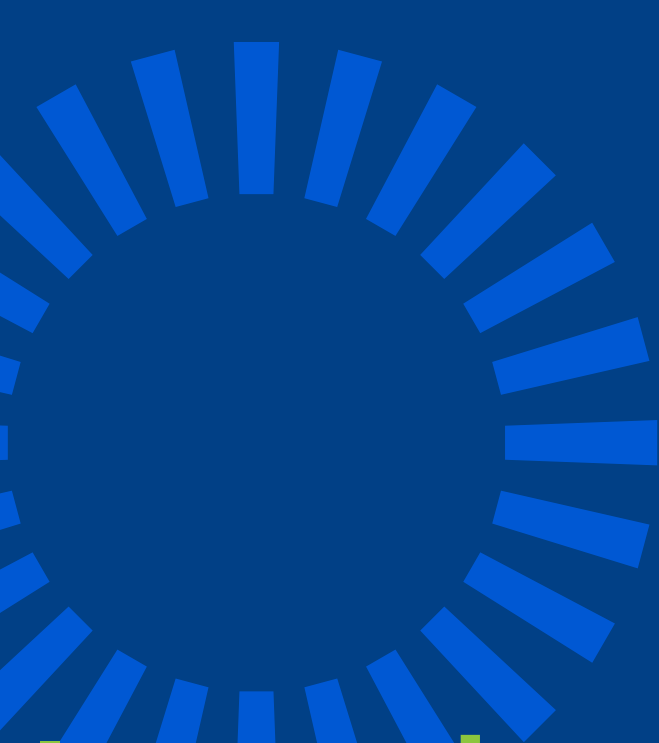




Introducing Windows 10 for IT Professionals Preview Edition

ED BOTT



Introducing Windows 10 for IT Professionals, Preview Edition

Ed Bott

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

Copyright 2015 © Microsoft Corporation

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

ISBN: 978-0-7356-9696-9

Printed and bound in the United States of America.

First Printing

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

This book is provided “as-is” and expresses the author’s views and opinions. The views, opinions and information expressed in this book, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

Microsoft and the trademarks listed at <http://www.microsoft.com> on the “Trademarks” webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

Acquisitions Editor: Rosemary Caperton

Project Editor: Christian Holdener; S4Carlisle Publishing Services

Editorial Production: S4Carlisle Publishing Services

Copyeditor: Roger LeBlanc

Contents

<i>Introduction</i>	<i>vii</i>
Chapter 1 An overview of the Windows 10 Technical Preview	1
What is Windows 10?	1
A new approach to updates and upgrades	2
The evolution of the Windows user experience	3
User accounts and synchronization	4
Windows apps	6
A new default browser	8
What's new for IT pros?	9
Security enhancements	9
Deployment and manageability	12
Virtualization	13
Chapter 2 The Windows 10 user experience	15
An overview of the new Windows user experience	15
The Settings app	17
Notifications Center and action buttons	18
Cortana	19
Modern apps in resizable windows	21
Navigation	22
Tablet Mode	23
File Explorer	24
Cloud connections	26

Chapter 3	Installing and deploying the Windows 10 Technical Preview	29
Compatibility and preparation.....		30
Enterprise deployment tools: A roadmap		31
Windows 10 installation options		32
Upgrade or clean install?		32
Choosing an account type		34
Which account type should you use?		39
Chapter 4	Security in Windows 10	41
The evolution of the threat landscape		41
Securing hardware.....		42
Securing the boot process		43
Locking down enterprise PCs.....		45
Securing data on local storage devices.....		45
Device encryption		46
BitLocker Drive Encryption.....		46
Remote business data removal.....		47
Securing identities		47
Blocking malware.....		51
Windows Defender		51
SmartScreen and phishing protection		51
Chapter 5	Deploying and managing Windows Store apps	53
Introducing the new Windows Store		53
How universal apps work		55
Distributing line-of-business apps		58

Chapter 6	Web browsing and Windows 10	59
	A brief history of Internet Explorer.....	59
	Browsing options in Windows 10	60
	Project Spartan.....	62
	Configuring Enterprise Mode in Windows 10	67
Chapter 7	Windows 10 networking	71
	Wireless networking enhancements	71
	Connecting to remote corporate networks.....	72
	Managing network connections	74
	Support for IPv6.....	76
Chapter 8	Virtualization and remote access	77
	Client Hyper-V.....	77
	Desktop virtualization options.....	81
	Application virtualization.....	84
	User Experience Virtualization (UE-V)	86
Chapter 9	Backup and recovery options in Windows 10	87
	Using Windows Recovery Environment.....	87
	Windows 10 and push-button reset options.....	90
	Refresh Your PC Without Affecting Your Files option	92
	Remove Everything And Reinstall Windows option	93
	Microsoft Diagnostics and Recovery Toolset.....	95
Chapter 10	Windows 10 on phones and small tablets	97
	The evolution of Windows 10 Mobile.....	97
	Installing the Windows 10 Technical Preview for phones.....	98
	What's inside Windows 10 Mobile	99

Introduction

I've written about Microsoft Windows for nearly a quarter-century, and in all that time I have never worked on a project like this one. Then again, I've never seen anything quite like Windows 10 from Microsoft, either.

This book is a preview, a work in progress about a work in progress. It offers a snapshot of the Windows 10 Technical Preview as of April 2015, on the eve of the BUILD Developers' Conference in San Francisco.

By design, this preview edition has a limited shelf life. After Microsoft releases Windows 10 to the general public this summer, I'll revise and expand the content in this edition to reflect the finished product.

Windows 10 represents a major transformation of the PC landscape. For IT pros who've grown comfortable managing Microsoft Windows using a familiar set of tools and best practices, this version contains a startling amount of *new*. A new user experience. A new app platform. New security features and new management tools.

My goal in this book is to help you sort out what's new in the Windows 10 Technical Preview, with advance notice of features that will be available in the finished product but aren't yet implemented. I've tried to lay out those facts in as neutral a fashion as possible, starting with an overview of the operating system, laying out the many changes to the user experience, and diving deep into deployment and management tools where it's necessary.

Although I've written in-depth guides to Windows in the past, this book is not one of those. It's also not a review. Only you can decide whether, and how and when, to incorporate Windows 10 into your enterprise, based on your own organizational requirements. This book is designed to serve as a rough guide so that you can get more out of your evaluation of the Windows 10 Technical Preview.

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.

The Windows 10 Technical Preview offers anyone an opportunity to not just try out the next version of Windows but to provide feedback about the new operating system, in real time, to the team that is building it. I encourage you to share your feedback about this book directly with me. E-mail your comments to me at feedback@realworldwindows.com.

Ed Bott

April 24, 2015

Acknowledgments

I'd like to thank Michael Niehaus, Chris Hallum, and Fred Pullen, who reviewed the content for this preview edition. I'd also like to thank the good folks at Microsoft Press—Anne Hamilton, Rob Linsky, and Rosemary Caperton—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 and writes regularly about technology for The Ed Bott Report at ZDNet.

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

<http://aka.ms/mspressfree>

Check back often to see what is new!

Errata, updates, & book support

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

<http://aka.ms/IntroWin10Preview/errata>

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

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

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

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback 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 the Windows 10 Technical Preview

Through the years, IT professionals have approached each new release of Microsoft Windows with mixed emotions.

The first reaction is, of course, eager anticipation. Most IT pros are in their line of work because they love technology, and a new version of Windows holds the promise of exciting new features and capabilities.

There's also a bit of trepidation. Historically, migrating an enterprise to a new version of Windows is a slow, cautious operation, with careful planning and staged deployments that can take years. As a result of that conservatism, many enterprises provide their workers with PCs that lag far behind the devices those workers use at home.

Windows 10 brings a long list of important changes that any IT pro should look forward to, including major improvements in the user experience, significant security enhancements, and a new web browser.

But the most significant change is designed to remove the anxiety that accompanies enterprise upgrades. The goal of Windows 10 is to deliver new features when they're ready, rather than saving them for the next major release. In fact, the very concept of a major release goes away—or at least recedes into the distant background—with Windows 10.

Terry Myerson, the Microsoft executive in charge of the operating systems division, calls it “Windows as a Service.” In fact, he argues, “One could reasonably think of Windows in the next couple of years as one of the largest Internet services on the planet. And just like any Internet service, the idea of asking ‘What version are you on?’ will cease to make sense . . .”

That process has already begun, with the launch in late 2014 of a Windows 10 Technical Preview aimed at IT pros and consumers. Those who have opted into the Windows 10 preview program are receiving major new features, bug fixes, and security updates through the tried-and-true Windows Update channel, with new updates arriving, on average, monthly.

In this chapter, I provide an overview of the Windows 10 Technical Preview, with a special emphasis on features and capabilities of interest to IT pros.

What is Windows 10?

When you think of Windows, you probably think first of conventional desktop PCs and laptops. The Windows 10 release encompasses a much broader range of devices, as Figure 1-1, taken from a Microsoft presentation, makes clear.



FIGURE 1-1 The Windows 10 family spans a wide range of devices, from phones to game consoles and the new HoloLens headset, with PCs in the middle.

Although all these devices share a great deal of common code, it's not the case that the same code will run on each device. The version of Windows 10 Enterprise for a 64-bit desktop PC, for example, is very different from Windows 10 Mobile or the Xbox OS.

But that common code has a big payoff when it comes to app development. Apps that are built on the Windows universal app platform can run on all Windows device families. They are also easier to manage and more secure than conventional Windows desktop applications, which run only on PCs.

A new approach to updates and upgrades

As I mentioned, the most revolutionary change in Windows 10 is the concept of continuous improvement. New features are delivered through Windows Update rather than being set aside for the next major release. In a major change of longstanding best practices, Microsoft now recommends that enterprise customers enable Windows Update for the majority of users, although the option to use Windows Server Update Services (WSUS) might still be available for some configurations.

In the Windows 10 Technical Preview, the more-or-less monthly new builds are delivered through Windows Update. Participants in the preview program can choose between two update speeds, also known as *rings*. Choosing the Fast ring makes new builds available as soon as they're released by Microsoft; opting for the Slow ring delays the availability of a new build until it's been thoroughly vetted by the Fast ring, with any bugs addressed via interim updates.

When Microsoft officially releases Windows 10 to the public, the preview program won't end. Members of the Windows Insider program will continue to receive early access to new updates, using the same Fast and Slow rings. Windows users who are not part of the preview program will receive updates for what's known as the "Current Branch." In addition, Microsoft has committed to an additional approach for enterprise customers who want a more stable environment, with a "Current Branch for Business" that is several months behind the consumer releases as well as "Long Term Servicing" branches that are appropriate for mission-critical applications.

The evolution of the Windows user experience

In the beginning, there was the Windows 95 Start button, which actually included the word *Start*. Clicking that button led to the Start menu, which was chock-full of shortcuts to programs, utilities, and settings. Both of these crucial parts of the user experience evolved significantly in appearance and functionality over the years, but a time traveler from 1995 would have no trouble recognizing the Start menu in Windows 7.

In a singularly controversial decision, the designers of Windows 8 removed the Start button and Start menu completely, replacing them with a full screen filled with live tiles instead of icons. The Start button returned in Windows 8.1, although its main function was to provide access to the Start screen. Now, by popular demand, the Start menu returns in Windows 10.

In the Windows 10 Preview (the April 2015 update), clicking the Start button opens a menu similar to the one shown in Figure 1-2.

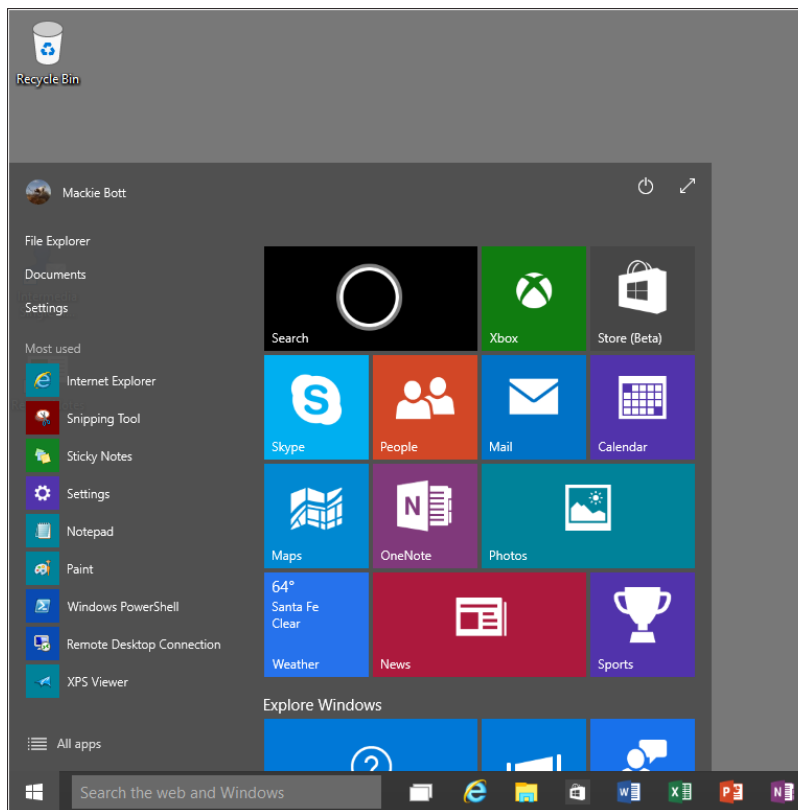


FIGURE 1-2 The Windows 10 Start menu blends elements of its Windows 7 predecessor with Windows 8 live tiles.

This Start menu design (which will undoubtedly change before the final Windows 10 release) contains some familiar elements, including links to common locations, a list of frequently used apps and programs, and power controls. The items on the right are live tiles, which work like their equivalents from the Windows 8.1 Start screen.

The search box, just to the right of the Start button, offers quick access to the local file system and to the web. With a few quick configuration steps, you can enable Cortana, the voice-powered personal assistant that debuted in Windows Phone and is now moving to the larger Windows 10 platform.

The double-headed diagonal arrow in the top-right corner expands the Start menu to fill the full screen. A separate option, called *Tablet Mode*, also expands the Start screen but makes additional changes designed to make Windows 10 more usable on tablets and hybrid PCs. Figure 1-3 shows Tablet Mode in action.

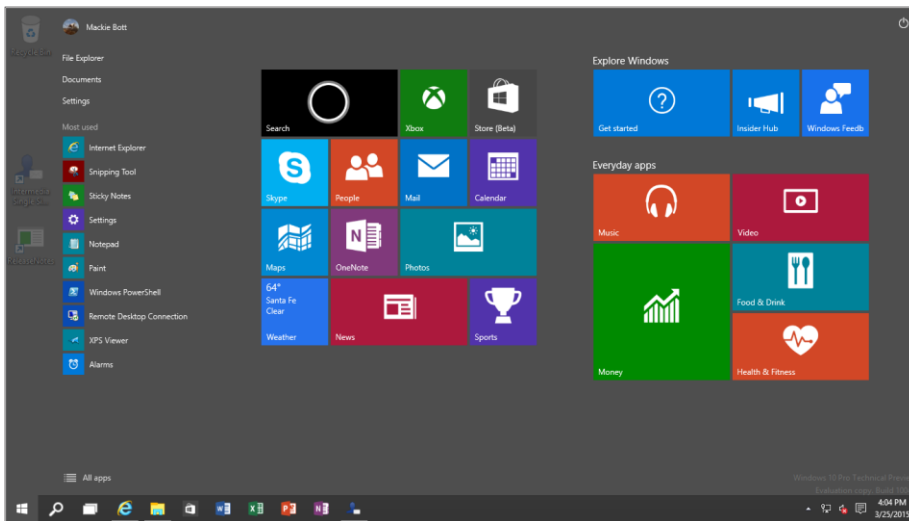


FIGURE 1-3 In Tablet Mode, the search box shrinks and the Start menu and apps fill the entire screen.

Several navigation elements that were added to Windows 8 have been removed for Windows 10. The Charms menu is gone, replaced on the right side of the screen by an Action Center that shows notifications and includes shortcuts to common tasks. Likewise, the Windows 8 navigation controls based on aiming a mouse pointer at corners are replaced by a new Task View, which also supports multiple virtual desktops.

For a more detailed look at how Windows 10 works, see Chapter 2, “The Windows 10 user experience.”

User accounts and synchronization

Anyone migrating to Windows 10 from Windows 7 should pay special attention to a new user account type, introduced in Windows 8. Signing in with a Microsoft account instead of a local account provides tightly integrated support for cloud-based services, along with easy synchronization of settings and apps between devices.

Figure 1-4 shows part of the new Sync Your Settings control, found in the Settings app.

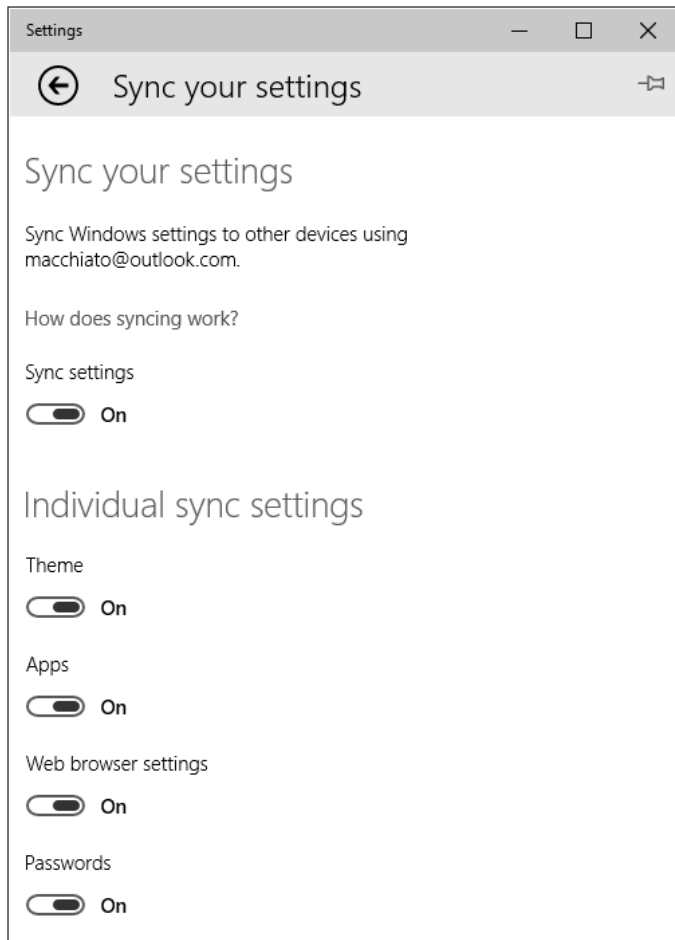


FIGURE 1-4 On devices where the user signs in with a Microsoft account, settings can be synchronized with other devices. Note the new visual design for the Windows 10 Settings app.

The list of settings that can be synchronized includes the layout of the Start screen as well as apps; previously purchased apps can be automatically downloaded and installed from the Store when you sign in with a Microsoft account on a new device. 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. In an enterprise setting, Windows 10 will include provisioning features that allow IT pros to manage this process.

One of the key features planned for Windows 10 is integrated access to cloud-based file storage in OneDrive and OneDrive for Business. Microsoft announced plans to release a unified synchronization utility that will handle both services, but that tool is not yet available for the Windows 10 Preview.

In enterprise deployments, 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.

Windows apps

Windows 10 includes support for virtually all desktop applications that are compatible with Windows 7. It also supports the latest generation of Windows apps (sometimes referred to as *modern apps*), which debuted in Windows 8 and have evolved significantly since that time. These apps are distributed through the Windows Store. (In enterprise deployments, IT pros can leverage the Windows Store to deliver line-of-business apps to users.)

In Windows 8 and 8.1, modern apps run in one of two modes: full-screen, or snapped to the side of the display. In Windows 10, these apps can run in a window. Figure 1-5, for example, shows a preview release of Microsoft Excel running in a resizable window on a Windows 10 PC.

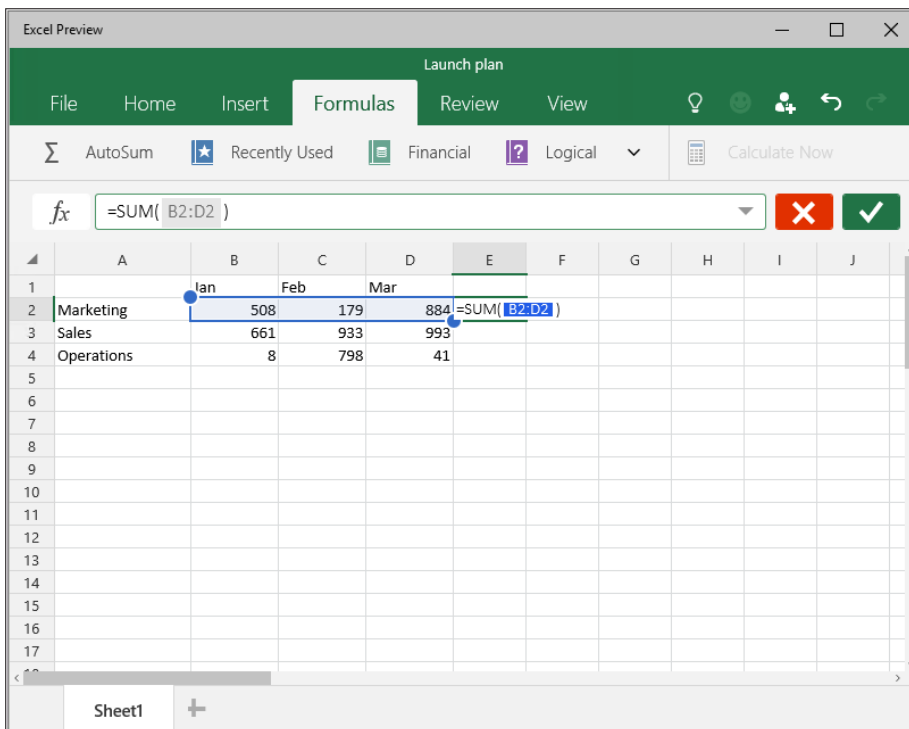


FIGURE 1-5 This Excel Preview app is available through the Windows Store and, like other modern apps in Windows 10, it can run in a resizable window.

As is the case with most modern apps, the Excel Preview (and its Office-mates Word and PowerPoint, which are also available as preview releases) is designed to deliver an excellent experience on touchscreen devices with small screens. These modern apps don't have the full feature set of their Windows desktop counterparts, but they're surprisingly useful nonetheless.

The Windows Store is in the process of being completely redesigned for Windows 10. In builds up to and including the March Update, the original Store and the new Store (labeled as "Beta") coexist side by side. Figure 1-6 shows a typical listing in the new Store, which has a cleaner design and offers a broader variety of products than just apps.

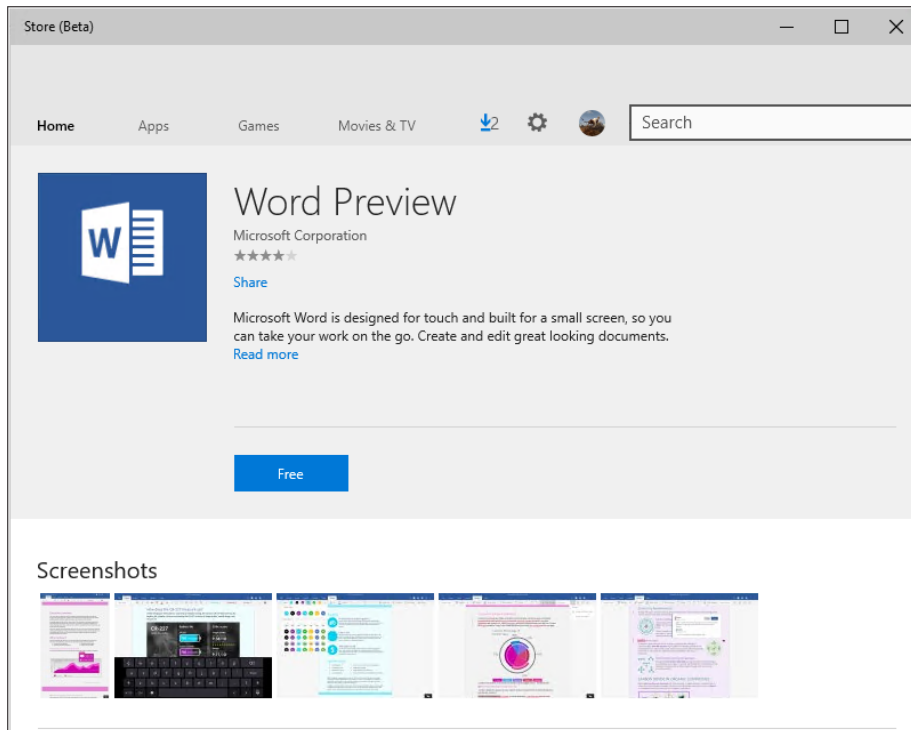


FIGURE 1-6 The Windows 10 Store (shown here in a Beta version) offers more than just apps.

