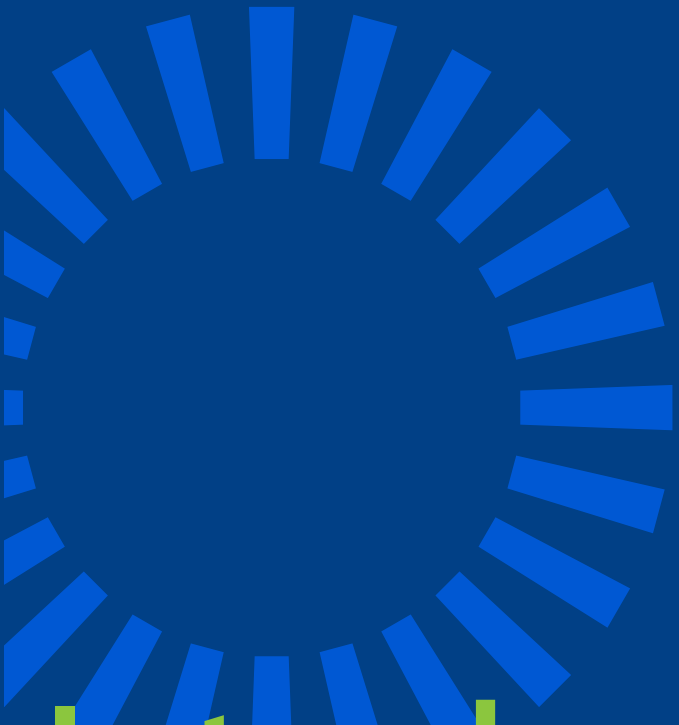


Microsoft

Introducing Windows 10 for IT Professionals

Technical Overview

ED BOTT

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

ISBN: 978-0-7356-9697-6

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*.

Acquisitions Editor: Rosemary Caperton
Project Editor: Christian Holdener; S4Carlisle Publishing Services
Editorial Production: S4Carlisle Publishing Services
Copyeditor: Roger LeBlanc

Contents

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

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

http://aka.ms/tellpress

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.

With the assistance of a skilled team at Microsoft Press, I wrote this book in two phases. The first edition, published in early 2015, was based on the Windows 10 Technical Preview. For this edition, I waited until the release of Windows 10 version 1511 in November 2015 so that I could include all of its enterprise-focused features.

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. New ways of deploying major upgrades.

My goal in this book is to help you sort out what's new in Windows 10, with a special emphasis on features that are different from the Windows versions you and your organization are using today. I've tried to lay out those facts in as neutral a fashion as possible, starting with an overview of the operating system, describing 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 starting point so that you can get more out of your evaluation of Windows 10, which is why I have also included many links to external resources.

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.

Windows 10 is a free upgrade for any PC running a properly licensed copy of Windows 7 or Windows 8.1 retail and OEM editions. If your organization has a Volume Licensing agreement for Windows Enterprise edition with Software Assurance, you also have

access to Windows 10 at no cost. Even if you have no immediate plans to migrate your organization to the next version of Windows, now is the time to evaluate this new operating system.

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

January 28, 2016

Acknowledgments

I'd like to thank Michael Niehaus, Chris Hallum, and Fred Pullen, who provided invaluable input for both editions of this book. 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.

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/introwin10/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 Windows 10

Microsoft 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 and to make it possible for organizations to take advantage of new technology when it's available, rather than years later. Historically, migrating an enterprise to a new version of Windows is a slow, cautious operation, with careful planning and staged deployments that can take several 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.

The goal of Windows 10 is to deliver new features when they're ready, as a free update, rather than saving them for a major release that might be years away. 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 this new delivery model "Windows as a Service." 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. In late 2014, Microsoft launched its Windows Insider program with a Windows 10 Technical Preview aimed at IT pros and consumers. Roughly 10 months later, after many updates and an unprecedented amount of feedback from members of the Insider program, Microsoft officially released Windows 10 to the general public.

Only three months after the initial release of Windows 10 on July 29, 2015, Microsoft said more than 110 million devices were already running Windows 10. Those Windows 10 early adopters received the first batch of new features, officially identified as version 1511, through the tried-and-true Windows Update channel in November 2015. By January 2016, more than 200 million people were running Windows 10.

In short, it's a new world for anyone charged with deploying and maintaining Windows in businesses of any size.

In this chapter, I provide an overview of Windows 10, 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 Windows 10–based operating system that powers the Xbox One game console.

But that common code has a big payoff when it comes to app development. Apps that are built on the Windows 10 universal app platform can run on all Windows 10 device families, delivered through a common Windows Store. 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) is still available for some configurations.

In the new "Windows as a Service" model, Microsoft plans to deliver significant upgrades, with new features, two or three times per year. That's a dramatically faster pace than the traditional Windows release scheme, in which new features were reserved for new versions released with great fanfare every three years or so.

To help IT pros adapt to this new, faster pace of change, Microsoft has built a new servicing model for Windows 10. Security updates continue to arrive on the second Tuesday of each month via Windows

Update, with additional reliability improvements, hardware driver updates, and the rare out-of-band security update also coming through Windows Update.

New features are delivered in larger update packages that are the equivalent of a complete in-place upgrade. Each new Windows 10 build proceeds through different "branches" on its way to the general public and business users. Figure 1-2 shows a conceptual diagram of how this development process works, with rough dates defining how long each testing/stabilization/bug-fixing period lasts before the build moves on to the next branch.

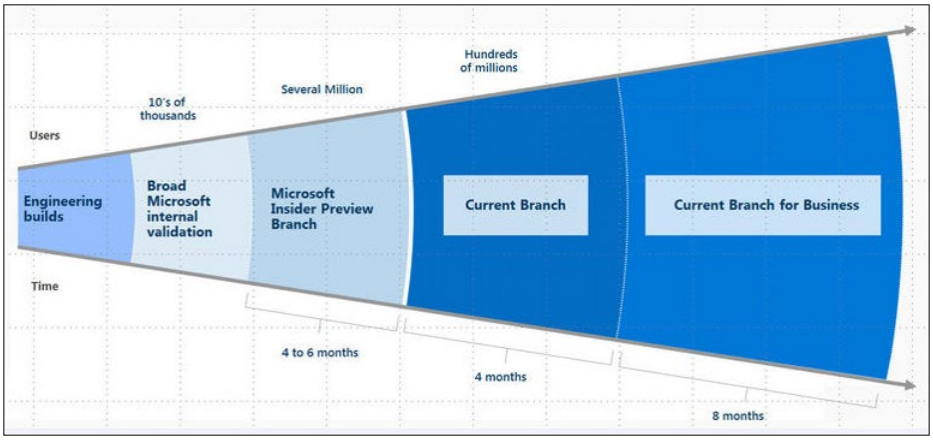


FIGURE 1-2 Each new Windows 10 version update goes through extensive internal and external testing before reaching the general public in the Current Branch. IT pros who prefer a more conservative approach can defer upgrades for longer.

Testers inside Microsoft get to use preview builds first, followed by members of the opt-in Windows Insider program, who use preview builds to provide feedback that Microsoft uses to identify bugs and fine-tune feature designs.

After a reasonable amount of polishing and bug-busting, a stable version is released to the general public. That's the Current Branch section shown in Figure 1-2.

Version 1511 was released to the Current Branch in November 2015. (The version numbering scheme corresponds to this release date, with the year and month in *yydd* format.)

Risk-averse IT pros who would rather watch and wait before deploying new code can choose to assign Windows PCs (Pro, Enterprise, and Education editions only) to a later branch, known as the Current Branch for Business. By choosing this option, you can defer upgrades until Microsoft releases them to that branch, typically four to six months after the upgrade is released to the Current Branch.

Version 1511, for example, was released to the Current Branch in November 2015, but it is not scheduled to hit the Current Branch for Business until sometime in the first half of 2016. When it does reach the Current Branch for Business, it will contain at least four months of reliability and security updates based on the experience of the tens or hundreds of millions of PCs in the Current Branch.

The Long-Term Servicing Branch

The most conservative option in the new Windows 10 delivery model is the Long-Term Servicing Branch (LTSB), which is not shown in Figure 1-2. This branch, available only in Windows 10 Enterprise edition, is intended for use on mission-critical devices, where new features are irrelevant and stability is paramount. When you deploy Windows 10 Enterprise LTSB on a PC or tablet, that device receives security and reliability updates only. Upgrading to a new LTSB version or deploying Current Branch updates requires a new license or a Software Assurance subscription.

For IT pros who want to stay ahead of the curve, Microsoft offers early access to preview builds through the Windows Insider program. Participants in the preview program can currently 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 has been thoroughly vetted by the Fast ring, with any bugs addressed via interim updates.

Participation in the Windows Insider program is voluntary, and you can leave the program at any time.

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 opened 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 Windows 10, clicking the Start button opens a menu similar to the one shown in Figure 1-3.

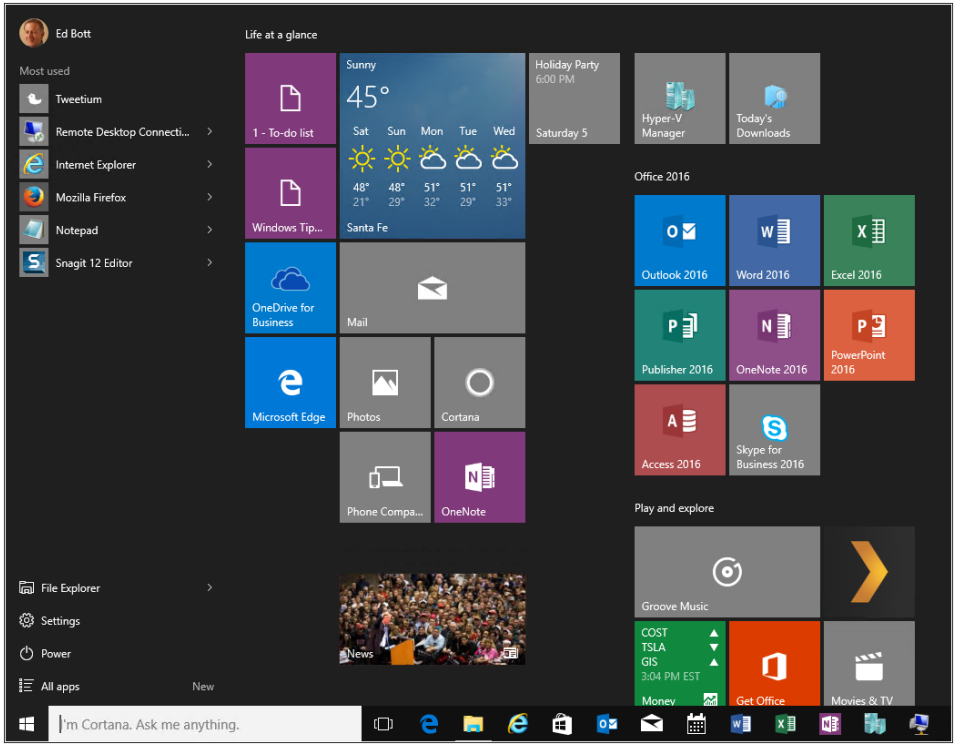


FIGURE 1-3 The Windows 10 Start menu blends elements of its Windows 7 predecessor with the live tiles that debuted in Windows 8.

This Start menu design (which evolved rapidly during the lengthy preview period before Windows 10's official 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 an essential part of the larger Windows 10 platform.

On a PC with a keyboard and pointing device, you can change the height and width of the Start menu. A separate option, called *Tablet Mode*, expands the Start menu to fill the entire screen and makes additional changes designed to make Windows 10 more usable on tablets, hybrid PCs, and other touchscreen devices. Figure 1-4 shows Tablet Mode in action.

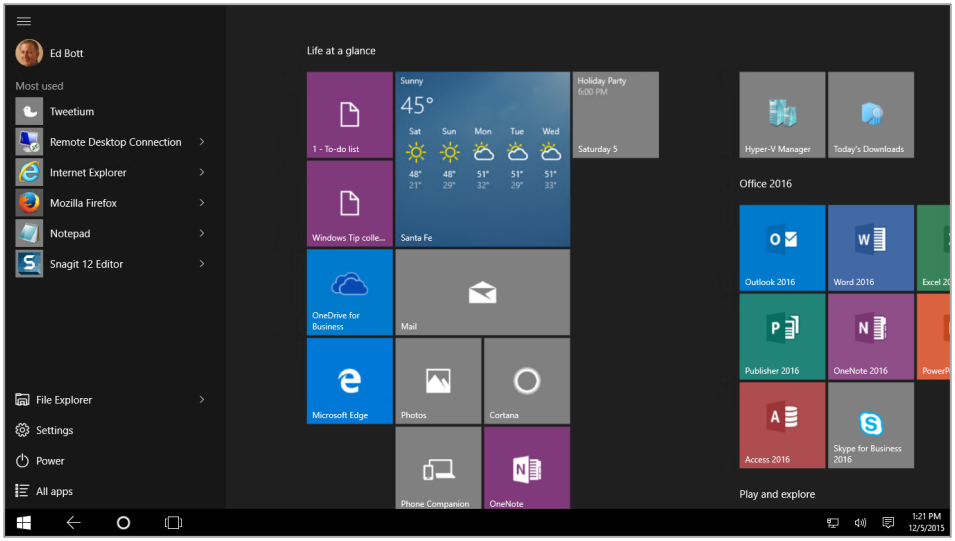


FIGURE 1-4 In Tablet Mode, the search box shrinks and the Start menu and apps fill the entire screen.

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.

More Info 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.

Windows 10 supports signing in with an Azure Active Directory account, which allows administrators to manage a PC or mobile device without requiring it to be joined to a domain. In addition, you have the option to add a work or school account to make it easier to sign in to Office 365 and other cloud services.

Figure 1-5 shows this feature in action, under Your Email And Accounts in the Settings app. In this case, I connected a Google Apps account for access to email, calendar, and contacts information, as well as an Office 365 account managed through Azure AD.

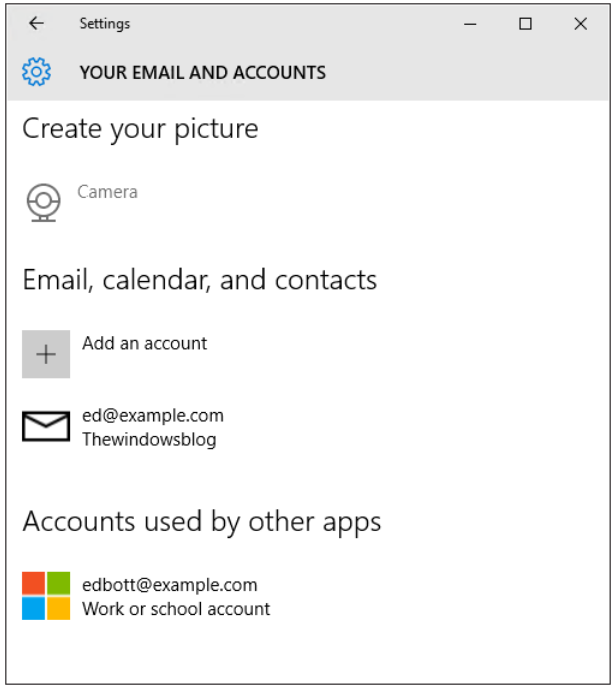


FIGURE 1-5 Connecting accounts to the primary account allows for easier access to email and corporate apps. The Windows flag logo on the Work Or School Account means it's managed by Azure AD.

