apps and the desktop to be resized in a flexible range of widths—side by side, in this example. On large, high-resolution displays, you can arrange up to four apps per display.

- Apps can interact with the operating system and with other apps using the controls on the charms menu. The Settings charm is the standard means for adjusting app-specific configuration options, which take over the top of the Settings pane as shown in the previous figure. The Share charm allows a user to send a selection from the current app to another app—to a new mail message or the (new in Windows 8.1) Reading List app, or to another LOB app that connects to a web service on your intranet.

  Figure 6-3 shows the Share charm in action, using a real-world example: If you want to encourage a colleague to install the official Twitter app from the Windows Store, you can find its listing in the Store, click the Share charm, and send that link via email. You can also bookmark the link in the Reading List app (new in Windows 8.1).

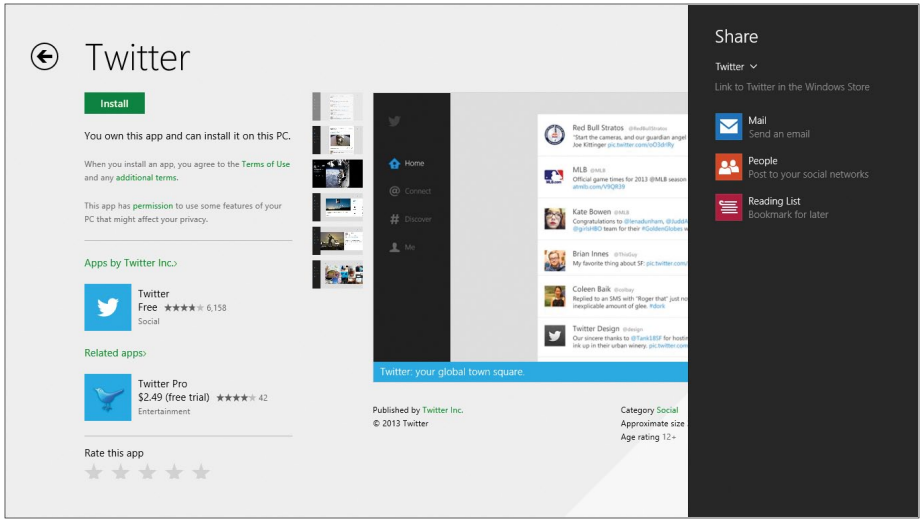


FIGURE 6-3 Using the Share charm allows you to share information between Windows Store apps. This example includes options to bookmark a link to a specific Store app or share it via email or a social network.

- Apps can trigger notifications and alerts, using standard APIs.
- In the interest of power management, a crucial factor on mobile devices, most Windows 8.1 apps are suspended within a few seconds when the user switches away from the app. Some apps (music players and apps that need to download files in the background, for example) can be configured for background operation.

MORE INFO **You can find more information on the app life cycle, including details about the inner workings of suspend and resume, at *http://msdn.microsoft.com/library/windows/apps/hh464925.aspx*.**

By default, apps in Windows 8.1 update automatically, with no user intervention required. This is a significant change from Windows 8, which used the Store's live tile to notify users that updates for one or more of their apps were available but required that those updates be installed manually. The auto-update option can be disabled using the App Updates options available from Settings in the Store. In managed environments, you can use Group Policy to disable access to the Store app. (See the final section of this chapter for more details.)

Distributing a Windows Store app

A finished app can be submitted to the Windows Store, where it is subject to a set of rules and must be approved for distribution. Distributing through the Windows Store makes an app available to the general public and has its own set of rules. After it is distributed in the Windows Store, the app is available to the public.

LOB apps distributed within an organization use an enterprise app store that is separate from the public Windows Store. These apps don't need to be certified by Microsoft, but they do need to be signed with a certificate that is trusted by one of the trusted root authorities on the system.

You'll have best results using a code signing certificate issued by an internal certificate authority or an external certificate vendor that is already part of the trusted root store. Except for limited testing purposes, avoid using the self-signed certificate generated automatically by Visual Studio when creating a new app project.

This section describes the process for each distribution route.

Publishing an app to the Windows Store

Distributing an app through the Windows Store involves multiple steps, starting with the requirement to open a developer account. You can choose either an individual account or a company account. For most readers of this book, a company account is the right choice, because it supports three types of advanced capabilities for apps:

- **enterpriseAuthentication** This capability allows the use of Windows credentials for access to a corporate intranet and is typically used in LOB apps that connect to servers within an enterprise.
- **sharedUserCertificates** Financial and enterprise apps require this capability to access software and hardware certificates, such as certificates stored on a smartcard and used for authentication.
- **documentsLibrary** Use this capability for apps that require programmatic access to the user's Documents library, rather than allowing access to that library using the file-picker control.

Use your developer account to register with the Windows Store and submit apps to Microsoft for approval. Every app is reviewed according to the terms described in the "Windows 8 app certification requirements" document (*http://msdn.microsoft.com/library/windows/apps/hh694083.aspx*).

The requirements for an app to be accepted, listed, and sold in the Windows Store include the following:

- The app must provide value and be fully functional.
- The app must provide more functionality than a simple website and can't just display ads.
- The app must behave predictably and reliably, even on low-powered computers.
- The app must support a snapped layout and suspend and resume to a reasonable state.
- The app must adhere to privacy and security practices, including the presence of a privacy statement and opt-in consent to share personal information.
- The app's content and subject matter must be appropriate for many audiences or be rated to prevent inappropriate age groups from accessing its content.
- The app must be identified easily with a unique name and other information.

MORE INFO **See *http://msdn.microsoft.com/en-US/library/windows/apps/br230836.aspx* for more information on the requirements for Windows app developers.**

The certification process to distribute an app through the Windows Store is a multistep process that begins when you upload the app package to Microsoft, where it's checked for compliance with various app certification requirements.

During the certification and review process, Microsoft performs the following tests:

1. Security tests, to verify that the app is not malicious.
2. 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 to perform the same tests and help ensure a successful test when performed by Microsoft.
3. Content compliance tests. As 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 digitally signs the app to prevent tampering, and then it publishes the app to the Windows Store. The publisher can set the release date and other aspects of the app.

MORE INFO **See *http://msdn.microsoft.com/windows/apps/* for more information on the process of developing and submitting an app to the Windows Store. See *http://msdn.microsoft.com/library/windows/apps/hh694062.aspx* for a checklist that can be helpful when preparing an app for submission.**

Distributing apps within an enterprise

Distributing an app within an enterprise (sideloading) requires that the client PCs be running Windows 8.1 Enterprise edition, Windows 8.1 Pro, or Windows RT 8.1. The most common scenario is to develop an LOB app and automatically push it out to computers within the organization. Aside from the edition of Windows 8.1 being used, there are three primary requirements for sideloading apps:

- The target computer must have sideloading enabled. (This is automatic when a Windows 8.1 Enterprise computer is joined to the domain. To enable sideloading on a Windows 8.1 Enterprise computer that is not joined to the domain or on a device running Windows 8 Pro or Windows RT, you must use a sideloading product activation key, which can be acquired through the Volume Licensing Service Center.)
- The Group Policy setting Allow All Trusted Apps To Install must be enabled.
- 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 6-4.

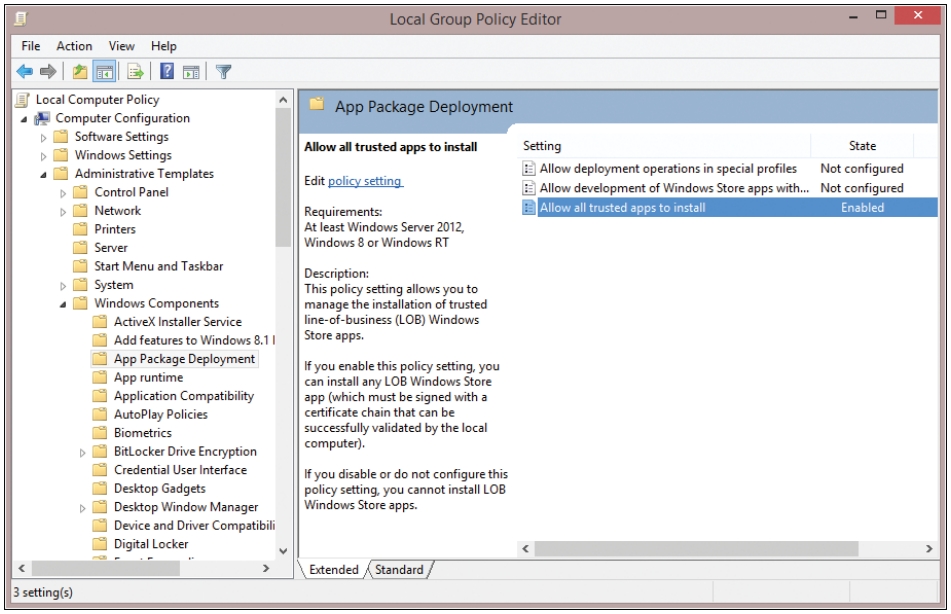


FIGURE 6-4 Configuring the Allow All Trusted Apps To Install Group Policy setting is a crucial step in allowing sideloading of internal apps that require the use of the Windows Store.

NOTE **The detailed steps for installing a sideloading product key on a device that's not domain-joined are 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.**

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` Windows PowerShell cmdlet. This cmdlet is run on the local computer where the app is being installed; this step can be scripted in an enterprise scenario.

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

After installing the app package, you must run a series of validation tests before publishing or deploying it. The Windows App Certification Kit is part of the Windows 8.1 Software Development Kit (SDK) and is also available as a standalone package. For details and download links, see *http://msdn.microsoft.com/en-US/windows/apps/bg127575*.

To create Windows Store apps for use with Windows 8.1, you must use the Windows App Certification Kit 3.0. This version includes performance and usability improvements over previous releases, but more importantly it includes tests that are essential for certifying Windows 8.1 apps. (It also supports the Windows 7, Windows 8, and Windows 8.1 Desktop App Certification Programs.)

The list of new tests includes the following:

- **Supported directory structure** Ensures that apps don't create a structure on disk that results in files longer than MAX_PATH (260 characters).
- **File extensions and protocols** Limits the number of file extensions and protocols that an app can register.
- **Platform appropriate files** Checks for packages that contain cross-architecture binaries.
- **Banned file check** Examines apps for use of outdated or prerelease components known to have security vulnerabilities.
- **JavaScript background tasks** Verifies that apps that use JavaScript have the proper close statement in the background task so that the app doesn't consume battery power unnecessarily.
- **Framework dependency rules** For all frameworks, ensures that apps are taking the right framework dependencies for Windows 8 and Windows 8.1.

The Windows App Certification Kit is a wizard-driven tool whose first step allows you to choose the Windows Store App option, which in turn leads to the list of tests shown in Figure 6-5.

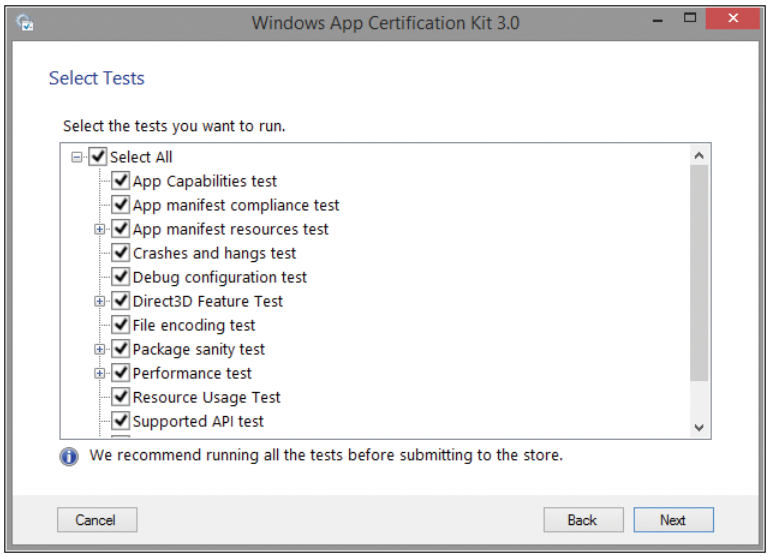


FIGURE 6-5 The Windows App Certification Kit runs your app package through a gauntlet of tests to verify that it meets the requirements for distribution.

The test cycle can take some time and should not be interrupted. When it completes, you see the results, as shown in Figure 6-6.

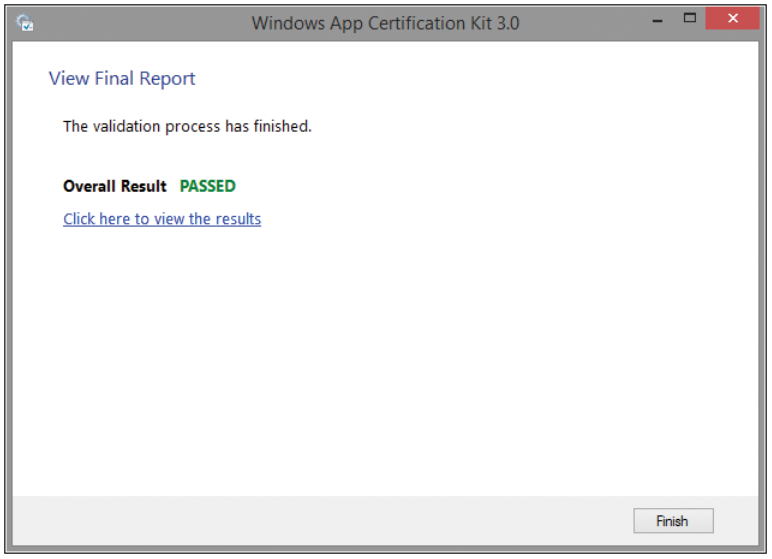


FIGURE 6-6 After your Windows Store app completes all tests, the results are shown here.

After your enterprise app is verified, you can deploy the app across your organization in one of two ways.

You can allow employees to install apps automatically through an enterprise app store, which is managed by System Center Configuration Manager R2 (required for Windows 8.1) or Windows Intune. This scenario does not require administrator rights. Using Configuration Manager, the user can visit an App Catalog website to find and install enterprise apps. Using Windows Intune allows the user to access apps from a Windows Store App called the Company App Portal.

You can install the app automatically for each user of the target device by using the Microsoft Deployment Toolkit, the Deployment Image Servicing and Management (DISM) tool, or the `Add-AppxProvisionedPackage` cmdlet in Windows PowerShell. These options add the app to the Windows image so that the app is installed for every user automatically, when the user signs in for the first time. This process is called *provisioning*.