MORE INFO For more details on these apps and on the changes to the Windows Store, see Chapter 5, "Deploying and managing Windows Store apps."

A new default browser

One of the signature features of Windows 10 will be a new default browser, code-named “Project Spartan.”

The new browser was not in early builds of the Windows 10 Technical Preview, making its first appearance (with an incomplete feature set) in April 2015. However, Microsoft has demonstrated its features publicly and has described its long-term goals. As Figure 1-7 shows, the “Project Spartan” browser has an uncluttered, touch-friendly interface with a few hidden features that include the ability to annotate webpages and integrate with Cortana, the Windows 10 personal assistant.

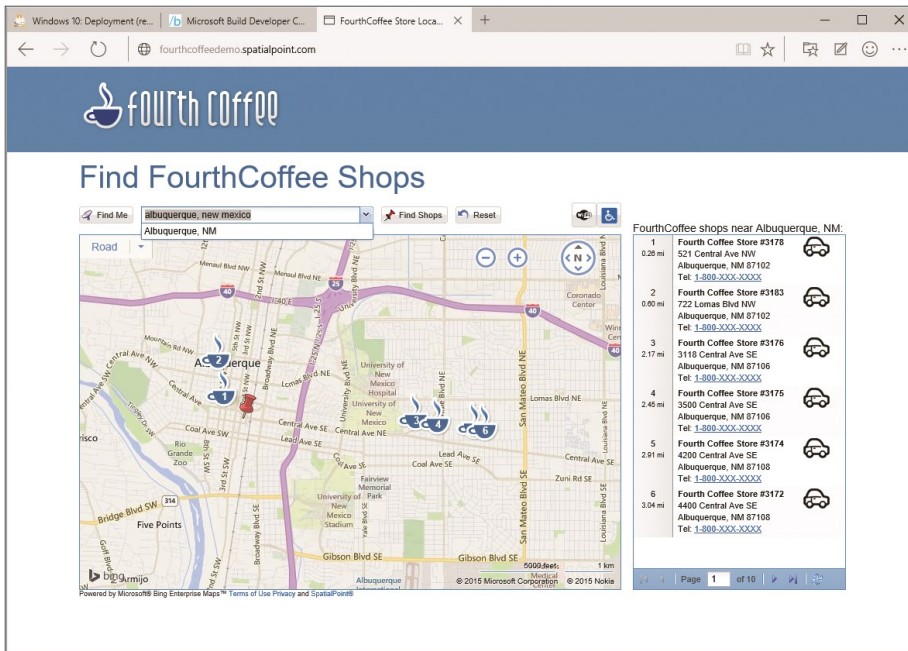


FIGURE 1-7 This “Project Spartan” browser will eventually be the default for Windows 10 devices.

If you’re wondering what happened to Internet Explorer, you’re not alone. Many line-of-business apps in enterprise deployments require Internet Explorer. Some apps require versions older than Internet Explorer 11, which will be the only supported version as of January 2016.

The good news for IT pros in those challenging enterprise environments is that Internet Explorer will continue to be available in Windows 10, with Enterprise Mode available as a feature for ensuring that older apps work properly.

You can read more details about this two-browser strategy in Chapter 6, “Web browsing and Windows 10.”

What's new for IT pros?

As an IT pro, your first concern is, of course, the users you support. 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 widescale deployment require? And most important of all, can you keep your business data and your networks secure and available?

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, Windows 8.1 added still more improvements, and Windows 10 ups the ante yet again.

The most significant new Windows 10 security feature involves a major improvement in authentication, based on biometric factors.

On Windows 10 devices that include the appropriate hardware, two new features will significantly ease the process of authenticating to the device and to online services:

- **Windows Hello** This feature uses biometric authentication—facial recognition, an iris scan, or a fingerprint—to unlock devices. The technology is significantly more advanced than existing biometric methods that are supported for basic authentication in Windows 8.1. For example, Windows Hello requires an infrared-equipped camera (using the same technology found in the Xbox Kinect sensor) to prevent spoofing identification using a photograph.

Enabling Windows Hello requires enrolling a Windows 10 device (PC, tablet, or phone) as trusted for the purposes of authentication. In that scenario, the enrolled device itself works as an additional proof of identity, supporting multifactor authentication.

- **Microsoft Passport** The second feature is based on a new API that works in conjunction with biometric authentication on an enrolled device to sign in to any supported mobile service. The Passport framework allows enterprise IT managers, developers, and website administrators to

provide a more secure alternative to passwords. During the authentication process, no password is sent over the wire or stored on remote servers, cutting off the two most common avenues for security breaches.

Windows 10 also leverages security features found in modern hardware (and originally enabled in Windows 8 and Windows 8.1) 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 10, 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 10 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 10 includes two signature features that will be new to any organization that is migrating directly from Windows 7:

- **Windows Defender** Previous Windows versions included a limited antispware feature called Windows Defender. Beginning with 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. Windows Defender includes network behavior monitoring as well. 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 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 the default Windows browser, which also protects users from websites seeking to acquire personal information such as user names, passwords, and billing data.

Windows 10 adds information-protection capabilities that make it possible to protect corporate data even on employee-owned devices. Network administrators can define policies that automatically encrypt sensitive information, including corporate apps, data, email, and the contents of intranet sites. Support for this encryption is built into common Windows controls, such as Open and Save dialog boxes.

For tighter security, administrators can create lists of apps that are allowed to access encrypted data as well as those that are denied access—a network administrator might choose to deny access to a consumer cloud file-storage service, for example, to prevent sensitive files from being shared outside the organization.

Two features should be of significant interest to anyone with responsibility for sensitive enterprise data:

- **Enterprise Data Protection** This feature is an evolution of Remote Business Data Removal (RBDR), a feature introduced in Windows 8.1 and significantly enhanced for Windows 10. Using this feature, administrators can mark and encrypt corporate content to distinguish it from ordinary user data. Policies control what employees can do with data marked as such, and when the relationship between the organization and the user ends, the encrypted corporate data is no longer available to the now-unauthorized user. This is a significant new feature, due in the Windows 10 timeframe but not yet available in preview builds.
- **Pervasive Device Encryption** Device encryption is available in all editions of Windows 10. 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 10 devices, BitLocker Drive Encryption can be turned on by the user, with the recovery key saved to a Microsoft account.

BitLocker in Windows 10 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 you've grown accustomed to in Windows 7 environments. 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.

A final security measure is appropriate for organizations with high-security needs, such as regulated industries, defense contractors, and government agencies concerned about online espionage. With Windows 10 Enterprise edition and specially configured OEM hardware, administrators will be able to use the Device Guard feature to completely lock down devices so that they're unable to run untrusted code.

In this configuration, the only apps that will be allowed to run are those signed by a Microsoft-issued code-signing certificate. That includes any app from the Windows Store as well as desktop apps that an organization has submitted to Microsoft to be digitally signed. These signed apps can also be delivered to employees through a customized Business Store. If your enterprise uses internal line-of-business apps that are sideloaded, they will need to be signed by an enterprise certificate.

This feature is not available in current Windows 10 Technical Preview releases. Chapter 4, “Security in Windows 10,” provides more information about these security features.

Deployment and manageability

Deploying Windows 10 in an organization is faster and easier than in Windows 7, thanks to new features originally introduced in Windows 8.1. Improvements in deployment processes for Windows 10 can make it even easier to standardize on a corporate configuration.

The traditional “wipe and load” option is still available for Windows 10 upgrades. That process involves capturing data and settings from an existing device, deploying a custom operating system image, injecting drivers and installing apps, and then restoring the data and settings.

An additional option is the in-place upgrade, in which Windows handles the process of migrating apps and data from an existing image to a new (standard) image. This process is similar to the upgrade process consumers use via Windows Update, but it’s managed by System Center Configuration Manager and the Microsoft Deployment Toolkit, both of which should be familiar to IT pros.

Windows 10 adds a new provisioning option, which transforms a device with an OEM installation of Windows 10 into an enterprise-ready device. This procedure removes unwanted items from the OEM configuration and adds items, apps, and configuration details that would have been part of a standard custom image. The result is the same as a wipe-and-load deployment, but simpler and more flexible.

MORE INFO For more information about planning and carrying out a Windows 10 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. These options, which have evolved significantly from their original Windows 8 versions, allow users to restore or repair a Windows 10 device without having to make an appointment with the help desk. The new recovery options in Windows 10 include a significant benefit: The restored operating system contains all current updates, meaning that the user doesn’t have to go through a tedious round of system updates after repairing the installation.

As with Windows 8.1, the reset option includes data-wiping capabilities that make it possible for a user to transfer a device to a new owner without worrying about inadvertently disclosing sensitive personal or business data.

Virtualization

Windows 10 includes a robust, built-in virtualization platform. This feature, called Client Hyper-V, will be familiar to organizations that tested or deployed Windows 8.1, but for those upgrading from Windows 7 it is a major addition to the 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 infrastructure of Windows 10 and can be managed easily by existing IT tools, such as System Center. VMs can be migrated between a desktop PC running Windows 10 and a Hyper-V environment on Windows Server. Client Hyper-V requires Windows 10 Pro or Windows 10 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 8, “Virtualization in Windows 10.”

In conjunction with Windows Server 2012 and later releases, Windows 10 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 10 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).

MORE INFO For more information about both of these features, see Chapter 8, “Virtualization and remote access.”

CHAPTER 2

The Windows 10 user experience

How you react to Microsoft Windows 10 depends to a great extent on what your Windows desktop has looked like for the past few years.

If you and your organization stuck with Windows 7 (especially if you completed a migration from Windows XP shortly before its end-of-support date in 2014), you'll have to adjust to a few new ways of working. The redesigned Start menu is the most obvious change, followed closely by the relocation of many system settings from Control Panel to the modern Settings app.

Ironically, the learning curve is considerably more complex if you and your users were early adopters of Windows 8. Not only will you have to learn the new elements of Windows 10, but you'll have to *unlearn* some of the techniques you mastered with Windows 8 and Windows 8.1.

Feedback to Microsoft after the release of Windows 8 made it clear that the radically revised user experience caused significant frustration. Even with the refinements introduced in Windows 8.1, the change in user experience was substantial for anyone accustomed to the familiar desktop and Start menu.

As a result, the Windows 10 user experience offers another significant round of changes, designed to bring together the best elements of Windows 7 and Windows 8.1 and smooth the transition between the familiar desktop ways and the new touch-friendly techniques.

In Windows 10, you and your users can take advantage of the rich new Windows apps on a traditional desktop PC or laptop, alongside familiar Windows desktop applications, interacting with those new apps in resizable windows. On a touch-enabled mobile device, you can turn on Tablet Mode, making it possible to work with apps in a full-screen setting, minus clutter and distraction.

A new set of navigation techniques replace the sometimes-confusing “hot corner” techniques from Windows 8, and the addition of virtual desktops in Windows 10 makes it possible to shift between groups of apps instead of shuffling windows around.

Regardless of your starting point, moving to Windows 10 requires a thoughtful and thorough plan for training and orienting new users, especially if they work primarily in a traditional desktop environment. This chapter describes what you need to know about the changes in the Windows 10 user experience so that you can make those plans intelligently.

An overview of the new Windows user experience

The Start screen is gone. The desktop is back.

That's the beginning of the Windows 10 user experience, but it's far from the entire story.

The new Start menu, shown in Figure 2-1, is divided vertically in two, just as its Windows 7 predecessor was, but its contents are a bit different.

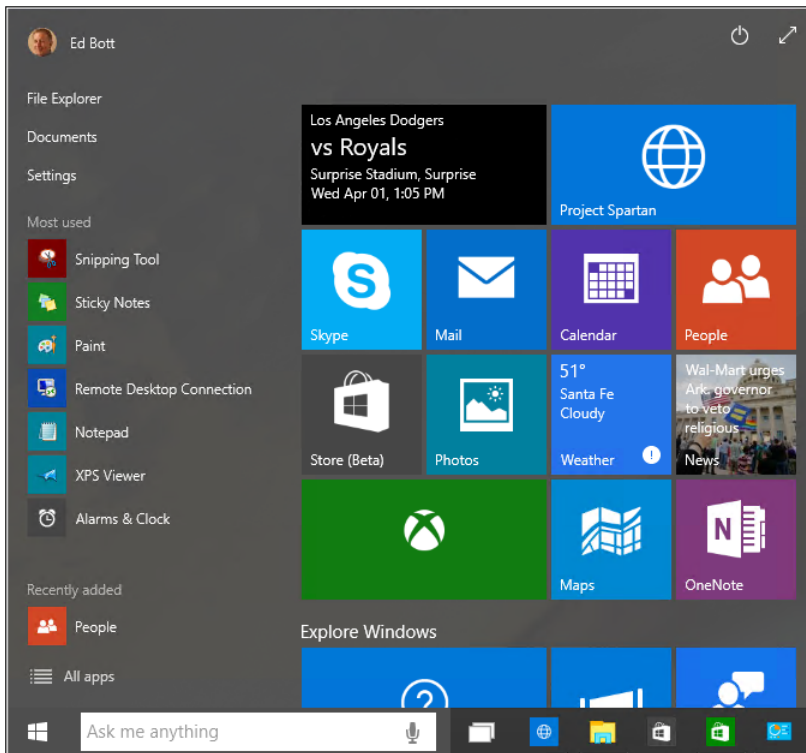


FIGURE 2-1 The new Start menu combines distinctive features from its predecessors in Windows 7 and Windows 8.1.

The left side contains the following, from top to bottom:

- An icon for the current user, which when clicked or tapped reveals a menu with options to lock the PC, sign out, switch accounts, or change account settings
- Shortcuts for File Explorer (Windows 7 users, note the name change), the current user's Documents folder, and the Settings app
- Shortcuts to frequently used and recently added apps
- An All Apps shortcut that replaces the left side of the Start menu with a scrolling list of installed apps and saved shortcuts—everything that was on its own screen in Windows 8.1

(The shortcuts to system settings from the Windows 7 Start menu aren't available here, but are instead on a hidden power user's menu, which is available when you right-click the Start button or use the Windows logo key + X shortcut.)

The Start menu contains a Power button (Sleep, Shut Down, Restart) that has been moved to the lower left in more recent builds than the one shown here. A two-headed diagonal arrow at the top right expands the Start menu to a full screen. In that configuration, the left side remains the same width, while the area devoted to live tiles expands to fill all available space.

Those live tiles work more or less the same as their counterparts in Windows 8.1. You can resize each tile, arrange them into groups, and give each group a descriptive name.

And it bears repeating: this is a preview. The layout and features of the Start menu will probably change significantly from the March snapshot you see here.

The Settings app

That Settings shortcut leads to the Windows 10 successor of Windows 8's PC Settings. The iconography, shown in Figure 2-2, is a distinctive change from the Windows 7 Control Panel.

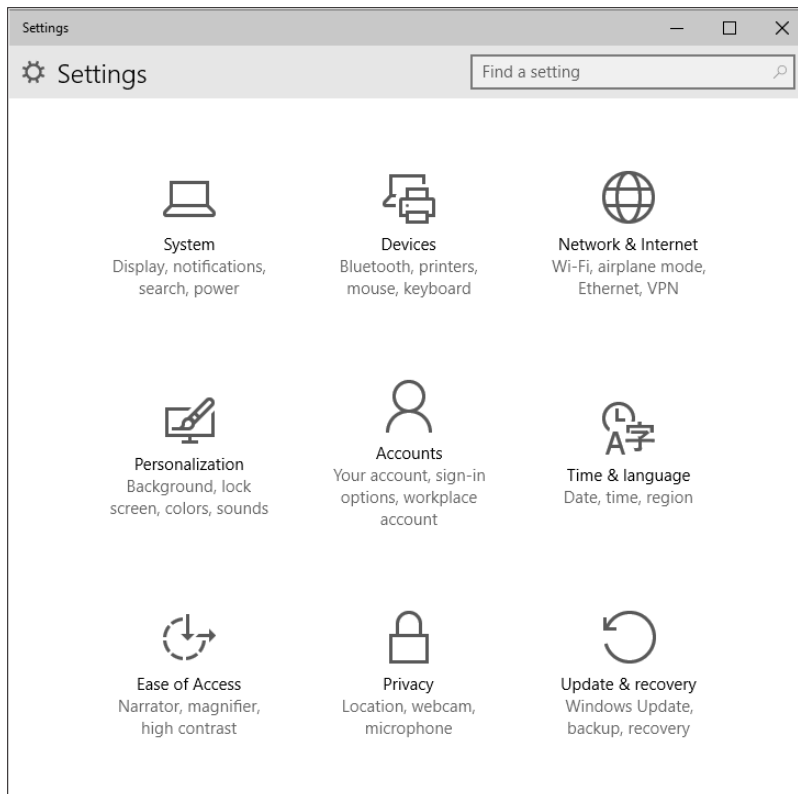


FIGURE 2-2 The Settings app is designed to be touch-friendly and to cover most common configuration tasks.

Speaking of Control Panel, it plays a diminished role in Windows 10 but is far from gone. Since the launch of Windows 8, each successive Windows release has moved more options into this app, usually (but

not always) removing the corresponding entry in the desktop Control Panel. This is an ongoing process as well, one that will undoubtedly continue after the official release of Windows 10.

The System pane, shown in Figure 2-3, is a case in point. In this preview release, clicking or tapping Power & Sleep offers only limited options. That shortcut in the bottom right, Additional Power Settings, leads to the familiar Power Options page in Control Panel.

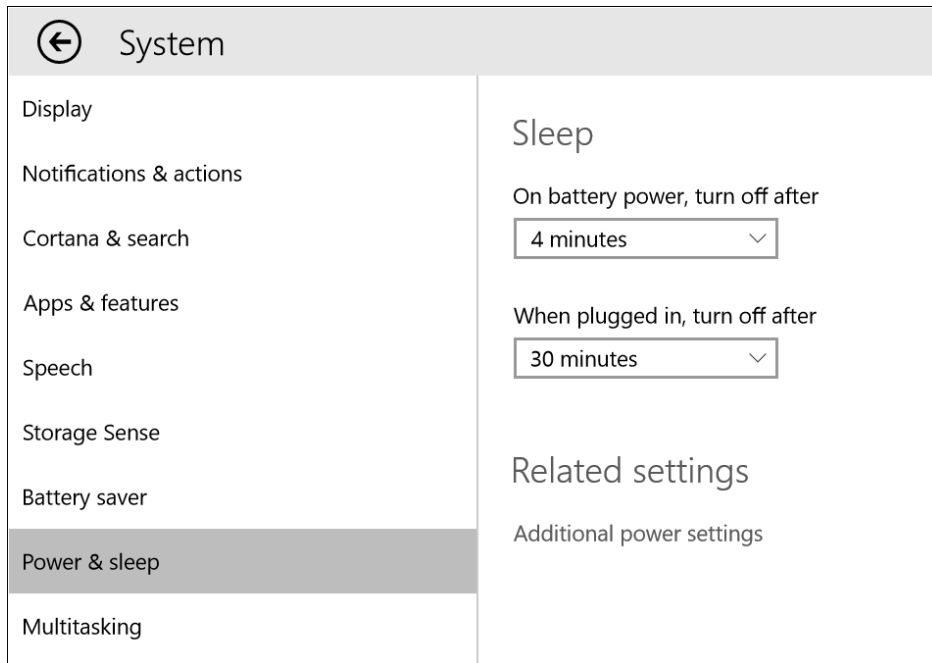


FIGURE 2-3 The number of options in the Settings app is growing steadily, but some tasks still require a trip to Control Panel.

In general, you're likely to find shortcuts for simpler tasks in the new Settings app, with complex or esoteric jobs (especially administrator tasks) requiring a trip to the desktop Control Panel and related utilities.

Notifications Center and action buttons

On a tablet or touchscreen-equipped PC running Windows 8 or Windows 8.1, swiping in from the right opens the Charms menu. In Windows 10, that menu is gone completely, replaced by a Notifications Center that groups app notifications in a single place, with a customizable group of one-tap action buttons at the bottom of the pane.

The icon just to the left of the system clock "lights up" if you have new notifications, going dark after you clear the list.

Figure 2-4 shows the Notifications pane open, with the group of action buttons expanded to show the full collection on this device instead of the top four.

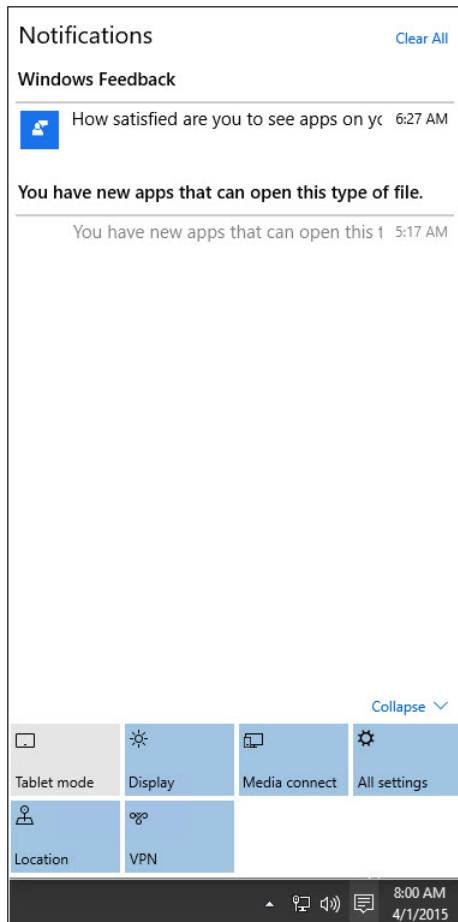
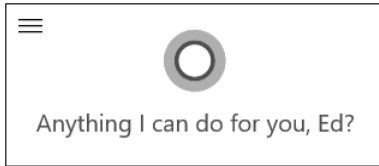


FIGURE 2-4 The Notifications pane shows messages from apps and online services, with action buttons at the bottom of the pane.

The list of four action buttons shown by default can be changed, and you can expand the group to show additional options. (Those options depend on the device itself.)

Cortana

Cortana is one of the signature features of Windows 10, adding a personality (with the name and voice taken from the Halo franchise on Xbox). Essentially, Cortana acts as a personal assistant, combining local and web search with the ability to understand spoken commands and enough smarts to convert those commands into tasks, appointments, or instructions.



Although Cortana has been part of Windows Phone for nearly a year, she appeared for the first time in the Windows 10 Preview in late January. Because much of Cortana's magical powers derive from web-based services, she's getting smarter with age. What you see in the current preview releases is a pale imitation of what you'll see after a year or two of continuous improvements.

The best way to understand Cortana is to type something into the box just to the right of the Start button, or click the microphone icon and say it instead. (If you don't enable Cortana, that box performs simple searches, sans personality.)

After you and your users get past the novelty of it all, take a look at Cortana's notebook, which is shown in Figure 2-5. That's where you can fine-tune the information—news, upcoming appointments, weather, reminders, and so on—that pops up instantly when you click in the "Ask me anything" box. (That summary is replaced with search results as soon as you start typing.)

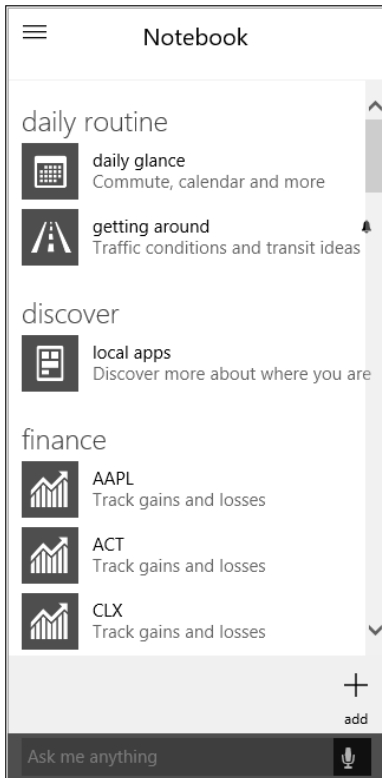


FIGURE 2-5 The Notebook offers users fine-grained control over what sort of information Cortana will assist with.

Modern apps in resizable windows

If you supported a group of users running Windows 8 or Windows 8.1, you probably heard familiar complaints based on a common theme: the experience of using modern Windows apps, mostly in a full screen, is dramatically different from the experience of using Windows desktop apps. The shift between those two modes of working is jarring, especially on the desktop.

The other challenge of Windows 8 and Windows 8.1 is navigating between apps. On a touchscreen, it's a reasonably fluid process: swipe from the left edge of the screen to switch between apps. But with a mouse or trackpad, the gesture for switching to another app requires moving the mouse pointer to the top-left corner, waiting for a row of thumbnails to appear, and then picking one.