The list of settings that can be synchronized includes the layout of the Start screen as well as apps; previously purchased apps can be downloaded and installed from the Store when you sign in with a Microsoft account on a new device. You can use this feature 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 includes provisioning features that allow IT pros to manage this process.

One key feature in Windows 10 is a universal synchronization client to manage access to cloud-based file storage in OneDrive and OneDrive for Business. The OneDrive for Business Next Generation Sync Client was released for Windows 10 in December 2015.

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 *Trusted Windows Store apps* or *modern apps*), a category that debuted in Windows 8 and has 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.)

The latest development platform for Windows 10 is called the *Universal Windows Platform (UWP)*. By using the UWP core application programming interface (API), developers can create a single app package that can run on devices with a wide range of sizes and capabilities, including phones, tablets, PCs, and even the Xbox One. Universal apps are delivered through the Windows Store.

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 1-6, for example, shows the free Word Mobile app running in a resizable window on a Windows 10 PC.

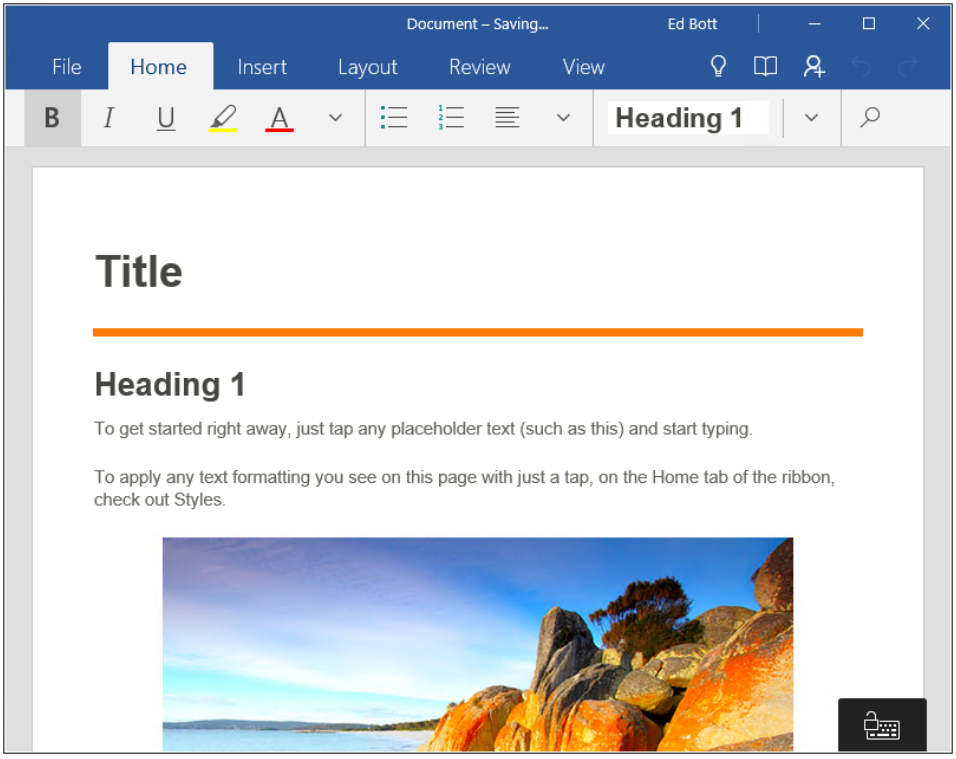


FIGURE 1-6 The Word Mobile app is available through the Windows Store. Like other modern apps in Windows 10, it can run in a resizable window.

As is the case with most modern apps, the mobile Microsoft Office apps available in the Windows Store (Word's Office-mates include Excel and PowerPoint) are designed to deliver an excellent experience on touchscreen devices with small screens. These lightweight apps don't have the full feature set of their Windows desktop counterparts, but they're ideal for reading and light editing tasks.

The Windows Store has been completely overhauled for Windows 10. Figure 1-7 shows a typical listing in the new Store, which has a cleaner design and offers a broader variety of products than just apps.

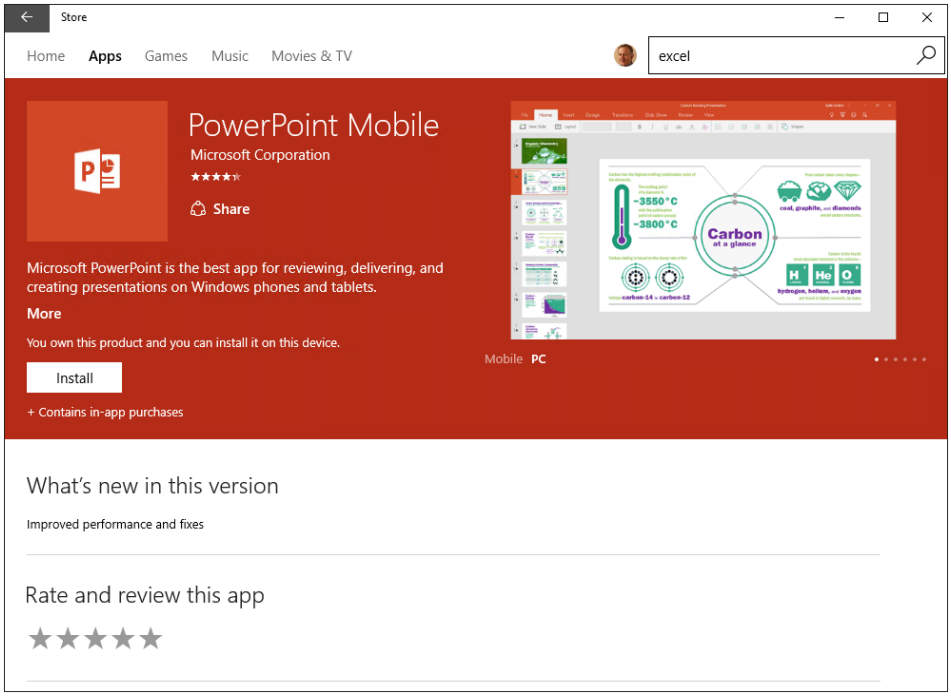


FIGURE 1-7 The Windows Store offers more than just apps—you can also find games, music, movies, and TV shows for purchase or for rent.

More Info For more details on these apps and on the changes to the Windows Store, including the Windows Store for Business, see Chapter 11, "Universal apps and the new Windows Store."

A new default browser

One of the signature features of Windows 10 is a new default browser, Microsoft Edge. Although its EdgeHTML rendering engine is based on the familiar Trident engine that has been part of Internet Explorer since its earliest days, the new engine is built with the goal of being highly interoperable with modern web standards.

The Internet Explorer development team says it removed 220,000 lines of code when it began modifying the Trident engine for EdgeHTML. That major pruning was essential to rid the new browser of compatibility baggage that contributed to Internet Explorer's poor reputation in the web development community. With that step out of the way, they added new and useful features, such as integration with Cortana, a new reading list, and the ability to annotate and share webpages. More importantly, the new browser offers excellent support for modern web standards and better interoperability with other modern browsers.

Microsoft Edge has been developing at breakneck speed since its first public appearance (with an incomplete feature set) in an April 2015 Insider preview release. The initial (July 2015) Windows 10

Current Branch release included Edge version 12; Windows 10 version 1511 is a major update that takes Edge to version 13. Windows Figure 1-8 shows the touch-friendly and uncluttered (practically Spartan) Microsoft Edge interface.

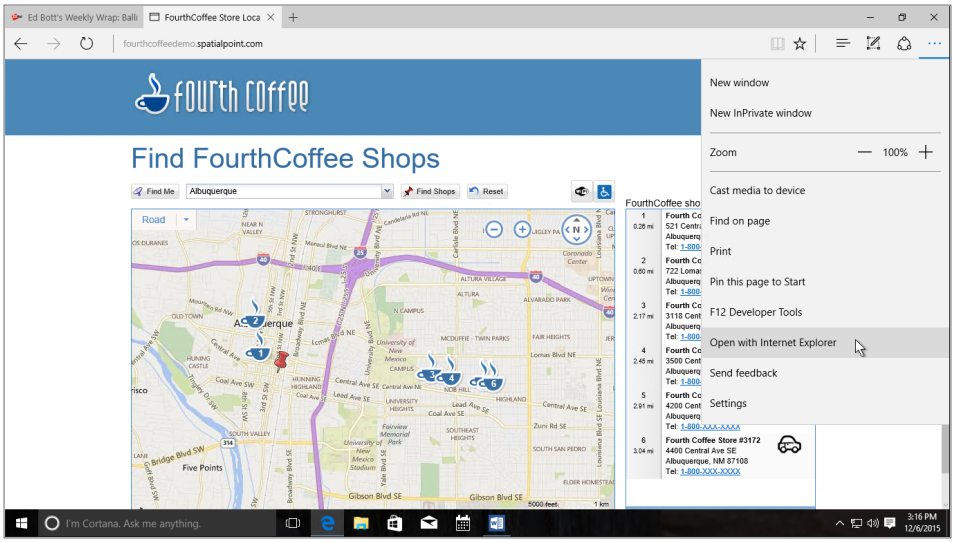


FIGURE 1-8 Microsoft Edge, the default browser for Windows 10 devices, includes a simple, uncluttered design with an option to open any page in Internet Explorer.

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 is 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.

More Info You can read more details about this two-browser strategy in Chapter 6, "Microsoft Edge and Internet Explorer 11."

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 wide-scale 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.

Greater control over updates and upgrades

From a network administrator's perspective, perhaps the most important Windows 10 improvement is Windows Update for Business, a feature that debuted in the Current Branch in version 1511.

Windows Update for Business (available only for Pro, Enterprise, and Education editions) uses Group Policy settings to allow administrators to delay updates by up to four weeks, in intervals of one week. The same settings support deferring upgrades in the Current Branch for Business (which are already a few months behind their Current Branch release) by up to eight additional months, in one-month intervals. Figure 1-9 shows these policy settings in the Local Group Policy Editor in Windows 10 Pro.

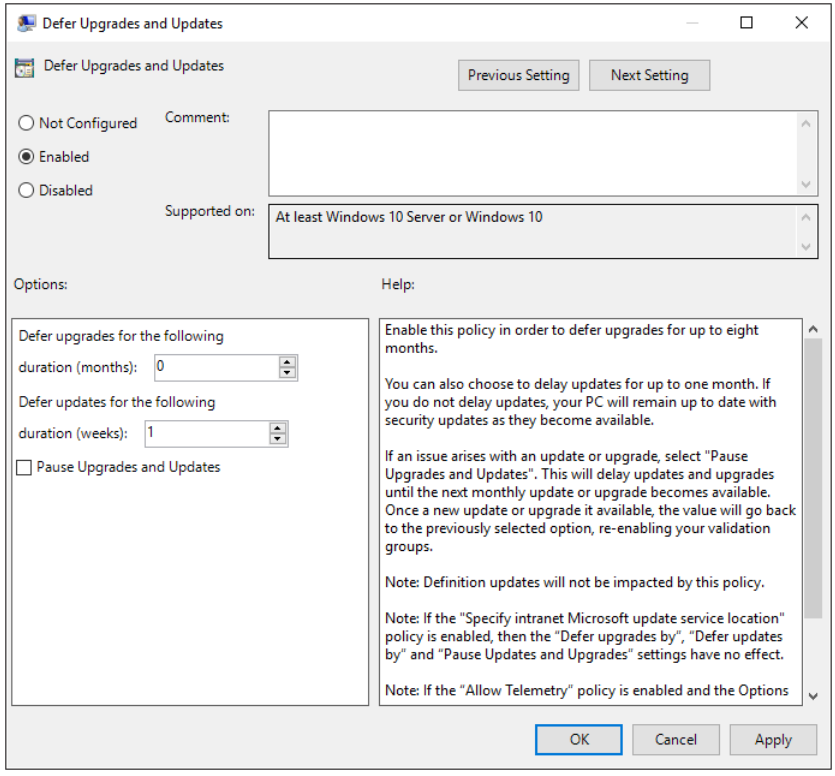


FIGURE 1-9 The Defer Upgrades And Updates Group Policy setting allows network administrators to delay updates for up to four weeks and defer Current Branch for Business upgrades by up to eight months.

More Info For more details about these and other Group Policy settings, see Chapter 15, "Group Policy in Windows 10."

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 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 antispyware 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.

An all-new feature in Windows 10, Credential Guard, uses virtualization-based security to isolate secrets (including domain passwords) so that only privileged system software can access them. This feature prevents common credential-theft attacks such as Pass-The-Hash and Pass-The-Ticket. Credential Guard must be enabled for each PC in an organization and works only with Windows 10 Enterprise edition.

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 to arrive in Windows 10 in 2016 but not available in current releases.
- **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 enable 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. With BitLocker, you can choose to encrypt only the used space on a disk instead of the entire disk. In this configuration, free space is encrypted when it's first used. This results in a faster, less disruptive encryption process so that enterprises can provision BitLocker quickly without an extended time commitment.

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, 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 also can 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.

More Info Chapter 5, "Security and privacy 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 it's simpler and more flexible.

More Info For more information about planning and carrying out a Windows 10 deployment, see Chapter 3, "Installation and activation."

On unmanaged devices, the new recovery options in Windows 10 help streamline the process of reinstalling the operating system. 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 but the most recent cumulative update, 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; 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, which you can use 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.

As illustrated in Figure 1-10, Windows 10 version 1511 introduces Trusted Platform Module (TPM) support for virtual machines, allowing those VMs to enjoy full encryption.

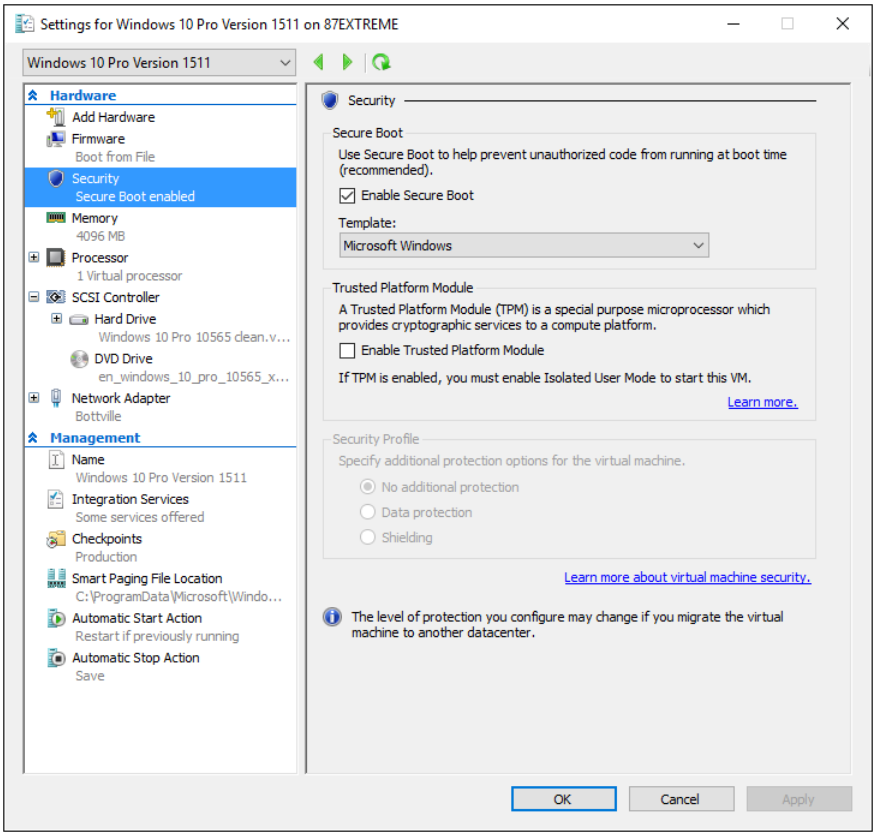


FIGURE 1-10 The November 2015 Windows 10 update, version 1511, includes significant improvements in Hyper-V security, including support for Secure Boot and TPM-based encryption.