> ***MORE INFO*** **For full details on how to provision LOB apps, see the "Add and Remove Apps Using DISM" topic at *http://technet.microsoft.com/library/hh852635.aspx*.**

To add an app to an image that has already been deployed, use the `Add-AppxPackage` cmdlet in Windows PowerShell. There is no limit to the number of apps you can add in this fashion.

To update an app, you must remove the provisioned app and then deploy the new version. The update is applied the next time the user signs in.

Note that you can install provisioned LOB apps on any Windows 8.1 or Windows RT 8.1 device. However, the apps will not run until the computer meets the sideloading requirements described earlier in this chapter by being joined to a domain or having a sideloading product key installed.

Managing Windows Store 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 6-7.

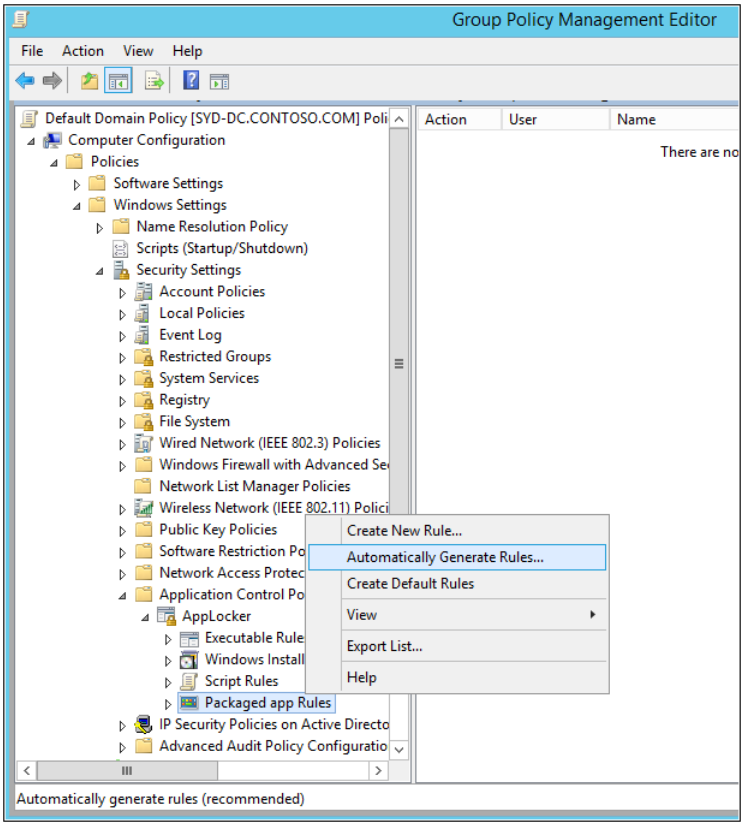


FIGURE 6-7 AppLocker managed through Group Policy Management Editor.

Creating the rules for Windows apps involves configuring rules within the Packaged App Rules section. Right-click this option to display a context menu that allows you to configure rules manually, use the Automatically Generate Rules option (recommended), or use the Create Default Rules option.

The Automatically Generate Rules option is the simplest route. Choosing this option runs a background command and then displays the dialog box shown in Figure 6-8.

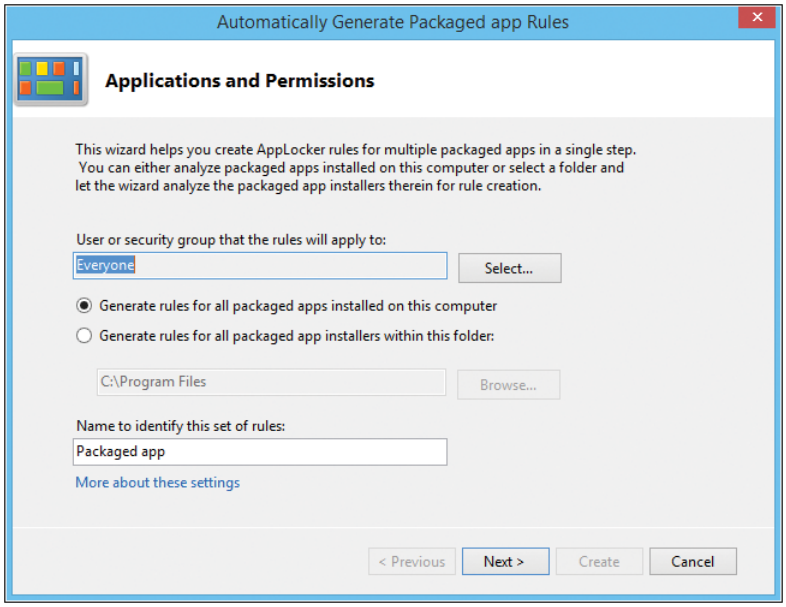


FIGURE 6-8 Choose this AppLocker option to automatically generate rules for currently installed apps on a target device running Windows 8.1.

The next step shows the number of packaged apps that were detected as well as the number of rules that will be automatically generated, as shown in Figure 6-9.

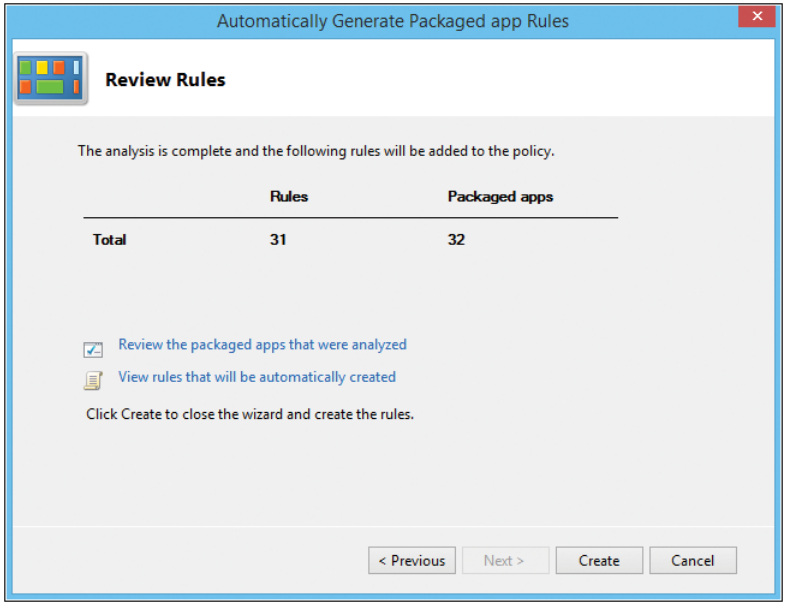


FIGURE 6-9 Before accepting this mass list of automatically generated rules, you should review the apps to ensure that the resulting rules match your organizational security policy.

As a final step, click Review The Packaged Apps That Were Analyzed. That opens a dialog box similar to the one shown in Figure 6-10, where you can clear the check box next to any item for which you do not want to generate a rule automatically.

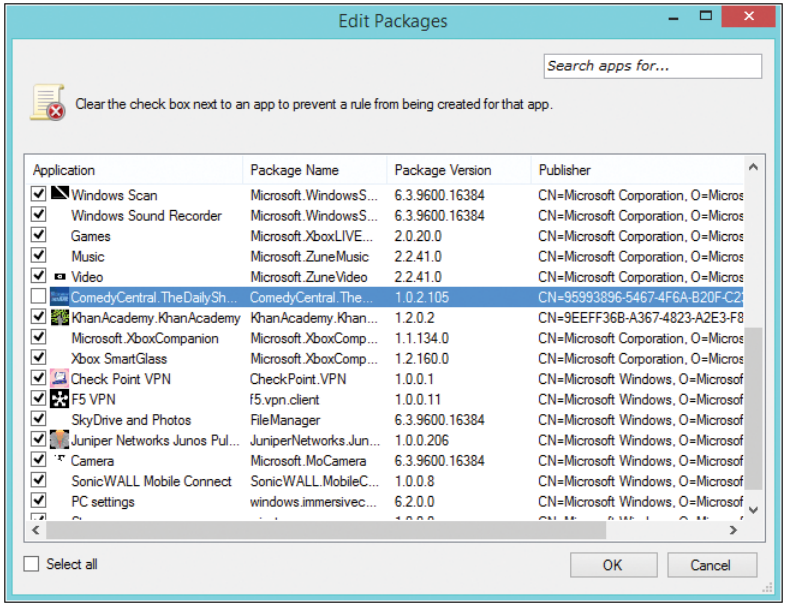


FIGURE 6-10 This dialog box allows you to choose which apps you want to include in your AppLocker rules list.

Choosing the Create Default Rules option from the context menu automatically generates a rule that allows all signed-in users to run all signed packaged apps, as shown in Figure 6-11.

FIGURE 6-11 The default rule allows any user in the Everyone group to run signed Windows Store apps.

For most organizations, this default is unacceptably broad and potentially allows unwanted apps to run. As an alternative, you can right-click this rule and use the Properties dialog box to change this policy from Allow to Deny. After that step is complete, use the Exceptions tab to specify apps that will be allowed to run.

If the process of configuring exceptions for individual apps seems too cumbersome, you can choose to add exceptions using installed packages. For this to work, the app must already be installed on the computer from which you're using AppLocker. Figure 6-12 shows the Local Group Policy Editor, where the default rule has already been set to Deny. Double-clicking the rule opens the Deny Properties dialog box.

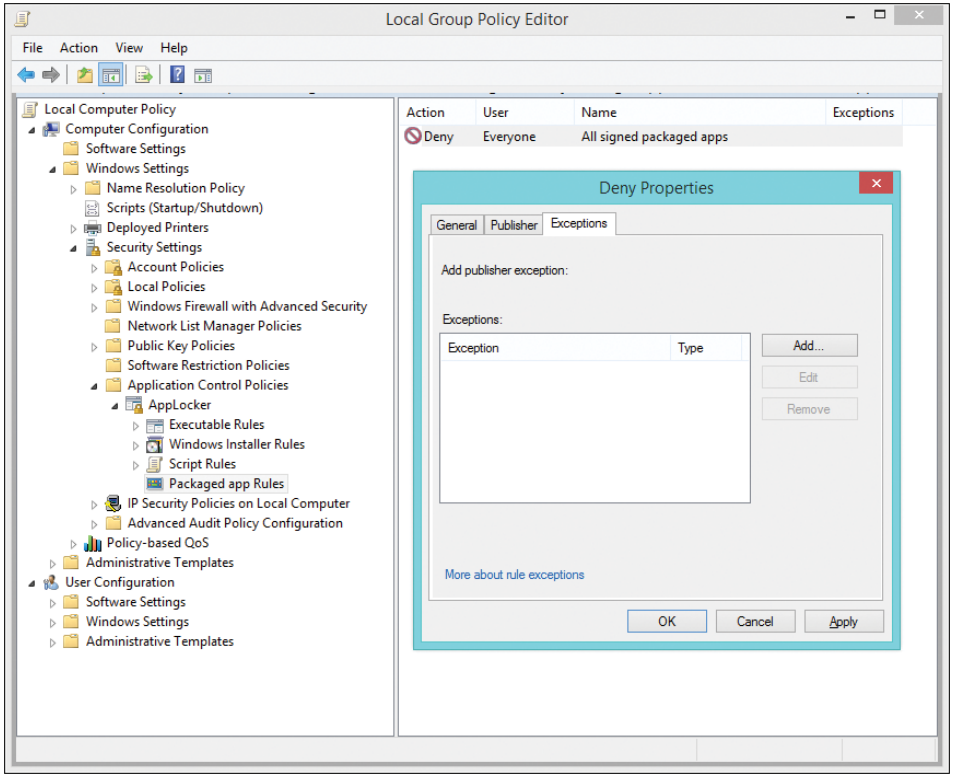


FIGURE 6-12 To add exceptions to a default rule that blocks the running of packaged Windows Store apps, use the Exceptions tab shown here.

Clicking Add opens a dialog box that allows you to select from a list of installed packaged apps (similar to the list shown earlier in Figure 6-10).

In a typical enterprise scenario, it's common practice 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 built-in Finance or Travel apps, for example.

CHAPTER 7

Recovery options in Windows 8.1

Modern businesses have a mix of managed and unmanaged devices to deal with. For conventional PCs that are deployed on a site where IT staff is readily available, any hardware or software problems can usually be dealt with quickly. In the case of a device that won't boot, you can use your deployment environment to restore a standard image and then restore the user's environment from the network.

Unmanaged devices, or managed mobile devices that are in use on the road, pose a different set of problems. For those situations, Windows 8.1 includes a set of recovery tools that are available for a user (perhaps with assistance from the help desk) to perform common repair operations, up to and including a complete refresh of the default operating system.

For organizations that have a volume license agreement with Software Assurance, an additional, extremely powerful resource is available: the Microsoft Diagnostics and Recovery Toolset (DaRT).

This chapter discusses all of these recovery options.

Using Windows Recovery Environment

What happens when a Windows 8.1 device won't boot? The starting point for all repair and recovery options is Windows Recovery Environment (Windows RE), which includes a handful of essential tools for troubleshooting issues, repairing startup problems, and (usually as a last resort) resetting or restoring the operating environment.

MORE INFO **See *http://technet.microsoft.com/en-us/library/hh825173.aspx* for a detailed technical overview of Windows RE.**

When you install Windows 8.1 using Setup, the Windows RE image file (WinRE.wim) is copied to a separate volume. This arrangement has several advantages: It allows the device to boot to the recovery tools even if the volume containing the Windows system files is damaged or protected by BitLocker Drive Encryption. It also prevents users from accidentally or deliberately modifying or removing these recovery tools. On Universal Extensible Firmware Interface (UEFI)–based PCs, the image is copied to a dedicated Windows RE Tools volume. On BIOS-based PCs, the image is copied to the System volume. In either case, the volume is formatted as NTFS.

If you use system images to deploy Windows 8.1, you need to manually configure the recovery partitions, a topic discussed later in this chapter.

Windows RE is based on Windows Preinstallation Environment (Windows PE), runs automatically, and attempts to repair the system if Windows detects a problem with booting the computer. The following scenarios cause Windows RE to run at start-up:

- Two consecutive failed attempts to start Windows
- Two consecutive unexpected shutdowns within two minutes after the boot process completes
- A Secure Boot error
- A BitLocker error on a touch-only device

When Windows detects any of these situations, it attempts an automatic repair. If the repair is unsuccessful, you are taken to the full Windows RE environment.

You can also start Windows RE manually, using any of the following techniques:

- Click the Settings charm, click Power, and hold the Shift key while clicking Restart.
- From PC Settings, click Update And Recovery, click Recover, and then click Restart Now (found under the Advanced Startup heading). Note that this option has been moved from its Windows 8 location, where it was found under the General heading.
- At a command prompt, run the `Shutdown /r /o` command.
- Restart the device using a USB flash drive or DVD that contains the Windows RE files. You can create this drive at any time using the RecoveryDrive.exe utility. The Windows RE files are also available if you boot from Windows 8.1 installation media and choose Repair Your Computer from the bottom of the Install Now screen.