Windows 10 leaves all that behind.

To address the first problem, modern apps can now run in resizable windows that can be dragged around the desktop, minimized to the taskbar, and otherwise managed just like Windows desktop applications.

The design standards for modern apps are still under development, but you can expect to see one element increasingly often. At the far left of the title bar is a "hamburger menu," so named because its three vertical lines resemble a stylized and not all that appetizing flat patty between two flat buns. Figure 2-6 shows the contents of that menu for the MSN Money app, which is included with the Windows 10 preview.

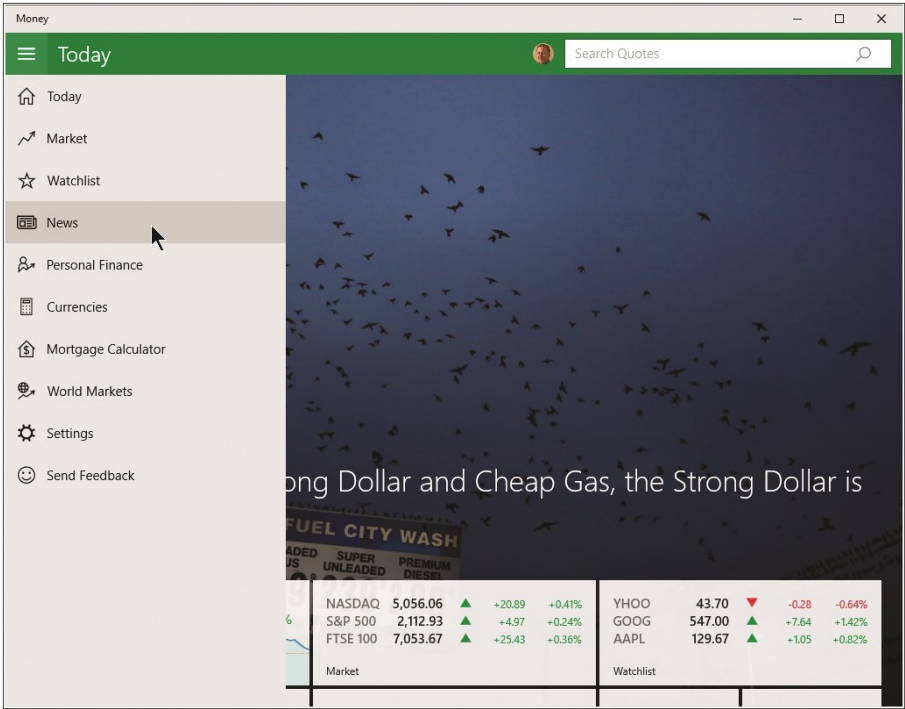


FIGURE 2-6 Windows apps, which used to run only in a full screen or snapped to the side, can now run in resizable windows. To find settings and app commands, use the hamburger menu.

Navigation

As I mentioned earlier, the “hot corner” navigation techniques of Windows 8 are no longer supported. Instead, Windows 10 lets you switch to Task view and then click or tap to choose the app you want from a collection of proportionally sized thumbnails showing all open windows.

On a tablet or touchscreen-equipped device, you can swipe from the left to open Task view. With a mouse and keyboard, press the shortcut Windows logo key + Tab or click the Task View button on the taskbar, just to the right of the search box.

Figure 2-7 shows Task view in operation on a PC running the Windows 10 Technical Preview, with four task windows available for switching.

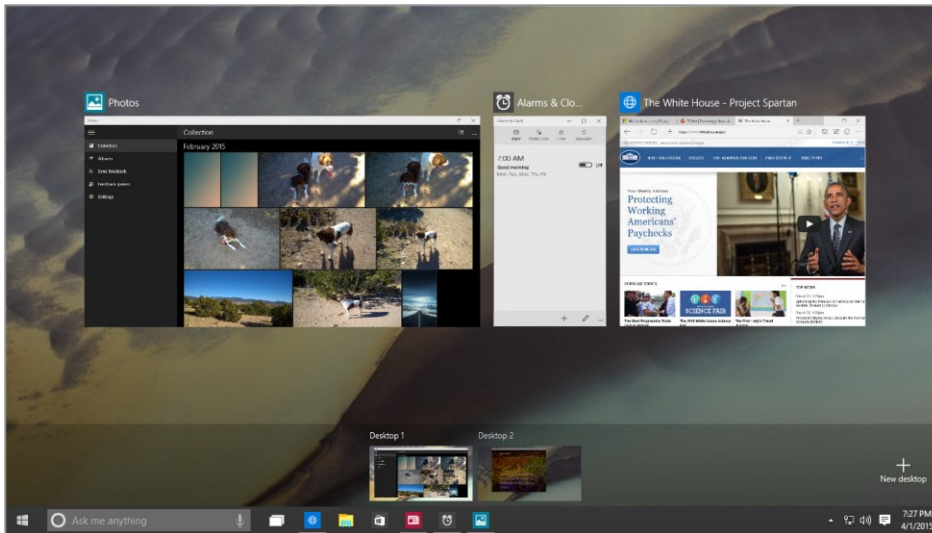


FIGURE 2-7 In Task view, every running app and every open settings page or File Explorer window gets its own thumbnail for quick task switching.

If you see only three running tasks in Figure 2-7, look more closely. The fourth program is running by itself on a second virtual desktop, which you can switch to with a click or a tap.

Windows 10 also improves, subtly but significantly, on the window-snapping behavior (also known as Aero Snap) from Windows 7. In Windows 10, you can snap a window to either side, where it will occupy half the screen, or to any of the four corners so that it occupies that quadrant of the display.

If you snap a window to either side, Windows 10 assumes you want to snap another window alongside it, perhaps to share data between a Microsoft Word document and a Microsoft Excel spreadsheet or to copy between File Explorer windows. To make picking that second snapped app easier for you, Windows

10 helpfully displays thumbnails of all other running windows alongside the one you just snapped, as shown in Figure 2-8. (Click anywhere else if you want to refuse the offer of snapping a second window.)

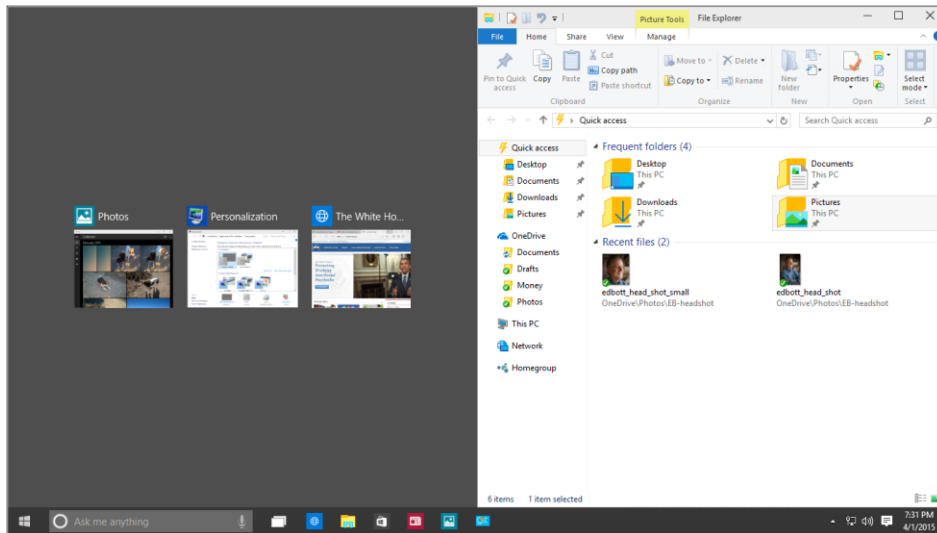


FIGURE 2-8 When you snap a window to one side of the screen, Windows 10 assumes you want to snap another window alongside it and displays thumbnails to let you choose.

Tablet Mode

Most of the changes I've described so far in this chapter are for the explicit benefit of people using a PC or laptop in the traditional fashion: with a keyboard and mouse or trackpad.

But if you are using a tablet (or a touchscreen-equipped hybrid device flipped for handheld use), the navigational challenges are different.

Enter Tablet Mode, which you can do by swiping in from the right and tapping the Tablet Mode action button at the bottom of the Notifications pane. (Tablet Mode also works well on a traditional PC if you want to run an important app in a full screen to make best use of available space and minimize distractions.)

Turning on Tablet Mode maximizes the Start menu, shrinks the search box to a single Cortana icon, and runs every app in full-screen mode. You can snap a window to the side of the screen, but when you do it occupies the full height of the display, and there's a thick black bar between snapped apps, as shown in Figure 2-9.

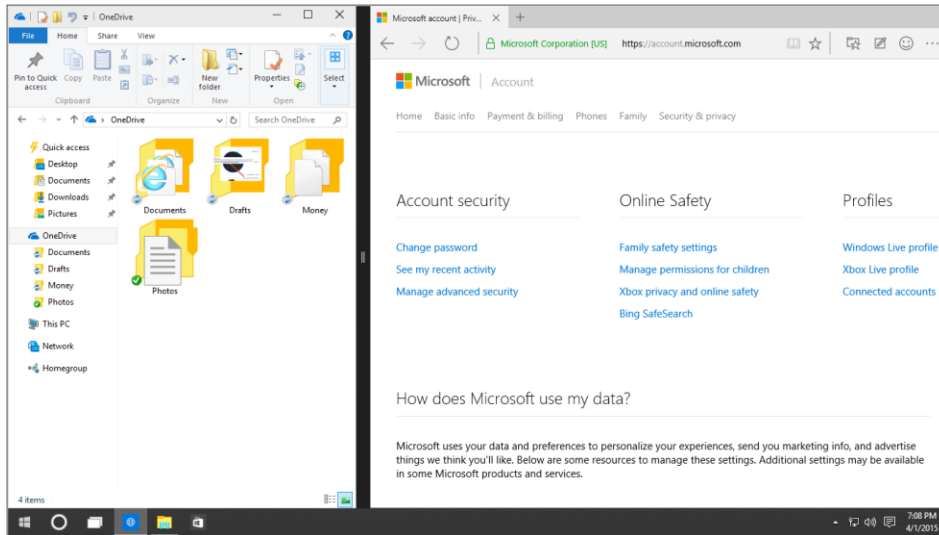


FIGURE 2-9 In Tablet Mode, resizable windows are not allowed. Apps run in full screen unless they're snapped side by side like this.

File Explorer

IT pros and power users spend a disproportionate amount of time managing files, which is why it's worth calling out some of the changes in File Explorer in Windows 10.

If you're moving to Windows 10 from Windows 7, the name change, from Windows Explorer to File Explorer, is new. The next most obvious change, which will be familiar to anyone who's used Windows 8.1, is the addition of Microsoft Office-style ribbons in place of menus and command bars.

Figure 2-10 shows a typical File Explorer window with a context-sensitive Picture Tools ribbon visible.

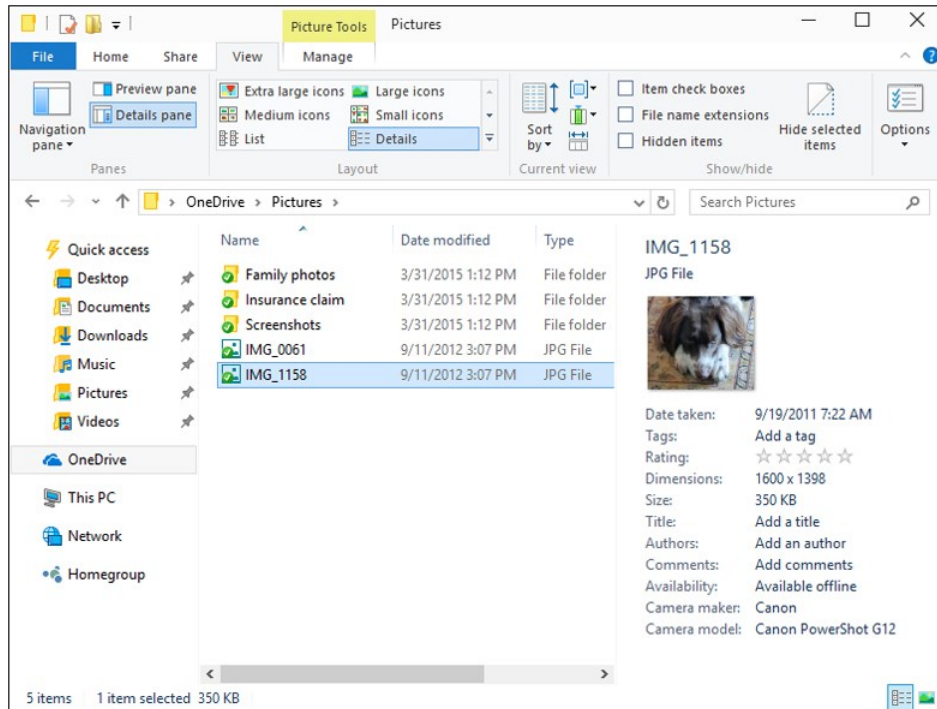


FIGURE 2-10 For anyone moving from Windows 7, the arrangement of commands into ribbons is the biggest change in File Explorer.

In the left pane, a customizable Quick Access list replaces the Favorites list from earlier versions. You can show or hide libraries. (They're hidden by default on a clean install.)

And searching for files is much easier because of the point-and-click options on the Search ribbon, which were introduced in Windows 8. The Search Tools ribbon, shown in Figure 2-11, appears automatically when you click in the search box.

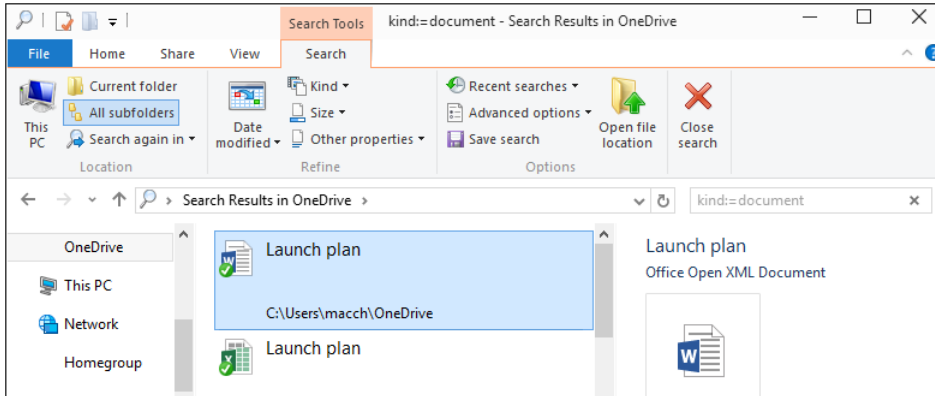


FIGURE 2-11 With Windows 10, clicking in the search box in File Explorer exposes these point-and-click options for filtering and finding files.

Some other subtle File Explorer changes in Windows 10 include a new Share icon that allows you to share a file, group of files, or folder with any app that supports share contracts. In the Folder Options dialog box, there's now a drop-down list to choose which top-level item from the left tree pane you want selected when you open a new File Explorer window.

Cloud connections

The long-term roadmap for Windows 10 includes a unified sync client that combines access to files stored on either or both of Microsoft's cloud-based storage services: OneDrive (a free consumer service that offers additional storage for a price) and OneDrive for Business, which is a feature of Office 365 Business and Enterprise accounts.

In the current Windows 10 Technical Preview, OneDrive for Business is missing completely, and the OneDrive client doesn't yet contain some improvements that are on the roadmap.

For now, the OneDrive client works reasonably well for syncing files. During setup or any time after, you can enable the option to save space by selecting specific folders instead of the entire contents of a OneDrive, as shown in Figure 2-12.

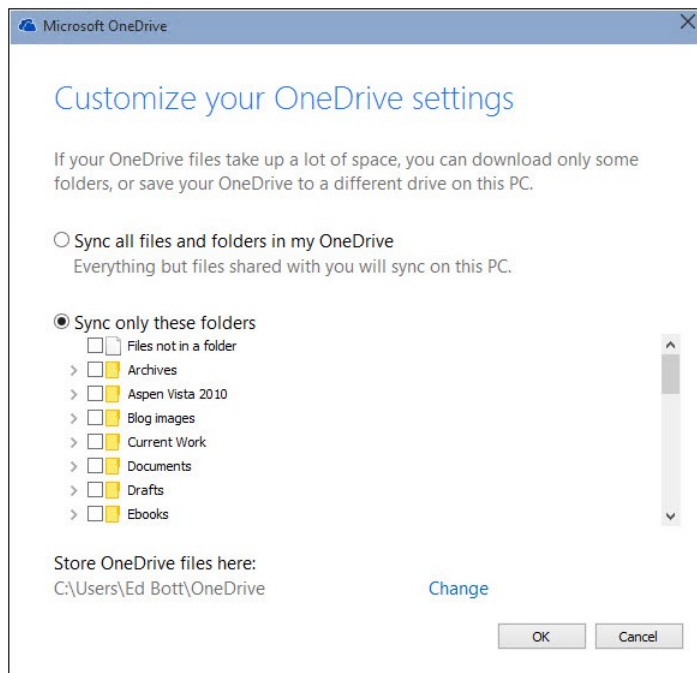


FIGURE 2-12 The current OneDrive sync client allows the space-saving option to choose specific folders instead of an entire library of files.

Again, this feature is likely to change significantly in the next year, so don't spend too much time obsessing over the details of the user experience.

CHAPTER 3

Installing and deploying the Windows 10 Technical Preview

For IT pros, the most important part of the job is figuring out how to balance two occasionally conflicting concerns: the legitimate needs of users for a customized and comfortable experience, on the one hand, and the organization's needs for security and manageability on the other.

You can adopt a refreshingly different set of priorities for the Microsoft Windows 10 Technical Preview. For enterprise customers, the main purpose of the preview is to evaluate an operating system that is a work in progress to provide feedback to guide Microsoft in its development process.

This preview release is not for broad deployment. In limited installations, independent of your organization's deployment and management infrastructure, you can experiment with considerably more freedom than if you were evaluating finished software and planning its deployment in a production environment.

Windows 10 is rolling out in phases. The first release, with a feature set that emphasizes the needs of consumers and small businesses, will be broadly available in summer 2015. The Windows 10 ecosystem should become even richer in the fall, as new devices appear in the market with hardware (biometric sensors, for example, as well as USB-C connections) that enables new Windows 10 features.

And unlike previous Windows releases, Windows 10 will continue to evolve, with new features, big and small, appearing as a part of the same cycle that supplies security and reliability updates. Members of the Windows Insider program will continue to see new features and provide feedback to Microsoft before those features are made available to all Windows 10 customers. If a feature isn't ready for widespread release in one update, it might appear a few months later.

The next version of Windows Server, built on the same foundation as Windows 10, is in a Technical Preview release now, with a planned final release available in 2016. Some features in Windows 10 Enterprise that require complementary features on the server side, by necessity, also will appear in 2016. In some cases, those new features might also require updates to current Windows Server versions.

Microsoft says the next release of System Center Configuration Manager, which will include support for Windows 10, is on the same track as Windows Server, with a 2016 release date. Updates to some currently supported pieces of the System Center infrastructure will also include support for Windows 10. System Center Configuration Manager 2012 and 2012 R2 will be updated to support management and deployment of Windows 10, while updates to Configuration Manager 2007 will add management support only.

That's a pretty unsettled landscape, which is why this chapter emphasizes processes for installing and configuring individual Windows 10 devices for evaluation purposes. I also include an overview of the roadmap for Windows 10 support in Microsoft deployment tools.

Compatibility and preparation

It's too early to begin planning a wide-scale Windows 10 deployment. But you can certainly make life easier on your future self by making some intelligent deployment decisions for your organization now.

The hardware requirements for Windows 10 are identical to those of Windows 7 and Windows 8.1, so any device that can run either of those operating systems should be capable of running the Windows 10 Technical Preview. In addition, most desktop applications that run on Windows 7 should also run on Windows 10.

Windows 8.1 is the best choice for existing touchscreen-equipped devices. It offers a straightforward upgrade path to Windows 10.

For conventional (non-touch) desktop PCs and laptops running Windows 7, there's an equally straightforward path to Windows 10. In fact, the current Windows 10 Technical Preview is available as an upgrade to Windows 7 for anyone who enrolls in the Windows Insider program and opts in for Windows 10 to be delivered through Windows Update.

NOTE For Windows 7 PCs, the most important additional step is upgrading to Internet Explorer 11 before January 12, 2016, when support for earlier versions of Internet Explorer officially ends. Beginning on that date, only the most current version of Internet Explorer available for a supported operating system will receive technical support and security updates. For full details on the Internet Explorer Support Lifecycle, see the FAQ at <https://support.microsoft.com/en-us/gp/microsoft-internet-explorer>.

To install Windows 10, you need sufficient free storage space (at least 16 GB for 32-bit versions and 20 GB for 64-bit) and sufficient installed RAM (a minimum of 1 GB for 32-bit, 2 GB for 64-bit), or the installation will be blocked. The processor must support Physical Address Extensions (PAE); Data Execution Protection, via the No-eXecute (NX) page-protection feature or the eXecute Disable (XD) bit feature; and Streaming SIMD Extensions 2 (SSE2). A small number of older PCs might be blocked from 64-bit installations because their processors don't support specific instructions like these: CMPXCHG16b, PrefetchW, and LAHF/SAHF.

The following device types are incompatible with Windows 10:

- The Surface RT, Surface 2, and other devices running Windows RT are not compatible with the Windows 10 Technical Preview and will not be upgradeable to the final release of Windows 10.
- Small tablets with 32 GB or less of storage that were configured using WIMBoot were blocked from upgrading to some releases of the Windows 10 Technical Preview. Microsoft has removed this limitation in current preview releases.
- The Windows 10 Mobile operating system, although closely related to Windows 10 in many respects, is delivered separately. The Windows 10 Technical Preview bits that are available for installation on PCs will not work on phones.

Enterprise deployment tools: A roadmap

As I mentioned in the introduction, most of Microsoft's enterprise deployment tools are on a different development cycle from that of the Windows 10 Technical Preview.

The next version of System Center Configuration Manager will include full support for deployment, upgrade, and management of Windows 10 desktop operating systems and associated updates. Microsoft also says it has plans to provide an update for System Center 2012 R2 Configuration Manager to support Windows 10 deployment, upgrade, and management. The Microsoft Deployment Toolkit (MDT) also will be updated with support for Windows 10.

As of early 2015, the Windows Assessment and Deployment Kit (ADK) is available in a preview release for Windows 10. (For download instructions and links to details about what's new, see <http://dev.windows.com/en-US/featured/hardware/windows-10-hardware-preview-tools>.)

Figure 3-1 shows the options available when you install the preview release of the Windows ADK.

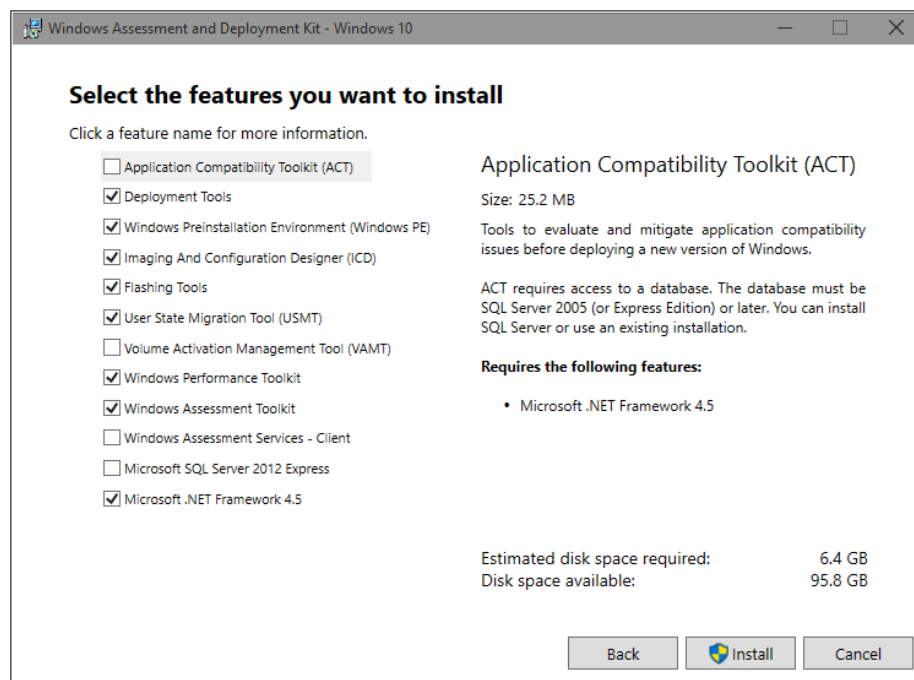


FIGURE 3-1 The individual options available with the new Windows Assessment and Deployment Kit are designed for IT pros and hardware manufacturers.