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, Enterprise, or Education; it also requires that specific hardware features be available on the host device.

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 of these benefits are available across different types of VDI desktops (personal VM, pooled VM, or session-based desktops).

More Info For more information about these features, see Chapter 8, "Hyper-V and desktop virtualization options."

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 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 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.

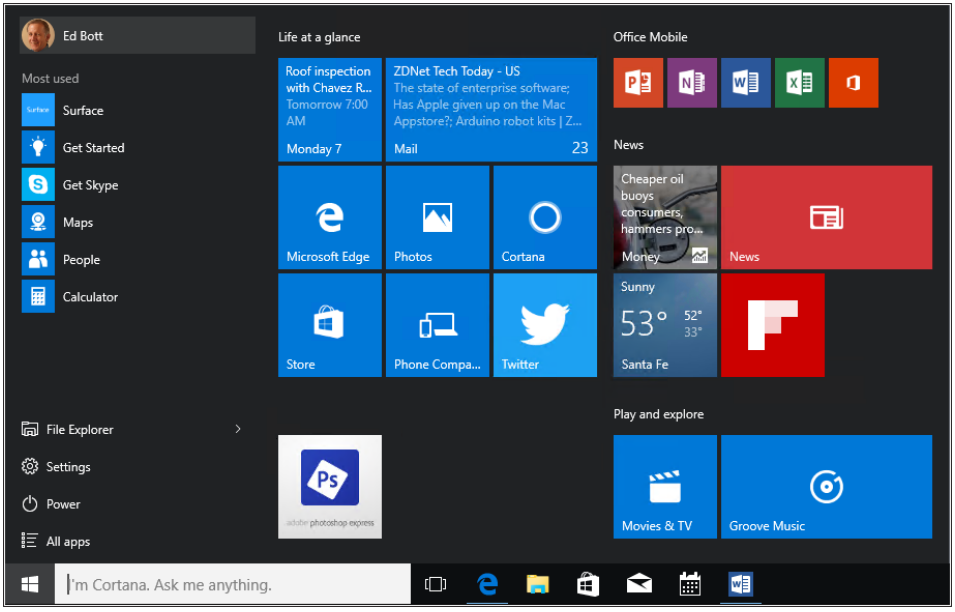


FIGURE 2-1 The new Start menu combines distinctive features from its predecessors in Windows 7 and Windows 8.1.

The default arrangement of the left column 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 to frequently used and recently added apps
- Shortcuts for File Explorer (Windows 7 users, note the name change), the Settings app, and a Power button
- 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

You can customize this list using options under the Personalization heading in Settings. You can also specify a standard Start layout (and prevent users from customizing it) using Group Policy. (See Chapter 15, "Group Policy in Windows 10," for more details on this option.)

The shortcuts to system settings from the Windows 7 Start menu aren't available on Start; instead, they're 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. Figure 2-2 shows this menu, which switched to a dark theme in Windows 10 version 1511.

FIGURE 2-2 This Quick Link menu appears if you press Windows logo key + X or right-click the Start button at the left of the taskbar.

The default Start menu contains a Power button (with the options Sleep, Shut Down, and Restart). You can adjust the size of the Start menu by dragging the top and side borders. (You can use the Personalization option to expand the Start menu to a full screen without enabling Tablet Mode, which I describe later in this chapter.)

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.

The Settings app

That Settings shortcut leads to the Windows 10 successor of Windows 8's PC Settings. The iconography, shown in Figure 2-3, is a distinctive change from the Windows 7 Control Panel.

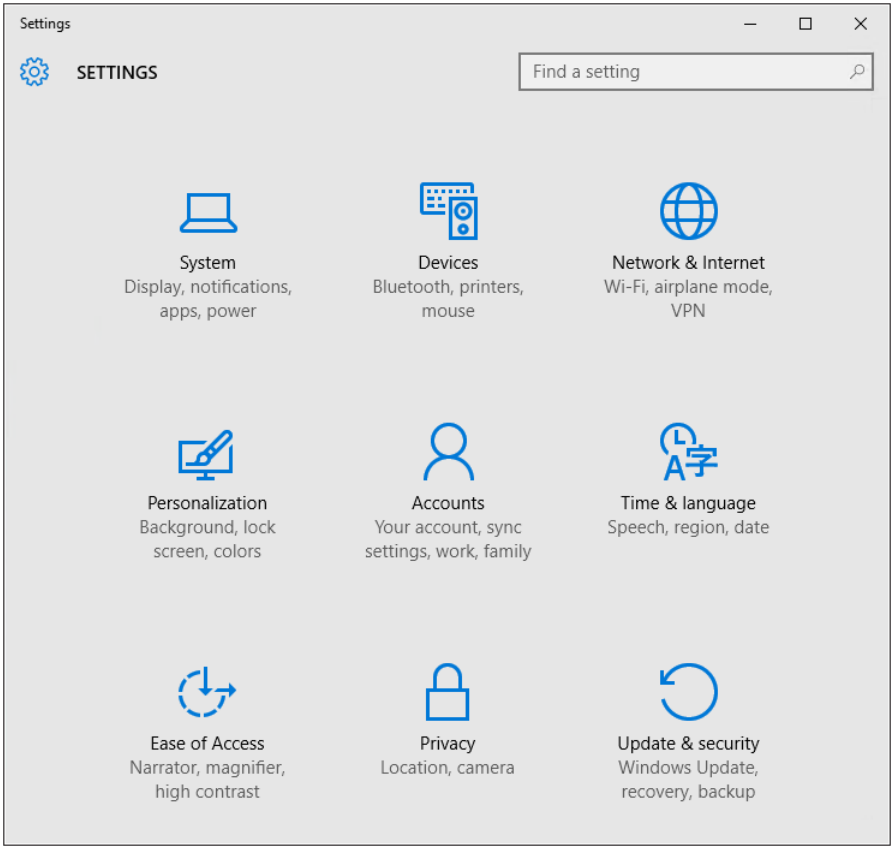


FIGURE 2-3 The Settings app is designed to be touch-friendly and to cover most common configuration tasks.

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 is continuing after the initial release of Windows 10.

The System pane, shown in Figure 2-4, is a case in point. In the most recent Windows 10 release, clicking or tapping Power & Sleep offers only limited options. The shortcut in the bottom right, Additional Power Settings, leads to the familiar Power Options page in Control Panel. (See Figure 2-5.)

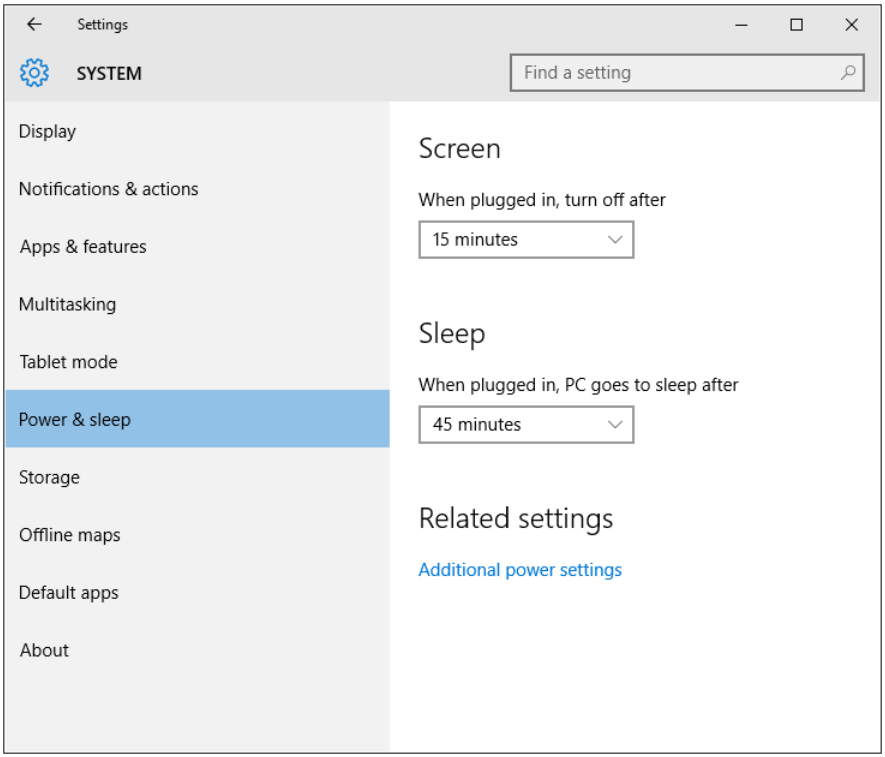


FIGURE 2-4 The number of options in the Settings app is growing steadily, but some tasks still offer only a limited selection.

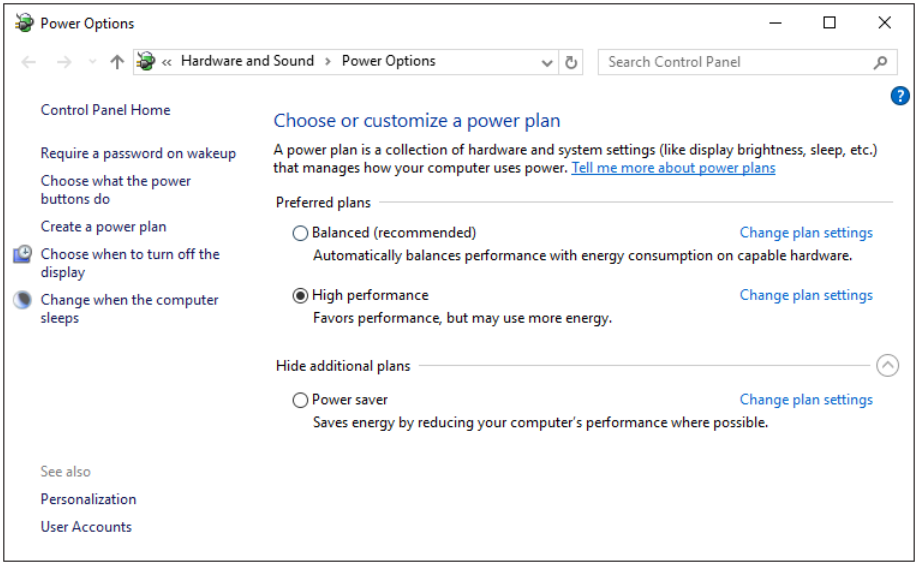


FIGURE 2-5 Less common configuration tasks such as these still require a trip to Control Panel.

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 and action buttons

In Windows 10, the Charms menu, a signature feature of Windows 8 and 8.1, is gone completely. On a tablet or touchscreen-equipped PC running Windows 10, swiping in from the right opens the Action Center, which 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 2-6 shows the Action Center open, with unread email messages, upcoming calendar appointments, and system messages available. The group of action buttons is expanded to show the full collection on this device instead of just the top four.

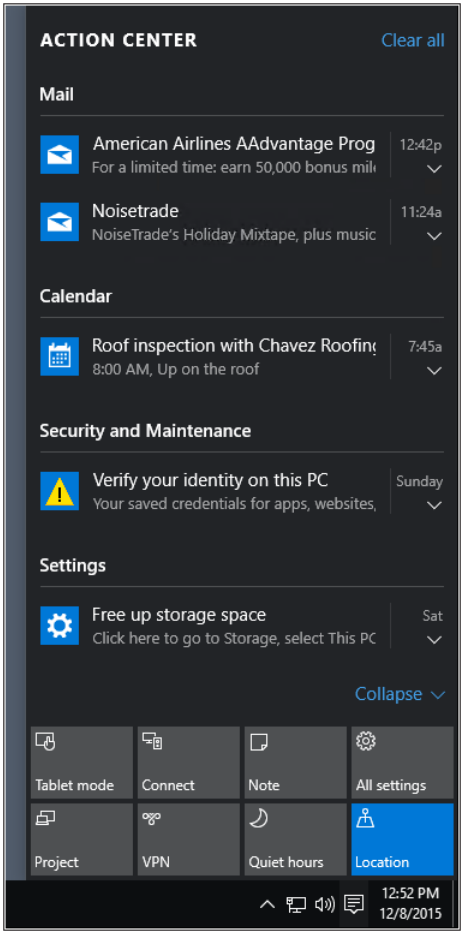


FIGURE 2-6 The notifications pane shows messages from apps, online services, and the operating system itself, with action buttons at the bottom of the pane.

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, combining local and web search with the ability to understand spoken commands and enough smarts to convert those commands into tasks, appointments, or instructions. Essentially, Cortana acts as a personal assistant, complete with an occasionally sassy personality (with the name and voice taken from the Halo franchise on Xbox).

Figure 2-7 shows Cortana's organizational skills at work.

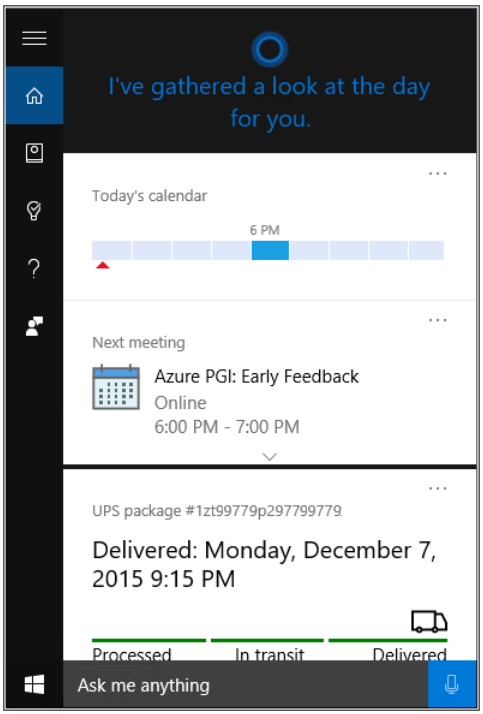


FIGURE 2-7 Cortana can manage your calendar, keep track of travel itineraries and shipments, provide news bulletins, perform calculations, and find answers on the web.

Cortana is not enabled by default on Windows 10. The first time you click in the box to the right of Start, Cortana gives you the option to enable it or leave the feature disabled. If you don't want users in your organization to interact with Cortana, you can disable the feature using Group Policy. Figure 2-8 shows the Allow Cortana setting, which is accessible under Computer Configuration > Administrative Templates > Windows Components > Search.