Any of those actions automatically restarts the device and displays the Choose An Option menu, shown in Figure 7-1.

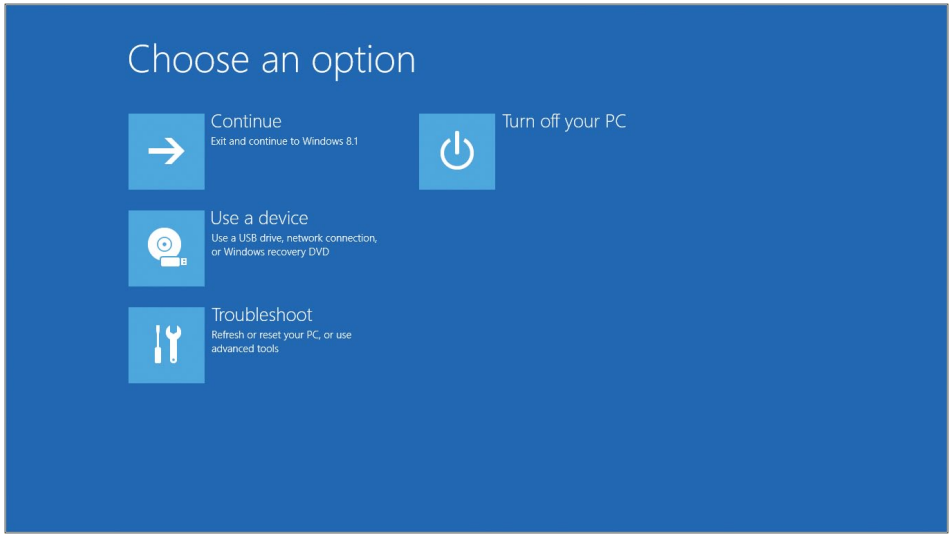


FIGURE 7-1 The Choose An Option menu is your entry to Windows Recovery Environment.

In the Choose An Option menu, clicking Continue allows the user to attempt to boot into the default operating system without taking any further action. (This is the correct option if the system booted into Windows RE because of a transient issue that doesn't need repair.) If multiple operating systems are installed on the computer, the Choose An Option menu might also display Use Another Operating System, which allows you to choose an alternative operating system to boot into.

Click Use A Device if you want to boot from a USB flash drive, DVD drive, or network boot server.

Clicking Troubleshoot opens the Troubleshoot screen, which displays three options:

- Refresh Your PC
- Reset Your PC
- Advanced Options

The Refresh and Reset options are covered fully later in this chapter.

If you click Advanced Options, you'll see a menu that resembles the one shown in Figure 7-2.

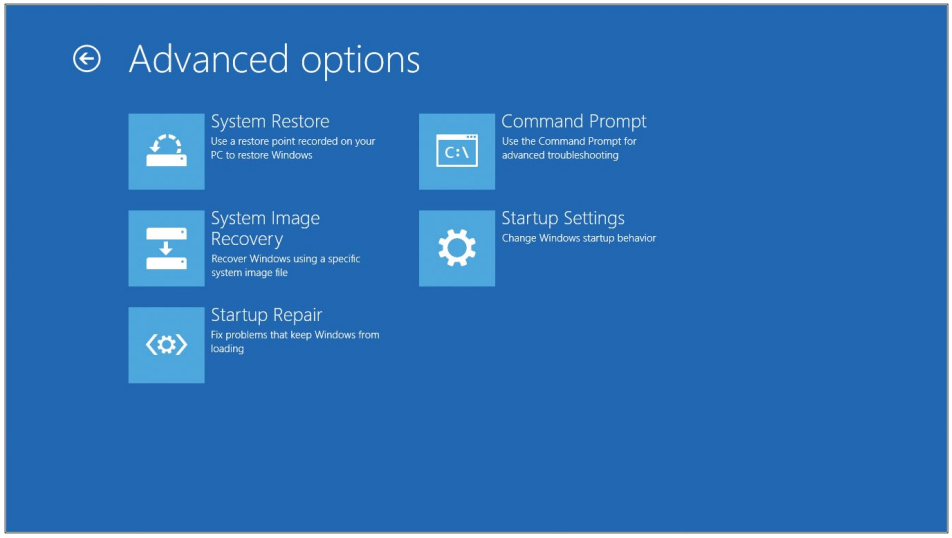


FIGURE 7-2 This Windows RE menu provides access to essential troubleshooting and recovery tools.

Table 7-1 lists the functions available from the Advanced Options menu, many of which are direct descendants of recovery tools found in previous Windows editions.

TABLE 7-1 Advanced options for recovery

Option	Description
System Restore	Allows you to choose a restore point created earlier and restore the system configuration.
System Image Recovery	Replaces everything on the computer with a system image created using the Windows 7 or Windows 8 Windows Backup utility. (In Windows 8.1, this utility is available in the desktop Control Panel, via the System Image Backup link, at the bottom of the File History option.)
Startup Repair	If you choose this option, Windows attempts to diagnose and automatically correct common boot problems.
Command Prompt	Opens an administrative command prompt, where you can use command-line tools such as Bootrec and Bcdedit.
Startup Settings	Changes the boot process so that you can alter other options.

MORE INFO **On a device that uses the UEFI, the Advanced Options menu contains an additional UEFI Firmware Settings option. If you're unable to reach this menu on a UEFI-equipped tablet, power down the device, press and hold the Volume Down hardware button, and then press the Power button. This is the only way to enable or disable Secure Boot, for example.**

Clicking Startup Repair allows you to manually attempt the same set of repairs Windows uses when it detects a failure and launches Windows RE automatically. (This feature was previously called Automatic Repair.) System Image Recovery requires a previously saved image from an external storage device.

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

The Startup Settings option displays several additional items that can be selected to help troubleshoot or correct a problem. Several options should be familiar if you've used the equivalent recovery options in earlier Windows versions, including Safe Mode (with Networking and Command Prompt options), debugging, and boot logging. New in Windows 8 and 8.1 are options you use to disable driver signature enforcement and early launch antimalware protection. These options should be used with extreme care, because they potentially expose the system to significant security risks.

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

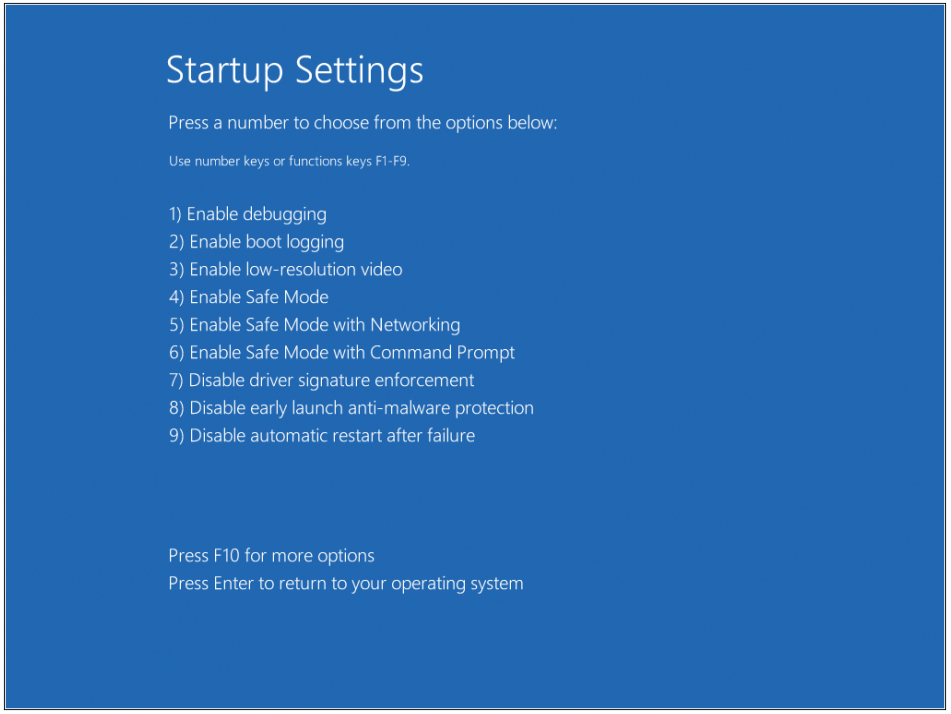


FIGURE 7-3 Use this Windows RE menu to restart using specific diagnostic and troubleshooting options.

Customizing Windows Recovery Environment

A command-line tool, REAgentC.exe, allows an administrator to configure a Windows RE boot image and a push-button reset recovery image, and to administer recovery options and customizations. You can run the REAgentC command on an offline Windows image or on a PC running Windows 8.1. See *http://technet.microsoft.com/library/hh825204* for more information on this tool.

Many organizations develop custom recovery tools to help troubleshoot, manage, and fix computer issues quickly. The recovery image on your organization's PCs can be configured so that these tools and other customizations are available on the Boot Options menu.

As noted earlier, Windows RE is based on Windows Preinstallation Environment (Windows 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/hh825110.aspx* for more information on using and customizing Windows PE.**

Prior to customizing Windows RE, you need to set up the environment. This involves several steps, as described in Table 7-2. These steps assume that you have downloaded and installed the ADK (*http://www.microsoft.com/en-US/download/details.aspx?id=39982*), that the ADK is running on a Windows 8.1 computer, and that you have the Windows product DVD available.

The overall process for customizing Windows RE is as follows:

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 an 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 Deployment Image Servicing and Management (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 varies depending on the needs of your organization, but it 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 custom tool to the Boot Options menu	You can add a tool that shows up within the Boot Options menu screen. See *http://technet.microsoft.com/library/jj126994.aspx* for more information specific to this process.
Add language packs	Language support must be added to both the Windows RE image and to each of the optional components included in the Windows PE image.
Add Windows PE optional components	Several optional components are available with Windows PE and can be added 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.**

Refresh and reset options

When you click Troubleshoot on the Choose An Option menu in Windows RE, the resulting menu (shown in Figure 7-4) includes two push-button reset options intended to allow users to recover or restore a system quickly: Refresh Your PC and Reset Your PC.

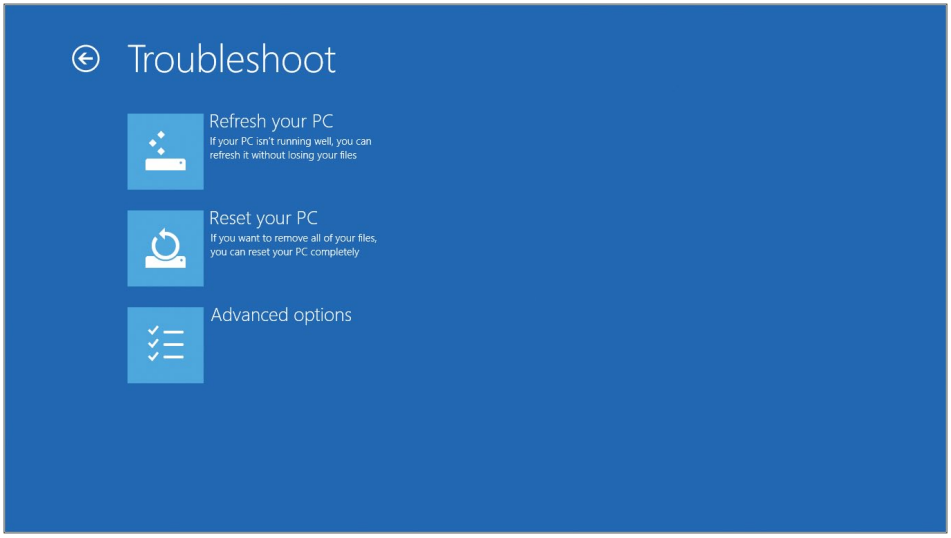


FIGURE 7-4 The two options at the top of this menu are intended to help users restore the original operating system configuration.

On PCs purchased through normal retail channels, the push-button reset recovery image is normally contained in a dedicated partition at the end of the hard drive. This arrangement makes it possible to delete the recovery image (after optionally copying it to external media). This recovery image can consist of a single image file or a set of split image files. Windows 8.1 adds the ability to compress this image file using a new file format with the file name extension *.esd* instead of using the standard *.wim* file.

In enterprise deployments, you can customize these push-button reset features using scripts that can install apps or preserve additional data. You can also use a custom image instead of the image included with an original equipment manufacturer (OEM) PC.

When a computer has repeated problems, many organizations choose to wipe the computer and restore it from their standard build image. The push-button reset options described here can accomplish the same result without wiping out potentially valuable data.

MORE INFO **For detailed instructions on how to customize a system image for use with push-button reset features, see *http://technet.microsoft.com/en-us/library/jj126997.aspx*.**

Refresh Your PC

The Refresh Your PC option changes all PC settings back to their defaults while retaining data files, personalization settings, and apps installed from the Windows Store. Files in the user's profile (except those in the AppData folder) are preserved, as are any folders created in the root of the system drive and on other partitions. Any desktop programs included in the recovery image are restored. All user-installed desktop programs are removed, and a list of removed programs is saved on the desktop.

The Refresh Your PC option boots into Windows RE and gathers user accounts, settings, data, and Windows Store apps. It then expands the operating system image file from the Recovery partition, moving the current operating-system files to a Windows.old folder. The contents of the following folders, including all subfolders, are completely replaced with the corresponding folders from the recovery image:

- \Windows
- \ProgramData
- \Program Files
- \Program Files (x86)
- %UserProfile%\AppData
- Any OEM folders added to the recovery image

After a reboot, the saved settings, data files, and apps are applied to the new operating system. This process can take several minutes to complete.

Note that the Refresh Your PC option requires a significant amount of free disk space to function—Microsoft recommends that you have at least enough space to hold the expanded operating-system image, plus a buffer of 20 percent of that space.

Reset Your PC

The Reset Your PC option removes all apps and user data, including user accounts and personalization settings. This option is useful when you plan to sell an existing PC or reassign it to a new employee.

Because this process, by design, involves significant data loss, the user must click through multiple warning screens that clearly describe what's about to happen. The reset process also includes an option to scrub data from the drive so that it cannot be easily recovered using disk utilities. As Figure 7-5 notes, the Fully Clean The Drive option can add hours to the process. Note that this option, while thorough, is not certified to meet any government or industry standards for data removal.