If you've used the ADK with previous Windows deployments, you should definitely evaluate this preview ahead of its final release. The new ADK includes some significant improvements:

- **Provisioning support** This capability allows you to create special packages that you can use to customize new Windows 10 devices, "provisioning" them for use in your enterprise without having to wipe the preinstalled OEM image and load a custom image of your own creation.
- **System file compression** You can run Windows 10 directly from compressed files. The effect is similar to WIMBoot, a feature that was introduced in the Windows 8.1 Update. The new process is more elegant (and much more efficient) because it uses individual files instead of a static Windows Image (WIM) file. When updating system files, Windows 10 replaces the old files instead of keeping both copies.

In addition, the ADK contains documentation for two useful features that are part of Windows 10:

- **Push-button reset** This feature, available since Windows 8, now incorporates system updates by default. When a user needs to use the Reset option to recover from a problem, the new image is fully up to date, with no need to reinstall new updates.
- **Partial language packs** Instead of adding full language packs (which can consume excessive disk space), you can add just the base user-interface files for a language. Windows will download the full language packs via Windows Update if needed when enabling features such as handwriting or voice recognition.

Windows 10 installation options

After Windows 10 is formally released, you'll be able to create images that you can deploy throughout your organization. During this evaluation phase, however, you'll perform most installations manually, using clean installs.

This section discusses the ins and outs of those options.

Upgrade or clean install?

The simplest option by far is an in-place upgrade. Eventually, you'll be able to automate this process in your organization on devices running Windows 7 or Windows 8.1, using the Microsoft Deployment Toolkit (MDT), System Center Configuration Manager, or an alternative software distribution tool.

For a single device, using Windows Update to initiate the Windows 10 upgrade is a perfectly reasonable choice. During the preview period, making the upgrade files available in Windows Update requires registering for the Windows Insider program (<https://insider.windows.com>) and then opting in to install the preview by running a small configuration utility.

This option is available on any device running Windows 8.1 or Windows 7, provided it meets the system requirements described earlier in this chapter. Figure 3-2, for example, shows the update ready to run on a Windows 7 PC.

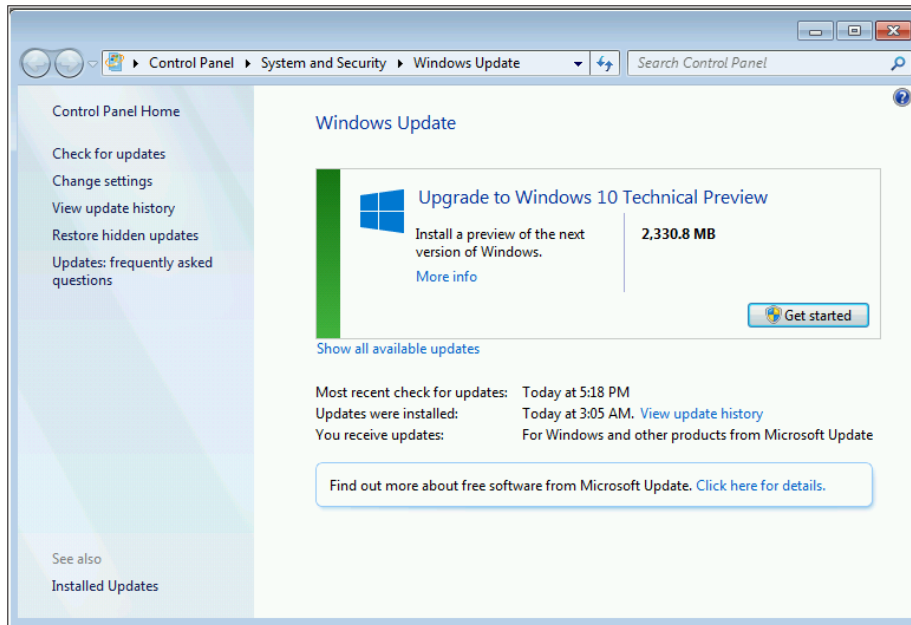


FIGURE 3-2 Despite the seemingly vast difference in version numbers, upgrades from Windows 7 to Windows 10 are fully supported through Windows Update.

The upgrade process is generally quick, with the biggest influence on total time being the speed of your Internet connection. In general, an installation should take no more than a couple of hours, and can be much faster. The image-based installation has been field-tested on hundreds of millions of PCs over the past few years. If something goes wrong, the Setup program will automatically roll back to the previous version of Windows with all data files and configuration details unchanged.

NOTE If you use a third-party, disk-encryption tool, take extra time before you even think about moving to Windows 10 on a device with encrypted storage. The in-place upgrade process should work flawlessly on systems protected with BitLocker encryption, but the Windows installer isn't able to access disks encrypted using third-party software. Your safest option is to disable all encryption before upgrading, and then restore the encryption after the upgrade is complete. Microsoft is working with the providers of encryption software to make this process smoother when Windows 10 is officially released.

You also can start an upgrade from Windows 7 or Windows 8.1 by using physical installation media or a mounted ISO file. Choosing this option kicks off the familiar Windows upgrade workflow.

In any of these upgrade scenarios, assuming the operation completed smoothly, the result is a device running the same Windows edition (Core, Pro, or Enterprise) as the pre-upgrade device. Data files, apps, and settings should be migrated completely in most situations, although it's possible you'll find small errors in the process, especially in preview releases.

To perform a clean install, you need to boot from installation media (a USB flash drive or a DVD, or an ISO file in the case of a virtual machine). If you choose to format the destination drive, the process is destructive, wiping out all apps and data. If you choose an existing volume but don't erase it, existing files are moved to a Windows.old folder, where they can be recovered in a pinch.

NOTE Don't delete the Windows.old folder unless you're desperately in need of disk space. In Windows 10, the existence of this folder allows you to roll back from Windows 10 to your previous Windows version from the Recovery option in the Settings app. Keep it until you absolutely need to delete it. If you decide that you no longer need those files and want to reclaim the space they're occupying, run the Windows Disk Cleanup utility (Cleanmgr.exe) as an administrator. Choose the Previous Windows Installation(s) option to get rid of those files permanently.

Choosing an account type

In an upgrade, Windows 10 preserves your existing user profile and prompts you to sign in using the same credentials as on the upgraded device. On a clean install, you need to create the first account from scratch. In Windows 10, you have three options:

- **Microsoft account** This is the default option for a personal device that isn't joined to a domain. A Microsoft account (which is the direct descendant of the former Passport and Windows Live ID services) uses an email address and password to enable a variety of cloud services. For Windows 10 devices, the most immediate benefits are the ability to sync settings and files (using OneDrive) between devices signed in with the same account. Depending on your network policy, it's possible to link a Microsoft account to a domain account so that a domain-joined machine can get the benefit of syncing settings.
- **Work account** As an IT pro, you're probably intimately familiar with domain accounts, which use Active Directory credentials to authenticate users and allow access to resources on a shared enterprise network. Windows 10 includes the option to connect to an Azure Active Directory account, which allows access to cloud-based resources such as Office 365. Setting up a work account can also allow mobile-device-management software on the corporate network to handle device enrollment and enforce company policies.

- **Local account** This account option is difficult to find in some Windows setup configurations, but it's still possible to enable this type of account. The credentials are stored only on the local device.

In a clean install, after you get past the license agreement and installation options, you'll reach a crucial stage of the Setup program. If you're using Windows 10 Enterprise, the setup program assumes you're doing so on a work device. If you're using Windows 10 Pro, you have a choice to make, as shown in Figure 3-3.

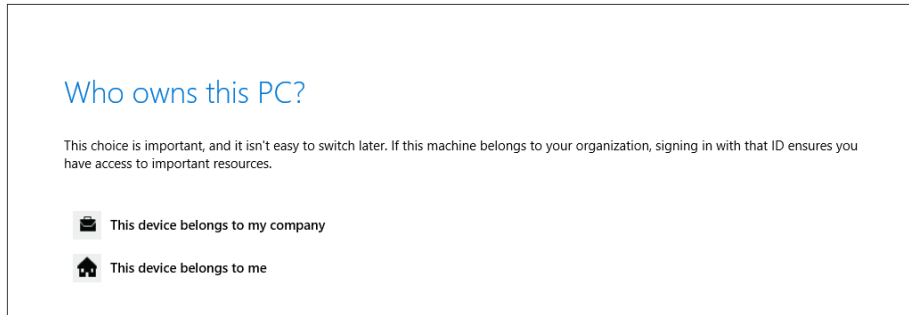


FIGURE 3-3 This option is visible only when performing a clean install of Windows 10 Pro.

Choosing the first option (This Device Belongs To My Company) and clicking Next leads to a slightly confusing dialog box that prompts you to set up "your work or school PC." That dialog box is intended for Azure Active Directory credentials, such as those linked to an Office 365 account. But first, you see a warning dialog box that includes this crucial caveat:

IMPORTANT If you plan to join your PC to your work domain, select Continue and choose the link to Set Up Windows with a local account instead. After you sign in to Windows with that local account, you can join your PC to the domain as you have in the past.

If you choose to enroll with your work account now instead of creating a local account, do not attempt to join your PC to the domain later. If you do, you won't be able to sign in to your PC.

That's a pretty clear warning. When you reach the Setup page shown in Figure 3-4, enter your workplace account *only* if you have Azure Active Directory credentials such as those with an Office 365 Enterprise account.

Set up Windows for this work or school PC

Sign in

ed@bottnet.com

••••••••

[Forgot your password?](#)

What account should I use?

If your organization uses Office 365 or other business services from Microsoft, use the same username and password to sign in here.

[Set up Windows with a local account](#)

[Privacy statement](#)

Cancel

FIGURE 3-4 Enter your credentials here only if you have an Azure Active Directory account. If you have an Active Directory domain, choose the local account option.

Choosing the local account setup leads to a page that should be familiar to anyone who has installed Windows in the past two decades. Figure 3-5 shows what to expect.

Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

Ed Bott

.....

.....

...

Back Next

FIGURE 3-5 The option to create a local account is well hidden, but still available.

If you tell Windows that you're setting up a personal device, you're taken by default to a setup page that strongly urges you to use an existing Microsoft account or create a new one. Figure 3-6 shows the two available options.

Get more when you sign in

 Sign in with your Microsoft account

[I forgot my password](#)

[Sign in](#)

Or create a new account

Use your favorite email address or phone number, or make a new email address.

[Sign up](#)

Here's why

To download new apps and games, you need to sign in. Your Microsoft account helps us make your experience just right for you, and helps you restore your info if anything happens to this PC.

[Privacy statement](#)

FIGURE 3-6 For most personal devices, using a Microsoft account provides significant benefits and is the best choice.

If you sign up with the same Microsoft account you use on other devices, any settings you chose to sync from those devices will be replicated on the new device. You'll also have access to the Windows Store and to any cloud services that are linked to that Microsoft account, including OneDrive, Outlook.com (formerly Hotmail) email, and Xbox services.

You can create a Microsoft account using any email address, including a personal address with a custom domain; you're not limited to the Microsoft-owned Outlook.com, Live.com, and Hotmail.com domains.

Although it's not immediately obvious, the option to create a local account is also available from this page. Click or tap Sign Up, as if you were planning to create a new Microsoft account. Ignore the boxes at the top of the page, shown in Figure 3-7, and instead click or tap the nearly invisible link in the lower-left corner, Connect My Account Later.

Create a Microsoft account

Create a Microsoft account to use on this PC and with Microsoft services like Outlook.com, OneDrive, Xbox, and Office. If you already use a Microsoft service, choose back to sign in with that email and password.

@

[Or use your favorite email](#)

Birthdate

[Connect my account later](#)



FIGURE 3-7 Although the primary purpose of this setup page is to create a new Microsoft account, it also includes a well-hidden link to create a local account.

Which account type should you use?

For evaluating Windows 10 in the enterprise, joining the device to the domain and signing in with a domain account is the best way to assess compatibility with your existing network. That option requires that you first create a local account.

Work accounts are appropriate for Office 365 and other Azure Active Directory deployments.

For all other situations, the best choice is a Microsoft account, especially if the owner of the device already uses Microsoft services and plans to use Windows 10 on other devices with the same account.

It's tempting for experienced Windows users to gravitate toward the comfort zone of local accounts, especially if you're concerned about the possibility that personal or business information will accidentally spill over into the evaluation environment.

In that scenario, a better choice than a local account is to create a new Microsoft account using a free Outlook.com address. Choose an alias that clearly identifies it as an evaluation account, and use its free file

storage and email capabilities strictly for testing purposes. That option lets you see the benefits of a Microsoft account with minimal risk.

And there's a singular advantage to that strategy as well: it allows you to turn on BitLocker encryption for the test device and save the recovery key to secure storage using the alias you created.

Security in Windows 10

Microsoft Windows 10 is far more effective than its predecessors when it comes to protecting your organization and your users from common and not-so-common threats. That shouldn't come as a surprise, of course. Since the Trustworthy Computing initiative in 2002, each new version of Windows has introduced significant security enhancements.

Most casual observers see the obvious manifestations of security, in the form of features that have a visible set of controls or warnings, such as Windows Defender and the SmartScreen filter that blocks potentially dangerous downloads. Windows 10 also enables crucial security features in 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.

Windows 10 also includes a new, potentially game-changing security feature that has the potential to eliminate the weakest link in present-day computer security. The new identity features in Windows 10, built around sophisticated biometric sensors and easy-to-use multifactor authentication, can completely replace passwords, eliminating an entire class of security threats.

In this chapter, I offer an overview of the multiple layers of security in Windows 10.

The evolution of the threat landscape

Computer security experts like to talk about the “threat landscape,” a wide-ranging and constantly evolving set of ways that malicious outsiders can attack devices and networks. In the past, hackers were motivated by personal fame and bragging rights. Today, organized criminal gangs have turned cyber attacks into big business, turning their victims' misery into profits with ransomware, click fraud, and identity theft. Politically motivated attackers might be more interested in stealing secrets or causing damage and disruption.

Malware and phishing attacks typically cast an indiscriminate net. By contrast, targeted attacks aim to exploit weaknesses in large organizations. Government agencies and companies that do business in sensitive industries—defense, banking, and energy, for example—have to be constantly aware of the potential for attacks from well-funded, technically skilled outsiders.

And don't assume that your organization is too small or inconsequential to be a target for computer crime. If your small business is connected to one of those large targets, even indirectly, as a subcontractor

or as part of the supply chain, you might find yourself in the crosshairs, with the attackers counting on being able to work their way up the food chain to bigger, even more lucrative targets.

The threat landscape certainly includes malware and intrusions, but it also includes data breaches, unauthorized access to local and network resources, and physical theft.

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 or visit a compromised website, for example.

Damage can escalate quickly if the attacker steals the identity of a support technician or network administrator who signs in to a compromised device using credentials that allow greater access to network resources.

You can also become a victim through no fault of your own, if a third party stores your credentials insecurely and then suffers a data breach.

Securing hardware

The first layer of protection for a Windows 10 device is the hardware itself. Key security features in Windows 10 (originally introduced in Windows 8.1) take advantage of modern hardware designs. Although you can install and run Windows 10 on older hardware, you'll get best results when these two capabilities 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 10, offering the Secure Boot capability and support for self-encrypted drives, for example. (I'll say more about both of those features later in this chapter.) UEFI has been a requirement for original equipment manufacturers (OEMs) to certify a system or hardware device for Windows 8 or later 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 features in Windows 10, including BitLocker drive encryption, Measured Boot, and Device Guard. I discuss all these features later in this chapter.

In addition, Windows 10 offers support for hardware devices that allows users to identify themselves using biometric information such as a fingerprint recognition, facial recognition, or an iris scan. Windows has had biometrics support since Windows XP. Windows 10 significantly improves the accuracy and integrity of the identification process; it also allows users to register devices as trusted, so that the biometric information becomes part of an easy-to-use multifactor authentication schemes. (I discuss these features in more detail later in this chapter, in “Securing identities.”)

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 10 supports multiple layers of boot protection that were introduced with Windows 8.1 and are not available in Windows 7 and earlier versions. Some of these features are available only if specific types of hardware are installed. Figure 4-1 shows how the boot process works in Windows 8.1 and later versions.

Windows Platform Integrity Architecture
(Windows 8.1 and later)

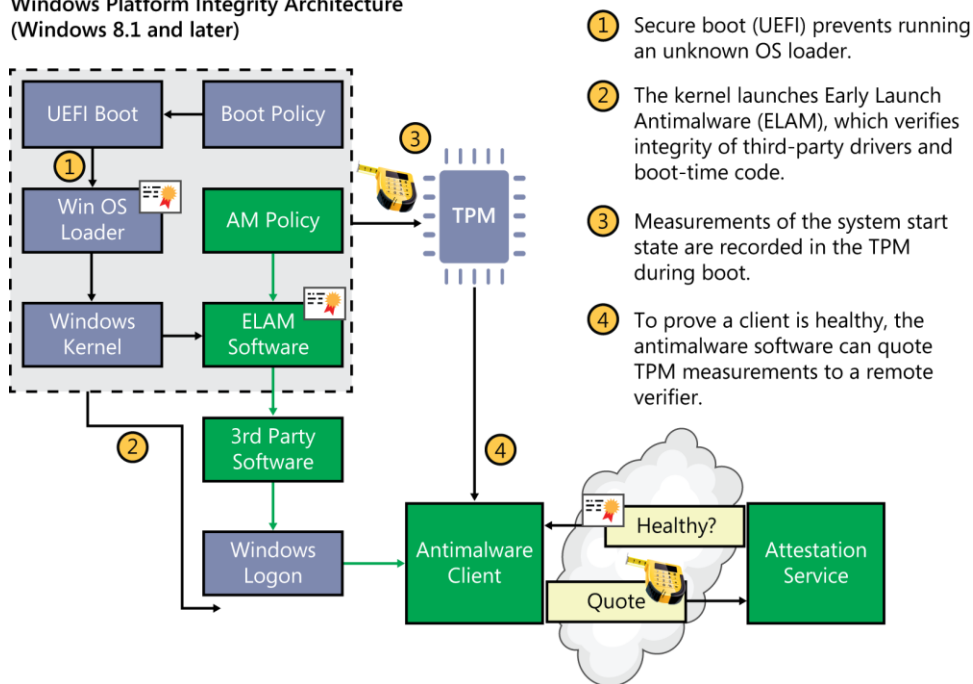


FIGURE 4-1 Security features in Windows 10, enabled on modern hardware, help prevent malicious software from tampering with the boot process.

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 and Windows 10 OS loaders are in that store, allowing the UEFI firmware to validate the certificate as part of its security policy. This feature must be enabled by default on all devices that are certified for Windows 8.1 or later under the Windows Hardware Certification Program.
- **Early Launch Antimalware (ELAM)** Antimalware software that's compatible with the advanced security features in Windows 8 and later versions can be certified and signed by Microsoft. Windows Defender, the antimalware software that is included with Windows 10, 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, which requires the presence of a TPM on a device running Windows 8.1 or a later version, 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.

For Windows 10 devices, Microsoft is introducing a new public API that will allow mobile-device-management software to access a remote attestation service called Windows Provable PC Health (PPCH). PPCH can be used to allow or deny access to networks and services by devices, based on whether they can prove they're healthy. Figure 4-2 shows how PPCH will work with Microsoft's cloud-based Windows Intune management service.

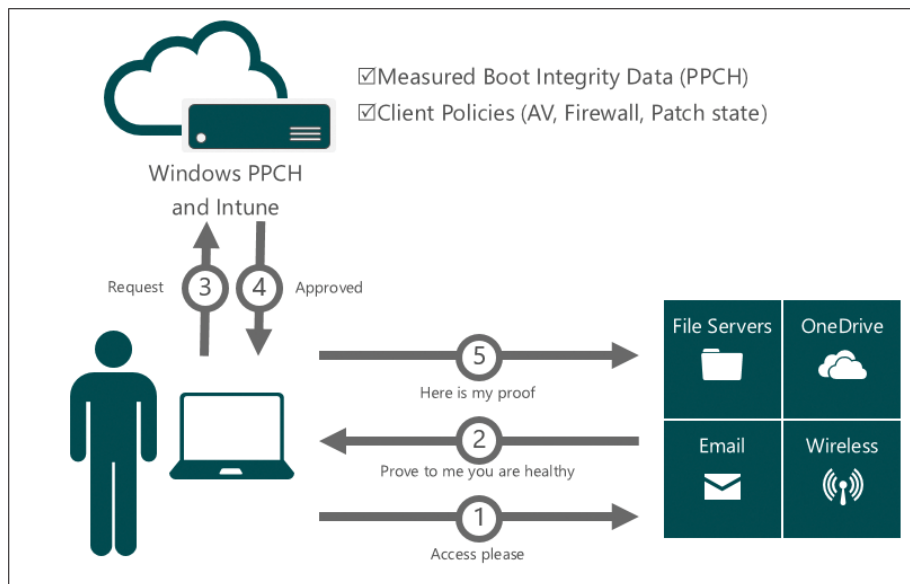


FIGURE 4-2 PPCH can check remote devices for signs of tampering and ensure compliance with policies, controlling access to networks and services based on the results.

Locking down enterprise PCs

Device Guard is a new feature that allows IT pros to lock down a device so tightly that it is incapable of running untrusted software, effectively neutering any attacker or exploit that works by convincing users to run a malicious program. In this configuration, which requires Windows 10 Enterprise edition, the only programs allowed to run are those that are trusted.

Even if an attacker manages to take over the Windows kernel, that person still won't be able to run malicious or unknown executable code, thanks to a key architectural feature of Device Guard. The trust decision for any application is performed using Windows Code Integrity services, which run in Virtual Secure Mode, a Hyper-V protected container that runs alongside Windows. This service makes trust decisions based on signatures that are protected by the UEFI firmware and protected by antitampering features.

If you're excited at the prospect of testing Device Guard, temper your enthusiasm, at least for now. This feature isn't available in preview editions yet.

Securing data on local storage devices

Mad genius cybercriminals exist mostly in movies and pulp fiction. 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 know that 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 remotely, 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 10 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 versions, which traditionally reserved that feature for business/enterprise editions. Encryption can be enabled out of the box on Windows 8.1 and later 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 or Windows 10, 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 OneDrive 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://onedrive.com/recoverykey>) and reseal 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. The Network Unlock feature 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 in Windows 10 encrypts data more quickly than in Windows 7 and earlier versions. With BitLocker in Windows 10, 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 later versions, 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 10 is able to identify an Encrypted Hard Drive device, and its disk-management tools can activate, create, and map volumes as needed. API support in Windows 8.1 and later versions allows 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 and later versions, 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.

Securing identities

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.

An attacker also can steal a user-access token from a compromised machine and then use that token to steal additional tokens. The attacker never has the user name or password, but possessing a stash of hashed credentials is good enough to allow persistent access over time. This technique is called a “Pass the Hash” attack.

Windows 10 includes fundamental architectural changes designed to fundamentally prevent both forms of attack.

For starters, beginning with Windows 10 the derived credentials (hashes) that are used in “Pass the Hash” attacks are moved into Virtual Secure Mode, the same Hyper-V protected container that is used for Windows Code Integrity services.

As part of this architectural change, Windows 10 implements new services called Next Generation Credentials, bringing identity protection to a new level. These features are not yet available as part of the Windows 10 Technical Preview, but the associated services are installed and waiting to be activated, as you can see from Figure 4-3.

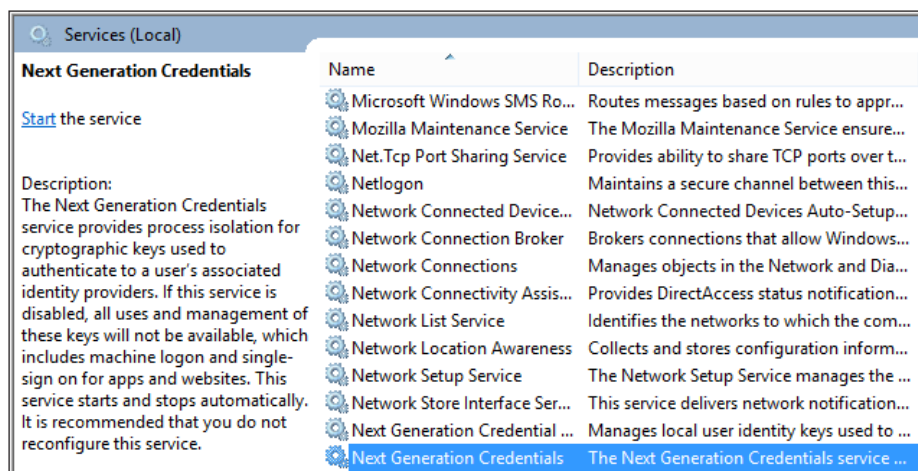


FIGURE 4-3 These two Next Generation Credential services are key to a revolution in identity that eventually will eliminate the need for passwords.