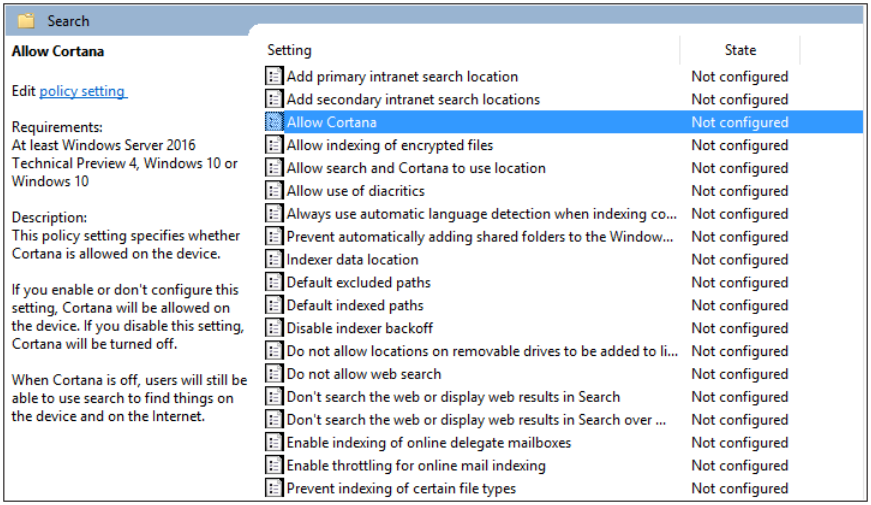


FIGURE 2-8 You can use this Group Policy setting to keep the Cortana service off managed PCs.

If you don't enable Cortana, the box to the right of Start performs simple searches of the local file system, settings, and the web, minus any personality and also without any connection to your personal data.

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 2015. Because much of Cortana's magical powers derive from web-based services, she's getting smarter with age. What you see in current releases is only a fraction of what you'll see after another year (or two or three) 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.

After you and your users get past the novelty of it all, take a look at Cortana's notebook (available from the icon just below Home in the navigation bar on Cortana's left edge). 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.)

The list of Notebook categories shown in Figure 2-9 isn't complete, and within each category the options can expand as Cortana becomes more capable. Scrolling down reveals more categories, including Weather, Sports, and Reservations, where you can allow Cortana to scan your email in search of restaurant reservations, movie times, and other likely events.

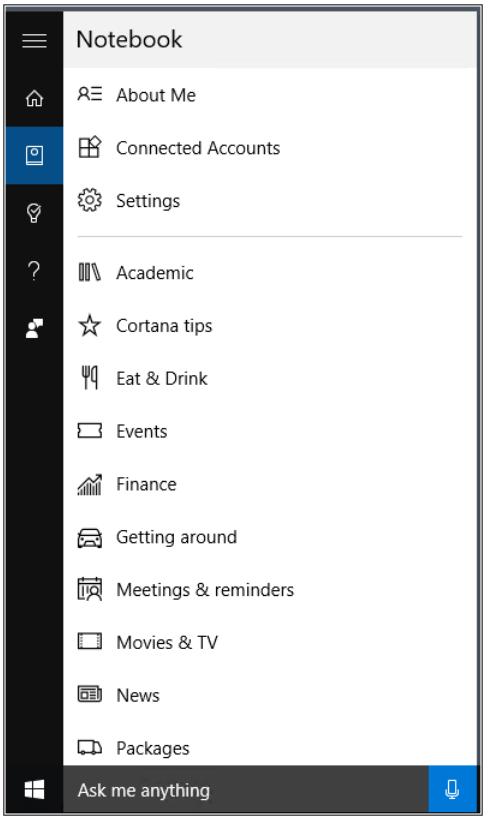


FIGURE 2-9 The Notebook offers users fine-grained control over what sort of information Cortana will assist with.

Universal apps in resizable windows

If you supported a group of users running Windows 8 or Windows 8.1, you know about the advantages of using Windows Store apps, which are easier to install, more secure, and generally easier to use on touchscreen devices. You've also probably heard familiar complaints based on a common theme: the experience of using Windows Store 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 for users who spend most of their time on the desktop.

The other challenge of using Windows Store apps in 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, Windows Store apps can now run in resizable windows that can be dragged around the desktop, pinned to the taskbar, minimized and maximized, and otherwise managed just like their Windows desktop counterparts.

The design standards for modern apps are still evolving, but you can expect to see one element increasingly often. In the upper-left corner, just below 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. Clicking or tapping the hamburger typically reveals a menu along the left edge of the screen that collapses to a thin row of icons when it's not in use. Figure 2-10 shows three different takes on the hamburger menu from three different built-in apps: Mail, News, and Photos.

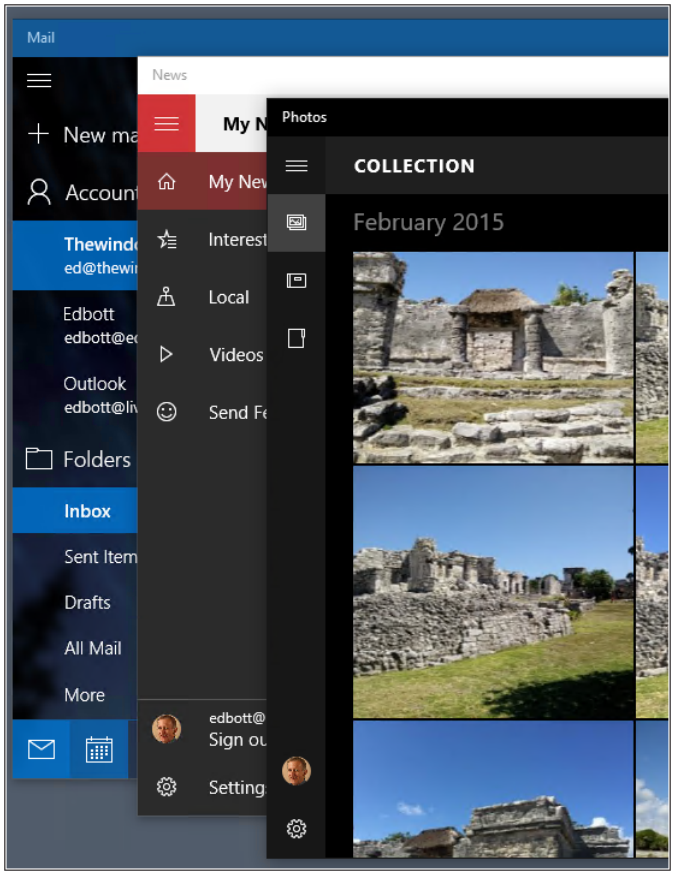


FIGURE 2-10 Windows apps, which used to run only in a full screen or snapped to the side, can now run in resizable windows. To find settings and app commands, use the hamburger menu in the upper-left corner.

Navigation

As I mentioned earlier, the "hot corner" navigation techniques of Windows 8 are no longer supported. Instead, in Windows 10 you can 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, swipe from the left to open Task view. With a mouse and keyboard, press the shortcut Windows logo key + Tab. In either mode, click or tap the Task View button on the taskbar, just to the right of the search box.

Figure 2-11 shows Task view in operation on a PC running Windows 10 version 1511, with six task windows available for switching.

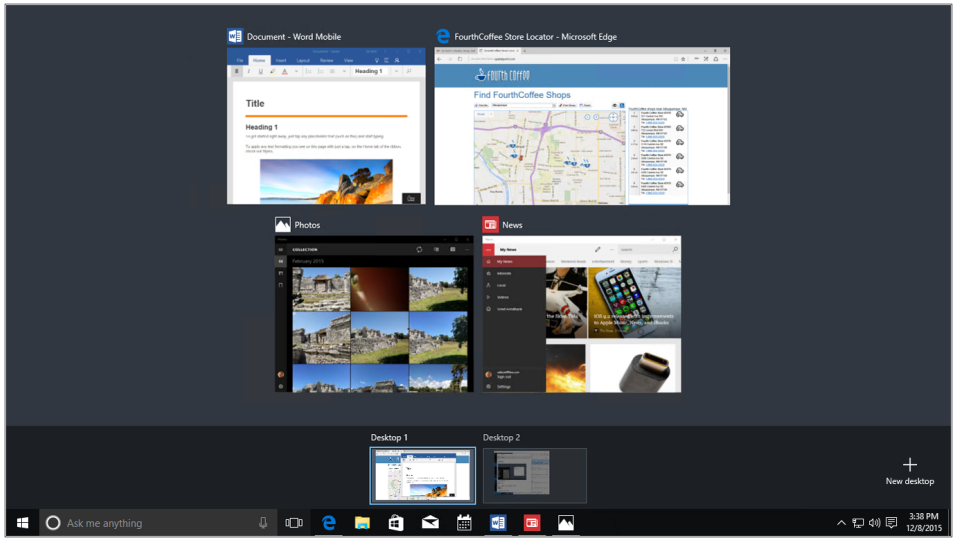


FIGURE 2-11 In Task view, every running app and every open settings page or File Explorer window gets its own thumbnail for quick task switching.

If you see only four running tasks in Figure 2-11, look more closely. Two additional programs are running 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 copy data from a webpage and paste it into a Microsoft Word document or to move files 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 2-12. (Click anywhere else if you want to refuse the offer of snapping a second window.)

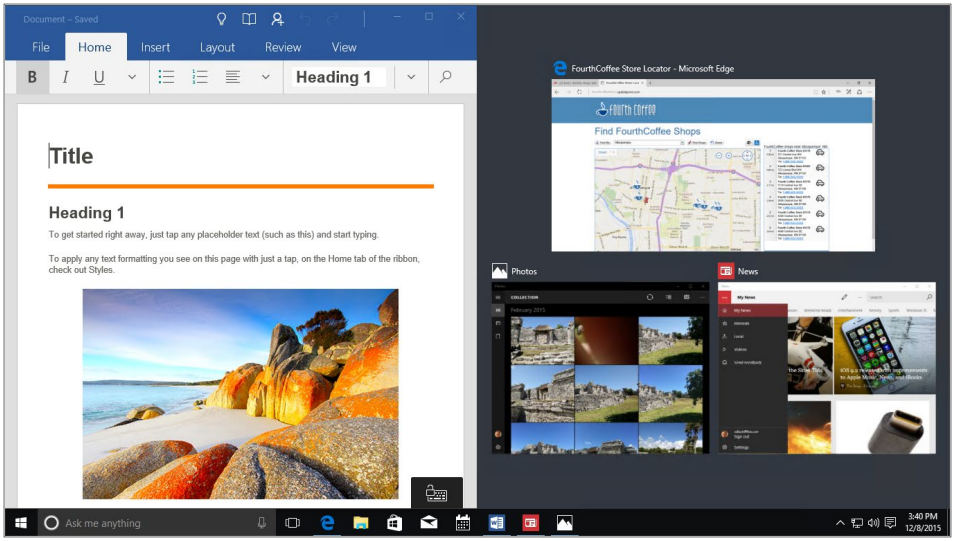


FIGURE 2-12 When you snap a window to one side of the screen, Windows 10 assumes you want to snap another window alongside it and displays thumbnails to let you choose.

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 access 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 for some people on a traditional PC: run an important app using the full screen to make the best use of the available space and minimize distractions. Note that the option isn't available with multiple monitors.)

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 2-13. (If that behavior seems reminiscent of how Windows 8 worked, you're right. But this time it's an option.)

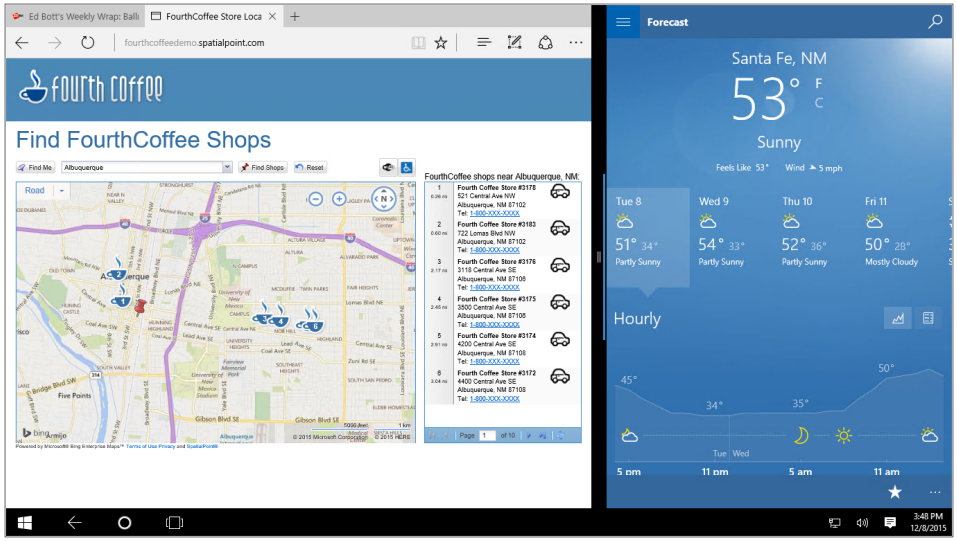


FIGURE 2-13 In Tablet Mode, resizable windows are not allowed. Apps run in full screen unless they're snapped side by side like this.

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 has used Windows 8.1, is the addition of Microsoft Office–style ribbons in place of menus and command bars.

Figure 2-14 shows a typical File Explorer window with a context-sensitive Picture Tools ribbon visible.

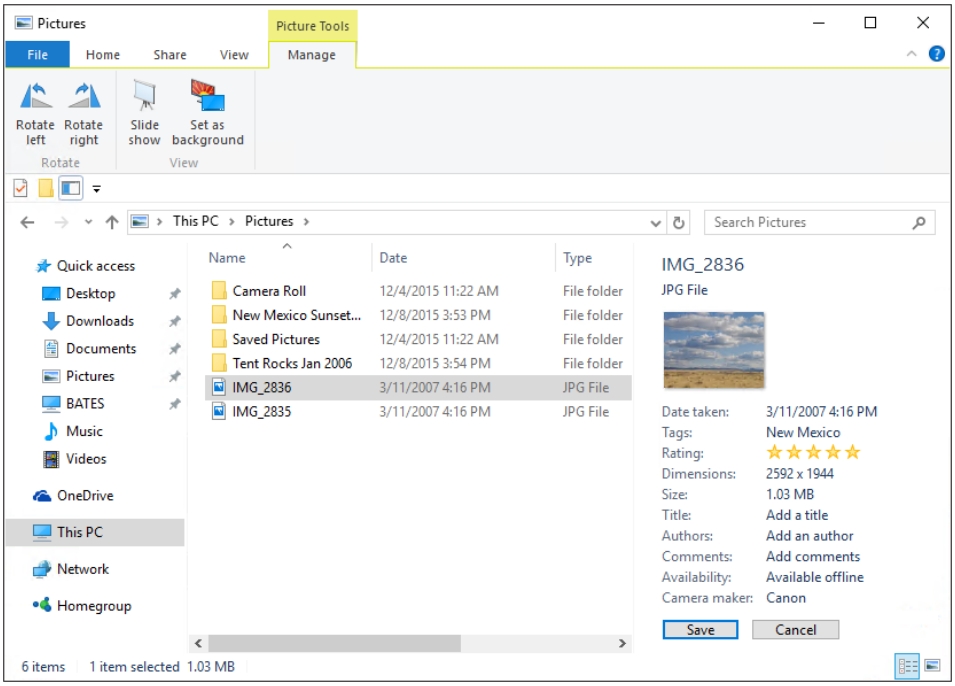


FIGURE 2-14 For anyone moving from Windows 7, the arrangement of commands into ribbons is the biggest change in File Explorer.