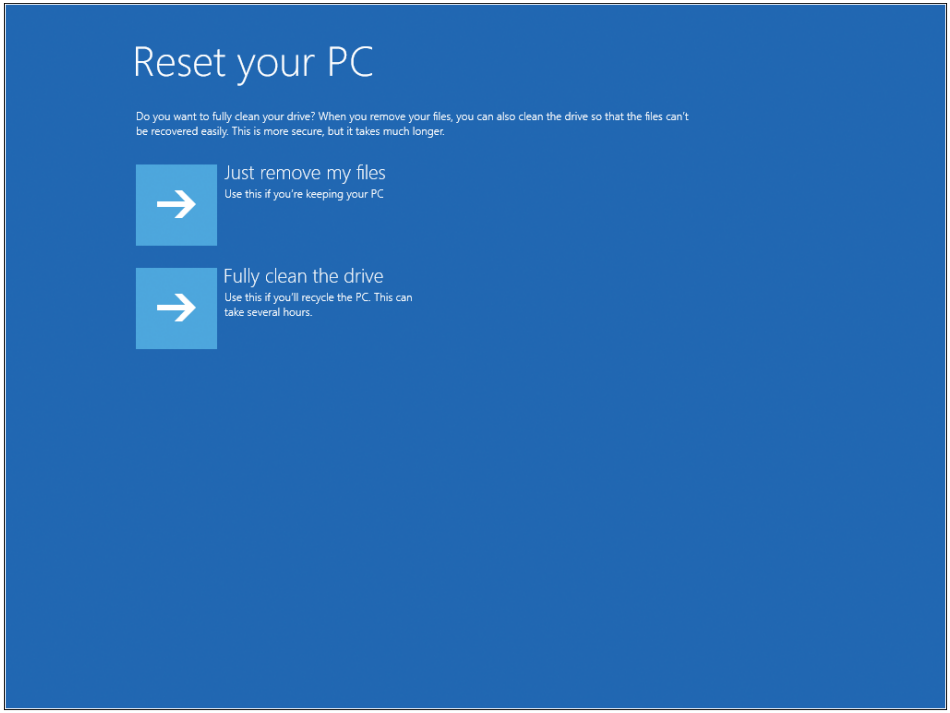


FIGURE 7-5 The Reset Your PC process includes an option to securely wipe the drive so that confidential data files can't be recovered by the next owner of the device.

During a reset, the PC boots into Windows RE. If the system contains multiple partitions that are accessible by the user (such as a dedicated data volume), the user is given the option to format the entire drive or just the Windows partition. All user accounts, data files, settings, applications, and customizations on the Windows partition are removed. The recovery image is applied to the newly formatted Windows partition, and a new Boot Configuration Data store is created on the system partition.

When the system restarts, the user must go through the standard procedures for setting up the PC and creating a new user account, a process formally known as the out-of-box experience (OOBE) phase.

Microsoft Diagnostics and Recovery Toolset

The Diagnostics and Recovery Toolset (DaRT) is part of the Microsoft Desktop Optimization Package (MDOP), which is available by subscription for volume-license customers with Software Assurance. It can also be acquired for evaluation purposes through Microsoft TechNet and MSDN subscriptions.

DaRT version 8 is designed to work with Windows 8. It will not install on a device running Windows 8.1, although a new version should appear around the time of General Availability and might be available by the time you read this.

The chief benefit of DaRT is that it provides extended recovery and repair options beyond those provided in Windows RE. DaRT supports UEFI boot and can create Windows Imaging Format (.wim) or ISO images that can be deployed with USB media. 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.

A default DaRT installation adds a Recovery Image Wizard that can be used to create an advanced recovery tool for IT professionals. As Figure 7-6 shows, this image can include a rich collection of tools that allows local users to perform a range of recovery tasks. This toolset includes Disk Commander, which can be used to repair damaged disk partitions and volumes; a Crash Analyzer, which makes sense of crash dump files; and a Hotfix Uninstall tool that can be used if a hotfix causes problems with a PC.

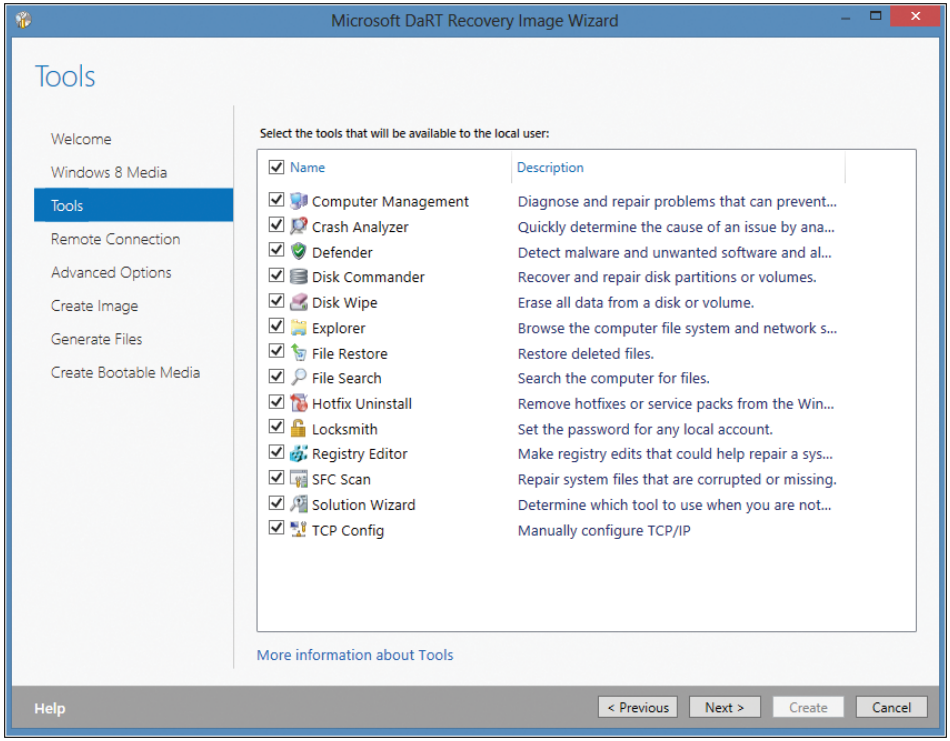


FIGURE 7-6 Using the DaRT Recovery Image Wizard, you can add any or all of these diagnostic and repair tools to the recovery image.

This image can be customized to add drivers and other items necessary to aid in the recovery of a computer.

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

- Manual boot with removable media such as a USB flash drive
- Manual installation as a recovery partition on the computer's hard drive
- Automated installation as a recovery partition using enterprise-deployment tools, such as System Center Configuration Manager
- As a network service delivered using Windows Deployment Services

Some organizations deploy DaRT as the default recovery partition in standard images. Doing so makes the recovery tools available at all times and eliminates the need for bootable removable media.

CHAPTER 8

Windows 8.1 and networks

One of the key design goals of Windows 8.1 is to enable mobility features in portable PCs and tablets. So it should come as no surprise that Windows 8.1 adds significant new features to the networking capabilities introduced in Windows 8. It also introduces some changes to the user interface for managing wireless connections.

What's new in Windows 8.1 networking?

The following wireless networking features are new in Windows 8.1:

- **Near field communication (NFC) tap-to-pair printing** Enabling printing support on an enterprise network can be difficult and confusing, with the worst-case scenario being that a sensitive document is sent to the wrong printer. Windows 8.1 devices that include NFC support can connect to an NFC-enabled enterprise printer with a simple tap. Existing printers can be NFC enabled with NFC tags.
- **Wi-Fi Direct printing** Wi-Fi Direct is a new standard that allows devices to connect to one another over a wireless network in peer-to-peer fashion, without requiring an access point. Although the most popular uses of the technology involve consumer scenarios such as media playback, the same technology can also be used on enterprise networks to allow easy and secure connections to printers without requiring additional drivers or software on a Windows 8.1 device.
- **Native Miracast wireless display** Miracast is another standard that uses Wi-Fi Direct to stream audio and video from a device to a Miracast-enabled display or projector. An obvious application in enterprise environments is to pair a Windows 8.1 tablet or laptop to a conference room projector with Miracast, then project your presentation without wires or dongles.

Mobile broadband support

Windows 8 introduced a built-in management tool and integrated, mobile broadband class driver to simplify the process of configuring mobile broadband connections on portable devices. The result is that virtually all mobile broadband devices work out of the box. Using the Windows Connection Manager, you can manage all wireless radios side by side.

Because mobile broadband connections often involve data caps, Windows 8.1 includes metered connection awareness features that allow you to turn off or delay potentially expensive network activities while a metered connection is in use.

Windows 8.1 adds support for broadband tethering, which allows you to share the data connection from a mobile broadband-enabled PC or tablet, turning the device into a personal Wi-Fi hotspot. This capability has been common in phones for several years and is now available in PCs and tablets that are capable of using those same mobile broadband connections.

Changes in the Wi-Fi user experience

Windows 8.1 also changes the user experience for connecting to conventional Wi-Fi access points. As in Windows 8, the availability of a wireless network is indicated by an icon that appears when you click the Settings charm. Clicking an available network from the list allows you to enter a wireless access key.

As in previous versions, Windows 8.1 maintains a list of wireless access points to which a device has previously connected. If you select the Connect Automatically check box, the access key is saved and synced to other devices that sign in using the same Microsoft account.

To view the properties of the current Wi-Fi connection, open PC Settings, click Network, and select the connection name from beneath the Wi-Fi heading. That displays a page like the one shown in Figure 8-1, where you can define a connection as Metered. This option is especially useful when a worker is traveling and connecting to networks that might charge by the amount of data transferred rather than by time.

Windows 8.1 automatically prioritizes networks using its own straightforward algorithm. Ethernet (wired) networks always have first priority, followed by Wi-Fi networks, and then mobile broadband. You can manually connect to a mobile network when a Wi-Fi network is in range, but your preference is saved only for the current session.

Each time you connect to a new wireless network, its name and properties, including an access key if you enter one, are added to the list of saved networks. When you choose the Connect Automatically check box, the connection information is saved and the network is added to the top of the list of preferred networks. The next time you're in range of that access point Windows 8.1 will automatically make a wireless connection. When resuming from standby, reconnecting to a wireless network is much faster than in previous Windows versions—Windows 8.1 is capable of connecting to a saved wireless network in less than two seconds.

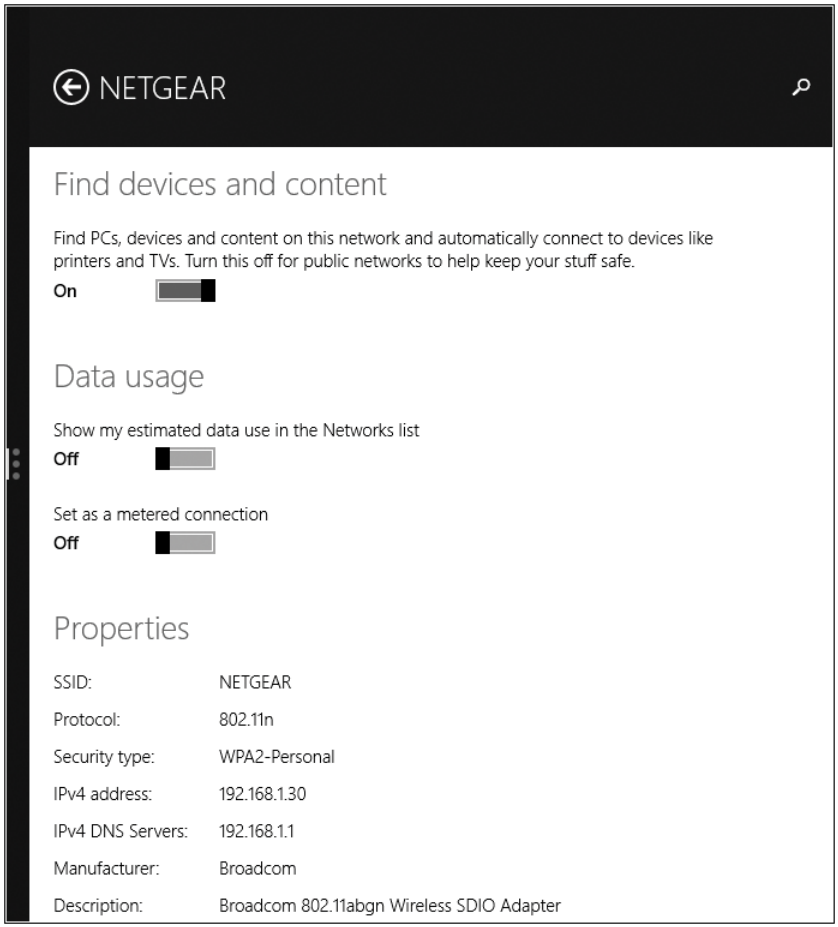


FIGURE 8-1 Using PC Settings, you can view and adjust properties for the currently connected Wi-Fi network.

Unlike in previous Windows versions, there's no easy way to view and manage saved network profiles other than the currently connected one. To see a list of all saved wireless profiles, you need to open a command prompt and use the following command:

```
netsh wlan show profiles
```

To delete a saved profile, use the following command:

```
netsh wlan delete profile name="profile_name"
```

The string following `name=` matches the name of the saved profile from the list you displayed earlier. Note that the profile name is not case-sensitive, but it must be enclosed in quotes.

The option to display a connection as metered lets you see total data usage on that connection, with an option to reset the counter when you start a new billing period. Figure 8-2 shows an example of metered usage monitoring.

FIGURE 8-2 Using PC Settings, you can view and adjust properties for the currently connected Wi-Fi network.

The Networks panel also provides easy access to Airplane Mode, which disables all internal network connections, including Wi-Fi, Bluetooth, GPS, and mobile broadband. Each individual component can be re-enabled from the Network panel in PC Settings.

Connecting to corporate networks

Remote networks are by definition untrusted. A worker who connects to a free Wi-Fi hotspot in an airport or uses a hotel's guest network runs the risk of having the connection intercepted by a malicious outsider, with potentially devastating consequences for data on a corporate network.

The solution, historically, is to use a virtual private network (VPN), which encrypts the connection between the corporate network and the remote PC so that packets traveling over the untrusted network are unreadable by an attacker.

VPN client improvements

Windows 8 included a basic VPN client. Windows 8.1 and Windows RT 8.1 add support for a wider range of VPN providers, including Check Point, F5, Juniper Networks, and SonicWall, in addition to the Microsoft client. Setting up a VPN connection is accomplished from the Network pane in PC Settings, as shown in Figure 8-3.