Although multifactor security is available for many devices and services today, it's limited to solutions such as smartcards and authenticator apps on devices such as smartphones. Windows 10 builds multifactor authentication into the operating system and device itself, eliminating the need for additional hardware security peripherals.

The crucial step with Windows 10 is enrolling a device with a consumer service or an enterprise authentication system. Once enrolled, the device itself becomes one of the factors required for authentication. The second factor is a PIN (the default option) or, on new systems with appropriate hardware support, biometric authentication, such as fingerprint recognition, facial recognition, or an iris scan.

Existing fingerprint readers will work with the new authentication measures. For facial recognition, new hardware that includes infrared capabilities is required.

The bottom line? Attackers who steal a cache of user names and passwords are out of luck. They need a user's physical device as well as the ability to transmit the user's credential, and that second step requires access to the user's PIN or biometric information.

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 enrolled device. This enrollment process doesn't require that the device be domain joined, making this feature especially useful in BYOD scenarios.

When this feature is available, a user will be able to enroll multiple devices with these new credentials. Alternatively, users can enroll a single device, such as a mobile phone, that effectively becomes their mobile credential, in a process that is similar to existing multifactor authentication systems. The combinations of an enrolled device and a PIN or biometric proof of identity enables sign-in to all PCs, networks, and web services, locally or remotely. And none of those devices, networks, or services require that a password be stored or transmitted. That makes it impossible for a thief to steal credentials using phishing techniques or other attacks.

The credential itself can be a cryptographically generated key pair (private and public keys) generated by Windows itself, or in an enterprise setting it can be a certificate provisioned to the device from existing PKI infrastructures.

Active Directory, Azure Active Directory, and Microsoft Accounts all support these new user credentials, which means Microsoft online services will support the new credentials with no extra work required. In addition, web services based on the Fast IDentity Online (FIDO) standard, which is supported by many banks and existing authentication providers such as RSA, will be compatible with these credentials as well. This should make it possible for enterprises and consumers to begin the essential step of moving away from passwords.

On consumer devices with the necessary hardware, the local sign-in feature is called Windows Hello. It allows a Windows 10 PC to unlock itself when a user sits down in front of the device, with a log-in screen like the one shown in Figure 4-4.

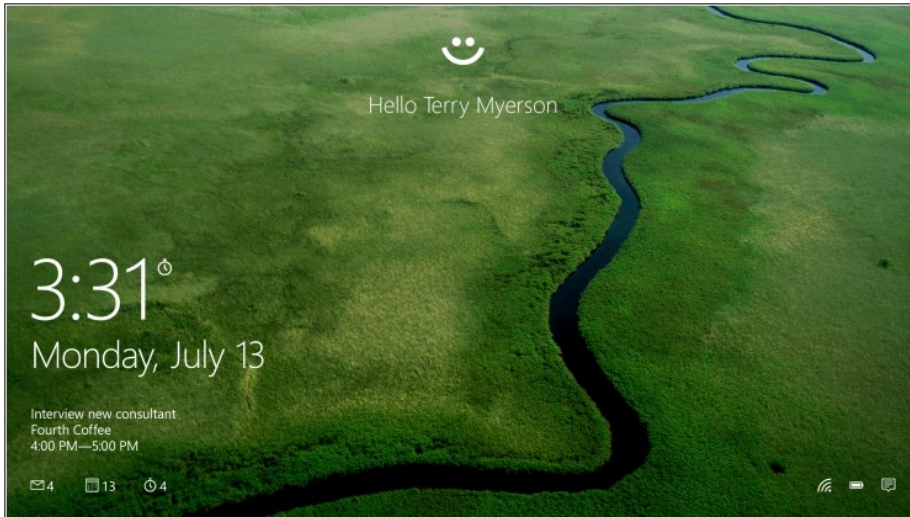


FIGURE 4-4 On consumer devices, biometric authentication allows local sign-in using a feature called Windows Hello.

Windows 10 supports existing fingerprint readers for authentication. Windows 8.1 introduced a system-wide, end-to-end process for enrolling fingerprints for authentication purposes. This experience is available in Windows 10 as well. Figure 4-5 shows the modern fingerprint enrollment experience.

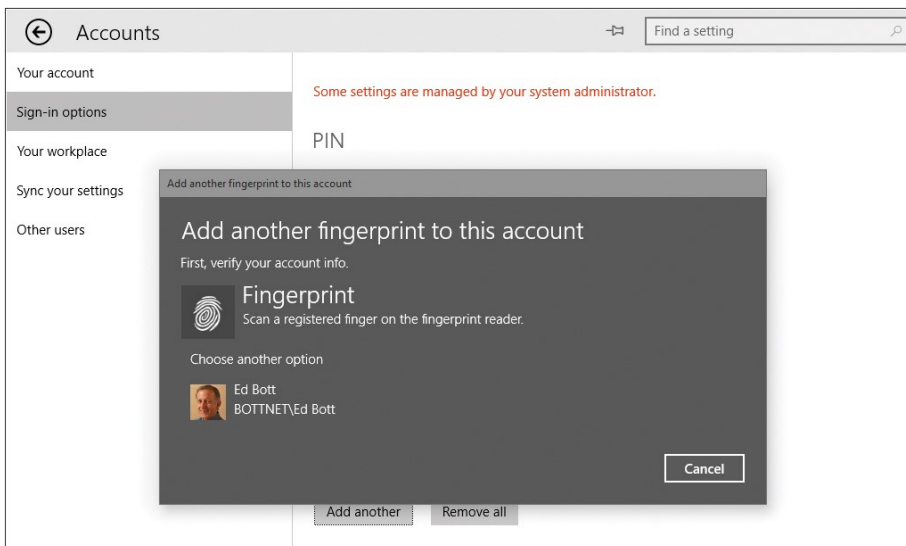


FIGURE 4-5 This end-to-end functionality for fingerprint authentication, complete with drivers, is built into Windows 10.

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 and Windows 10 increase the level of entropy significantly from Windows 7, 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. Beginning with Windows 8, hardware-based DEP support is a requirement; Windows 10 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 Defender

In Windows 7, Windows Defender is the name of a limited antispysware solution. Beginning with Windows 8 and continuing in Windows 10, Windows Defender is a full-featured security solution (and 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 10, Windows Defender also 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.

SmartScreen and phishing protection

Windows 10 includes two separate but related features that share a common name: *SmartScreen*. The basic security principle behind SmartScreen (which was first introduced in Windows 8) is simple: it's much more effective to stop malicious code from running in the first place than to remove it after it has 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.

Local administrators can override the block manually. 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.

Deploying and managing Windows Store apps

The fundamental dividing line between Microsoft Windows 7 and its successors is the ability of those successors to run a new class of apps, optimized for touch and mobile use and distributed through the Windows Store, in addition to familiar Windows desktop programs.

Windows 10 expands this capability in two important dimensions, thanks to the availability of a unified Windows core that runs on a broad range of devices. The Windows 10 universal app platform allows developers to build apps that can run unmodified on all those devices, from phones and small tablets to PCs and the Xbox game console. It also allows those apps to be delivered in a single package, through a single store, to all those devices.

In the Windows 10 Technical Preview, this new, unified store exists as a beta alongside the old Windows Store. Although you can see hints of what will be available in the new store, the real benefits won't be available until Windows 10 is released.

For IT pros whose concerns focus on deploying, managing, and securing enterprise apps, the most interesting developments are still to come. Eventually, Windows 10 will include several new features designed to make the store more useful for delivering universal Windows apps and traditional desktop applications in a managed environment through secure business portals.

Because of the fluid nature of the new Windows Store, this chapter is brief and forward-looking.

Introducing the new Windows Store

Although there are superficial similarities between the new Windows 10 Store and its Windows 8.1 predecessor, a closer look reveals big changes.

For starters, the new store offers more than just apps. Figure 5-1 shows the Store (Beta) app in the April update to the Windows 10 Technical Preview, with categories for buying digital content, such as games, movies, TV shows, and music alongside apps.

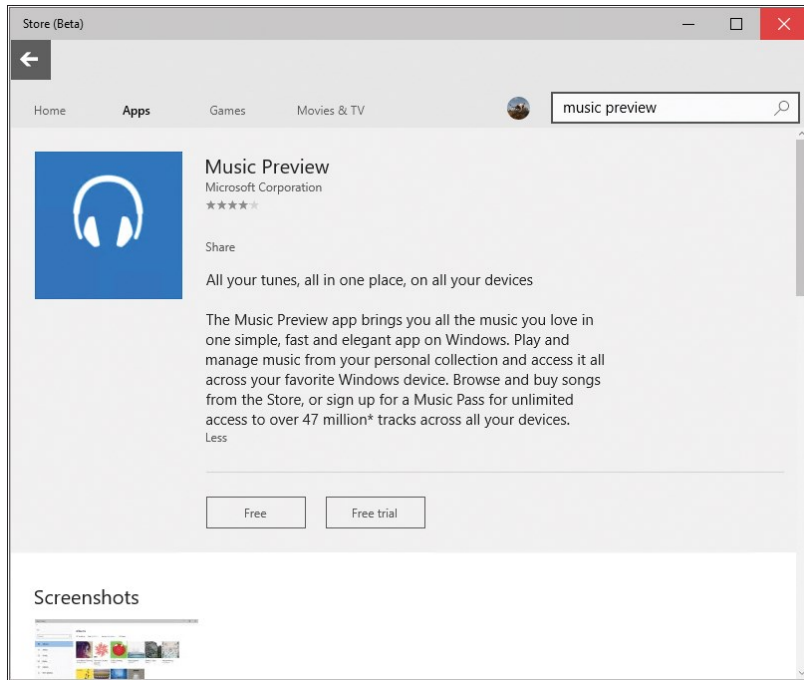


FIGURE 5-1 The updated Windows Store offers excellent search capabilities and access to more than just apps.

The new Store also includes a more detailed summary of the current status of downloads and app installs, with the capability to pause, resume, and cancel downloads. Figure 5-2 shows this feature in action.

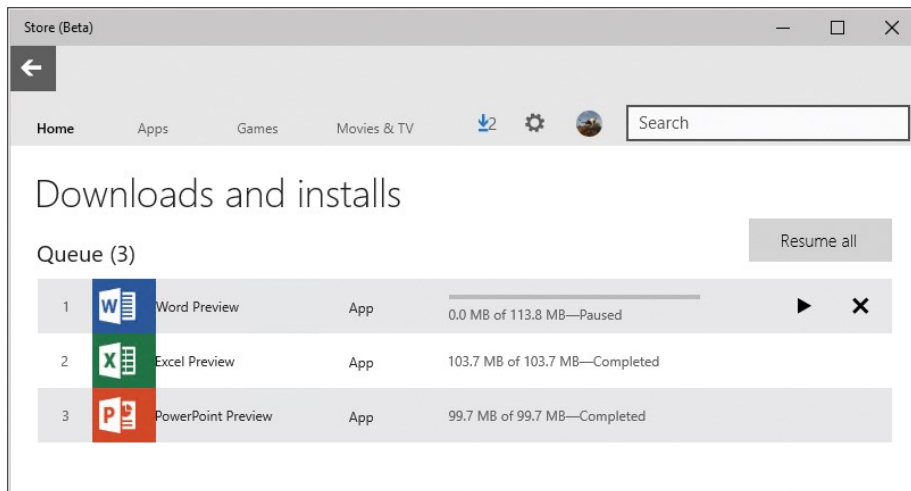


FIGURE 5-2 A menu just to the left of the settings icon lets you click to view and manage current app downloads and installs from the Store.

In Windows 8.1, the public Windows store is the primary means for users to acquire apps, using a Microsoft account and various payment options. With the new Windows 10 Store, enterprise options are considerably richer.

Before we get to that story, though, it's useful to discuss the differences between apps written for Windows 8.1 and the new universal apps.

How universal apps work

Universal apps in Windows 10 have the following characteristics in common with the first generation of modern apps, written for Windows 8 and Windows 8.1:

- 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. Apps can also trigger notifications and alerts, using standard APIs.
- 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.

Because universal apps can run on various screen sizes and orientations, the user experience is *adaptive*, with screen layouts and controls that look and work in an appropriate way depending on their size. This advantage is most obvious on phones and small tablets, but you can see the shift in experience on a conventional Windows 10 PC just by resizing a window.

Figures 5-3 and 5-4, for example, show two views of the Settings app, one in a window wide enough to display the navigation bar on the left, and the other resized to be as narrow as possible.

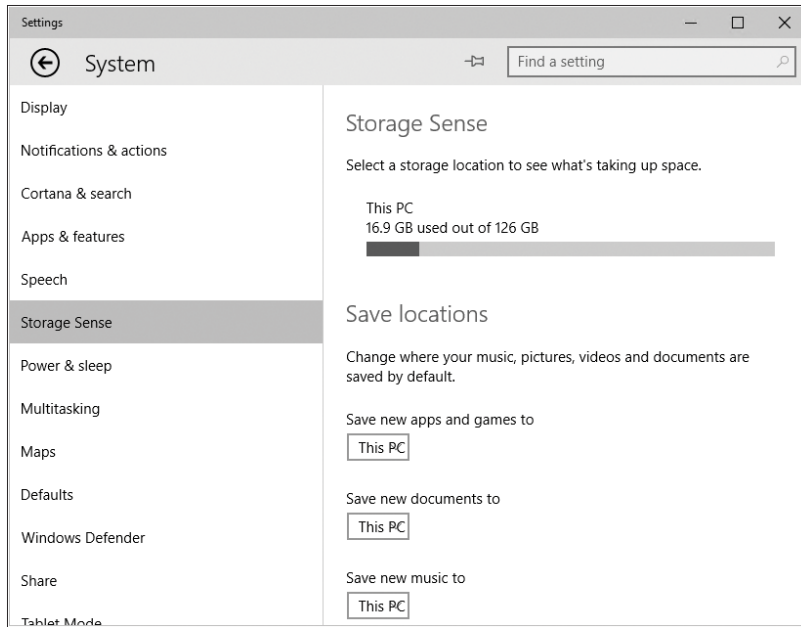


FIGURE 5-3 The adaptive user experience in Windows 10 allows a universal app to show you more information when screen real estate is available.

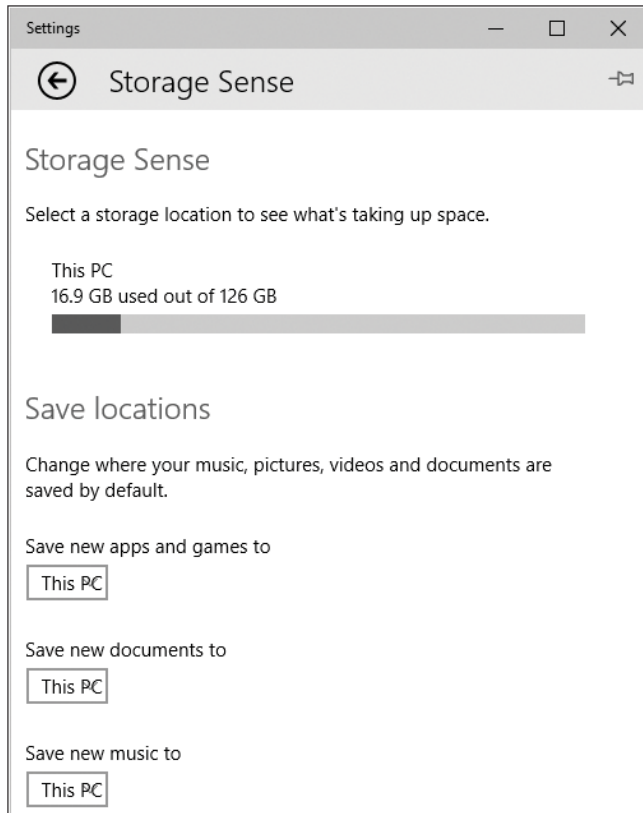


FIGURE 5-4 By contrast, a universal app on a small screen adapts to the minimal space by hiding the navigation pane.

All editions of Windows 10 include a selection of Microsoft-authored universal apps that demonstrate these principles while also performing useful functions: the Calculator and Alarms & Clock apps offer excellent examples of this adaptive user experience.

Universal apps share a common group of user controls that also adapt to how the user is interacting with the app—offering larger targets for touch interaction compared to the smaller targets offered when the user taps with a pen or uses a traditional pointing device such as a mouse, for example.

In the interest of power management, a crucial factor on mobile devices, most Windows Store apps are suspended within a few seconds of 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.

Windows 10 universal apps also include support for natural user inputs, such as speech, inking, gestures, and even user gaze.

By default, apps in Windows 10 update automatically, with no user intervention required. 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.

Distributing line-of-business apps

Enterprises running Windows 10 can develop universal line-of-business (LOB) apps and make them available to users inside their organization. These apps can be deployed in either of two ways: through a custom Business Store, managed and deployed by the Windows Store, 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 10. For example, an organization might choose to remove the Sports app or prohibit it from running.

The process of distributing a Windows 10 app through a private Business Store requires that an enterprise have Azure Active Directory accounts for each user in the organization. These accounts are used instead of Microsoft accounts. Installation files are managed and deployed by the Windows Store, which also tracks license usage. Updates are delivered via normal update channels—Windows Update or Windows Server Update Services (WSUS).

LOB apps distributed within an organization without using the Windows Store don't need to be signed by Microsoft, nor do they require Azure Active Directory accounts. They do, however, need to be signed with a certificate that is trusted by one of the trusted root authorities on the system.

In this scenario, installation files are downloaded and deployed using the organization's own infrastructure. Apps can be installed as part of a custom installation image or sideloaded using System Center Configuration Manager or mobile-device-management software.

I'll have a much more detailed discussion of these options in the final edition of this book.

Web browsing and Windows 10

Over the past two decades, the web has played an increasingly important role in our everyday lives. These days, apps connected directly to cloud-based services are able to bypass the web for some tasks, but it's still impossible to imagine a world in which we don't use a web browser many times a day, every day, to look things up and get things done.

Meanwhile, in the workplace, legacy apps are being replaced with web services hosted in (and managed from) a browser window. And an increasing number of business tasks that once would have been hosted on a local server are now being run from the cloud, managed from, yes, a web browser.

Those realities make web-browsing features crucial to any computing device, regardless of size. Whether you're using a phone, a small tablet, a laptop, or a hulking desktop workstation, you need to be able to click a link with a high degree of confidence that the destination page will work properly.

In Windows 10, Microsoft includes two distinct web browsers, one so new (as I write this) that it's still going by its code name, "Project Spartan." The other, destined to live on in business settings for years to come, is good old Internet Explorer, with the addition of an Enterprise Mode for resolving compatibility headaches.

In this chapter, I look at the reasons behind the two-browser solution as well as details about what you can accomplish with each one.

A brief history of Internet Explorer

At the turn of the 21st century, Internet Explorer ruled the web. Then, for a few years too many, Microsoft put Internet Explorer development on autopilot. That left a giant competitive opening, and over the past dozen years, alternative web browsers and development tools, some of them quite good, emerged. For many developers, especially those working on non-Windows platforms, Internet Explorer became a pesky item on a compatibility checklist rather than a serious development target.

Microsoft has been positively sprinting in recent years to catch up to the competition in terms of performance and standards compliance and to win back developers. Internet Explorer 11, which is available for Windows 7, Windows 8.1, and the Windows 10 Technical Preview, is an excellent competitor, fast, and generally compliant with web standards.

The trouble is, most enterprise deployments of Windows aren't taking advantage of the speed and standards compliance of the latest Internet Explorer release but are instead stuck on an old version, one

that's slow and increasingly unable to keep up with the modern web. The reason is most often compatibility with legacy web apps that typically require Internet Explorer 8 to work properly.

The problem is exacerbated by the fast-paced development cycles of competing browsers, including Google Chrome and Mozilla Firefox, which push out automatic updates for their Windows browser far more frequently than Internet Explorer does.

In general, that fast update cycle means anyone using Chrome or Firefox has quicker access to features based on the latest web standards. Meanwhile, Microsoft's overly generous support life cycle has allowed older versions of Internet Explorer to remain in use years longer than is sensible on the fast-changing modern web.

As of January 12, 2016, that all comes to an end. On that date, Microsoft is changing its support life cycle for Internet Explorer. Under the new policy, only the most recent version of Internet Explorer available for a supported operating system will receive technical support and security updates.

For the first time, only one version of Internet Explorer, Internet Explorer 11, will be officially supported on PCs running Windows 7, Windows 8.1, and Windows 10. A feature called *Enterprise Mode for Internet Explorer 11*, which I discuss later in this chapter, is designed to address compatibility issues in the enterprise.

But Internet Explorer won't be the default Windows web browser for new PCs running Windows 10. That honor goes to the new, yet-to-be-named browser currently identified by its code name, "Project Spartan." Enterprises may still choose to make Internet Explorer their default browser across all supported Windows versions, but otherwise Internet Explorer will be relegated to a compatibility.

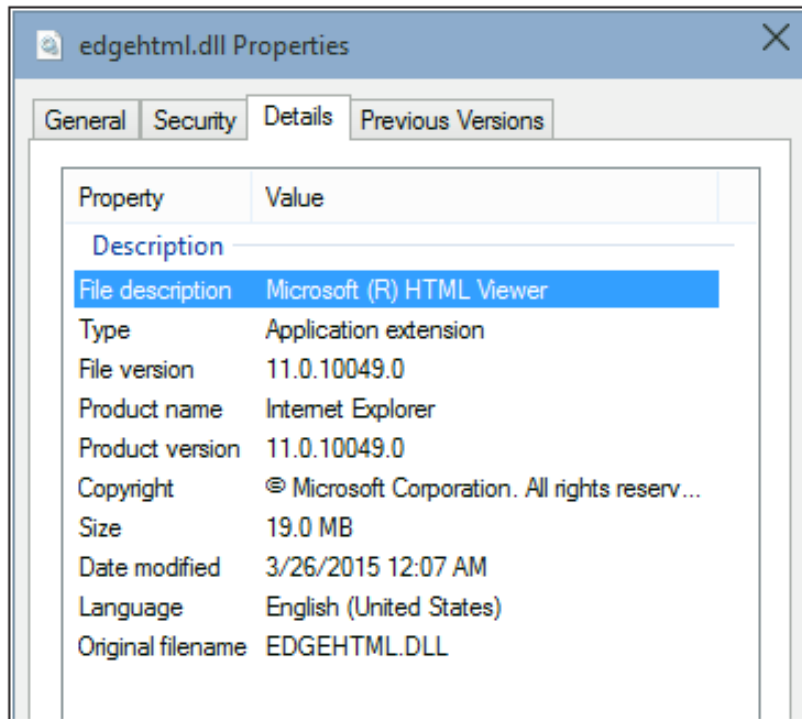
In the next section, I explain the similarities and differences between the two Windows 10 browsers.

Browsing options in Windows 10

The two-browser strategy for Windows 10 isn't a new idea. Windows 8 and Windows 8.1 also included two browsers, one with the conventional Windows desktop interface and the other with a modern, touch-friendly design intended for full-screen use on tablets. Despite the different designs, the two browsers shared a great deal of common code, most notably the Trident rendering engine, which has been at the core of Internet Explorer since its earliest days.

Windows 10 also includes two browsers, each with a different design and different methods of user interaction. More importantly, though, Windows 10 includes two different rendering engines:

- **EdgeHTML (EdgeHTML.dll)** is the new HTML viewer. Although its starting point was the original Trident engine, it has since diverged significantly. The new engine deliberately eliminates large chunks of legacy code designed to emulate older Internet Explorer versions, including the versioned document modes that determine how previous versions of Internet Explorer render a page. Although compatibility with standards is an important goal of EdgeHTML, interoperability is even more important: Microsoft says its developers have invested significant effort in EdgeHTML to help developers avoid having to deal with cross-browser inconsistencies.



- **Trident (MSHTML.dll)**, the rendering engine that has been part of Internet Explorer for nearly two decades, will continue to be available as a stable, consistent web platform for use in Internet Explorer 11. Trident will continue to receive security and compatibility updates for all supported Windows platforms, including Windows 10, with new features and support for additional web standards being added exclusively in the new rendering engine.

NOTE For a detailed list of the status of web-standards support in both rendering engines, see <https://status.modern.ie>. Standards that are implemented only in EdgeHTML (Touch Events, for example) are currently identified as Preview Release. With a few exceptions, those standards that are listed as Under Consideration or In Development will be available only in EdgeHTML.