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.)

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 2-15, appears automatically when you click in the search box. Additional point-and-click search filters are available from the search box itself.

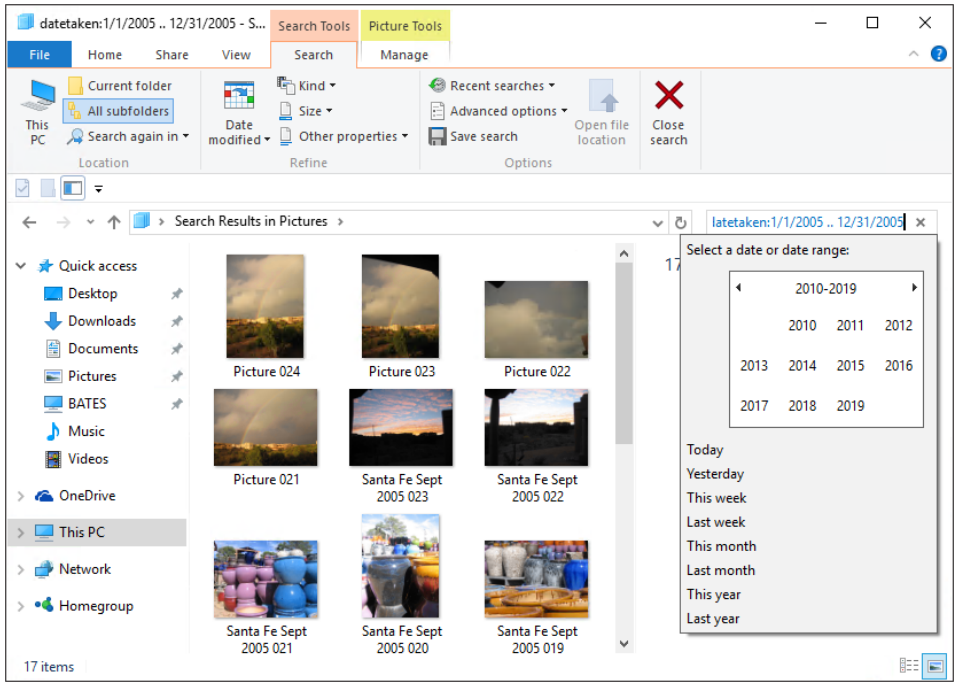


FIGURE 2-15 With Windows 10, clicking in the search box in File Explorer exposes the Search Tools tab of the ribbon, with point-and-click options for filtering and finding files.

Some other subtle File Explorer changes in Windows 10 include a new Share icon you use 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 is a free consumer service that offers 5 GB of free storage, with additional storage available as a paid add-on or with an Office 365 Home or Personal subscription. OneDrive for Business is a feature of Office 365 Business and Enterprise subscriptions that offers personal storage as part of a work or school account.

As of December 2015, the OneDrive synchronization client is updated independently of Windows.

A new unified OneDrive client is now available. It includes the capability to connect to both business and consumer OneDrive accounts, setting up top-level nodes for each in the navigation bar in File Explorer. During the initial setup for the sync client (or any time after), you can enable the option to save space by selecting specific folders instead of the entire contents of a OneDrive data repository, as shown in Figure 2-16.

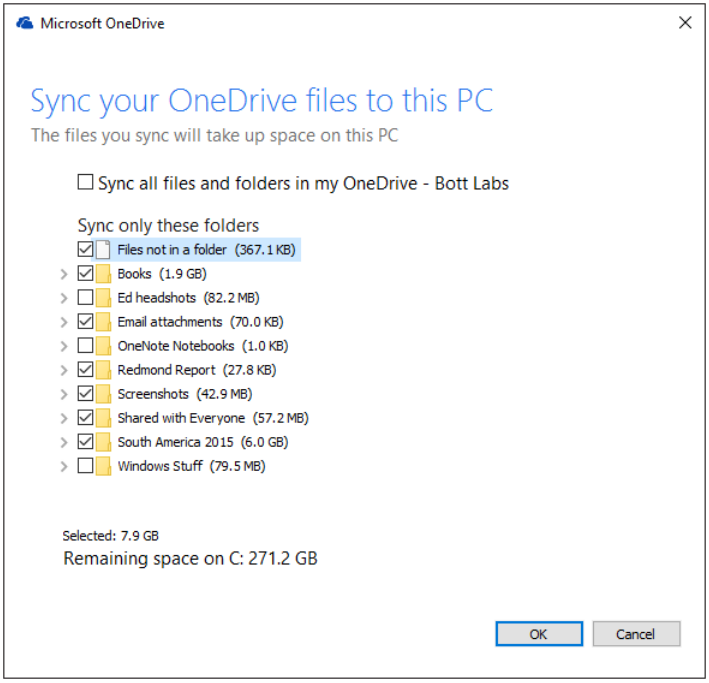


FIGURE 2-16 The new, unified OneDrive sync client included with Windows 10 allows OneDrive for Business users the space-saving option to choose specific folders instead of syncing an entire library of files.

One feature that was available with Windows 8.1 and early preview releases of Windows 10 is called *file placeholders*. This feature allowed File Explorer to display the full contents of a OneDrive data store without actually syncing all those files. That feature was removed from Windows 10 in a preview release in late 2014, with Microsoft explaining that the feature caused too many problems in usability and reliability. The OneDrive development team says this capability (or its equivalent) will return in a future release of the sync client.

CHAPTER 3

Installation and activation

Setup and activation are essential first steps for any new Microsoft Windows 10 PC, with different tools and techniques available to you depending on whether you're upgrading a single PC or deploying Windows 10 across an enterprise. This is the first of two chapters about this crucial topic, focusing on interactive installations (clean installs and upgrades) for individual PCs. Chapter 4, "Deploying Windows 10 in the enterprise," covers enterprise deployment tools and techniques.

For small businesses and home offices that don't have a full-time, formal IT infrastructure, deployment tools aren't necessary or practical. But even if you have a robust deployment environment in your workplace, it's tremendously useful to understand how to set up a Windows 10 PC from scratch. Knowing these skills makes it possible to manage pilot projects in your organization as well as maintain systems you buy or upgrade for use at home or for after-hours experimentation.

This chapter covers the three most common setup options: upgrades from earlier operating systems, clean installs, and new PCs with Windows 10 preinstalled. It also includes a detailed discussion of Windows activation. The details of setup and activation are sufficiently different in Windows 10 that it's worth paying close attention here.

Compatibility and preparation

If you've already begun planning a wide-scale Windows 10 deployment, congratulations! You're ahead of the vast majority of your peers. But even if you aren't ready to begin a major migration, you can certainly make life easier on your future self by doing two things now:

- First, take inventory of your existing hardware and make some intelligent decisions for future purchases.
- Second, start some pilot projects to familiarize yourself and other members of the IT staff with Windows 10.

Existing touchscreen-equipped devices running Windows 8.1 offer a straightforward upgrade path to Windows 10, using Windows Update.

For conventional (non-touch) desktop PCs and laptops running Windows 7 Service Pack 1, there's an equally straightforward path to Windows 10. In fact, Windows 10 is available as a free upgrade on any PC with a properly activated copy of Windows 7 or Windows 8.1 (also known as "Genuine Windows").

Windows 10 is also compatible with most virtualization software, including Hyper-V in Windows Server installations and Windows 8.1 PCs.

System requirements

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 Windows 10. In addition, most desktop applications that run on Windows 7 should also run on Windows 10.

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 following device types are incompatible with Windows 10:

- The Surface RT, Surface 2, and other devices running Windows RT are not compatible with Windows 10.
- Some older CPUs lack capabilities that are required by Windows 10. 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). In addition, 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 Windows 10 Mobile operating system, although closely related to Windows 10 in many respects, is delivered separately. Windows 10 editions built for installation on PCs will not work on phones.

Supported upgrade paths

Upgrading via Windows Update offers the simplest experience, preserving all installed desktop programs, Windows Store apps, personal files, and settings. When you use this option, the Windows 10 upgrade edition is the equivalent of the previous edition. Thus, Windows 7 Home Premium upgrades to Windows 10 Home, and upgrading from Windows 7 Professional and Ultimate or Windows 8.1 Pro results in an installation of Windows 10 Pro.

You also can upgrade from a lesser edition—from Windows 8.1 Core to Windows 10 Pro, for example. I'll say more about upgrade options later in this chapter.

Creating and using installation media

With Windows 10, Microsoft is making installation media widely available to the general public for the first time ever. To get started, visit Microsoft's Get Windows 10 page, at *http://www.microsoft.com/en-us/software-download/windows10*. To upgrade a single PC with the least fuss, click the Upgrade Now button and follow the prompts.

For a more flexible set of options, including the ability to create a bootable USB flash drive or DVD with the Windows 10 installer files, scroll down that page, and download a lightweight utility called the Media Creation Tool. Figure 3-1 shows this tool in action, after choosing the Create Installation Media For Another PC option.

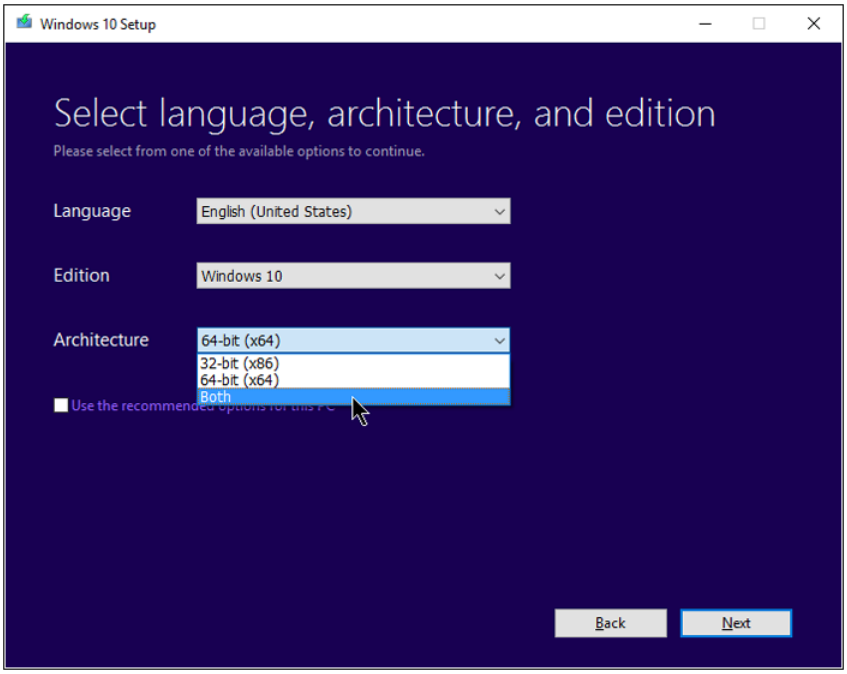


FIGURE 3-1 The Media Creation Tool downloads Windows 10 installation files that can be used on multiple PCs and in virtual machines.

By default, the check box in the lower-left corner is selected, so options that are appropriate for the current system are preselected. If you're downloading the installation files to upgrade multiple PCs, clear this check box (as I've done in Figure 3-1) and select the options you need from the three drop-down lists on this page. Select a language (nearly 40 languages are available as of December 2015), an edition (most people will choose Windows 10 rather than the obscure Windows 10 N edition, which is legally required as part of an antitrust settlement and lacks media-playback features), and an architecture (32-bit, 64-bit, or both).

You can use the next set of options, shown in Figure 3-2, to download the files and immediately create a bootable USB flash drive for multiple installations or, as an alternative, download the same files in a disk image file (ISO) format.

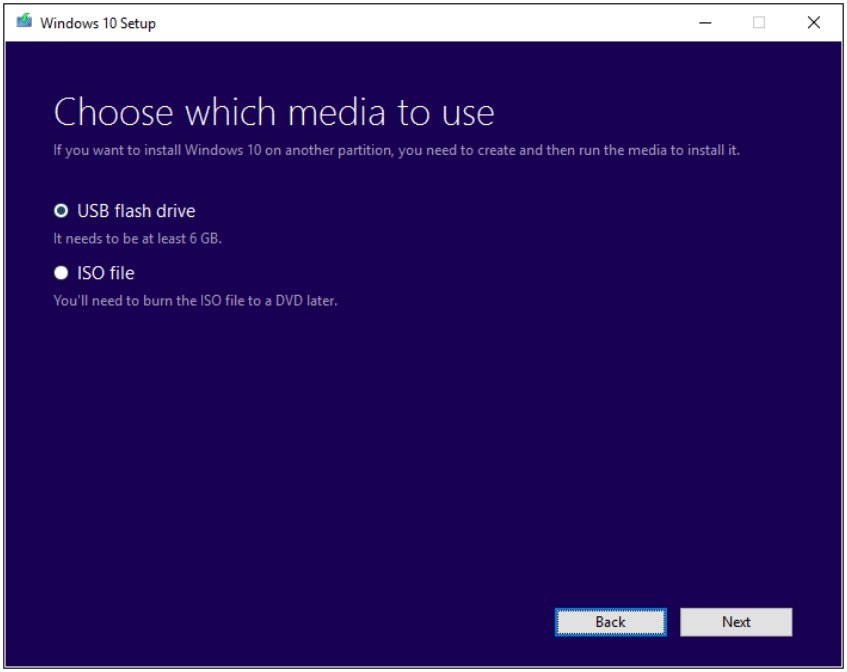


FIGURE 3-2 You use the Media Creation Tool to create a bootable USB flash drive immediately or save the installer files as an ISO disk image.

The ISO format is the most versatile of all and should be your first choice if you want maximum flexibility. You can, for example, double-click an ISO file to mount it as a drive in Windows 8.1 or Windows 10 and then run Setup from the mounted drive. You can also attach an ISO file to a virtual machine (VM) as a virtual DVD to do a clean install or an upgrade in that VM.

Creating a bootable flash drive from an ISO file is also easy. Choose the option from Windows 8.1 or Windows 10 to create a recovery drive (but don't select the option to copy system files). After that process is complete, mount the ISO image in File Explorer and drag its contents to the recovery drive, overwriting any existing files. After the copy is complete, you have a bootable Windows 10 installation drive.

Installation media for Windows 10 Enterprise isn't available through that tool. Instead, you need to use one of the following options:

- Customers with a Volume License agreement can get the latest ISO files from the Volume Licensing Service Center.
- MSDN subscribers can sign in to the MSDN download center and find a wide range of files, including Enterprise and Education editions, intended for use in developing and testing applications.
- If you don't have either of those paid options available, consider downloading an evaluation version of Windows 10 Enterprise, good for 90 days of unrestricted usage. You'll find details and download links at *https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise*.

New rules for activation

Product activation has been a part of Windows for the past 15 years, starting with Windows XP. Like its predecessors, Windows 10 requires activation as part of the license agreement. Typically, that process is automatic, with Windows checking a product key (or other authorized method) against an activation server to confirm that the installed version of Windows matches the product key, and the device is authorized to use the associated Windows license.

Windows 10 allows you to complete setup without entering a product key, for reasons I explain a bit later in this section. You can skip the product key and postpone activation, but doing so means certain features aren't available.