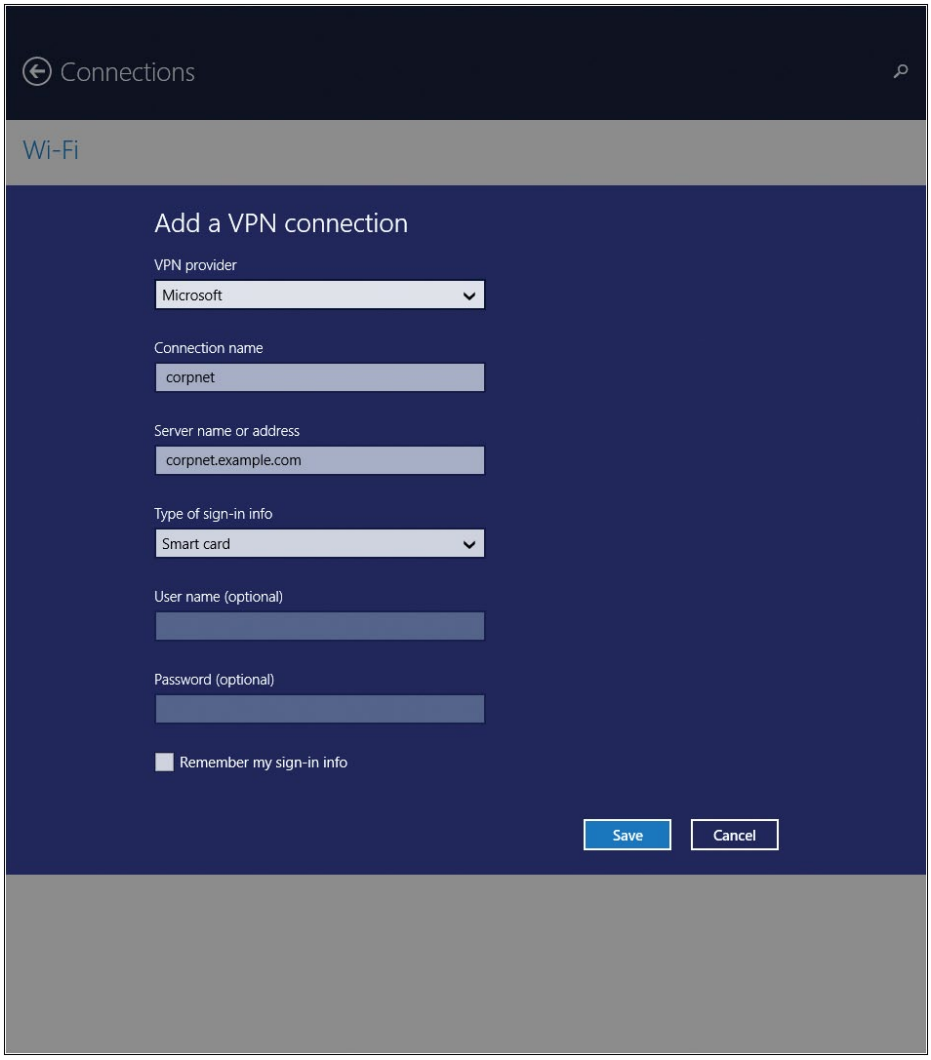


FIGURE 8-3 The built-in VPN client supports multiple VPN providers and allows the use of smartcards and one-time passwords in lieu of usernames and passwords.

The other major new feature in Windows 8.1 is the ability to automatically trigger VPN connections when you select an app or resource that requires the VPN. If you access your company's intranet site from a remote network, for example, Windows 8.1 automatically prompts you to sign in with one click. This feature is available with third-party VPN providers when using the built-in VPN client.

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 in Windows Server 2012 R2 and Windows 8.1 are designed to work optimally together.

BranchCache supports two modes:

- **Hosted Cache mode** In this configuration, 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.
- **Distributed Cache mode** Using this option saves the cache on individual client machines. This quick deployment cache method is best suited for small offices with fewer 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

Remotely connecting to corporate network resources through a VPN involves hassles, starting with configuration headaches and continuing with potential security problems if users do not frequently reconnect to the network to receive security and Group Policy updates. The improved VPN client in Windows 8.1 reduces some of this friction, but there's an even better solution.

DirectAccess allows remote users to securely access shared resources, websites, and applications every time they connect their DirectAccess-enabled mobile device to the Internet. DirectAccess does not require frequent logins or access maintenance, and it 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.

DirectAccess requires Windows 8.1 Enterprise edition and Windows Server 2012 or later.

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 local networks, allowing homes and small businesses to have one IPv4 address but multiple devices connected to the Internet. The widespread use of NATs makes location-based services less effective and degrades many applications that rely on direct communication.

To remedy these issues, IPv6 was created with unimaginable scale, offering 3x10^38 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 are being implemented. This allows devices to be configured with both IPv6 and IPv4 addresses. In Windows 8 and 8.1, if an IPv6 address is present, it will automatically take connection priority over the IPv4 address. Because some applications do not support IPv6, Windows will automatically select the correct connection for applications, using a method called *address sorting*. These advanced Windows features indicate that Windows 8.1 is fully capable of supporting the IPv6 Internet.

Windows Server 2012 R2 expands support for IPv6 in Group Policy and allows these new settings to be used with Windows 8.1. The expanded support includes the following:

- TCP/IP printers can be configured to use IPv6 addresses.
- In any Group Policy preference, item-level targeting can be used to set an IPv6 address instead of an IP address range.
- For VPN connections, a Use IPv6 check box is available.

More details about these settings are available at *http://technet.microsoft.com/en-us/library/dn265973.aspx*.

CHAPTER 9

Virtualization in Windows 8.1

In its most common configurations, Windows 8.1 is installed on a physical device, with the operating system, apps, and data running directly from local storage media. That approach has undeniable advantages in terms of performance, but it also causes management headaches for administrators. If the local storage on that physical device fails, its data is gone for good, for example. And switching to a different device means that the user no longer has access to her familiar environment.

The solution to these and other challenges is *virtualization*, which comes in multiple forms. Windows 8.1 Pro and Enterprise include the capability to create virtual machines that can run other copies of Windows, even different editions, using the same professional-strength hypervisor found in Windows Server products. In corporate settings, administrators can use server-based virtualization tools to give users access to apps or entire desktop environments, which can be delivered to a wide range of device types.

This chapter explains how each of these different virtualization options works in Windows 8.1.

> ***MORE INFO*** **Virtualization topics could fill an entire book all on their own, so this chapter just scratches the surface. For detailed discussions and lab guides for all types of virtualization solutions, see the Microsoft Desktop Virtualization website at *http://www.microsoft.com/dv*.**

Let's start with the simplest solution of all, one that requires only the most minimal setup to get started.

Client Hyper-V

Windows 8 was the first version of Windows to include a built-in hypervisor, which allows developers and IT pros to create virtual machines running Windows or alternative operating systems, primarily for test and evaluation purposes. Client Hyper-V is also a useful compatibility tool, allowing users to run programs that require earlier versions of Windows without having to give up the benefits of Windows 8.1.

Client Hyper-V uses the same technology and virtual machine formats as in Windows Server 2012 and Windows Server 2012 R2, which allows you to move virtual machines between server and client machines and run them without modification. Client Hyper-V runs on 64-bit versions of Windows 8.1 Pro and Enterprise. It supports 32-bit and 64-bit guest operating systems, which can be created on the fly from physical installation media or by mounting an ISO file. You can also create a virtual hard disk (VHD) from a physical disk, even one that contains a running operating system, using the Windows Sysinternals Disk2vhd tool, available from *http://technet.microsoft.com/en-US/sysinternals/ee656415*.

> ***MORE INFO*** **In enterprise environments, the Virtual Machine Manager in System Center allows you to convert physical computers into virtual machines. For an overview of the process, see "How to Deploy a Virtual Machine by Converting a Physical Computer (P2V)," at *http://technet.microsoft.com/en-us/library/hh368990.aspx*.**

Client Hyper-V is not enabled in a default installation of Windows 8.1 Pro or Enterprise. Before you can use it on an individual PC or as part of a standard image, you need to first confirm that you're running a 64-bit operating system, that the host machine supports Second Level Address Translation (SLAT), and that this feature is enabled. Most modern 64-bit PCs designed for enterprise use include this capability.

To enable Client Hyper-V, follow these steps:

1. From the desktop Control Panel, click Programs, and then select Programs And Features.
2. Select Turn Windows Features On Or Off.
3. Select the Hyper-V option, and make sure that the additional items beneath it are selected as well, as shown in Figure 9-1. Click OK, and then restart the PC to enable the features.

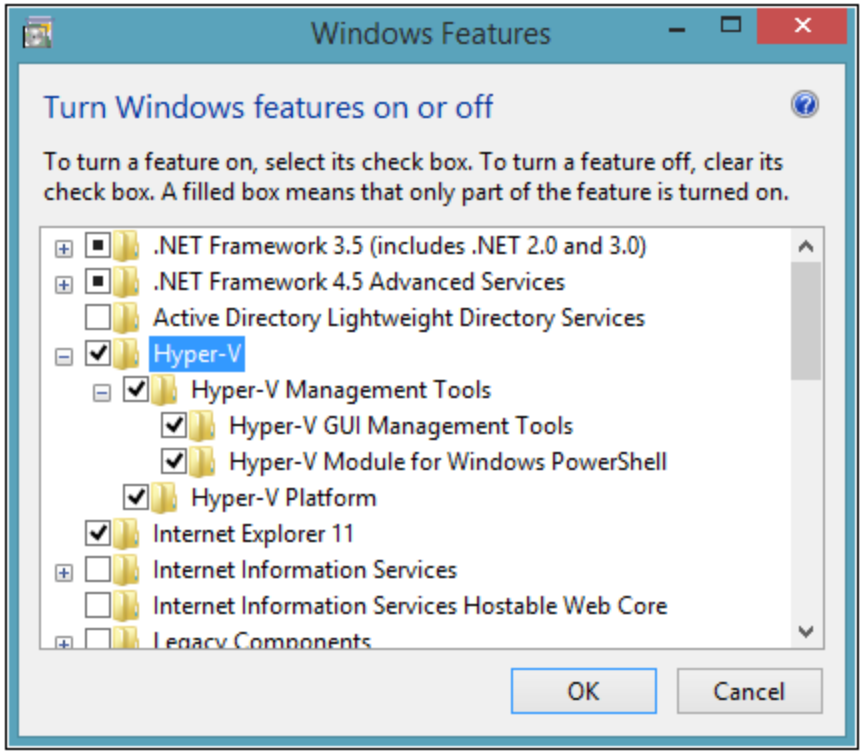


FIGURE 9-1 The Client Hyper-V components must be enabled using this dialog box.