Project Spartan is a relatively recent addition to the Windows 10 Technical Preview, showing up in publicly available preview builds some five months after the program began. For those builds, Microsoft allowed preview program participants to enable the EdgeHTML engine in Internet Explorer 11 by typing **About:flags** in the address box and then enabling experimental features, as shown in Figure 6-1.

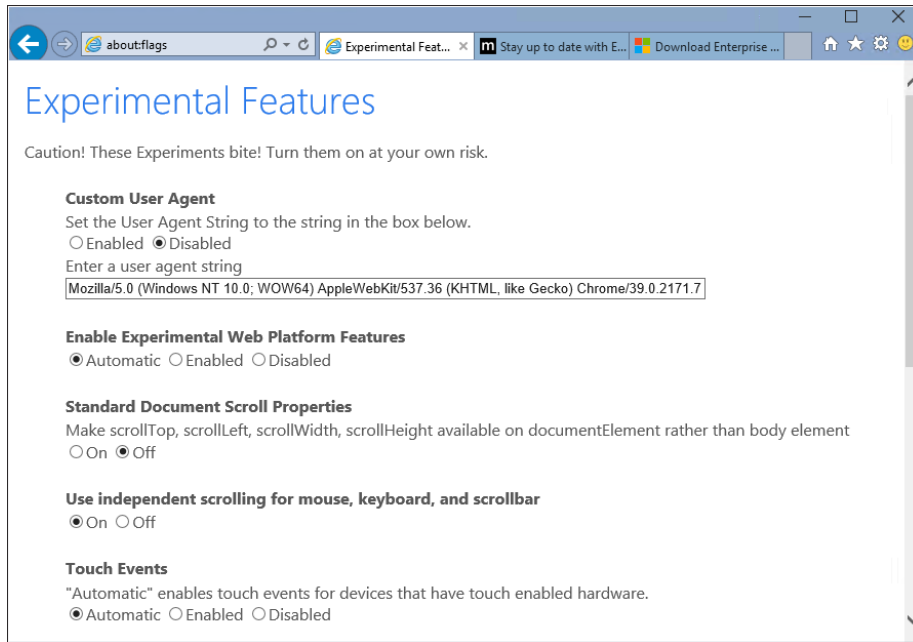


FIGURE 6-1 Entering **about:flags** in the Internet Explorer address bar unlocks these advanced settings.

The Experimental Features page also contains an option to experiment with user-agent strings, a primary troubleshooting tool for determining whether a webpage is rendering incorrectly because it's coded to sniff for a particular browser version rather than test for the existence of specific features. The **About:flags** page is likely to change as Windows 10 nears its official release, but some experimental features may still continue to be available.

A lot can and will change between the preview and final releases, so the next section, which describes Project Spartan, is of necessity brief.

Project Spartan

As I write this section, in early April 2015, the Project Spartan browser has been available for only a few days. It is very much an early look at a work in progress, as the 0.10 version number shown in Figure 6-2 suggests. That screenshot also shows the deliberately minimalist nature of the Project Spartan interface.

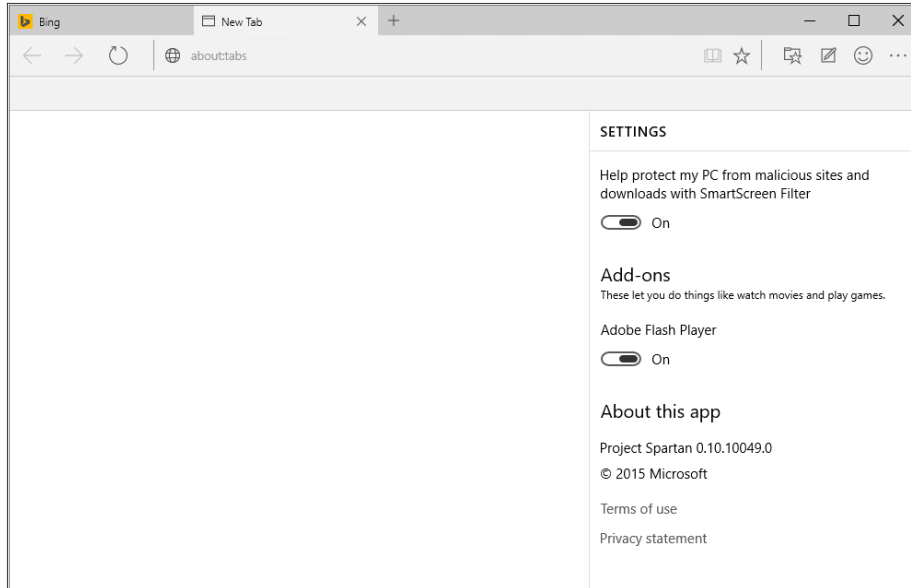


FIGURE 6-2 The minimalist design of the Project Spartan browser includes this Settings pane.

In this preview release, the only available add-on is Adobe Flash Player, which is built into the browser in the same way that it's included with Internet Explorer 11. There is also a native PDF viewer. Microsoft will allow third-party developers to write add-ons for Project Spartan using Javascript, a strategy that is consistent with the approach used by competing browsers.

The Project Spartan browser includes a handful of signature features that can be evaluated in preview releases. One is Reading View, an option that should be familiar to anyone who has used the modern version of Internet Explorer in Windows 8 or Windows 8.1. Clicking the Reading Mode button in the address bar strips away ads and extraneous elements and reformats the text and graphics of an article to make it easier to read. This view is especially useful on smaller screens, such as smartphones and tablets running Windows 10.

Figure 6-3 shows the same page in side-by-side views. The original layout is on the left; the Reading View version is on the right.

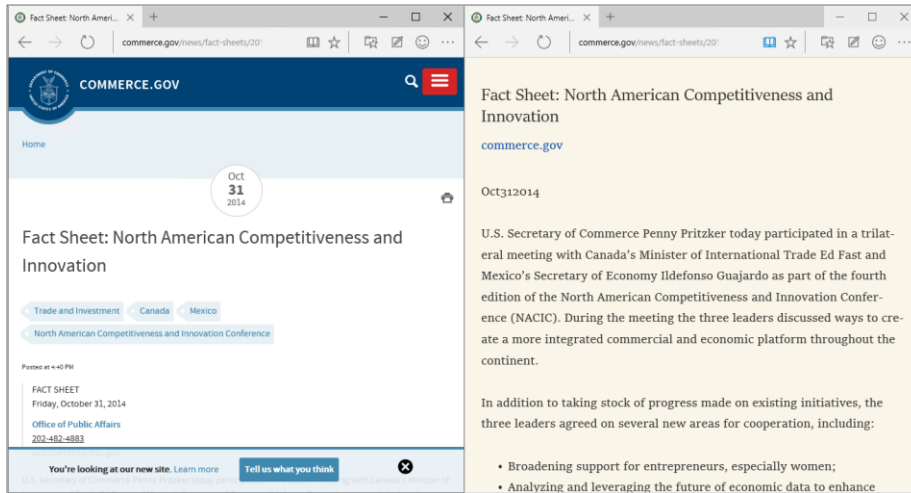


FIGURE 6-3 Enabling Reading View strips away extraneous elements from the original page (left) and reformats text for easier reading (right).

Another signature aspect of Project Spartan is its Web Note feature, which you use to annotate a web page and then save your notes for later reference or to share with a friend or colleague.

The note-taking tools are on a toolbar that's hidden until you activate it by clicking or tapping the Make A Web Note button on the Project Spartan toolbar. Figure 6-4 shows this toolbar in action.

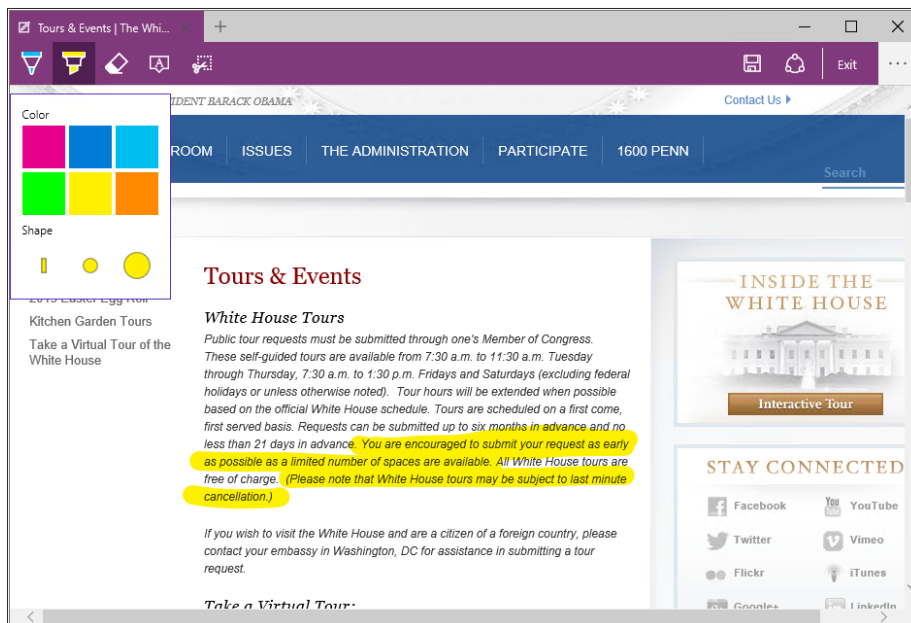


FIGURE 6-4 This is an early version of the Web Note feature in the Project Spartan browser.

As with most modern browsers, with Project Spartan you can save the current page as a Favorite, view your browsing history, and see a list of current and past downloads. One addition to this standard selection is a feature called Reading List. Clicking the star at the end of the address bar displays a dialog box in which you can choose whether to save the current page as a Favorite or add it to the Reading List.

By design, items on the Reading List are intended to be temporary, for pages you don't have time to read now and want to save for later. That's in contrast to Favorites, which are (at least in theory) intended for sites you visit regularly.

Saved items on the Reading List appear in a pane, with thumbnails, as shown in Figure 6-5.

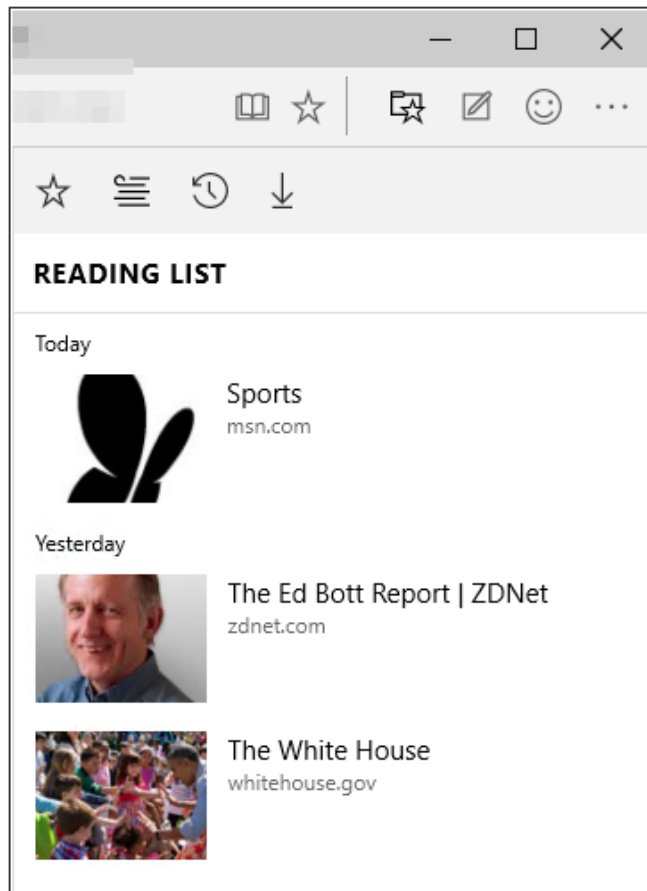


FIGURE 6-5 The Reading List is an alternative to Favorites, sorted by date saved.

NOTE Windows 8.1 includes a Reading List app that performs a similar function, using the Share charm with the modern version of Internet Explorer to save links for later review. That app still exists in the Windows 10 Technical Preview, but its contents are not linked to the identically named feature in Project Spartan.

The Project Spartan browser includes direct hooks to Cortana. When you browse to a page that Cortana recognizes, you're given the option to get additional information. Visit the home page for a popular restaurant, for example, and Cortana will offer hours, directions, reviews, and other information. If you choose to view the extra information, it appears in a pane at the right side of the page, as in Figure 6-6.

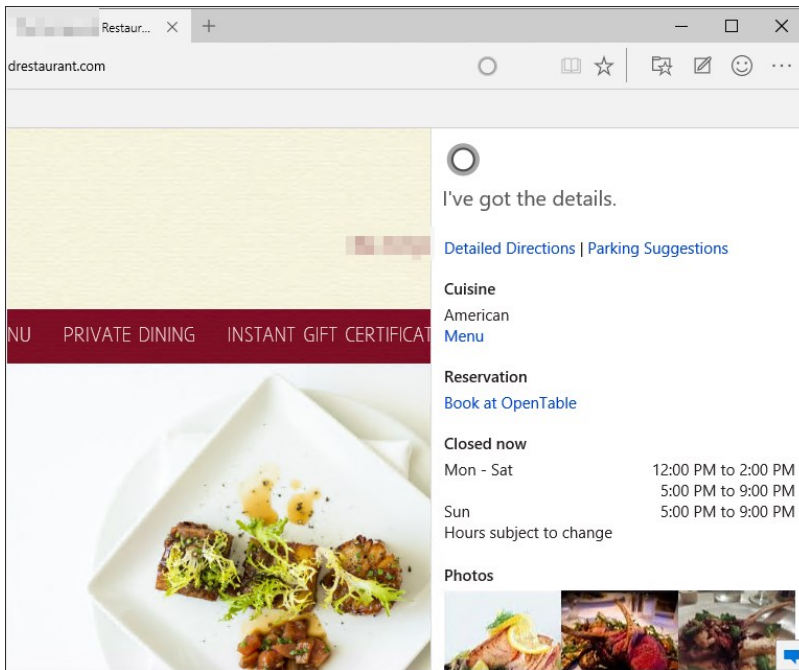


FIGURE 6-6 Cortana is integrated into the Spartan browser and offers additional information for some webpages.

Cortana is also available if you select a word or phrase, then right-click and choose "Ask Cortana," or if you begin to navigate to a web page for an interest you've chosen to track. For example, if you've chosen to track a flight tomorrow and you begin to type in the address of your airline, Cortana will immediately tell you if your flight is on time—without having to visit the website, navigate to the flight status page, and enter the flight information manually.

Unlike Internet Explorer, Spartan will receive smaller, iterative updates on a regular basis—similar to other browsers, and in keeping with the promise of Windows as a service—so it's likely that it will become more feature-rich over time.

Configuring Enterprise Mode in Windows 10

In Windows 10, Internet Explorer 11 behaves the same as Internet Explorer 11 on Windows 7 or Windows 8.1, using the Trident engine. This should help ease some Windows 10 migrations and reduce or eliminate compatibility issues for customers who have already upgraded to Internet Explorer 11. In enterprise deployments, Microsoft recommends Internet Explorer 11 as a stable, reliable web platform for complex LOB apps designed to run in a web browser.

By comparison, Project Spartan renders all webpages using the new EdgeHTML engine, using a modern standards mode. You can switch to Internet Explorer 11 for sites that are on your intranet as well as those included on a managed list of sites or on a Microsoft-managed Compatibility View list of public websites. Spartan can also identify sites with legacy technology, such as ActiveX controls, and offer to manually switch to Internet Explorer 11 for backward compatibility.

For external and internal sites that require a different document mode to render properly, particularly sites designed for older versions of Internet Explorer, you can enable Enterprise Mode and then create a list of sites with custom settings for each one. Once configured, there's nothing that end users need to know or do; Internet Explorer will switch modes as needed to render the site or web app in the correct mode.

Enterprise Mode is available for all editions of Internet Explorer 11 but is turned off by default. You won't be able to use Enterprise Mode unless it is turned on by enabling a Group Policy Object or setting a registry key.

Enterprise Mode works by checking addresses against a list of websites. When a site matches an address on this list, Internet Explorer 11 will use the specified mode. On Windows 10, Project Spartan will switch to Internet Explorer 11 automatically for sites on the Enterprise Mode Site List.

To enable Enterprise Mode, you need to change a Group Policy setting. This can be accomplished using domain settings or, for a single Windows 10 device, you can use the Local Group Policy Editor (Gpedit.msc). Navigate to Computer Configuration, Administrative Templates, Windows Components, Internet Explorer, and then enable the Use The Enterprise Mode IE Website List policy, as shown in Figure 6-7.

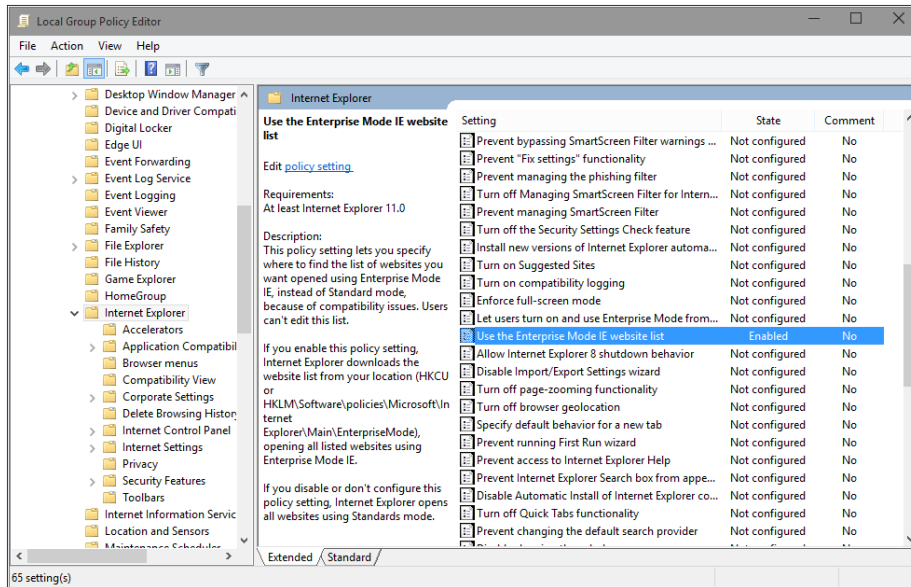


FIGURE 6-7 Turning on Enterprise Mode requires changing this Group Policy setting.

You can also enable Enterprise Mode using the Registry Editor (Regedit.exe). To enable Enterprise Mode for the currently signed-in user account only, edit the *SiteList* value (type **REG_SZ**) in HKCU\Software\Policies\Microsoft\Internet Explorer\Main\EnterpriseMode. (You may have to create that key and its associated value if they don't already exist.)

To turn on Enterprise Mode for all users on the PC, edit the *SiteList* value (type **REG_SZ**) in HKLM\Software\Policies\Microsoft\Internet Explorer\Main\EnterpriseMode.

Simply enabling this setting isn't enough. You also have to specify where the Enterprise Mode site list is stored. To enter the location of your Enterprise Mode site list in Local Group Policy Editor or in Regedit, use the appropriate syntax (substituting the correct server, user, and page names, as needed):

- **HTTP location:** http://localhost:8080/sites.xml
- **Local network:** \\network\share\sites.xml
- **Local file:** file:///c:\Users\<user>\Documents\testList.xml

Figure 6-8 shows the syntax for an Enterprise Mode site list stored in a shared folder on my local network.

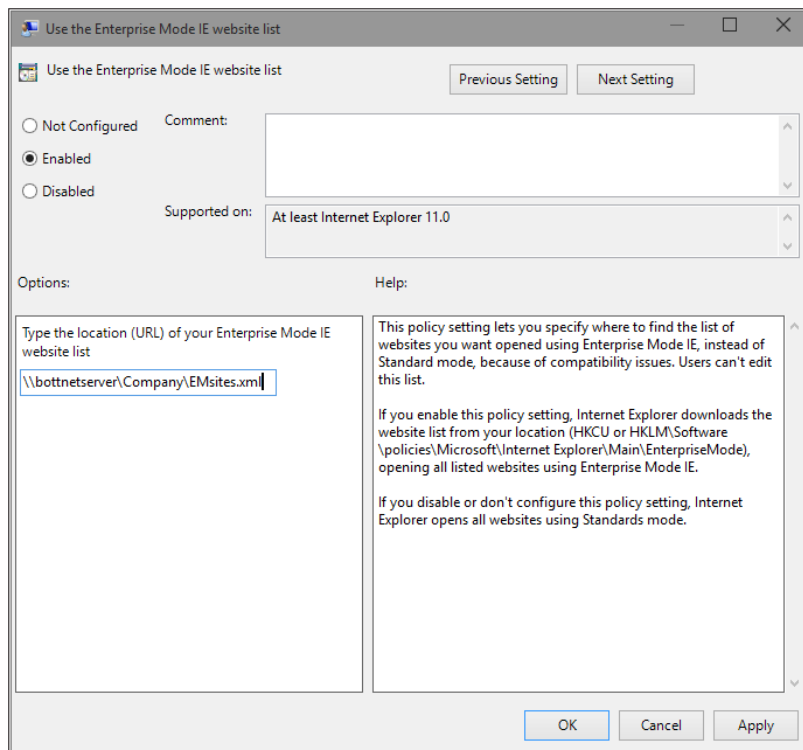


FIGURE 6-8 Enter the file location of the Enterprise Mode site list here or in the appropriate key in Registry Editor.

To add and edit sites on this list, install the Enterprise Mode Site List Manager utility, available from the Microsoft Download Center: <http://www.microsoft.com/en-us/download/details.aspx?id=42501>.

You can use this utility to add sites, singly or in batches, and specify Enterprise Mode (essentially equivalent to the Compatibility View settings from Internet Explorer 8) or enter custom document modes, as shown in Figure 6-9.

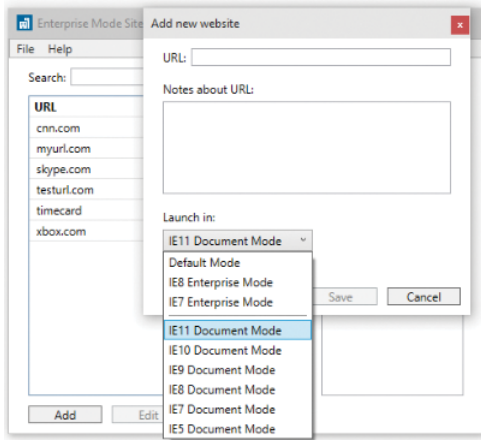


FIGURE 6-9 Use the Enterprise Mode Site List Manager utility to edit the contents of a local or shared list.

For more details on how to use Enterprise Mode, see the TechNet site at <http://technet.microsoft.com/ie>. You can also view the Internet Explorer blog for additional information, such as troubleshooting tips, at <http://blogs.msdn.com/b/ie/archive/2015/03/02/making-it-easier-for-enterprise-customers-to-upgrade-to-internet-explorer-11-and-windows-10.aspx>.

Windows 10 networking

One of the key design goals of modern Microsoft Windows versions is to help people be more productive on mobile devices. So it should come as no surprise that many features described in this chapter are focused on portable devices, including small tablets.

Many features described in this chapter represent extensions of capabilities introduced in Windows 8 and 8.1. Some require complementary capabilities on a remote server. Others are hardware-dependent, and their impact won't be truly visible until devices that include the required hardware are available to "light up" the corresponding Windows 10 features.

Wireless networking enhancements

The single biggest change under the hood in Windows 10 is a new Wireless Driver Interface (WDI) driver model. This feature allows for a universal WLAN driver package that supports native functionality in both desktop and mobile versions of Windows 10.

One benefit of the WDI driver model is that cellular and Wi-Fi connections can be managed using the same networking stack. It also offers greater reliability, with the capability to recover quickly when a device hangs for firmware-related reasons. The new driver model also supports MAC address randomization to increase security and privacy.

There are also enhancements for Bluetooth devices, both classic and low-energy (LE), with improved audio through support for wideband speech and the aptX audio codec. The latter provides audio quality equivalent to a wired connection over Bluetooth. And on devices that require higher security it's possible to use management software to force Simple Secure Pairing (SSP). That option limits the class of Bluetooth devices that can connect to a device (keyboards and mice only, for example) to reduce the attack surface.

Three emerging wireless standards are supported with features that were introduced in Windows 8.1 and are enhanced for Windows 10:

- **Near field communication (NFC)** Windows 8.1 introduced tap-to-pair printing support, which allows laptops and mobile devices that include NFC support to connect to an NFC-enabled enterprise printer with a simple tap. Existing printers can be NFC enabled with NFC tags. Windows 10 Mobile adds the infrastructure that can turn a mobile device into a virtual credit card, supporting Host Card Emulation alongside the existing support of Universal Integrated Circuit Card (UICC) Secure Elements. That combination makes tap-to-pay systems possible on Windows 10 Mobile devices.