You can check the activation status of a Windows 10 device from Settings, Update & Security, on the Activation tab. Figure 3-3 shows this information for a system that was upgraded from Windows 8.1 Pro to Windows 10 Pro.

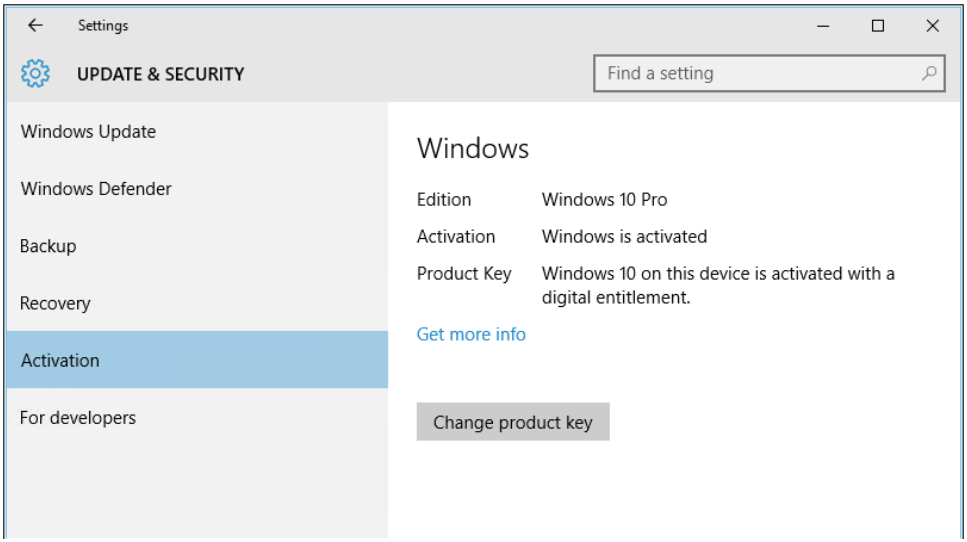


FIGURE 3-3 Windows 10 adds a new activation type called a *digital entitlement*, which doesn't require entering a product key for activation.

The concept of activation using a "digital entitlement" is new in Windows 10 and is created when you upgrade a PC that is currently running a properly activated copy of Windows 7 or Windows 8.1. If you start Setup from within that older Windows version, you do not need to enter a product key. Windows confirms that the underlying system is properly activated and creates a digital entitlement based on the unique hardware ID. (This behavior, of course, is predicated on the free upgrade offer that runs for one year after the initial release of Windows 10. Microsoft hasn't said what will happen on July 29, 2016, when that year is up.)

If you are using bootable installation media to perform a clean install on a PC that was previously upgraded and given a digital entitlement, you do not need to enter a product key during setup. After

the installation is complete, Windows contacts the activation servers and sends the hardware ID. (It's hashed, so it can't be used to identify the specific device.) When the server finds a stored digital entitlement for that hardware ID, the system is activated automatically.

If you are using bootable installation media to perform a clean install on a PC that has never been upgraded to Windows 10 and activated, you will need to enter a product key to activate the system. If your installation media is for Windows 10 version 1511 (build 10586) or later, you can enter a product key from a matching edition of Windows 7, Windows 8, or Windows 8.1. That option also results in a digital entitlement, and there's no further need to enter that product key.

You can see even more detailed activation information about the current Windows installation by opening an administrative Command Prompt window and entering the command **slmgr.vbs /dlv**. Figure 3-4 shows the extremely detailed output for the same system whose activation status was shown in Figure 3-3.

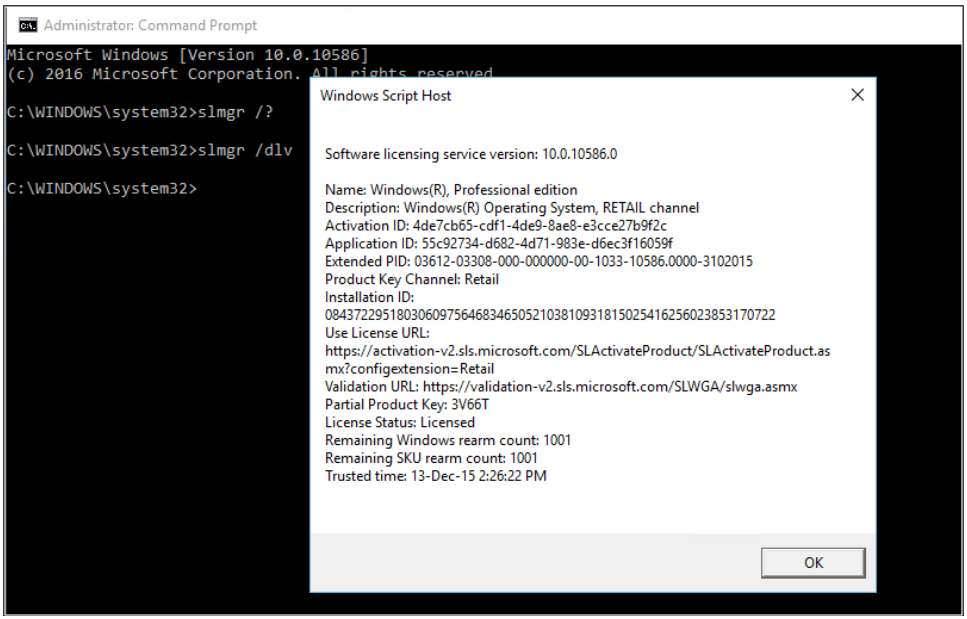


FIGURE 3-4 Use the Slmgr.vbs script to view the licensing status. (Try the –? switch to see all available options.)

Of course, other activation options are available as well:

- New PCs with Windows 10 preinstalled by the manufacturer are activated automatically by the OEM. The license information is coded into the firmware of the device, allowing reinstallation of the same Windows 10 edition without requiring a product key.
- Retail and OEM copies available through resellers include a product key that can be used to activate a specific Windows 10 edition that has never been activated.
- Volume License customers can use Multiple Activation Keys or a Key Management Server to activate properly licensed copies of Windows 10 Enterprise.

Windows 10 installation options

On a new PC that arrives with Windows 10 preinstalled, all the work of setup and activation is done at the factory. Your only responsibility is to go through the out of box experience (OOBE) by creating a new user account or signing into an existing one.

Upgrades and clean installs, by contrast, require a full setup, which proceeds in multiple phases. If you've made it this far into this book, I don't need to tell you how Windows Setup works. Instead, allow me to point out some interesting options you'll encounter along the way.

The simplest option by far is an in-place upgrade. For larger deployments, you can automate this process 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. (You can read more about that in Chapter 4.)

For a single device, using Windows Update to initiate the Windows 10 upgrade is a perfectly reasonable choice. During the preview period and for the first few months after the official release of Windows 10 in July 2015, Microsoft delivered a utility program called Get Windows 10 to all eligible PCs. This add-in placed an icon in the notification area offering the user the opportunity to reserve an upgrade. Beginning in late 2015, Microsoft began offering the upgrade option as an Optional update and plans to deliver the installer as a Recommended update beginning in early 2016.

Figure 3-5, for example, shows the update ready to run on a Windows 7 PC.

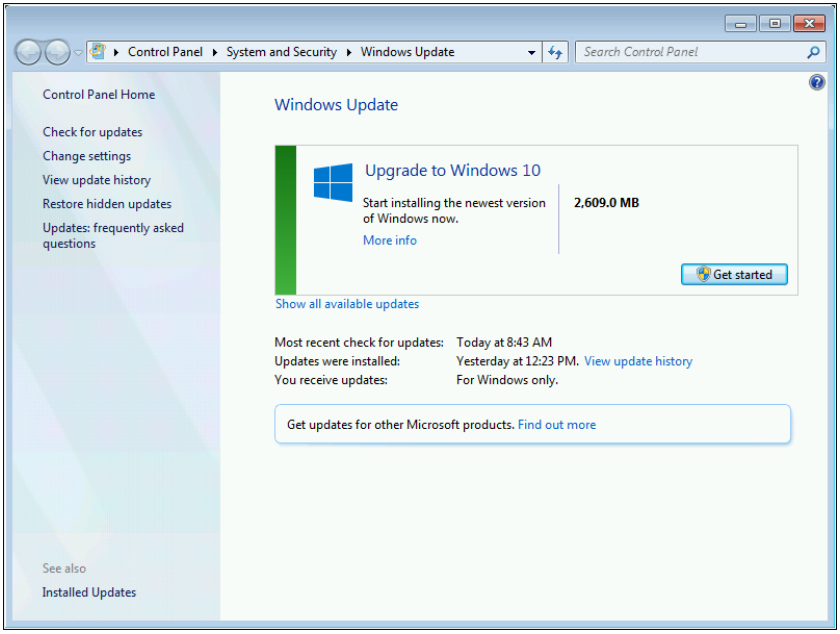


FIGURE 3-5 Despite the seemingly vast difference in version numbers, upgrades from Windows 7 to Windows 10 are fully supported through Windows Update.

When started from Windows Update, the upgrade process offers no options. All user accounts, desktop programs, apps, and data files are migrated in place. In general, an installation should take no more than a couple of hours, and it 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 run the encryption software again after the upgrade is complete. Check with the provider of any third-party encryption software before upgrading to ensure that the software is compatible with Windows 10.

You also can start an upgrade from Windows 7 or Windows 8.1 by using physical installation media or a mounted ISO file and double-clicking Setup from the installation source. Choosing this option kicks off the familiar Windows upgrade workflow. It also offers additional options at the start, as shown in Figure 3-6.

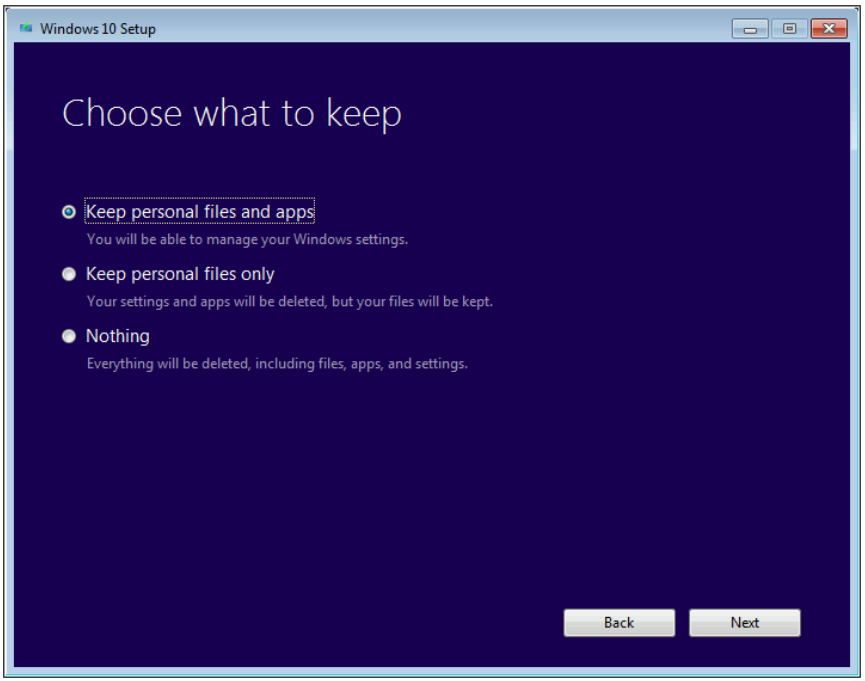


FIGURE 3-6 When you start an upgrade from an existing copy of Windows 7 or 8.1, choosing the last option on this list performs the equivalent of a clean install.

If your goal is to get a fresh start, with no previously installed apps or settings, you can choose the Keep Personal Files Only option. That preserves any data files (including downloads) but otherwise creates a default Windows 10 installation. Choosing the last option, Nothing, is the equivalent of a clean install.

Following that choice, setup runs through a series of operations and eventually ends up with the option to sign in to an account.

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 if you chose to keep them.

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. (You can read more about this feature in Chapter 9, "Backup, recovery, and troubleshooting options.") If 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 remove the Windows.old folder and its contents permanently.

Creating and managing user accounts

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 various cloud services. For Windows 10 devices, the most immediate benefits are the ability to purchase apps and digital content from the Windows Store and to sync settings and files (using OneDrive) between devices signed in with the same account. Depending on your network policy, you might be able 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 also 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.

Which account type should you use?

For evaluating Windows 10 in the enterprise, joining the device to a 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.

Signing in with an Azure AD account is appropriate for company-owned devices for which all management is done through Azure Active Directory.

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.

There's another advantage to that strategy as well: it allows you to turn on BitLocker encryption for supported test devices and save the recovery key to secure online storage using the alias you created.

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 3-7.

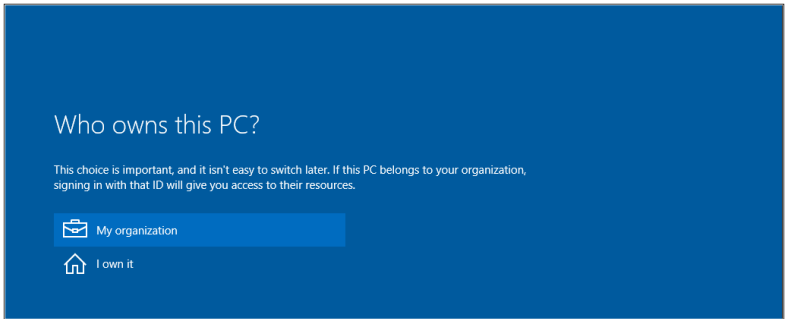


FIGURE 3-7 This option is visible only when performing a clean install of Windows 10 Pro.

Choosing the first option (My Organization) and clicking Next leads to a second page with options to join Azure AD or a domain, as shown in Figure 3-8.

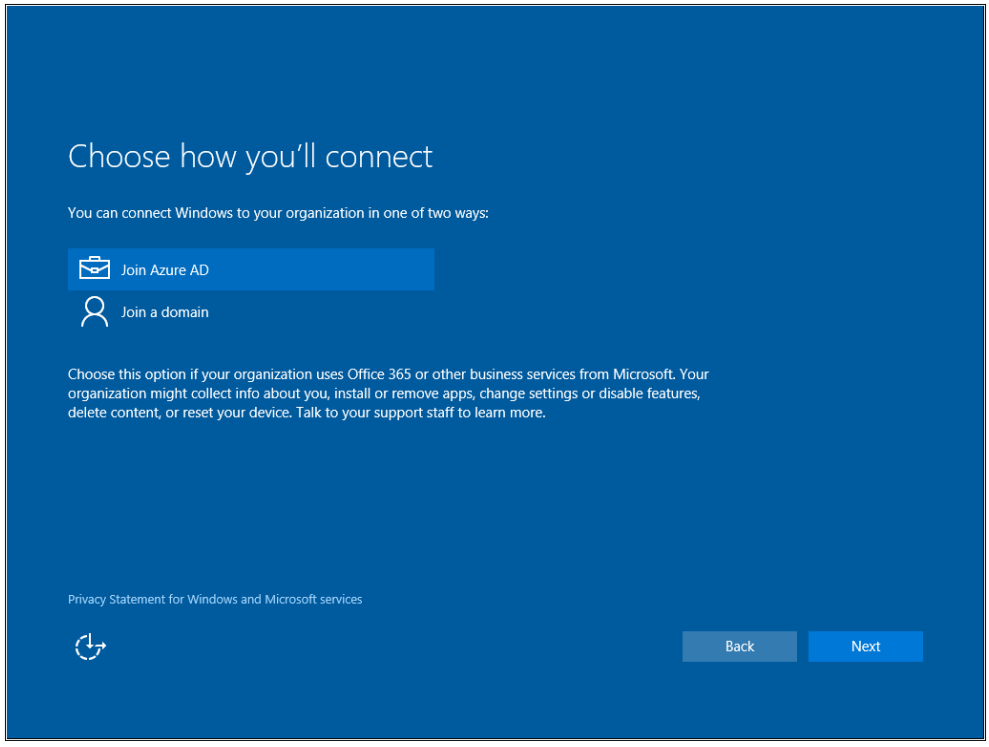


FIGURE 3-8 Choose the first option only if you want your Azure Active Directory administrator to manage your PC and its settings.