To enable Client Hyper-V using Windows PowerShell, use the following cmdlet:

```
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 virtual machines (VMs) through Hyper-V Manager or the Hyper-V Module for Windows PowerShell. Figure 9-2 shows the settings for a virtual machine running Windows 8.1 Enterprise.

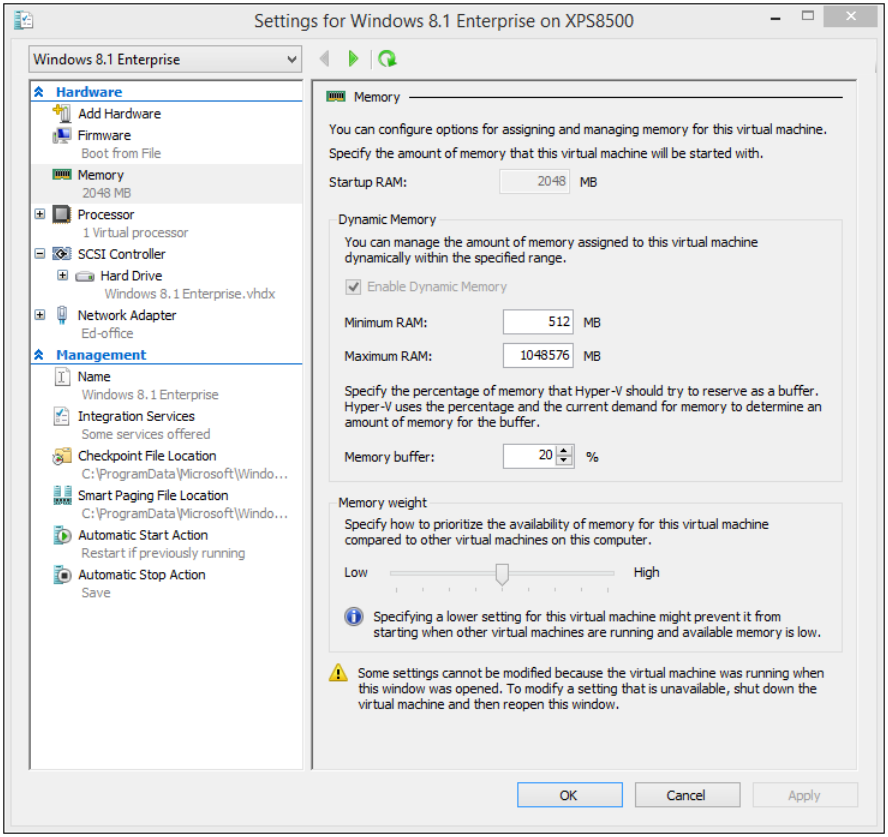


FIGURE 9-2 One useful feature of Client Hyper-V in Windows 8.1 is the capability to use Dynamic Memory, which allows the host machine to provide the VM with memory when it's needed.

You can use the Virtual Machine Connection program to work with VMs or access them via Remote Desktop. Note that a Hyper-V machine can use up to 12 monitors, with support for wireless networks and sleep and hibernate states on the host machine. Hyper-V machines do not natively support audio or USB devices, although these capabilities can be enabled via Remote Desktop by specifying local resources on the device running the Remote Desktop client. Multitouch capabilities are not available with a Hyper-V VM, although single-touch capability is available when used on compatible hardware.

Desktop virtualization options

In a world where users are likely to switch frequently among multiple devices, some of them unmanaged, it's important to provide a way for those users to access a familiar, consistent working environment securely. For enterprises, Microsoft provides a range of solutions that allow these managed desktops to run in the data center. Users can access these hosted desktops for work, keeping their personal environment separate.

Windows 8.1, Windows Server 2012 R2, and the Microsoft Desktop Optimization Pack (MDOP) offer virtualization solutions that provide a rich user experience, virtually identical to that on a physical desktop. Additional server-side solutions allow virtualization of individual apps and of the user experience. In the data center, administrators can effectively manage apps and data and ensure that security and compliance policies are properly enforced.

These desktop virtualization options are powered by Remote Desktop Services (RDS) in Windows Server 2012 and Windows Server 2012 R2. RDS provides a single platform to deliver any type of hosted desktop, while RemoteFX provides a consistently rich user experience:

- **Rich experience** RemoteFX uses a built-in software graphics processing unit (GPU) or hardware GPU on the server to provide 3-D graphics and a rich multimedia experience. RemoteFX also offers USB redirection and multitouch support so that users can be productive even on tablets. Performance is consistent even 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. It also supports lower-cost disk storage like Direct Attached Storage.
- **Streamlined management** A simplified wizard makes setting up desktop virtualization easier with automatic configuration of VMs. The management console on the server 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.

MORE INFO **For more information about Remote Desktop Services, including a series of useful lab guides to help you set up a test environment, see *http://technet.microsoft.com/en-us/library/hh831447.aspx*.**

Using RDS, you can deliver virtualized desktops using any of the following methods:

- **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 a user logs 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 option is a variation on the traditional terminal services approach to desktop virtualization.

NOTE **With pooled VMs and session-based desktops, users can personalize their experiences, although they cannot install applications. Roaming user profiles and folder redirection enable personalized environments, while 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 the user's profile folder and persists between sessions.**

Regardless of the common benefits of these methods, your choice of which one to use depends on various considerations, as described here and summarized in Table 9-1:

- **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 (that is, 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 or later. In VM scenarios, however, Windows 8.1 is running in the VM, allowing installation of applications that are compatible with that client operating system. Administrators control applications installed on pooled VMs.
- **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, because 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 than personal VMs, in which each user uses an individual image.
- **Cost** Because session-based virtualization offers the highest densities and a single image, it is usually easier to manage at the lowest cost. Pooled VMs have the single-image and management benefits of session-based virtualization, 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. Organizations can reduce overall costs by taking advantage of lower-cost storage options, application virtualization, dynamic memory, and user-profile disks.

TABLE 9-1 Choosing the right desktop virtualization option

	Session-Based Desktop	Pooled VMs	Personal VMs
Personalization	**	**	***
Application compatibility	**	***	***
Ease of management	***	**	*
Cost effectiveness	***	**	*

* = Good; ** = Better; *** = Best

Application virtualization

Microsoft offers two solutions for application virtualization, both available in Windows Server 2012 and Windows Server 2012 R2. The first is RemoteApp, a 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, which is part of MDOP. It works by packaging apps that can be streamed from a server and run without requiring an application installation. Users can access their applications dynamically from almost anywhere on any authorized PC just by clicking and running a package. The resulting experience is no different from what the user would experience if the app were running locally.

Virtual applications run in their own self-contained virtual environments on users' PCs. This eliminates application conflicts—you can actually run different versions of the same program on the same PC, even running apps that prohibit side-by-side installations on the same PC. 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 use a sequencer app, like the one shown in Figure 9-3, to create the application package, which is saved using the file name extension .appv. The sequencer monitors the installation process, which you can choose to do manually if you prefer.

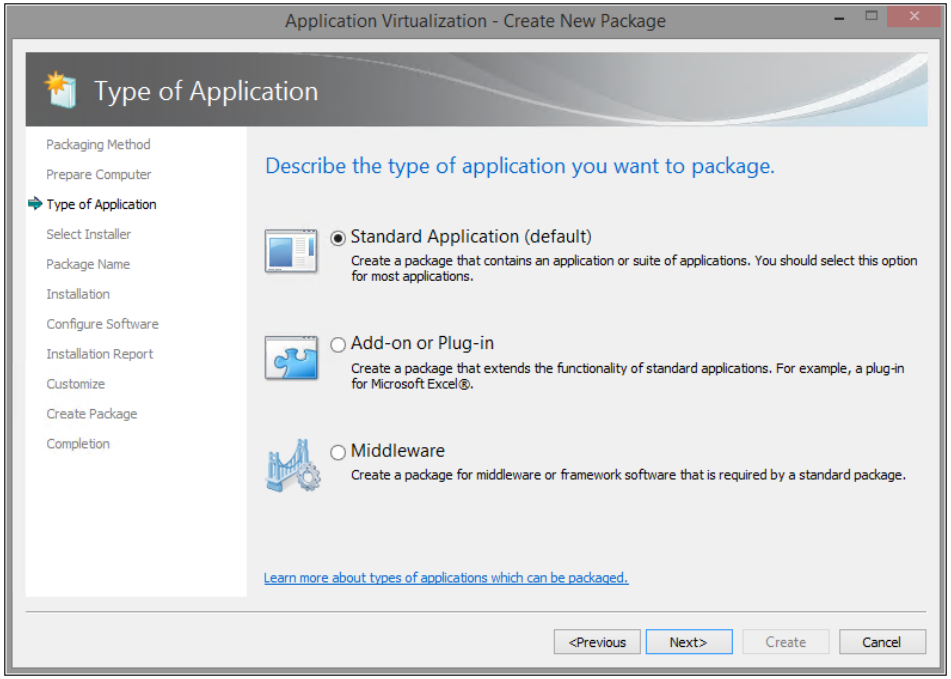


FIGURE 9-3 The App-V Sequencer creates an app package that can be deployed across the network without requiring local installations.

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, which was released at the same time as Windows 8, offers a web-based management interface and support for Windows PowerShell, to enable scripting of complex or repetitive tasks. Dynamic configuration options allow you to deliver a single package with different customizations for different groups of users. You can also package applications and their dependencies separately to make the updating process easier.

App-V 5.0 SP2 will debut after the release of Windows 8.1 as part of a new version of MDOP. It comes in desktop and RDS versions and offers usability and performance improvements. It also adds the capability to install apps that use shell extensions and to include runtime dependencies like MSXML and Visual C++ libraries.

User Experience Virtualization (UE-V)

User Experience Virtualization (UE-V) debuted in MDOP along with Windows 8. This enterprise feature allows administrators to centralize applications and Windows settings in the data center, enabling users to access their desktop applications virtually anywhere, on their choice of devices.

UE-V 2.0, which is designed for the next version of MDOP, adds support for Windows Store apps, including apps purchased through the Store and line-of-business (LOB) apps deployed internally. Administrators can define which Windows Store apps are synchronized; all apps that are included in a default Windows 8.1 installation are configured so that personalized settings for those apps roam across devices. This release also includes a new Company Settings Center that allows users to control which settings are synced across devices, troubleshoot issues that occur with those devices, and sync settings manually rather than wait for an automatic sync. Figure 9-4 shows this feature in action.

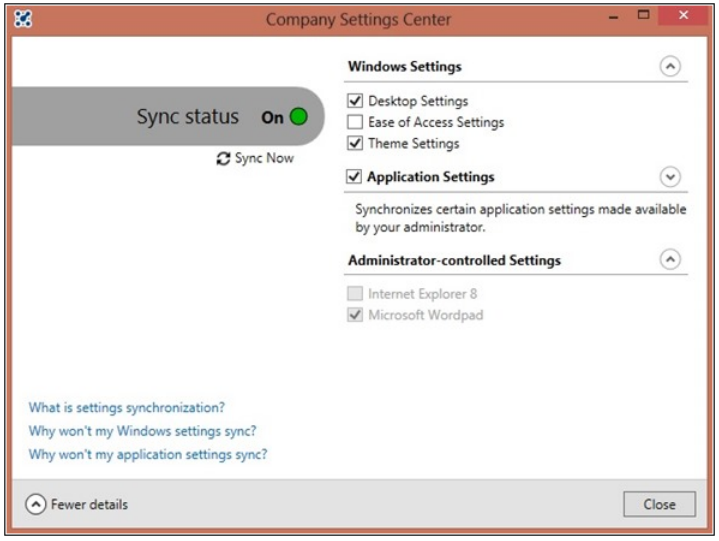


FIGURE 9-4 The Company Settings Center, new in UE-V 2, allows administrators to grant users more control over which settings are synced between devices.

UE-V 2 includes a new sync provider that now allows a sync at specific, administrator-defined intervals (with the default being every 30 minutes), in addition to the normal triggers, such as lock and unlock and connections to RDS. Unlike with its processor, this new sync engine does not require the Offline Files feature.

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

Although UE-V roams user settings, Folder Redirection complements UE-V by centralizing user data folders (Documents, Pictures, Videos, and so on) 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 and 8.1 works largely the same as it did in Windows 7. Users have full-time access to their documents, pictures, videos, and other files from any PC.

A new feature called Work Folders offers significant improvements over Folder Redirection and Offline Files. (Most notable is the ability to sync files on devices that aren't domain-joined.) You can read more about this feature in Chapter 11, "Managing mobile devices."

CHAPTER 10

Windows RT 8.1

Windows RT is a recent addition to the Windows family, originally debuting alongside Windows 8 in October 2012. Windows RT 8.1 was released at the same time as Windows 8.1. It is not sold in retail or original equipment manufacturer (OEM) packages, as other members of the Windows 8.1 family are, nor is it available to Volume License customers. Instead, it is available pre-installed on PCs and tablets powered by ARM processors, such as the Microsoft Surface with Windows RT and the Surface 2, which is the first device powered by Windows RT 8.1.

The power-sensitive, efficient design of Windows RT 8.1 helps hardware manufacturers design and build thin and lightweight devices with remarkable battery life. The main focus for Windows RT 8.1 is running cloud-enabled, touch-enabled, web-connected apps based on the Windows Runtime (WinRT); these are, with very rare exceptions, the same apps available in the Windows Store on Windows 8.1.

As befits a brand-new platform that is still developing rapidly, Windows RT 8.1 devices are in small supply, especially when compared with the massive market for general-purpose PCs running x86 and x64 Windows editions. In enterprise environments, Windows RT 8.1 is suitable for specific use cases, especially where extreme mobility is a top requirement. However, Windows RT 8.1 devices are not general-purpose PCs, and knowing their limitations is crucial to deciding whether (and if so, where) Windows RT 8.1 has a place in your organization.

This chapter discusses the features and capabilities of Windows RT 8.1. For more details on how to manage these devices, see Chapter 11, "Managing mobile devices."

What Windows RT 8.1 can and can't do

In general, Windows RT 8.1 has the same features as the base edition of Windows 8, including the desktop versions of File Explorer and Control Panel as well as the modern PC Settings. This section discusses in detail the significant exceptions that apply to all devices on the Windows RT platform.

First, and by far most important, Windows RT 8.1 does not support the installation of Windows desktop programs. Any software compiled for Intel-compatible x86/x64 chips will not run on any release of Windows RT. This includes any program that uses an MSI installer or an EXE file. Although it might be theoretically possible, there is currently no supported way for third-party developers to adapt and compile their existing Windows desktop apps to run on the Windows RT platform, nor has Microsoft announced any plans to change the fundamental design of the platform in this regard.

In Windows RT 8.1, a handful of Microsoft apps are included with the operating system, including a Windows RT–specific edition of Microsoft Office (discussed in the following section). Any additional apps can be installed only through the Windows Store and run in the sandboxed WinRT environment. The benefits of this design are obvious: users can't knowingly or unknowingly install malicious or buggy desktop programs that can destroy data, steal confidential information, and cause reliability and performance issues.

Those benefits come at a price, however, which is a much greater lack of backward compatibility than any other Windows 8.1 edition. If you are considering deploying Windows RT 8.1 in an enterprise setting, this fact could have a very large influence on your final decision. Here are some of the questions you should ask:

- **Are Windows RT 8.1 drivers available for the devices I use?** The operating system includes class drivers that support most mouse, keyboard, printer, camera, scanner, smartcard, Bluetooth, and storage devices on ARM processors. As a result, many devices, such as USB storage devices, work as soon as you plug them in. The list of compatible printers is large but not complete. Wired network devices are also an area of potential compatibility concern. To check device compatibility, visit *http://www.microsoft.com/en-us/windows/compatibility/CompatCenter/Home*. For business-critical devices, don't rely exclusively on a compatibility list; hands-on testing is essential in that case.
- **Do essential services require utilities written for desktop Windows?** Take a close look at any online services you use to confirm that they will work in Windows RT 8.1. Online file storage services, for example, often depend on a helper application to synchronize files between the cloud and the local file system. Windows RT 8.1 adds that capability for Microsoft's cloud storage system, SkyDrive. Third-party services do not have that capability at this time.

> ***NOTE*** **Microsoft has agreed to change the name of its SkyDrive service for legal reasons. The working of the service will be unchanged.**

- **Do I need access to alternative web browsers?** Internet Explorer 11 is the only browser available in Windows RT 8.1. If you require the use of third-party browsers, you should choose a PC with an x86/x64 or Atom processor running Windows 8.1.
- **Are web plugins essential to my business?** Internet Explorer 11 on Windows RT 8.1 does not support the installation of any third-party plugins, including password managers, video players, and runtime engines. This is true even when using Internet Explorer on the desktop. Adobe Flash support is built in to Internet Explorer 11 (both the desktop and immersive browser experiences), and updates are delivered automatically along with other Windows RT 8.1 updates.
- **Does my business rely on any Office add-ins?** As I explain later in this chapter, Office 2013 RT is included with Windows RT 8.1. Although it's capable of most tasks you expect from a modern version of Office, it lacks the capability to run many common add-ins and plugins. It also lacks support for macros, which means any custom document templates based on macros will not work properly on a Windows RT 8.1 device.
- **Can my business-critical apps run in a WinRT or web-only environment?** If your business relies on a Windows desktop program to handle accounting, point-of-sale transactions, or custom line-of-business (LOB) activities, you need to find a replacement that runs on Windows RT 8.1. The only alternatives are WinRT apps (from the Windows Store or written in-house) or web apps that run acceptably in Internet Explorer 11.
- **Is my network architecture compatible with Windows RT 8.1?** The feature list for Windows RT 8.1 includes support for some virtual private network (VPN) and mobile broadband clients, but you need to confirm support for the specific network features your business uses.

In addition, some features that are available on Windows 8.1 PCs are not available on Windows RT 8.1 devices:

- The Storage Spaces feature is not available.
- The desktop Windows Media Player utility is unavailable.
- Windows RT 8.1 devices cannot be joined to a domain.

The Local Group Policy Editor (Gpedit.msc) is available in Windows RT 8.1, but the Group Policy Client service must be enabled before local policies will be applied.

Windows PowerShell on Windows RT 8.1 also lacks some features found in x86 and x64 Windows 8.1 editions. Scripting access to the Microsoft .NET Framework, for example, is not supported, and the PowerShell Integrated Scripting Environment (ISE) found in other editions is not included in Windows RT 8.1.

Office 2013 RT

Windows 8.1 includes Microsoft Office 2013 RT as a standard feature. This unique edition of Office is compiled to run on ARM processors. Although the user experience and feature set for individual programs are similar (and in many cases identical) to the corresponding Office editions built for x86 and x64 processors, it cannot be upgraded to other Office 2013 editions, including those that are part of Office 365. Office 2013 RT updates are delivered only through updates to Windows RT 8.1.

These are touch-optimized, desktop versions of Microsoft Word, Excel, PowerPoint, OneNote, and Outlook. Outlook was not included in the original release of Windows RT; if you install the Windows RT 8.1 update on a device running the original release of Windows RT, the Office 2013 RT programs are updated, with Outlook added to the lineup. Figure 10-1 shows the Backstage view in Office 2013 RT, with connections to SkyDrive and other online services.

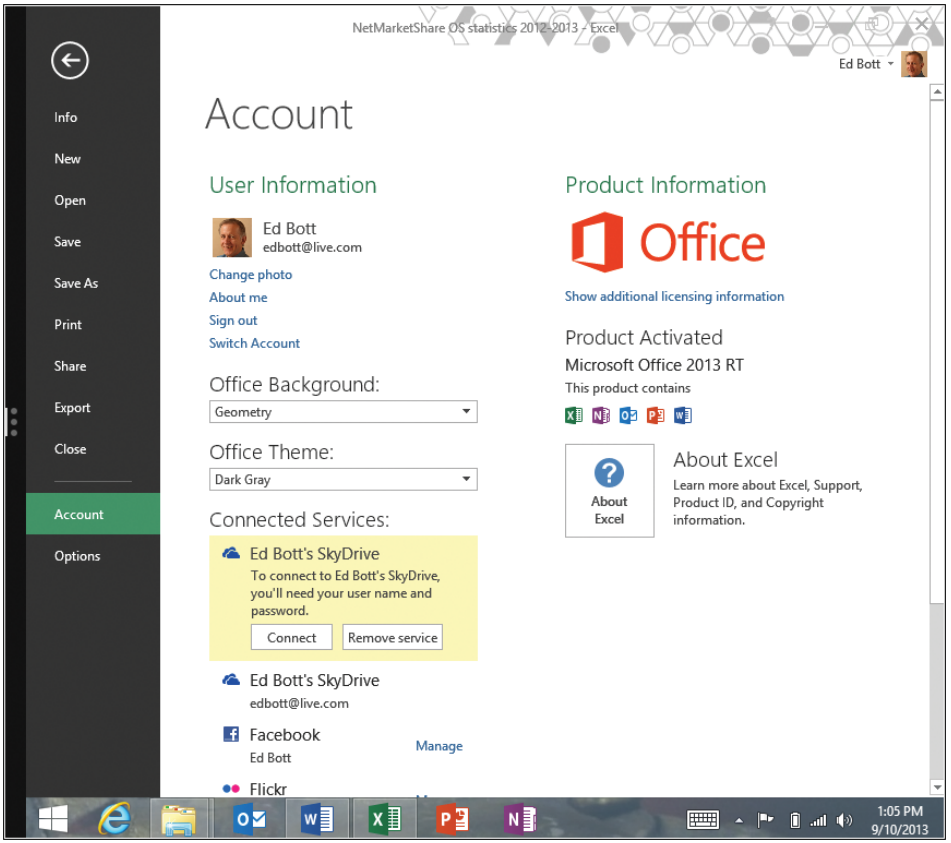


FIGURE 10-1 Every copy of Windows RT 8.1 includes Office 2013 RT, with the five programs shown here. It allows connections to online services but cannot be replaced with a different edition.

Two additional free Office apps are available from the Windows Store. The OneNote and Lync apps provide a subset of the functionality in their desktop equivalents.

The Office 2013 RT license agreement is identical to the license for Office Home and Student 2013. Note that these programs are not licensed for commercial use, and they lack support for most add-ons (and all macros), which might limit their usefulness in some types of enterprise deployments.

It is possible to upgrade the usage rights for Office 2013 RT to permit commercial use. This can be done when the Windows RT device is a companion device for the primary user of a device with one of the following Office licenses:

- Business editions of Office 365 include commercial use rights that extend to Office 2013 RT. Qualifying editions include Office 365 ProPlus, Office Small Business Premium, Office 365 Midsize Business, and Office 365 Enterprise (E3/E4).
- Office Standard and Professional Plus 2013 include this offering as a secondary use right.
- An enterprise with a Volume License agreement can purchase commercial-use rights for Office that enables a Windows RT device for use in business scenarios.

Connecting to corporate networks

The ability to connect to wireless networks is a core feature of Windows RT 8.1. The original release of Windows RT did not support wired network adapters at all. Windows RT 8.1 adds a built-in Ethernet adapter class driver for USB network adapters that have been specifically designed for InstantGo (Connected Standby) operation.

In addition, Windows RT 8.1 supports a variety of corporate networking features, described in this section.

The use of VPNs helps protect the integrity and security of corporate networks from being compromised over external networks whose security can't always be guaranteed. The Windows RT 8.1 VPN client allows connections to Windows servers and can connect to third-party VPN servers using standard protocols: PPTP, L2TP, and IKEv2. The client can be configured directly or with scripts or a central device-management tool.

New in Windows RT 8.1 is built-in support for third-party clients from F5, Dell SonicWall, CheckPoint, and Juniper.

In addition, Windows RT 8.1 includes improved support for multifactor authentication, including through the use of virtual smartcards.

Finally, Windows RT 8.1 includes the same two Remote Desktop clients available in other Windows 8.1 editions: one for use on the desktop, and the other a WinRT app designed for the touch-friendly immersive interface. Either of these clients can be used to access desktop and app sessions on a remote PC or a RemoteApp server.

Access to data

Windows RT 8.1 supports the same types of local storage as other Windows 8.1 editions, allowing you to access built-in hard drives and flash storage as well as devices connected through USB ports. In addition, you can access the following types of remote data sources with the following limitations:

SkyDrive Windows RT 8.1 adds the capability to sync files and folders from SkyDrive to local storage. (This capability was not available in the original release of Windows RT.) In addition, with an active Internet connection, you can access files from remote SkyDrive folders.

SkyDrive Pro Some editions of Office 2013 include a SkyDrive Pro client utility that can sync files from a cloud-based SharePoint personal site document library and make them available for offline use on a local drive. This capability is not included with Office 2013 RT and cannot be added. As a result, SkyDrive Pro files are available from within Office programs or through Internet Explorer 11, only with an active Internet connection.

Network shares Shared folders are available in File Explorer using standard Windows networking protocols. Because Windows RT 8.1 doesn't support domain-based credentials, you might need to specify an alternate user ID and password (or use a smartcard) to provide authenticated access. Note that the client-side caching (CSC) functionality found in Windows 8.1 Pro and Enterprise—support for offline files and folder redirection—is not available in Windows RT 8.1. You can, however, use Work Folders, a technology discussed in more detail in Chapter 11.

CHAPTER 11

Managing mobile devices

Although it probably didn't seem so at the time, network management used to be relatively simple. Workers sat down at a desk, where they logged on to a company-issued PC and connected to company-owned resources on company-managed servers.

Today, that's all changed.

In our new Bring Your Own Device (BYOD) world, workers expect to be able to do their job from anywhere, using any device, with full access to their work resources and data. That proliferation of devices makes many traditional management techniques impractical at best and often technically impossible. Yet you still have the challenge of securing confidential data and maintaining compliance with regulations that affect your industry.

Fortunately, a new generation of standards-based management tools, from Microsoft and other companies, allow you to provide access to corporate apps and information while still maintaining effective control over those resources.

Mobile device management strategies

For the wide range of devices in your organization, Microsoft offers two primary management tools:

- System Center Configuration Manager 2012 R2 adds support for Windows 8.1. It offers full management capabilities over traditional domain-joined Windows PCs, including those running Windows To Go and Windows Embedded. It also works with Apple-branded devices running OS X.

- Windows Intune is a cloud-based service that can manage PCs running Windows 8.1 and Windows RT 8.1, as well as mobile devices running Windows Phone 8, iOS, and Android. You don't have the same control as with a fully managed, domain-joined PC, but you can effectively exercise light control over predictable scenarios.

The key to successfully integrating your workers' personal PCs and tablets into a mobile device management strategy is a set of open standards that use the Open Mobile Alliance Device Management protocols—OMA-DM 1.2.1, to be specific. These protocols allow communication with cloud-based management services using secure HTTP.

This management agent is available on most mobile devices, and it is included by default with all editions of Windows 8.1, including Windows RT 8.1, with no additional software required. For company-owned and managed PCs, you can deploy the full Configuration Manager client. For personal devices that employees bring in as part of a BYOD strategy, joining the domain as a fully managed device is either impractical or impossible—personal devices running the Core edition of Windows 8.1 or Windows RT 8.1 lack domain-join capabilities. In that case, you can use Windows Intune to perform light management capabilities.

Management tools that support OMA-DM—including Microsoft Windows Intune, MobileIron, and AirWatch—can perform a variety of useful tasks:

- Hardware and software inventory
- Configuration of key settings
- Installation and configuration of modern line-of-business (LOB) applications
- Certificate provisioning and deployment
- Data protection, including the ability to wipe a lost or stolen device

Two additional features that are new in Windows 8.1 and Windows Server 2012 R2 can also be used as part of a BYOD strategy. Workplace Join enables a personal device to be authenticated on the enterprise network and allowed to access corporate resources and applications. Work Folders is a simplified file synchronization feature that personal devices running Windows 8.1 can use to securely store and access files from a corporate network.

This chapter looks at all of the preceding strategies.

System Center 2012 R2 Configuration Manager

System Center 2012 R2 Configuration Manager is the most recent release of Microsoft's comprehensive management tool for Windows systems (physical and virtual) and Windows-based mobile devices. When used in combination with Windows Intune, it provides a unified management environment that supports both company-owned and personal BYOD devices.

Configuration Manager is a user-centric tool designed to work with your organization's Active Directory infrastructure. This means that it associates hardware assets with specific

users, allowing fine-tuned management of exactly which software and features are available to users. Configuration Manager also provides IT pros with a comprehensive reporting platform and deployment options.

Using Configuration Manager, you can perform the following functions:

- **Application management** A set of tools and resources allow you to package, manage, deploy, and monitor applications in the enterprise.
- **Endpoint protection** Security, antimalware, and Windows Firewall management features are included.
- **Compliance settings** Use built-in tools to assess and, if necessary, adjust the configuration of client devices to meet compliance requirements.
- **Company resource access** New in the System Center 2012 R2 release is a set of tools and resources you can use to grant remote access to resources by setting up Wi-Fi profiles, virtual private network (VPN) profiles, and certificate profiles. For example, you can install trusted root CA certificates for your enterprise to authenticate Windows 8.1 and Windows RT 8.1 devices on corporate Wi-Fi hotspots and VPNs.
- **Remote connection profiles** Also new in the System Center 2012 R2 release are tools to help you create and deploy remote connection settings to devices, making it easier for users to connect to their computer on the corporate network.
- **Operating system deployment** You can create operating-system images and deploy them to computers that are managed by Configuration Manager, as well as to unmanaged computers, by using PXE boot or bootable media.
- **Inventory** As an administrator, you can collect detailed information about hardware, software, data files, and license usage on managed devices.

Configuration Manager also includes remote control tools for help desks and capabilities for deploying software updates.

One of the most important changes in System Center 2012 R2 Configuration Manager is the ability to configure enrolled devices as company-owned or personal-owned. Personal devices are not domain-joined and do not have the Configuration Manager client installed. These mobile devices report software inventory only on company content. Wipe and retire functions also provide the option to remove only company content from these devices, preserving personal content and apps.

You can use Windows Intune (described in the next section) to manage Windows 8.1 devices that are not joined to the domain and do not have the Configuration Manager client installed.

MORE INFO **For a more detailed discussion of new features in this release, see "What's New in System Center 2012 R2 Configuration Manager," at *http://technet.microsoft.com/en-us/library/dn236351.aspx*.**

Windows Intune

Windows Intune uses a unified web-based administration console to provide cloud-based device-management features, software-deployment capabilities, and security capabilities. Because it is a cloud-based management tool, the console does not require a VPN connection to your local domain. Windows Intune does not require any established infrastructure, although it works well in combination with Configuration Manager.

One of the signature features found in Windows Intune is its customizable company portal, which is also available with Configuration Manager 2012 R2. The company portal is an interface customized with downloadable applications that IT administrators can make available for an organization. The company portal also allows users to directly contact IT and request remote assistance. Figure 11-1 shows a sample company portal.

FIGURE 11-1 The company portal is a customizable destination where administrators can make apps available for users on a self-service basis.

In addition to offering remote application and service features, the company portal feature allows an administrator to use a remote security wipe utility to clear data from the device the next time it connects to the Internet.

Workplace Join

With Windows 8.1, a PC that is domain joined can access corporate resources (if allowed to do so by administrator-assigned permissions), and IT can control the PC through Group Policy and other mechanisms. Personal devices that aren't joined to the domain have no such capabilities.

Windows 8.1, in combination with Windows Server 2012 R2, adds a new feature called Workplace Join, which provides a middle ground between this all-or-nothing access scenario. With Workplace Join, users can register personal devices on the corporate network using Active Directory, without joining the domain. On the server side, administrators can create rules that allow a user to access corporate resources only when they sign in on a device that has been registered via Workplace Join (and is therefore trusted). This security feature offers administrators the ability to control access to corporate resources without requiring sign-on with an Active Directory account or applying group policy.

Workplace Join is currently available for all Windows 8.1 editions as well as iOS devices. Here's how it works with Windows 8.1.

On the server side, there are three requirements:

- The Windows Server 2012 R2 version of Active Directory Federation Services (ADFS) must be installed.
- Two custom DNS entries are required. One is automatically created by ADFS; the second resolves to enterpriseregistration.*yourdomain* (where *yourdomain* is your enterprise domain). The DNS record must be accessible internally and can optionally be available in external DNS.
- A Secure Sockets Layer (SSL) certificate must resolve correctly to the ADFS and enterpriseregistration DNS records.

Once this infrastructure is set up, a Windows 8.1 client registers on the network using the Workplace Join option under Network, in PC Settings, as shown in Figure 11-2.

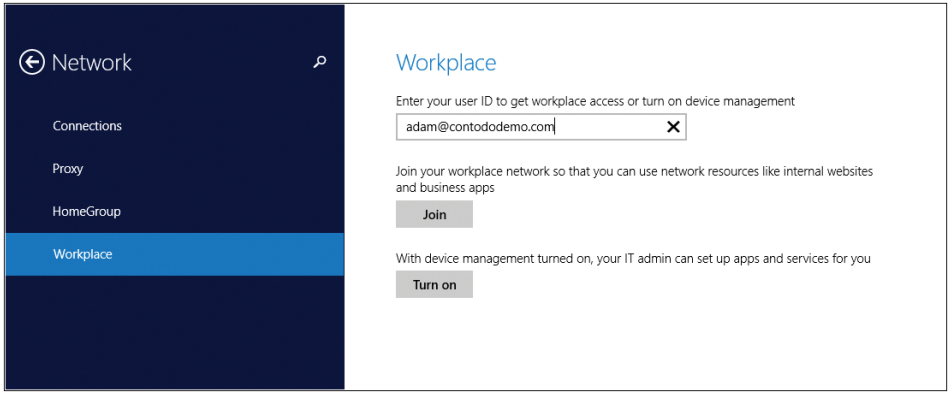


FIGURE 11-2 To register a device on the network, enter your email address as it's shown in Active Directory and then click Join in this PC Settings page.

Assuming the administrator has set up multifactor authentication (a highly recommended configuration), the user next sees a response from the server, as shown in Figure 11-3.

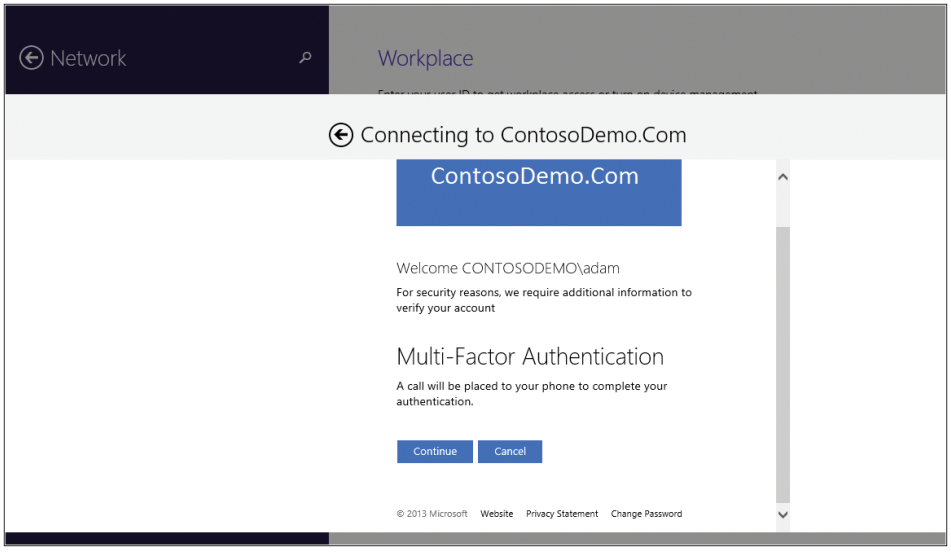


FIGURE 11-3 The recommended configuration for Workplace Join includes multifactor authentication.

Successfully completing the WorkPlace Join process installs a certificate in the local user account on the device and links it to Active Directory. That certificate acts as a "thumbprint" for the device, allowing domain members to sign in to corporate resources. (For auditing purposes, ADFS records details of the domain account that performed the registration, but any domain member is eligible to use the registered device.)

Workplace Join offers a solution to a common BYOD problem: some devices cannot be domain joined, either because one device is a personal device or because the device is running an operating system that doesn't support domain join.

Work Folders

Work Folders is another new feature supported by default on Windows 8.1 devices that connect to Windows Server 2012 R2. With Work Folders enabled, a user can securely sync data to her device from a user folder located in the corporate data center, allowing the user to work with it offline. Files created or modified in the local copy of the folder sync back to the file server in the corporate environment. You can set up Work Folders on a multitude of devices running Windows 8.1, iOS, or another supported platform. If you store all your personal work files in the Work Folders location (with as many subfolders as you want to create), they'll roam with you to all your devices.

If this feature sounds familiar, that's because it is, at least at a low level. This is a new generation of the client-side caching (CSC) technology that has been part of Windows networks for many years, powering folder redirection and Offline Folders. The difference is that Offline Folders requires that a device be joined to the domain. That excludes any personal devices running consumer versions of Windows. It also doesn't work with tablets running operating systems other than Windows.

Windows 8.1 devices do not need to be domain joined for synchronization with personal files. Your domain credentials unlock access to Work Folders. As a result, you can use Work Folders on a device running Windows RT 8.1 and still maintain secure offline access to files.

On the server side, you enable Work Folders by installing the feature as part of the Windows Server 2012 R2 File Services role. Doing so installs a new panel where you can define a server file location to be synced with a specific user and then either create a DNS entry or publish a custom URL to reach the shared files.

Setting up Work Folders also enables Individual Rights Management (IRM) and Dynamic Access Control (DAC) for files in the shared location. Using these capabilities, administrators can designate specific documents as company resources, which can then be managed to prevent unauthorized access from the local device.

On the client side, syncing is natively integrated into the file system. To connect to Work Folders, you start in the desktop Control Panel\System And Security\ by clicking the Set Up Work Folders option shown in Figure 11-4.

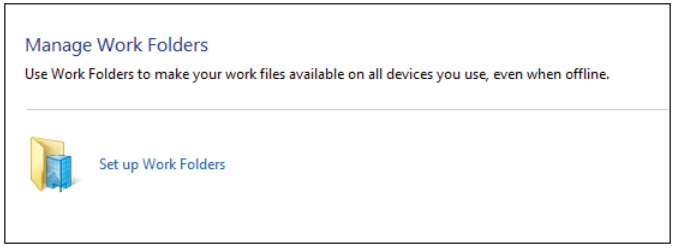


FIGURE 11-4 The Work Folders capability is built into the desktop Control Panel in all editions of Windows 8.1.

That, in turn, leads to a dialog box where you enter either your email address or the URL that the administrator established. In either case, when you click Next you will be prompted to enter your domain credentials to establish the connection, as shown in Figure 11-5.

After you successfully authenticate, the next step of the setup process (shown in Figure 11-6) notifies you that administrators can apply security policies to data files in the Work Folders share, including the right to remotely delete them. Some device capabilities such as encryption and a password-protected screen lock might be required.

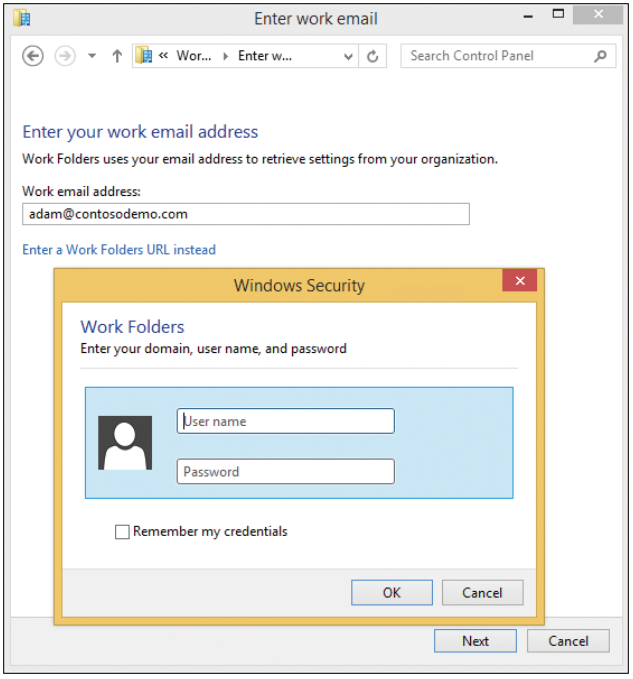


FIGURE 11-5 Connecting to the Work Folders share requires that you enter an email address or a custom URL and then authenticate using your domain credentials.

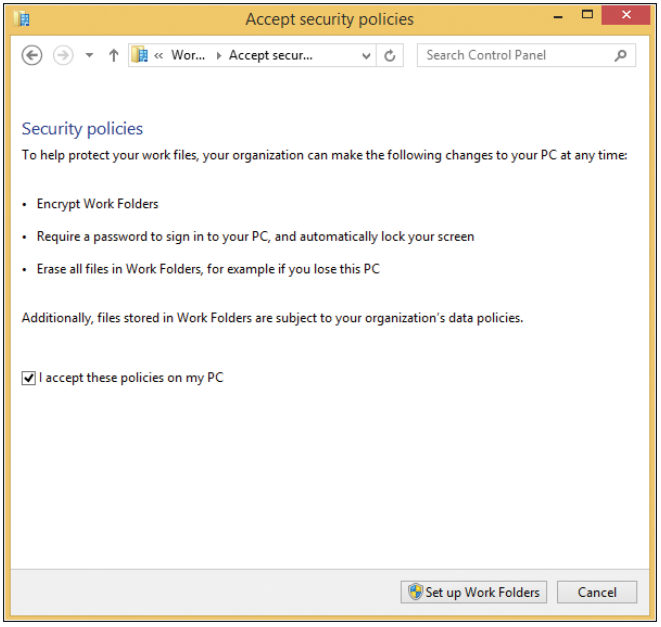


FIGURE 11-6 The final step in setting up Work Folders on a Windows 8.1 device contains a notification about security policies that must be accepted before the feature is enabled.

The Work Folders feature is similar in concept to other Microsoft file-related features—specifically, SkyDrive and SkyDrive Pro. What makes it different?

SkyDrive is a consumer service intended for storage of personal files. It's connected to a Microsoft account and can't be centrally managed or backed up. That makes it unsuitable for enterprise data.

SkyDrive Pro provides access to SharePoint resources and is designed primarily for data collaboration in teams, with strong workflow-related features. It can be securely managed, but its extensive feature set means it's unnecessarily complex for simple file storage and synchronization between devices.

Work Folders doesn't have any file-sharing features, but it's incredibly easy to use. This feature can optionally be set up outside the firewall, a configuration that allows access without requiring a VPN connection. The administrator can require that Workplace Join be enabled, preventing a potential attacker (or a careless employee) from accessing files using untrusted devices. On Windows 8.1 and Windows RT 8.1, it doesn't require the installation of a sync utility—it just works. A Control Panel app, shown in Figure 11-7, lets you view usage statistics and provides some simple management tools. Beyond that, no additional configuration is necessary.

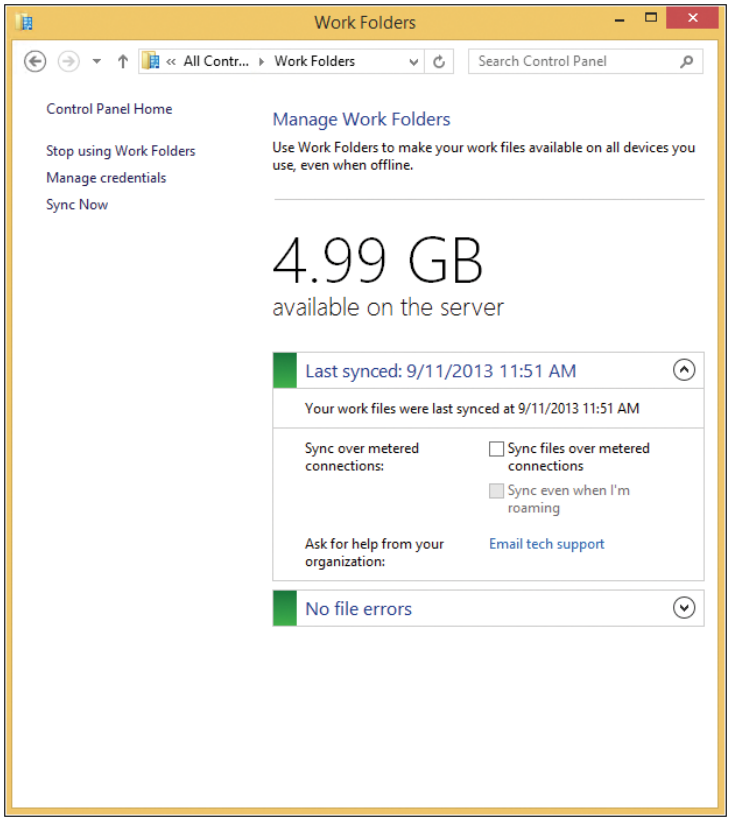


FIGURE 11-7 This simplified management interface lets you view the status of your synced Work Folders and manually sync files, view any file errors, and stop using Work Folders on the current device.

Web Application Proxy

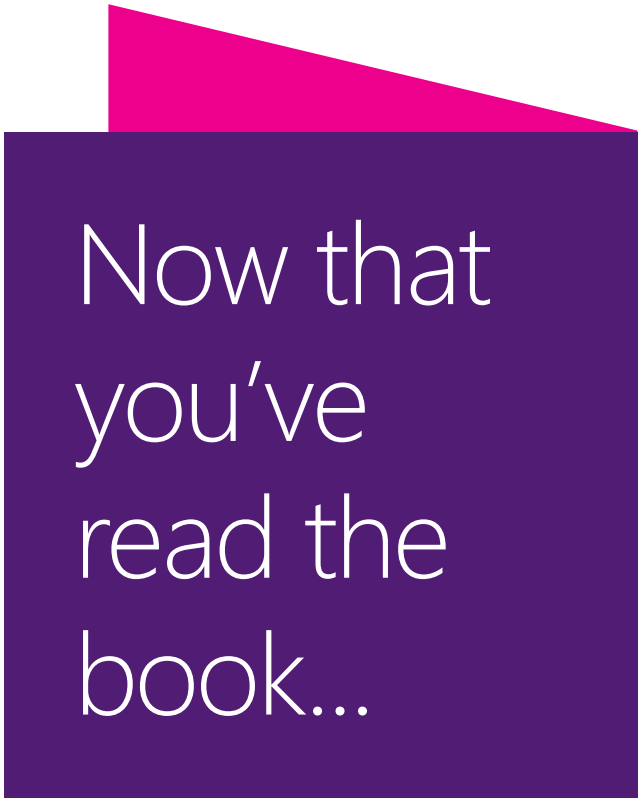
The Web Application Proxy is a new role service in the Windows Server Remote Access role. It provides the ability to publish access to corporate resources and enforce multifactor authentication, as well as apply conditional access policies to verify both the user's identity and the device he is using.

On mobile devices, this feature can be used to improve the user experience of Workplace Join. By connecting an ADFS server to the Web Application Proxy, users can connect to resources with multifactor authentication enforced, as well as receiving verification that the device being used for access is registered (and therefore trusted).

Device lockdown (Assigned Access)

This feature is new in Windows 8.1 (Pro and Enterprise editions only) and in Windows RT 8.1.

Using the Assigned Access feature allows the device to run a single Windows Store app while restricting access to all other apps and features (including web browsers, email, games, and other potential sources of confusion or distraction). That's a useful feature in kiosk applications, where you want customers to be able to view product or service information in a controlled environment. It's also ideal in classrooms (for a test-taking application, for example) and for point-of-sale, check-in, and other line-of-business apps that management might want to use exclusively on a device.



Tell us what you think!

Was it useful?
Did it teach you what you wanted to learn?
Was there room for improvement?

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

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

Microsoft