- **Wi-Fi Direct** This is a relatively new standard that allows devices to connect to one another over a wireless network in peer-to-peer fashion, without requiring an access point. New API support in Windows 10 means that applications can discover, pair with, and connect to devices automatically, without requiring user intervention. The same technology also can be used on enterprise networks to allow easy and secure connections to printers without requiring additional drivers or software.
- **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. Miracast support is built into all Windows 10 devices, allowing users to pair a Windows 10 tablet or laptop to a conference room projector with Miracast, and then project a presentation without wires or dongles. Microsoft's Wireless Display Adapter, for example, plugs into the HDMI input on a large television or other display and requires no setup.

Many of these connections can be made with a tap of the Media Connect button, at the bottom of the Action Center beneath any waiting notifications. Figure 7-1 shows Windows 10 ready to connect to a Microsoft Wireless Display Adapter, a Bluetooth-enabled audio headset (previously paired with this device), and a Bluetooth-equipped PC.

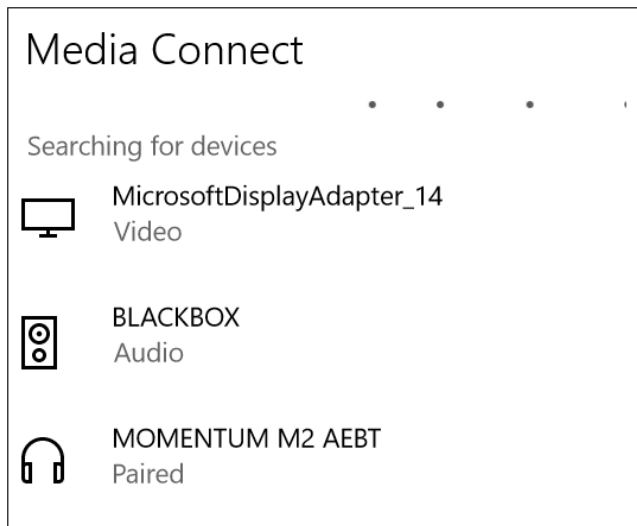


FIGURE 7-1 Tapping the Media Connect action button discovers any available Bluetooth, Wi-Fi Direct, or Miracast devices and gives users the ability to make connections with a single tap.

Connecting to remote 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.

Windows 8 included a basic VPN client. Windows 8.1 added support for a limited selection of VPN providers, including Check Point, F5, Juniper Networks, and SonicWall, in addition to the Microsoft client. Windows 10 expands this capability to any VPN solution provider, with distribution through the Store.

Windows 10 includes improvements in 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, you'll be able to sign in with one click. It also includes the option for an always-on VPN session, essentially treating a remote device as a full-time member of the corporate network.

Per-application VPN support works in the opposite direction as well, with administrators allowed to create a list of apps that can access enterprise resources through the VPN and block others. Figure 7-2 shows this feature in operation.

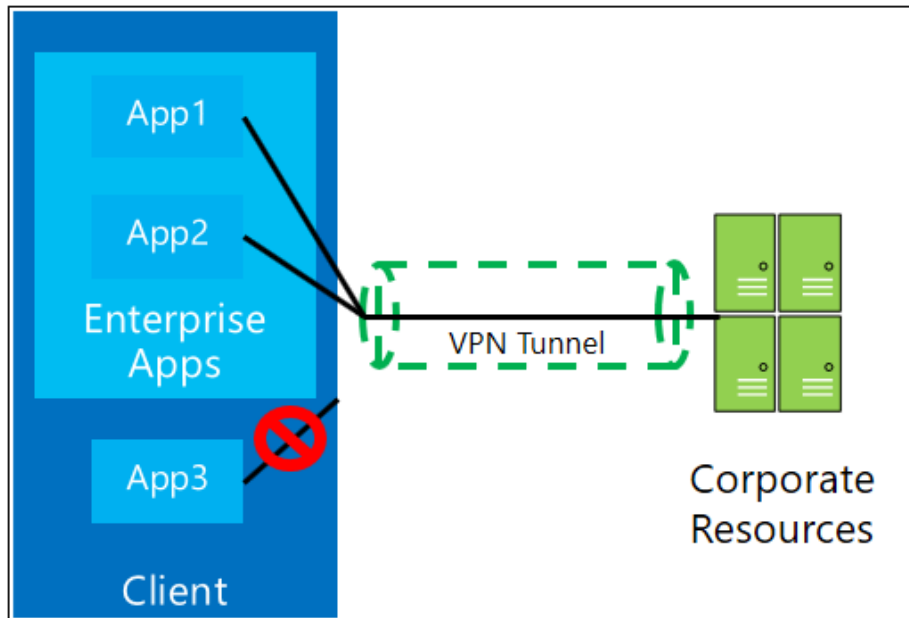


FIGURE 7-2 Administrators can create lists of apps authorized to access corporate servers over a remote network, blocking all other apps.

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. A better solution is DirectAccess, a feature available in Enterprise editions of Windows 10 that requires a connection to Windows Server 2012 or later.

DirectAccess allows remote users to securely access shared resources, websites, and applications whenever their DirectAccess-enabled mobile device is connected to the Internet. DirectAccess does not require frequent logins or access maintenance, and it even gives remote-computer-management capability to administrators without an established VPN connection. This availability of a constant connection minimizes frustration and improves efficiency in everyday “out-of-the-office” needs.

Figure 7-3 shows the simple settings for a properly configured DirectAccess connection.

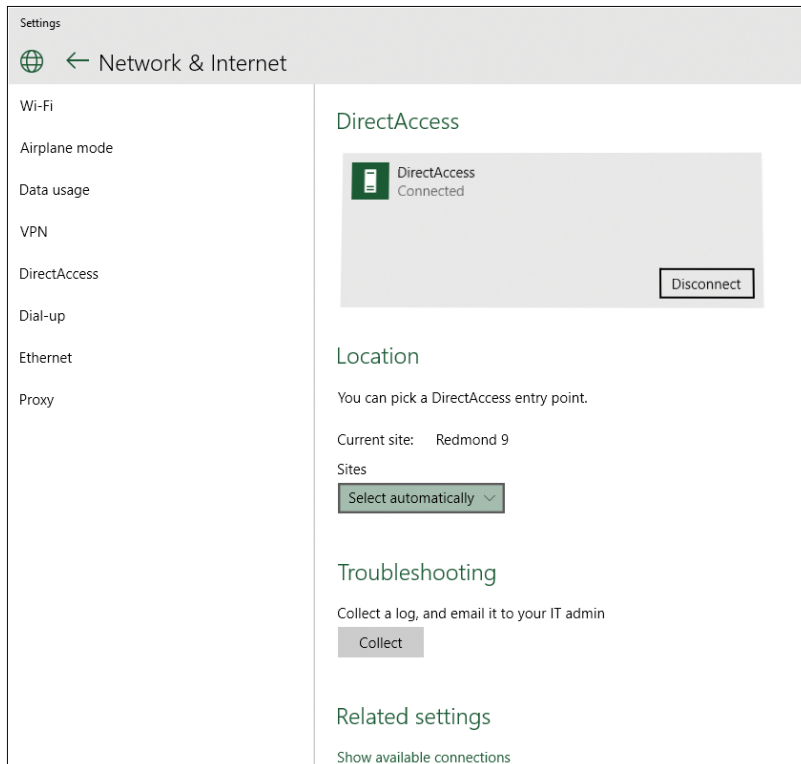


FIGURE 7-3 DirectAccess connections provide the security of a VPN without the hassles of setting up or constantly disconnecting and reconnecting.

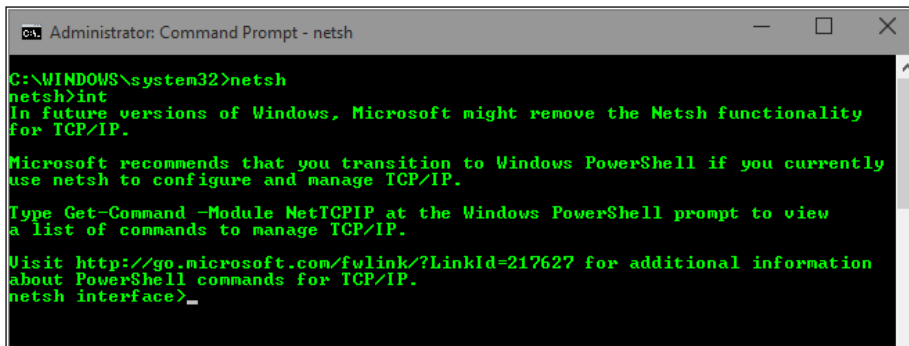
Managing network connections

One of the most frustrating aspects of using a preview release is discovering that an important feature is missing or incomplete.

That’s been the case with anyone trying to adjust network settings in early Windows 10 Technical Preview builds. The user-accessible knobs and levers for tweaking network connections are making the

transition from the old-style Network and Sharing Center to the new Settings app. In some cases, that means familiar tools are temporarily unavailable.

That's as good an excuse as any to brush up on one's Windows PowerShell skills, with a special emphasis on the network management cmdlets. And if you've relied on the Netsh command-line scripting utility in the past, it's time to make the switch to PowerShell. The older Netsh functionality is being deprecated in Windows 10, as Figure 7-4 makes clear:



```
C:\WINDOWS\system32>netsh
netsh>int
In future versions of Windows, Microsoft might remove the Netsh functionality
for TCP/IP.

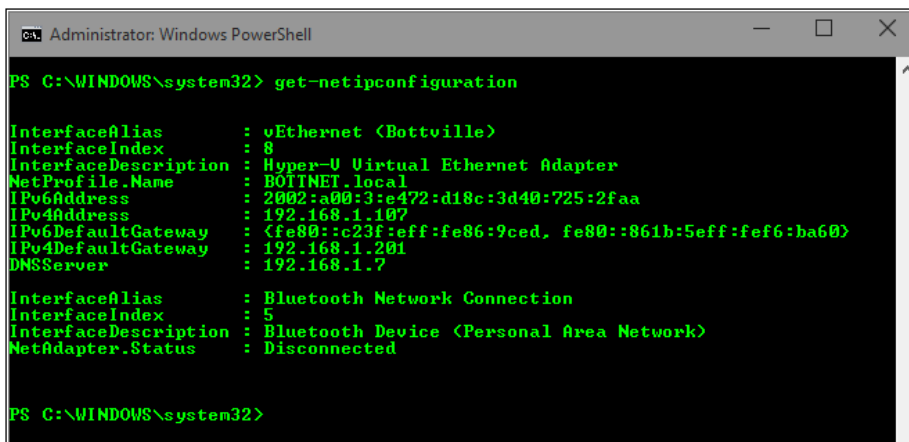
Microsoft recommends that you transition to Windows PowerShell if you currently
use netsh to configure and manage TCP/IP.

Type Get-Command -Module NetTCPIP at the Windows PowerShell prompt to view
a list of commands to manage TCP/IP.

Visit http://go.microsoft.com/fwlink/?LinkId=217627 for additional information
about PowerShell commands for TCP/IP.
netsh interface>
```

FIGURE 7-4 The venerable Netsh command-line utility is still available in Windows 10, but it's being phased out in favor of PowerShell cmdlets.

Fortunately, everything you can do using Netsh can be done with PowerShell, which also does much more. There are dozens of cmdlets in the Net-TCP/IP category alone, including `Get-NetIPConfiguration`, which returns a concise list of details for the current network, such as the one shown in Figure 7-5.



```
PS C:\WINDOWS\system32> get-netipconfiguration

InterfaceAlias      : vEthernet {Bottville}
InterfaceIndex      : 8
InterfaceDescription : Hyper-V Virtual Ethernet Adapter
NetProfile.Name      : BOTNET, local
IPv6Address          : 2002:a00:3:e472:d18c:3d40:725:2faa
IPv4Address          : 192.168.1.107
IPv6DefaultGateway   : <fe80::c23f:eff:fe86:9ced, fe80::861b:5eff:fef6:ba60>
IPv4DefaultGateway   : 192.168.1.201
DNSServer            : 192.168.1.7

InterfaceAlias      : Bluetooth Network Connection
InterfaceIndex      : 5
InterfaceDescription : Bluetooth Device {Personal Area Network}
NetAdapter.Status    : Disconnected

PS C:\WINDOWS\system32>
```

FIGURE 7-5 Simple PowerShell cmdlets provide the ability to view and change network settings in Windows 10.

You can use other cmdlets, including `New-NetIPAddress` and `Set-DnsClientServerAddress`, to change network settings—in this case, the local IP address and DNS server address for a network adapter.

For a full list of network-related PowerShell commands, see <https://technet.microsoft.com/en-us/library/hh826123.aspx>.

Support for IPv6

The transition from IPv4 to IPv6 networks is well under way, but it still has a long way to go. Windows 10 fully supports IPv4 networking, of course, but the supply of available IPv4 addresses has officially dried up. The use of network address translation (NAT) allows homes and small businesses to share a single IPv4 address, but the widespread use of NATs makes location-based services less effective and degrades many applications that rely on direct communication. As the Internet of Things takes hold and every device within range has its own direct connection to multiple networks, the problems only become more acute.

To remedy these issues, IPv6 was created with unimaginable scale, offering 3×10^{38} available IP addresses (enough for every living human to have billions of personal, unique IPv6 addresses). 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.

Modern versions of Windows (beginning with Windows 8) automatically give an IPv6 address priority over an IPv4 address. Because some applications do not support IPv6, Windows will automatically select the correct connection for applications, using a method called *address sorting*.

Windows Server 2012 R2 expands support for IPv6 in Group Policy and allows these new settings to be used with devices running Windows 8.1 or later. 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>.

Virtualization and remote access

In its most common configurations, Microsoft Windows 10 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 10 Pro and Enterprise include the capability to create virtual machines (VMs) 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 10.

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 desktop version of Windows to include a built-in hypervisor, which allows developers and IT pros to create virtual machines (VMs) 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 the latest version of Windows.

Client Hyper-V uses the same technology and virtual-machine formats as in current versions of Windows Server, 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 10 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, you can use the Virtual Machine Manager in System Center 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>.

The Hyper-V management tools in Windows 10 should look very familiar if you’ve used this feature in Windows 8.1 or Windows Server 2012 R2. Windows 10 adds some important features that IT pros will appreciate:

- **Production checkpoints** This option, which is enabled by default in new VMs created with the Windows 10 Technical Preview, allows the creation of checkpoints that use the Volume Snapshot Service to create “point in time” backups that can easily be restored. This feature is especially useful for testing scenarios and is more robust than the older checkpoint technology, which simply saved the state of a VM. Figure 8-1 shows this feature in the configuration settings for a VM.

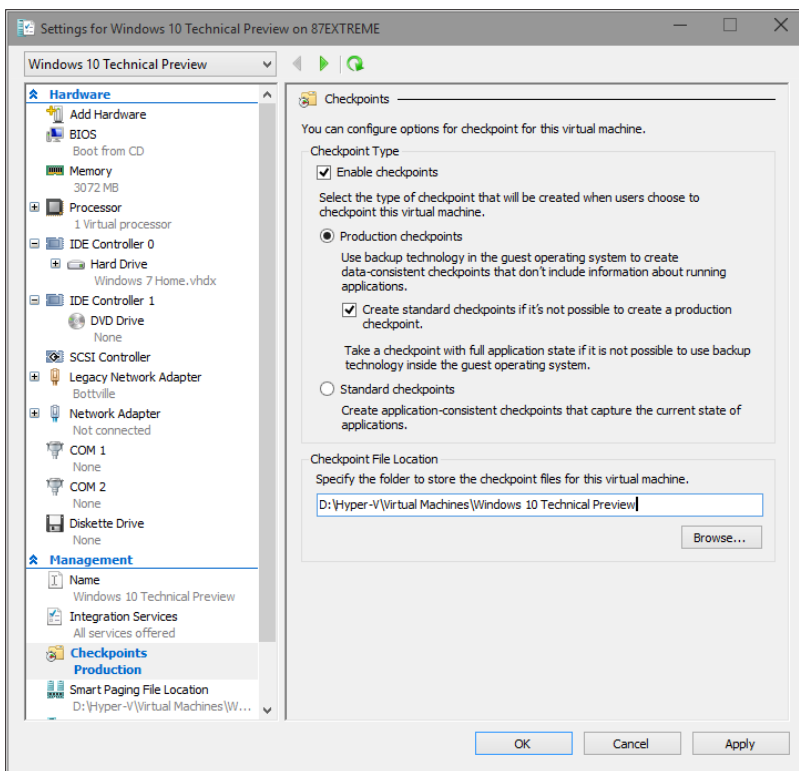


FIGURE 8-1 Production checkpoints, which create a full backup using Volume Snapshot technology, are new in Windows 10.

- **New configuration file format** VMs created in the Windows 10 Technical Preview use configuration version 6.2 and save configuration information in a new binary file format that is more robust than the older XML-based format. The new configuration files use the .VMCX extension for virtual machine configuration data and the .VMRS extension for runtime state data.
- **Hot add memory and network adapter** You can adjust the amount of memory assigned to a VM while it is running, even if Dynamic Memory isn't enabled. This option works for both generation 1 and generation 2 VMs. On VMs created using the Generation 2 option, you can also add or remove a network adapter while the virtual machine is running.
- **Connected Standby compatibility** When the Hyper-V role is enabled on a computer that uses the Always On/Always Connected (AOAC) power model (such as a Microsoft Surface Pro 3), the Connected Standby power state is available and works as expected. This configuration causes power-management problems on Windows 8.1.
- **Hyper-V Manager improvements** The Hyper-V management console in the Windows 10 Technical Preview supports more remote-management scenarios (including management of Hyper-V running on earlier versions of Windows desktop and server releases). It also allows the use of alternate credentials for managing Hyper-V on a remote computer or server.

Client Hyper-V is not enabled in a default installation of the Windows 10 Technical Preview. 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 8-2. Click OK, and then restart the PC to enable the features.

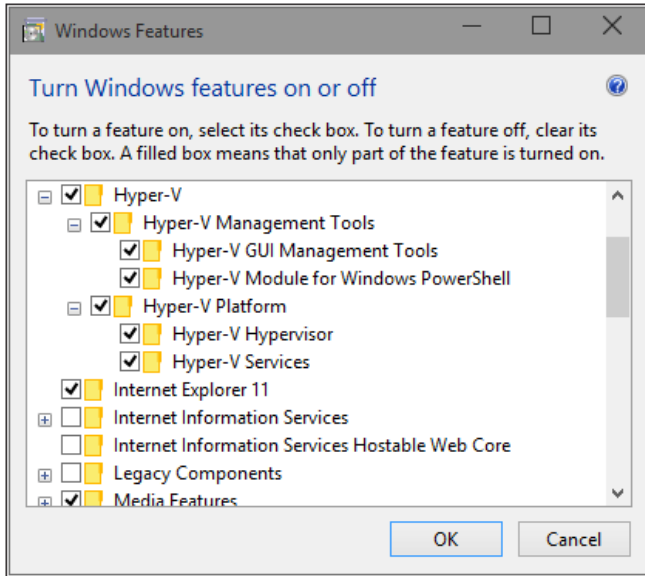


FIGURE 8-2 The Client Hyper-V features must be enabled using this dialog box.

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 VMs through a wizard in the Hyper-V Manager or using the Hyper-V Module for Windows PowerShell. Figure 8-3 shows the wizard for creating a new VM interactively.

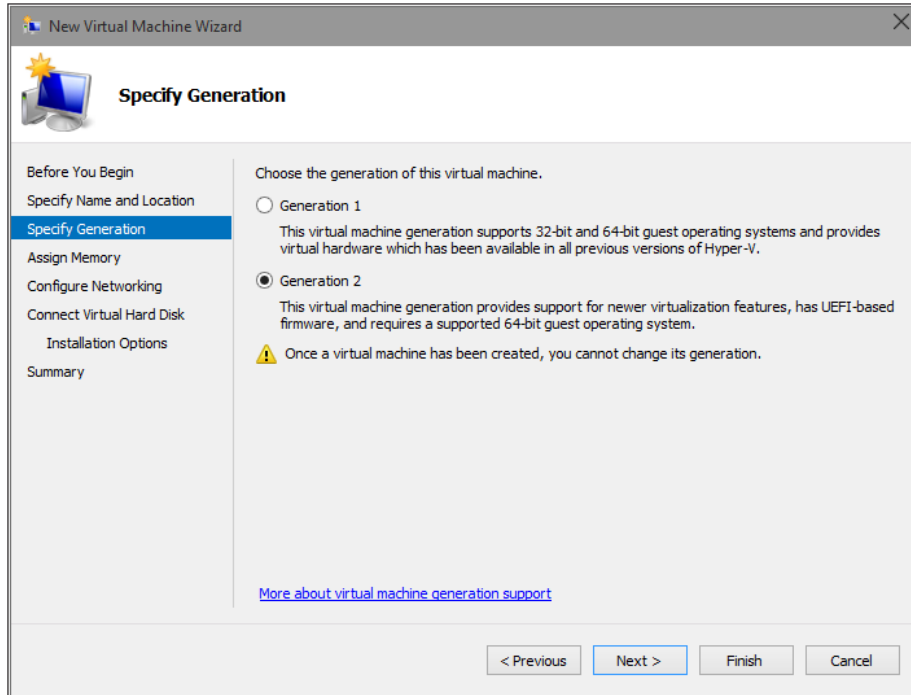


FIGURE 8-3 Client Hyper-V in Windows 10 supports Generation 2 virtual machines, which are based on UEFI and require a 64-bit operating system.

You can use the Virtual Machine Connection program to work with VMs or access them in an enhanced session, using a variant of Remote Desktop technology. 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 audio and connections to some types of USB devices 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 they can ensure that security and compliance policies are properly enforced.

Microsoft has not yet announced plans for an MDOP upgrade for Windows 10, but it's reasonable to assume that option is on the roadmap. Assuming a new MDOP is available, the final version of Windows 10 (perhaps with an additional update) should deliver comparable desktop virtualization options.

The engine that powers virtual desktops is Remote Desktop Services (RDS) in Windows Server 2012 and Windows Server 2012 R2 (and, presumably, in the next version of Windows Server, which is built on the same code base as Windows 10 and is also in a technical preview now). 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 8-1:

- **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 8-1 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 (and presumably due for improvement in the next release of Windows Server, in 2016).

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.

Figure 8-4 provides a high-level picture of how this type of virtualization works in an enterprise.

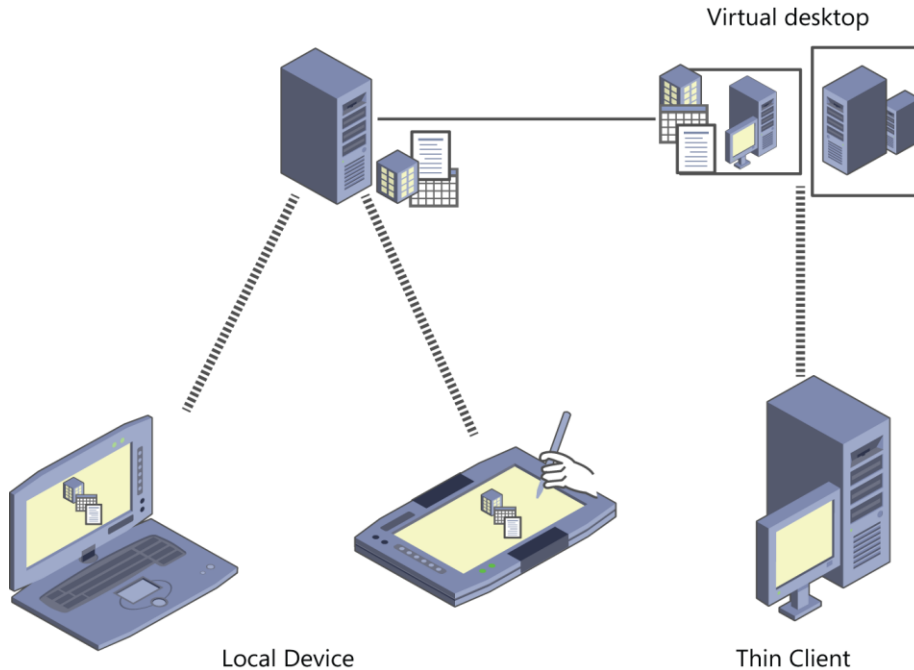


FIGURE 8-4 Virtualized applications can be delivered to local devices using App-V or deployed as part of a virtual desktop using RemoteApp, without requiring local installations.

An App-V administrator uses a sequencer app 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.

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 SP3 is the current release included as part of MDOP. It comes in desktop and RDS versions and offers usability and performance improvements as well as 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.