The first option works only with existing Azure Active Directory credentials, such as those linked to an Office 365 account. The second option, somewhat confusingly, assists you in creating a local account, which you can then join to your domain. Enter your workplace account in the box shown in Figure 3-9 *only* if you have Azure Active Directory credentials such as those with an Office 365 Business, Enterprise, or Education account and you want to use that account as the primary sign-in address rather than linking it as a work account.

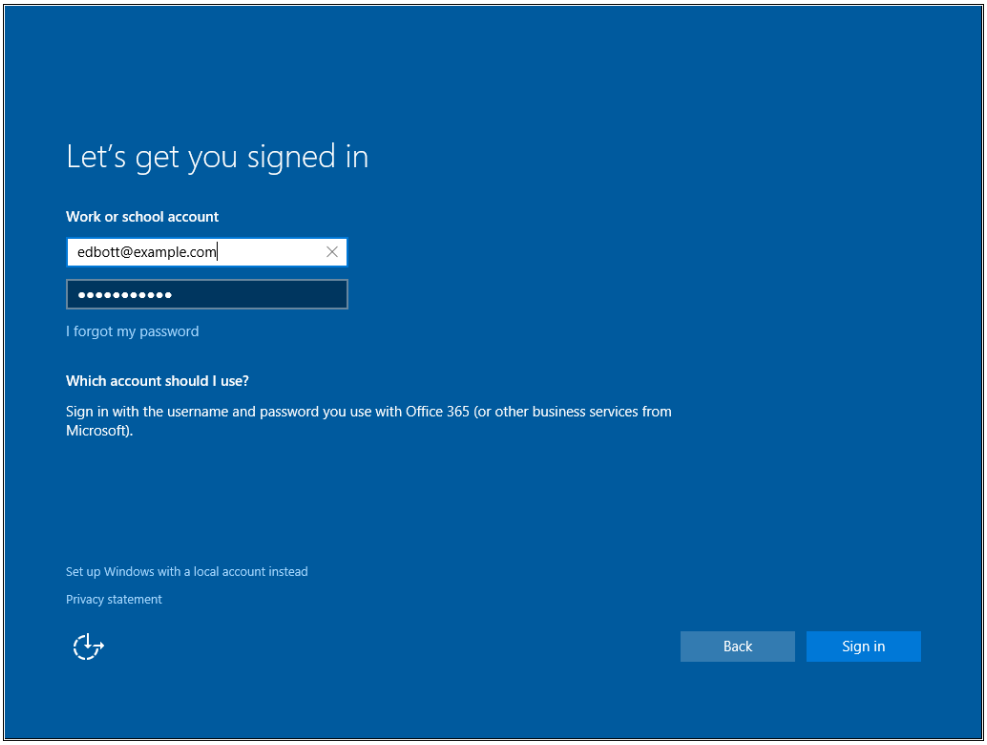


FIGURE 3-9 Enter your credentials here only if you have an Azure Active Directory account. If you plan to join a local Active Directory domain, choose the local account option instead.

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 3-10 shows what to expect.

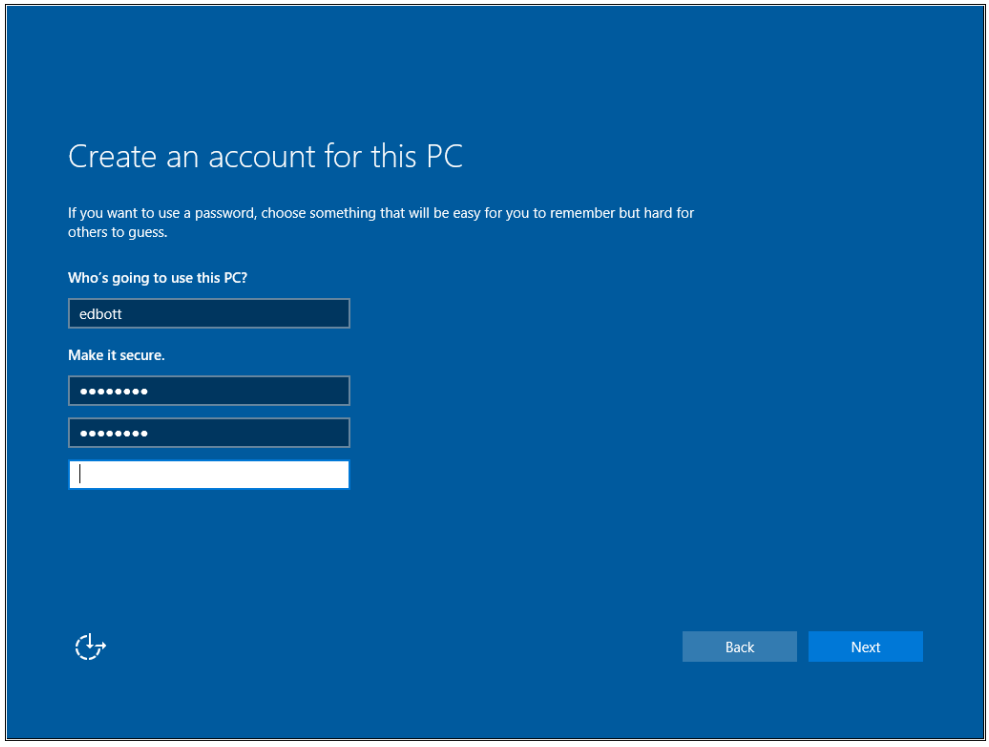


FIGURE 3-10 The option to create a local account is well hidden, but still available.

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 3-11 shows the available options.

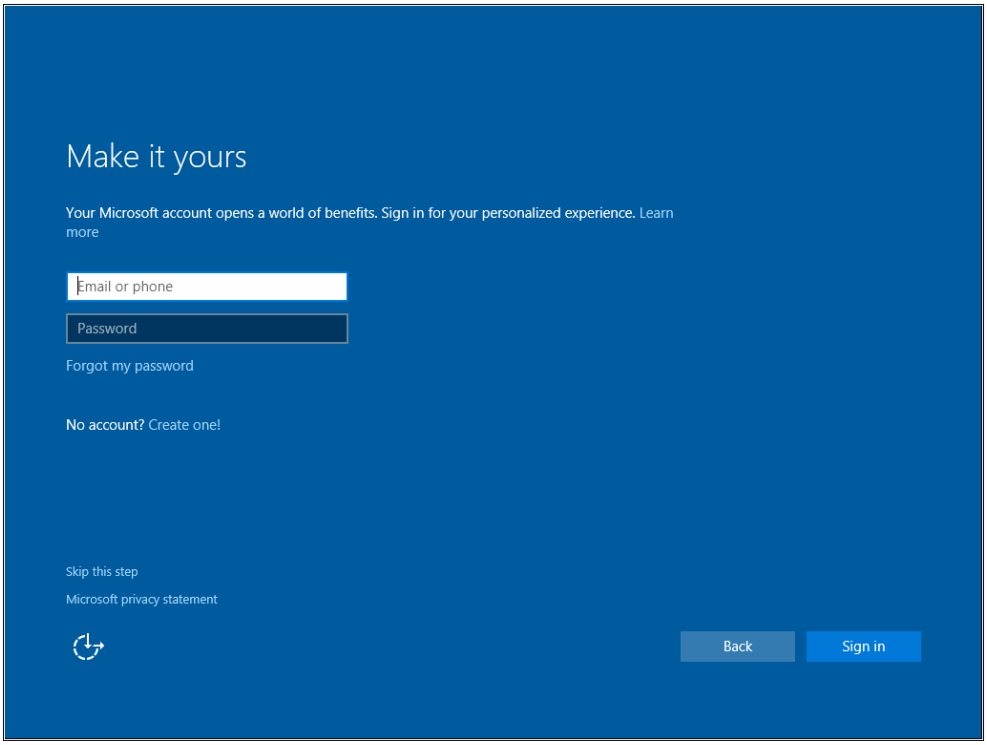


FIGURE 3-11 For most personal devices, using a Microsoft account provides significant benefits and is the best choice.

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 Outlook.com (formerly Hotmail) email, OneDrive, and Xbox services.

You can create a new Microsoft account from this screen 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 Skip This Step to open a local account using the form shown earlier in Figure 3-10.

CHAPTER 4

Deploying Windows 10 in the Enterprise

For IT pros, the job of deploying computing resources throughout an organization has historically been cyclical. A new wave of hardware becomes the catalyst for a major operating-system upgrade, and then the priority shifts to keeping that platform unchanged (except for security updates) for the sake of stability, often for years, until it's time for another wave of disruptive upgrades.

That rhythm changes, dramatically, with the arrival of Microsoft Windows 10. For enterprise customers who are currently standardized on Windows 7 or Windows 8.1, the first step is to move the organization to Windows 10. After that migration is complete, the next goal becomes finding an update rhythm that keeps the organization current with new features. If you're cautious, you might choose to remain several months behind the mainstream update cycle for consumers (the Current Branch), but that's a far cry from the status quo, which sees entire organizations working with operating-system versions that are five years old or more.

Microsoft's new development process, with freely available preview releases, makes it possible for you to get a head start on the process by testing your organization's applications against builds that are still months away from release. Instead of beginning your testing after a major release, you can be well along in the evaluation process by the time that release ships.

The deployment and management infrastructure you use on your enterprise network is also shifting to a more rapid development cadence, similar to that of Windows 10. And 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 a Windows 10 release later in 2016. In some cases, those new features might also require updates to current Windows Server versions.

Here's an example of just how quickly that development cycle is moving. In December 2015, Microsoft released a new version of System Center Configuration Manager (SCCM), with support for deploying, updating, and managing Windows 10. Less than two weeks later, the same team released a preview update with important new features. Recent updates to older editions of the System Center infrastructure also include support for Windows 10.

That's a rapidly changing landscape, which is why this chapter emphasizes getting familiar with those new deployment and management tools as part of a pilot program.

Deployment scenarios

As I mentioned at the beginning of this chapter, the dawn of the "Windows as a Service" era requires a change in the deployment rhythm to which you've probably grown accustomed.

Traditionally, you've had two Windows deployment options:

- The "wipe and load" scenario starts with a standard image, built to work with company-owned hardware and apps. Using deployment tools, you completely replace the existing image on a new PC (or one that needs to be reimaged for support reasons or as part of the reassignment process to a new employee).
- In-place upgrades have historically been shunned by IT pros, who can usually recite horror stories of failed upgrades. Beginning with Windows 8, however, the upgrade process was completely redesigned to make it fast and extremely reliable, with easy rollback capabilities for the rare instances in which something goes wrong.

Windows 10 adds a third deployment option with the ability to create provisioning packages that can transform an existing image on a new PC. This option is still in its early stages but has great potential for future deployments.

Through the years, many IT pros responsible for large Windows-based networks have settled on the wipe-and-load option as the default solution for new operating-system deployments. That option works fine for every-three-year deployments and for occasionally provisioning new devices. It's also a perfectly reasonable way to make the transition from your current Windows 7 or Windows 8.1 base to Windows 10, especially if you're introducing new apps as part of the operating-system upgrade.

But that option isn't cost-effective when the operating system is receiving multiple upgrades per year. Building new images every four to six months and managing data migration and application reinstallation for multiple enterprisewide deployments every year isn't necessary.

In the "Windows as a Service" era, the far more reasonable alternative is the in-place upgrade. That's exactly what Microsoft did when deploying Windows 10 to its tens of thousands of employees worldwide. The corporate deployment effort used the Operating System Deployment (OSD) feature in System Center 2012 R2 Configuration Manager SP1 to offer automated in-place upgrades to users running Windows 7, Windows 8, and Windows 8.1.

Microsoft's deployment offered two options. Users were allowed to initiate the upgrade from the Software Center at a time that was convenient to them. Figure 4-1 shows how this user-initiated ("pull") option works.

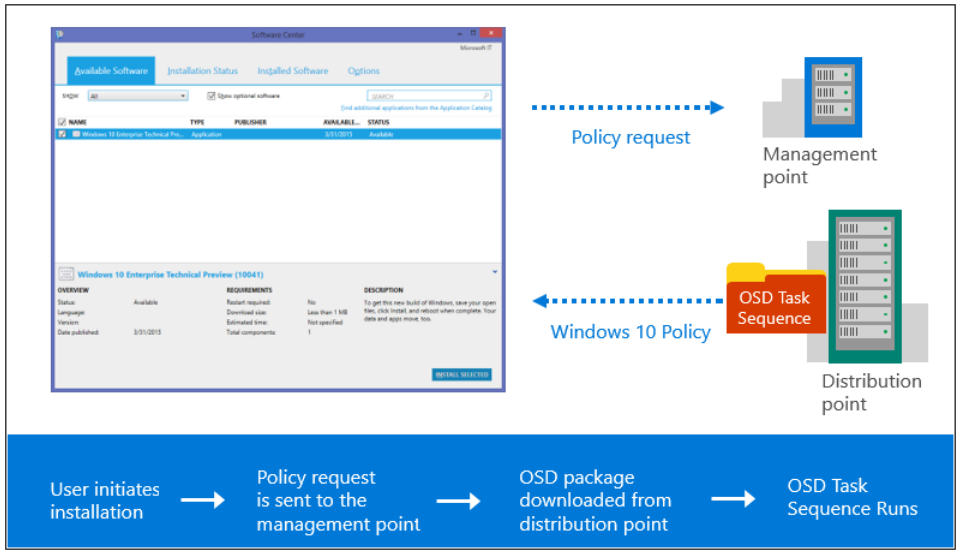


FIGURE 4-1 Microsoft IT used this process to allow users to choose when they wanted to begin the upgrade process to Windows 10.

These user-initiated upgrades used the same Windows setup engine found in consumer versions of Windows 10, which performs a series of compatibility checks to avoid known issues with apps, drivers, BIOS versions, and other issues that could prevent installation from completing successfully. Assuming the target system passed those checks, the installer performed the upgrade.

Figure 4-2 shows the OSD task sequence as it appeared in Configuration Manager. The process for building this sequence is wizard-driven, with options for configuring tasks to run before the upgrade and to perform actions in the event of a failure.