The most recent release, UE-V 2.1, adds support for Windows Store apps, including apps purchased through the Store and line-of-business (LOB) apps deployed internally. By default, it synchronizes many Windows settings (desktop backgrounds, for example); Microsoft Office 2010 and Microsoft Office 2013 applications; Internet Explorer 11; all preinstalled Windows apps; and a number of Windows desktop applications.

A Company Settings Center 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.

MORE INFO You can learn more about UE-V at <https://technet.microsoft.com/en-us/library/dn458926.aspx>.

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. Users have full-time access to their documents, pictures, videos, and other files from any PC.

A new feature called Work Folders, introduced in Windows 8.1, offers significant improvements over Folder Redirection and Offline Files. (Most notable is the ability to sync files on devices that aren't domain-joined.)

Backup and recovery options in Windows 10

Historically, IT pros have relied on “wipe and load” as the solution for most issues with a Microsoft Windows device. Microsoft and third-party software developers have supplied a bumper crop of tools to make the process of creating enterprise images easy. Restore that image, and the user is on her way.

That strategy works fine with devices that an organization owns, especially when those devices are dedicated to straightforward roles and connected to the corporate network. If a desktop PC is having issues that don’t respond to quick troubleshooting, you can use your deployment environment to restore a standard image and then restore the user’s environment from the network.

But modern businesses increasingly have a mix of managed and unmanaged devices, in the hands of an increasingly mobile workforce. Bringing a company-owned, managed device in to IT staff is not an option for a traveling employee, and unmanaged devices pose an additional set of problems in organizations that encourage workers to bring their own devices. For those situations, Windows 10 includes a set of recovery tools that a user (perhaps with assistance from the help desk) can use to perform common repair operations, up to and including a complete refresh of the default operating system.

Windows 10 introduces major changes in the way the so-called “push-button reset” process works, eliminating the annoying problem of restoring an image that requires hours of updating before it’s useful and dramatically reducing the amount of space required as part of a standard install.

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 Windows 10 won’t start properly when you power on a PC or mobile device? 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 and repairing startup problems.

You can start Windows RE from Windows 10 installation media, from a recovery drive, or from the recovery partition on a device, if that option is available. The initial Choose An Option menu allows the user to click Continue to attempt to start 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 users to choose an alternative operating system to boot into. The Use A Device option allows a user to boot from a USB flash drive, DVD drive, or network boot server.

Clicking Troubleshoot opens the Troubleshoot screen, which displays options similar to those shown in Figure 9-1.

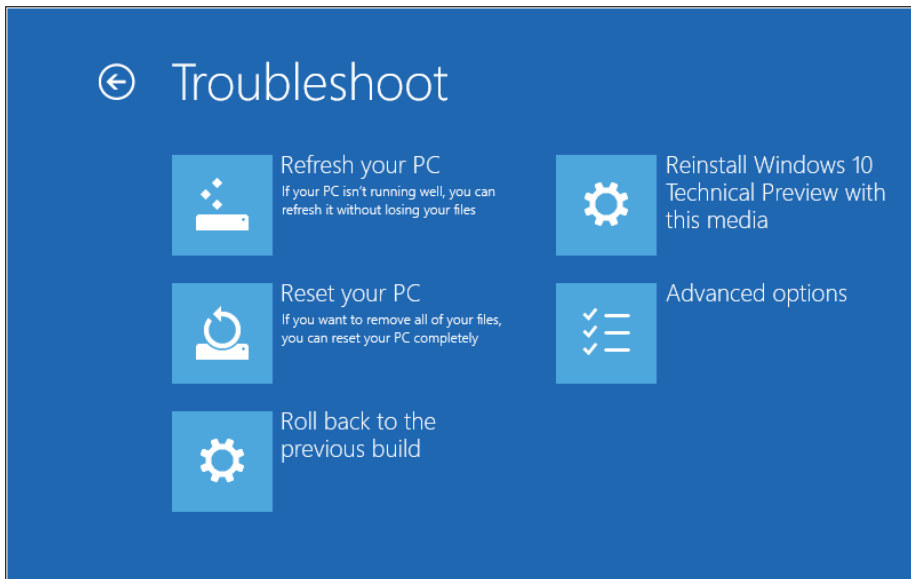


FIGURE 9-1 When you start a Windows 10 device from recovery media, choose Troubleshoot to display these Windows Recovery Environment options.

You can use the first two Windows RE options to restore Windows 10 using the push-button reset feature. These options also are available from the Update & Recovery page in Settings, for use with systems that are able to start up properly. The Refresh and Reset options are covered fully later in this chapter.

The Reinstall option is new in Windows 10, as is Roll Back To The Previous Build. The latter option is available only if the current installation is an upgrade that saved the previous build's files in the Windows.old folder.

If you click Advanced Options, you'll see a menu that resembles the one shown in Figure 9-2.

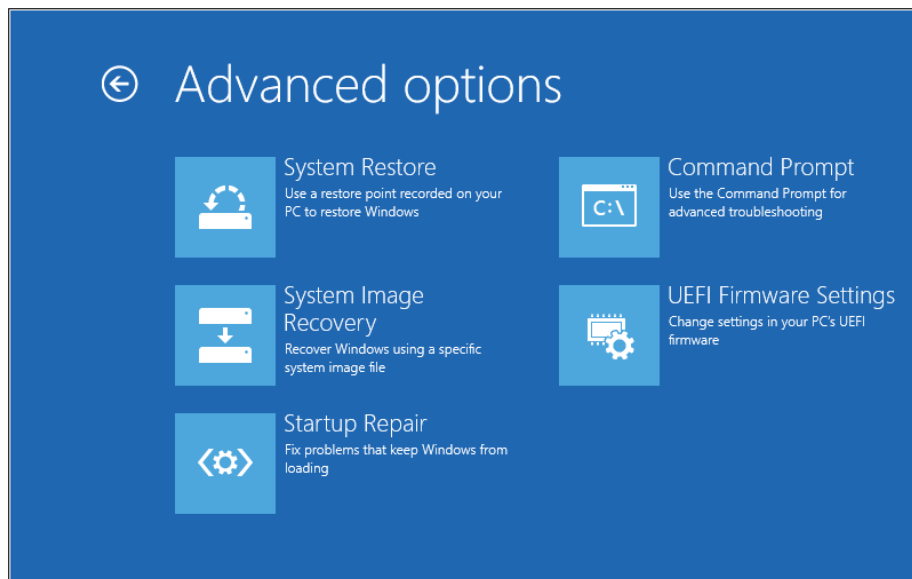


FIGURE 9-2 This Windows RE menu provides access to essential troubleshooting and recovery tools.

Table 9-1 lists the functions available from the Advanced Options menu, many of which are direct descendants of recovery tools found in previous Windows editions.

TABLE 9-1 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 Backup utility from Windows 7 or later. (In the April update to Windows 10 Technical Preview, 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.
UEFI Firmware Settings	Allows you to change startup settings such as boot device order and Secure Boot. On an older PC with a legacy BIOS, this option leads to the Startup Settings menu instead.

MORE INFO If you're unable to reach the UEFI Firmware Settings option via Windows RE 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.

You can click Startup Repair 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 UEFI Firmware Settings menu restarts the system and allows you to change startup settings stored in the device's firmware.

Note that you can customize the Windows Recovery Environment as part of a standard image. I'll provide more details on how to accomplish that task in the next edition of this book.

Windows 10 and push-button reset options

One revolutionary feature introduced in Windows 8 was a method of allowing end users to restore a clean copy of Windows without the need for separate installation media.

When a computer has repeat problems and standard troubleshooting can't uncover the cause, the traditional approach for most IT pros is to wipe the computer and restore it from a standard build image. The push-button reset options described here can accomplish the same result more quickly and without wiping out potentially valuable data.

On PCs that were originally purchased through retail channels running an original equipment manufacturer (OEM) version of Windows 8 or 8.1, the push-button reset recovery image is normally contained in a dedicated partition at the end of the hard drive. This recovery image can consist of a single image file or a set of split image files, with or without compression. You can recover the space used by that recovery partition on a PC running Windows 8.1, but doing so removes the ability to refresh or reset the operating system.

In Windows 10, this recovery image and its associated partition are no longer required. Instead, Windows 10 accomplishes recovery operations by rebuilding the operating system to a clean state using existing system files.

MORE INFO On an OEM PC that was originally shipped with Windows 8 or Windows 8.1, upgrading to Windows 10 leaves the existing recovery partition untouched. (This option does not apply to PCs with Windows 8.1 installed using the WIMBoot option.) You can use this option to restore the originally installed operating system if necessary. If you determine that the old recovery partition is no longer needed, you can remove it using Windows 10's built-in tools, including the Disk Management console, the DiskPart command-line utility, or Windows PowerShell commands.

This approach has several advantages:

- It significantly reduces the amount of disk space required for a clean installation, allowing that space to be used for data files and apps. The impact of this design is especially profound on tablets and other devices with a small amount of built-in storage (32 GB or less).
- With this design, push-button reset is available on all PCs running Windows 10, not just OEM PCs or those where a corporate IT department has created a custom recovery image.
- The operating system and drivers are restored to the most recent rollup state, with all updates except those installed in the last 28 days. (This design allows recovery to succeed when a freshly installed update is the source of problems.) By contrast, in Windows 8 and Windows 8.1, the recovery image restores the PC to its state as shipped from the factory. On a two-year-old PC, that rollback requires the user to download two full years' worth of updates.

For OEM PCs, any customized settings and desktop programs installed by the manufacturer are restored with the Windows 10 refresh or reset. These customizations are saved in a separate container, which is created as part of the OEM setup process. Note all language packs installed on the system at the time the push-button reset was initiated are restored.

Desktop programs are not restored and must be manually reinstalled. All Windows apps included with Windows 10 by default (Weather, Music, and Outlook Mail and Calendar, for example) are restored, along with any provisioned Windows apps that were added to the system by the OEM or as part of an enterprise deployment.

App updates are downloaded and reinstalled via the Store automatically after recovery. All user-installed Windows apps are discarded and must be reinstalled from the Store.

As I noted earlier, you can initiate a refresh or reset from Windows RE or from the Settings app, as shown in Figure 9-3.

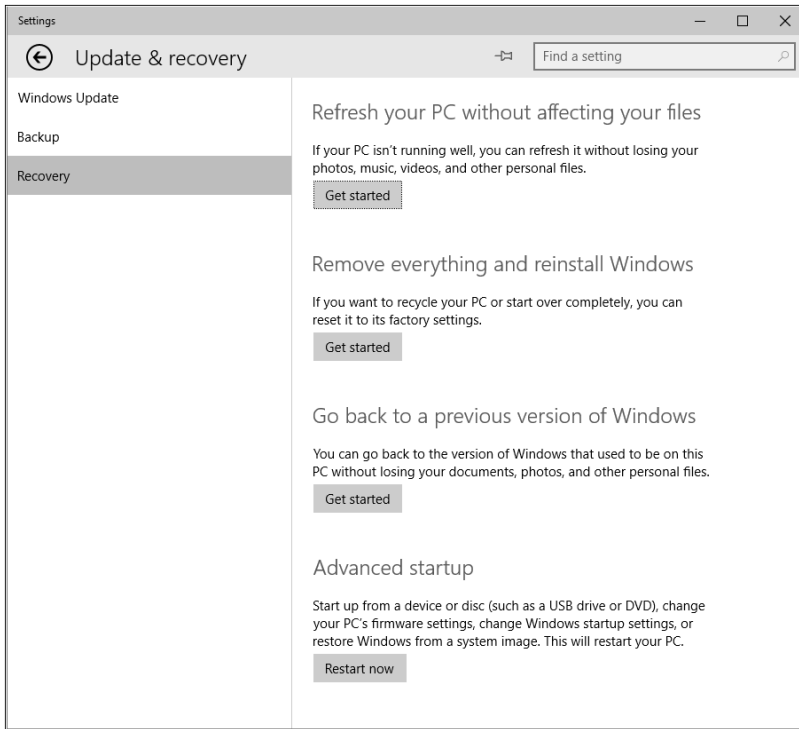


FIGURE 9-3 The two top options shown here are available with any Windows 10 PC.

At the time of this writing, the available documentation for push-button reset features had not been updated for the significant changes in Windows 10. I will add that link and more details in a later edition of this book.

The next two sections describe these two recovery options in more detail.

Refresh Your PC Without Affecting Your Files option

The Refresh Your PC Without Affecting Your Files option changes all 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. All user-installed desktop programs and Windows Store apps 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 uses the next-to-last system rollup to create a new, clean instance of the following folders, including all subfolders:

- \Windows
- \ProgramData
- \Program Files
- \Program Files (x86)
- %UserProfile%\AppData

Any apps and settings created as part of the original OEM image are restored from the customization container for those changes.

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.

In Windows 8.1, the Refresh Your PC option required a significant amount of free disk space to function—Microsoft has not yet published guidance on how much disk space will be required as a result of the changes in Windows 10.

Remove Everything And Reinstall Windows option

This option (called Reset Your PC in Windows 8.1) removes all apps and user data, including user accounts and personalization settings. This option is useful when you plan to sell or give away 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 easily be recovered using disk utilities. As Figure 9-4 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.

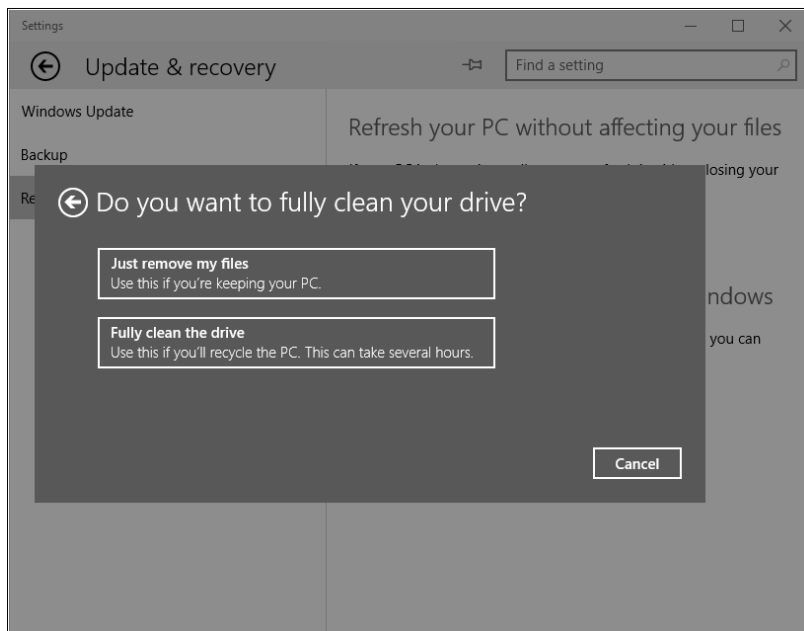


FIGURE 9-4 The Reset Your PC process includes an option to securely wipe the drive so that confidential data files can't be recovered easily.

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.

The reset option doesn't completely eliminate the need for recovery media, which is still required for the following scenarios:

- If operating system files have been heavily corrupted or infected by malware, the reset process will probably not work.
- If there's a serious issue in a rollup update that is more than 28 days old, the reset might not be able to avoid that problem.
- If a user chooses the wrong language during the OOBE phase on a single-language SKU, a complete reinstallation might be required.

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 also can be acquired for evaluation purposes through Microsoft MSDN subscriptions.

Each version of DaRT is designed to work on a specific version of Windows. The version of DaRT designed for devices running Windows 8.1 will not install on the Windows 10 Technical Preview; a new version should appear within a few months after the release of Windows 10.

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 also can 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 image for IT professionals that allows local users to perform a range of recovery tasks. The current version of this DaRT 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.

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.

Windows 10 on phones and small tablets

As an IT pro, your first concern is probably about supporting Microsoft Windows 10 on desktop PCs and laptops. But the unified Windows 10 platform is designed to run on more than just PCs. For phones and small tablets, that means Windows 10 Mobile.

The version of Windows 10 that runs on mobile devices is built on the same core code as Windows 10 for desktop PCs, and it runs the same universal apps, delivered through the same Windows Store, as its desktop counterpart.

The first public release of Windows 10 Technical Preview for phones was in February 2015, with only a handful of phones supported. An updated preview release in April extended coverage to a much larger device population but is still far from complete, especially compared with Windows 10 builds for desktop PCs. In April, Microsoft also released several Microsoft Office apps—Word, Excel, PowerPoint, and OneNote—for use on mobile devices.

Although the roadmap for this version of Windows 10 includes small tablets, that category exists only in theory today. You can install the Windows 10 Technical Preview for phones on devices like the Lumia 1520, which has a 6-inch screen and can easily act like a tablet. (In fact, phones with extra-large screens are sometimes referred to as “phablets” because of their ability to shift roles between phone and tablet.)

This chapter provides a brief overview of what to expect from Windows 10 Mobile, beginning with a quick history lesson.

The evolution of Windows 10 Mobile

In its roughly five years of existence, the Windows Phone platform has undergone several major shifts, with each such change bringing the mobile and desktop operating systems closer together. Windows Phone 8, for example, was the first version to be based on the Windows NT kernel used in the desktop operating system; it was released in October 2012, the same time as Windows 8 for desktop PCs.

Windows Phone 8.1, released in mid-2014, introduced Cortana, the personal digital assistant, as well as the first wave of universal apps capable of sharing data and licensing between desktop and mobile platforms.

Windows 10 Mobile drops the word *Phone* from the name. That’s not just a semantic distinction; instead, it reflects the intent for this operating system to power small tablets, including models based on the same ARM processors used in phones and small tablets that run other operating systems.

NOTE This isn't the first Microsoft operating system capable of running on tablets built with an ARM processor. Windows RT, which powers the Surface RT and Surface 2 as well as several third-party devices, was essentially Windows 8 recompiled for use with ARM processors. Windows RT devices will not be upgradeable to Windows 10, although Microsoft has announced that a future update will bring a few unspecified Windows 10 features to Windows RT devices.

Windows 10 will be a free upgrade for all phones currently capable of running Windows Phone 8.1, although its availability on some devices might be limited by the mobile carrier or hardware manufacturer.

Installing the Windows 10 Technical Preview for phones

There are two requirements to evaluate Windows 10 Technical Preview on a phone.

First, you need a supported device, with at least 8 GB of storage, running Windows Phone 8.1. The list of supported devices, as well as additional hardware requirements, is here:

<http://windows.microsoft.com/en-us/windows/preview-supported-phones>.

Next, you need to install the Windows Insider app from the Store and sign in using the same Microsoft account you used to enroll in the desktop preview program. Choosing the Get Preview Builds option, shown in Figure 10-1, allows the device to download and install preview builds.

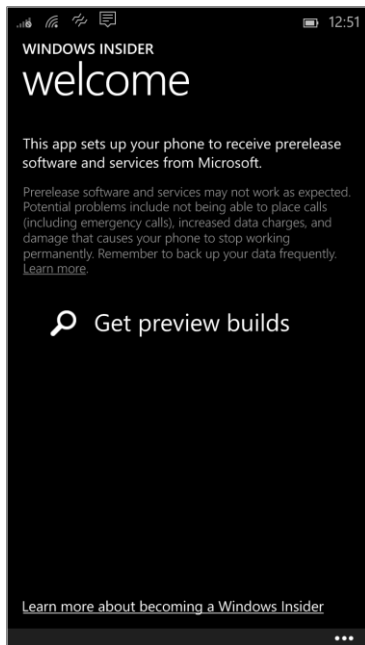


FIGURE 10-1 Install this Windows Insider app on a supported phone to enable access to the Windows 10 Technical Preview for phones.

As with the preview program for desktop releases, you can specify whether you want the device to be on the Fast or Slow ring. You must choose one of the two options when enrolling for the first time, as shown in Figure 10-2.

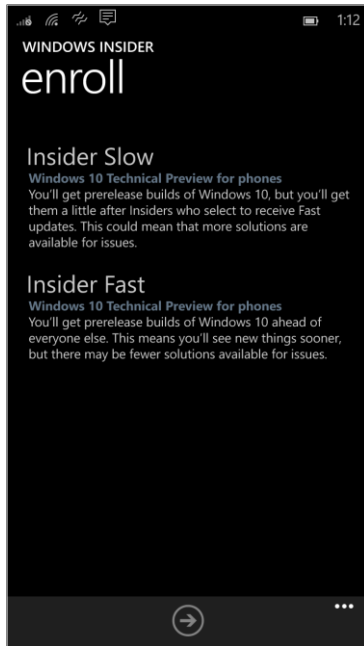


FIGURE 10-2 The Windows 10 Technical Preview for phones includes the same Fast and Slow rings as in the desktop preview program.

To see which ring your device is currently enrolled in, tap the ellipsis (three dots) at the bottom of the Windows Insider app and then tap About from the menu of options. To switch from Insider Fast to Insider Slow, or vice versa, run the enrollment process again.

Removing a device from the preview program and restoring it to Windows Phone 8.1 requires a separate utility, the Windows Phone Recovery Tool, available at <http://go.microsoft.com/fwlink/p/?LinkId=522381>. This requires a USB connection to the phone; the utility identifies the phone, downloads the current operating-system image for that device, and then replaces the preview build with the downloaded version.

What's inside Windows 10 Mobile

Some aspects of the Windows 10 experience on a phone are defined by the form factor. Having a row of status icons at the top of the screen, for example, isn't necessary on larger devices but is crucial on a phone, for quickly checking cellular signal strength and remaining battery life.

But in many other respects, the Windows 10 Mobile interface closely resembles its desktop counterpart, hewing to a common set of design principles with appropriate modifications for the smaller screen.

The Settings app, shown in Figure 10-3, is an excellent illustration. The iconography is similar to what appears in the Settings app on a desktop PC running the Windows 10 Technical Preview, with just a few subtle changes.

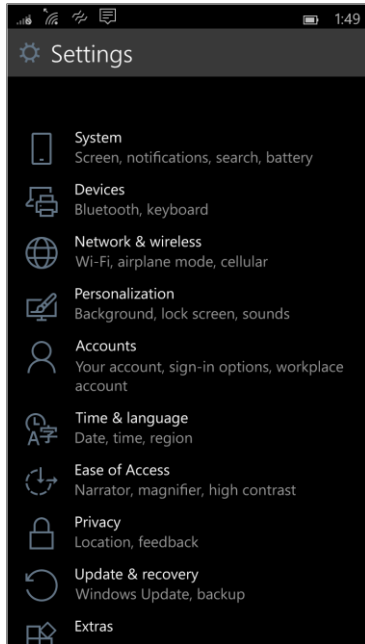


FIGURE 10-3 The Settings app on a mobile device looks nearly identical to its desktop counterpart, with only minor differences, such as the System icon.

Similarly, Windows 10 on a mobile device handles notifications in a way that follows the same organizing principles as the desktop version—with notifications appearing in a list, categorized by source, and a group of action buttons for quick access to common settings. Figure 10-4 shows the mobile Notifications center, which you summon with a downward swipe.

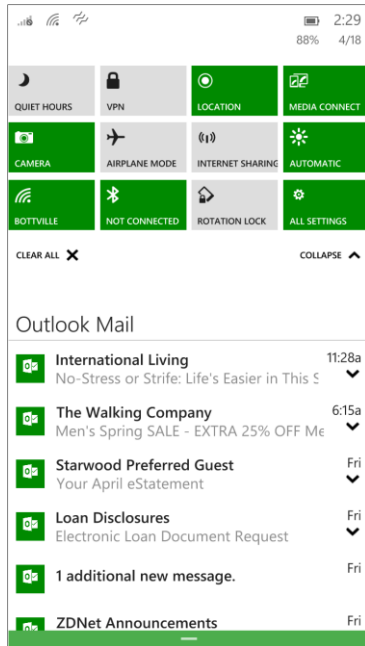


FIGURE 10-4 Just as in Windows 10 on the desktop, the Notifications center contains action buttons for one-tap access to common settings.

Two aspects of these notifications are noteworthy. First, the status of each notification syncs across devices, so if you clear a notification on your mobile device it's also marked as read on your desktop. In addition, you can interact with some notifications directly—replying to a text message directly from this screen rather than having to open the Messaging app, for example.

Much of the usefulness of Windows 10 Mobile will be delivered by its apps, of course—specifically, the first-party apps developed by Microsoft and delivered as part of Windows 10. In the early preview builds, this list includes new Outlook Mail and Calendar apps, Maps, and Photos. The universal Office apps are available through the Windows Store.

From an IT pro's perspective, one of the most important features in this release is its support for device encryption. Although this capability was also available in Windows Phone 8.1, enabling it required a connection to an Exchange ActiveSync server.

I'll have a much more detailed look at Windows 10 Mobile in the final edition of this book.



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

www.microsoftvirtualacademy.com/ebooks

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

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

Microsoft Press



Now that
you've
read the
book...

Tell us what you think!

Was it useful?

Did it teach you what you wanted to learn?

Was there room for improvement?

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

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



Microsoft