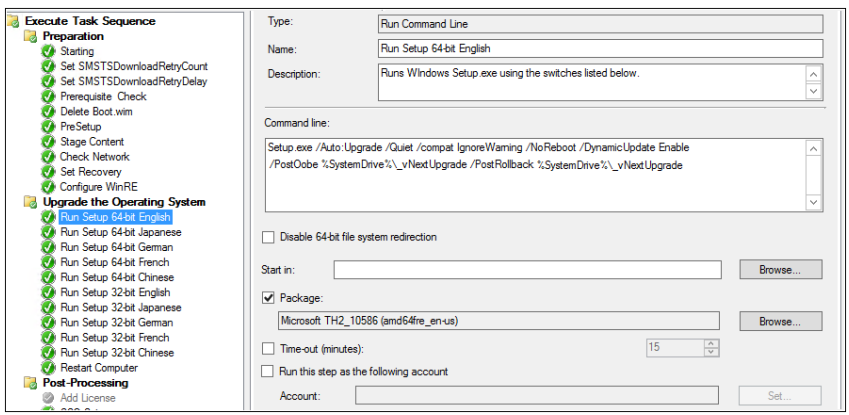


FIGURE 4-2 Use a wizard to build a sequence of tasks that allows you to deploy a Windows 10 upgrade using "pull" or "push" techniques.

The installation files were delivered over the corporate network, with upgrade-specific content coming from the public Windows Update servers.

For employees who hadn't upgraded by a specified date and time, Microsoft IT was able to "push" the upgrade package out as a scheduled activity. Typically, these enforced upgrades were scheduled on Tuesdays and Thursdays during the lunch hour. By the time users returned from lunch, they were able to complete the brief final setup steps and begin using Windows 10.

Note For a detailed discussion of how Microsoft IT performed the Windows 10 upgrade, download and read the white paper (in Word .docx format) from *https://www.microsoft.com/en-us/download/details.aspx?id=50377*.

The result? Approximately 85 percent of the user base was upgraded within four weeks. By contrast, the Windows 7 deployment in 2009, which used the more traditional custom imaging solution and task sequence steps, took nearly a year to move 80 percent of employees from their previous operating system.

Enterprise deployment tools: An overview

Microsoft's enterprise deployment tools span all the scenarios I discussed previously in this chapter. As with so many Windows-related tasks, you have almost an embarrassment of riches to choose from in terms of tools. There are few right or wrong choices, although there are some strongly suggested best practices. In general, you should choose the tools that work best with your existing or planned infrastructure.

Although it's possible to use these tools individually, they're most effective when you create a solution using a management tool such as Microsoft Deployment Toolkit (MDT) or Microsoft System Center Configuration Manager.

Microsoft Deployment Toolkit 2013

As of this writing (early 2016), Microsoft Deployment Toolkit 2013 Update 2 is the most recent version available. (For full details about MDT, see *https://technet.microsoft.com/en-us/windows/dn475741.aspx*. The download link is here: *https://www.microsoft.com/en-us/download/details.aspx?id=50407*.)

Don't let the older date fool you. This release supports deployment and upgrade of all Windows 10 editions, including the Enterprise LTSB and Education editions. It also supports the Windows ADK for Windows 10 and includes the latest task-sequence binaries for integration with System Center 2012 R2 Configuration Manager SP1 and later for Windows 10 deployments.

Figure 4-3 shows a custom image in the process of being created, with the option to use custom drivers rather than applying drivers using Plug and Play.

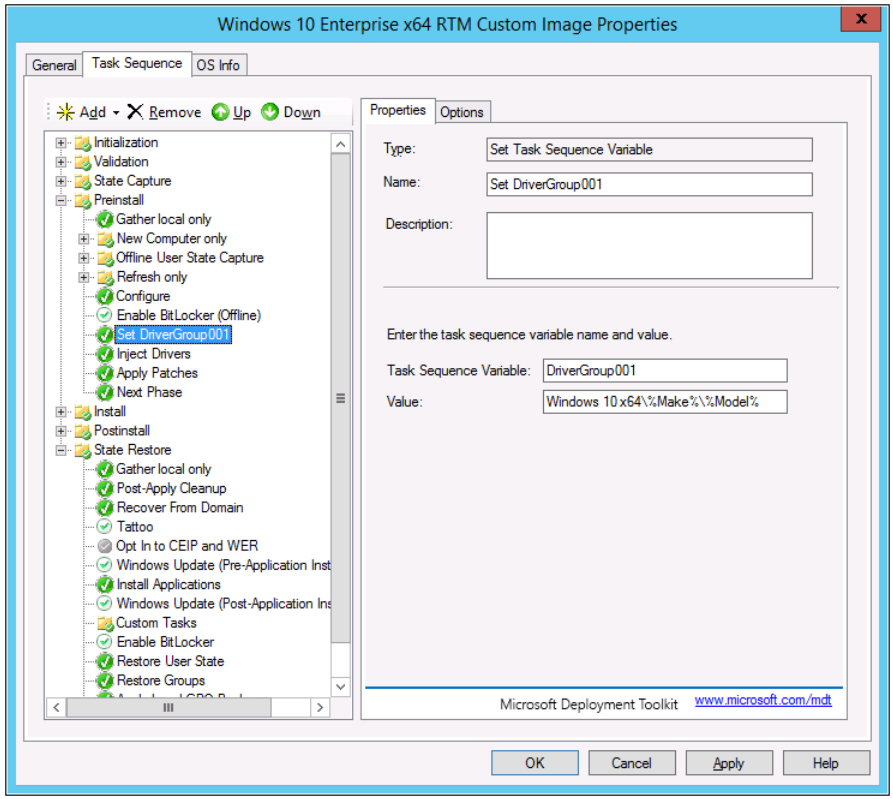


FIGURE 4-3 The Microsoft Deployment Toolkit offers the ability to build task sequences that can apply an operating-system upgrade to PCs on your network.

Windows Assessment and Deployment Kit

The Windows Assessment and Deployment Kit (ADK) for Windows 10 contains essential tools for automating a large-scale deployment of Windows 10. Regardless of whether you use MDT or SCCM as your deployment manager, you'll need parts of the ADK to complete the deployment.

If you've used the ADK with previous Windows deployments, you should definitely evaluate the latest version. The new ADK includes some significant improvements:

- **Provisioning support** Using this capability, you can create special packages for customizing 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 and there's 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.

If you're familiar with previous releases of the ADK, you'll find some interesting additions in this release, including the Windows Imaging and Configuration Designer, the Windows Assessment Toolkit, the Windows Performance Toolkit, and several new and improved deployment tools. The latter group includes an updated Windows Driver Kit (WDK), Hardware Lab Kit (HLK), Software Development Kit (SDK), and Assessment and Deployment Kit (ADK).

Beginning with this release, the Windows ADK documentation is available on the MSDN Hardware Dev Center, at *https://msdn.microsoft.com/library/windows/hardware/dn927348(v=vs.85).aspx*.

Figure 4-4 shows the options available during installation of the Windows ADK.

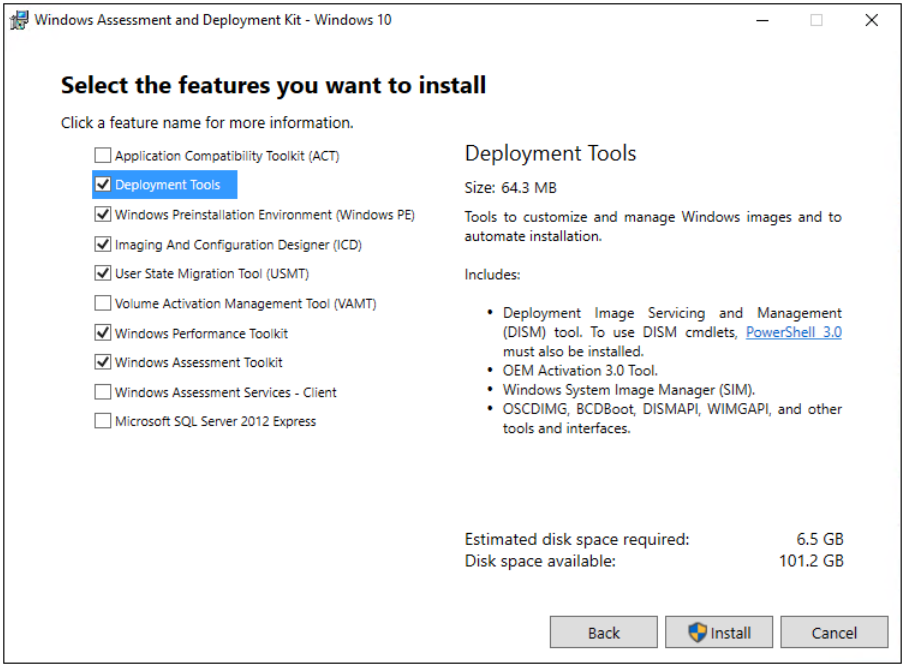


FIGURE 4-4 The individual options available with the new Windows Assessment and Deployment Kit are designed for IT pros and hardware manufacturers.

The following list describes some crucial pieces of the ADK and how they're useful for deployment tasks, including management of custom images:

- **Deployment Image Servicing and Management (DISM)** This tool is used to mount and service Windows images. Using this tool, you can customize an offline image and add drivers, enable or disable Windows features, add or remove packages and Universal Windows apps, and upgrade the Windows edition. DISM also includes PowerShell cmdlets.
- **Windows Preinstallation Environment (Windows PE)** This is the (very) small operating system that typically resides on a boot device such as a USB flash drive or DVD. It's used to boot a computer that doesn't already have a Windows version installed. Windows PE is also used for data recovery and repair operations.
- **Windows System Image Manager** Use this tool to create and customize answer files that change Windows settings and run scripts during installation.
- **Windows Imaging and Configuration Designer (Windows ICD)** New in Windows 10, this tool allows you to create provisioning packages that can be used to customize Windows 10 devices of any type without re-imaging. You also can use it to build and deploy an image for Windows 10 desktop editions. I discuss this in more detail later in this section.
- **User State Migration Tool (USMT)** The purpose of this venerable tool is to migrate user profiles from an old operating system to a new one, typically as part of a wipe-and-load deployment.
- **Windows Assessment Toolkit and Windows Performance Toolkit** These tools are intended primarily for OEMs to assess the quality and performance of systems or components.

Windows ICD is worth a deeper discussion (and a longer look in your evaluation). As Figure 4-5 shows, the starting point follows the same design principles as modern apps, with a tile-based layout.

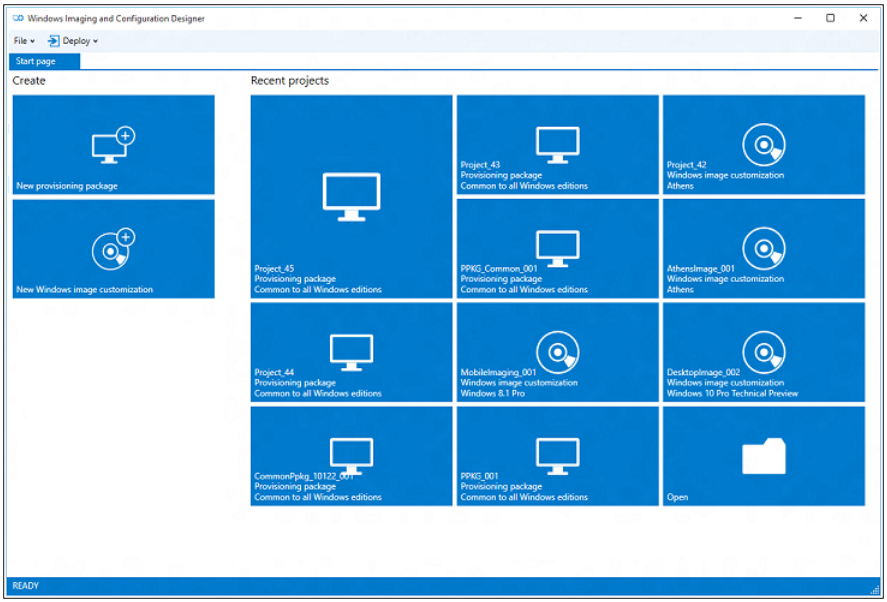


FIGURE 4-5 The Windows Imaging and Configuration Designer (ICD) allows you to create provisioning packages that can be used to customize an existing image or can be applied to a running system.

Using the Windows ICD requires that you install additional features from the ADK, including the Deployment Tools collection, Windows PE, and the USMT.

On the Customizations page, shown in Figure 4-6, you can define the settings in a provisioning package; you can also add applications, drivers, features on demand, language packages, and Windows updates.

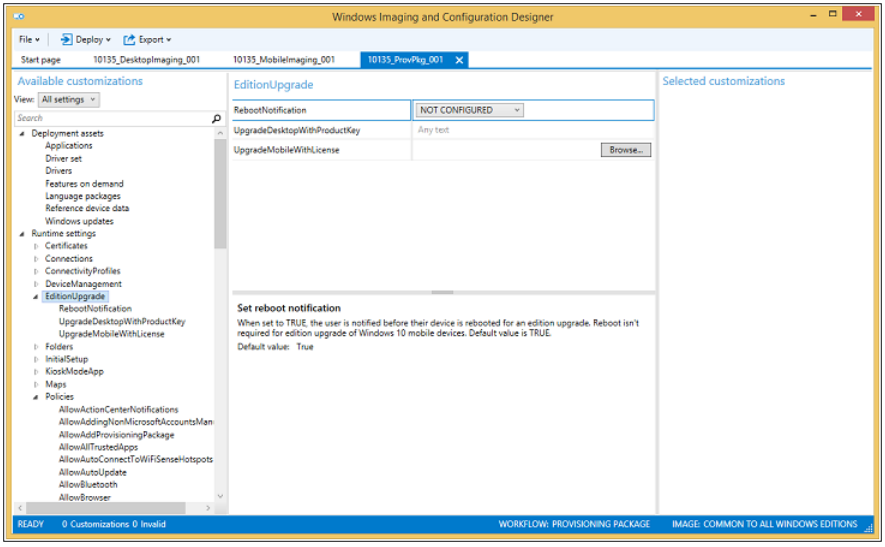


FIGURE 4-6 The Windows ICD customization options are extensive, including the ability to upgrade an edition as part of the process of applying the package.

CHAPTER 5

Security and privacy 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.

And in an age where a new data breach seems to make the news every week, concerns over privacy are increasingly common. To make "Windows as a Service" possible, Windows 10 collects diagnostic and analytic data from PCs, including information about device capabilities, error reporting, and usage statistics.

In this chapter, I offer an overview of the multiple layers of security in Windows 10 and detail your privacy options for individual PCs and managed networks.

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, transforming 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, for example—you might find yourself in the crosshairs, with the attackers counting on being able to work their way up 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 webpages or documents attached to an email message, 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 that supports high-grade encryption and prevents tampering with or unauthorized export of certificates and encryption keys. The TPM might be implemented as a standalone microcontroller or included as part of another component, such as a network module or a system on chip (SoC) integrated circuit. The TPM performs cryptographic operations and stores 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 of 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, 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 easy-to-use multifactor authentication schemes. (I discuss these features in more detail later in this chapter, in "Securing identities.")

With the appropriate hardware support, Windows 10 can also take advantage of virtualization technologies to isolate core operating system services so that they are protected from attackers even if the Windows 10 kernel is compromised. The Hypervisor Code Integrity service ensures that all code running in kernel mode, including drivers, is working as it was designed. In addition, a new feature called Credential Guard isolates the Local Security Authority (LSA) service to protect domain credentials as well as those stored within Credential Manager.

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 5-1 shows how the boot process works in Windows 8.1 and Windows 10.

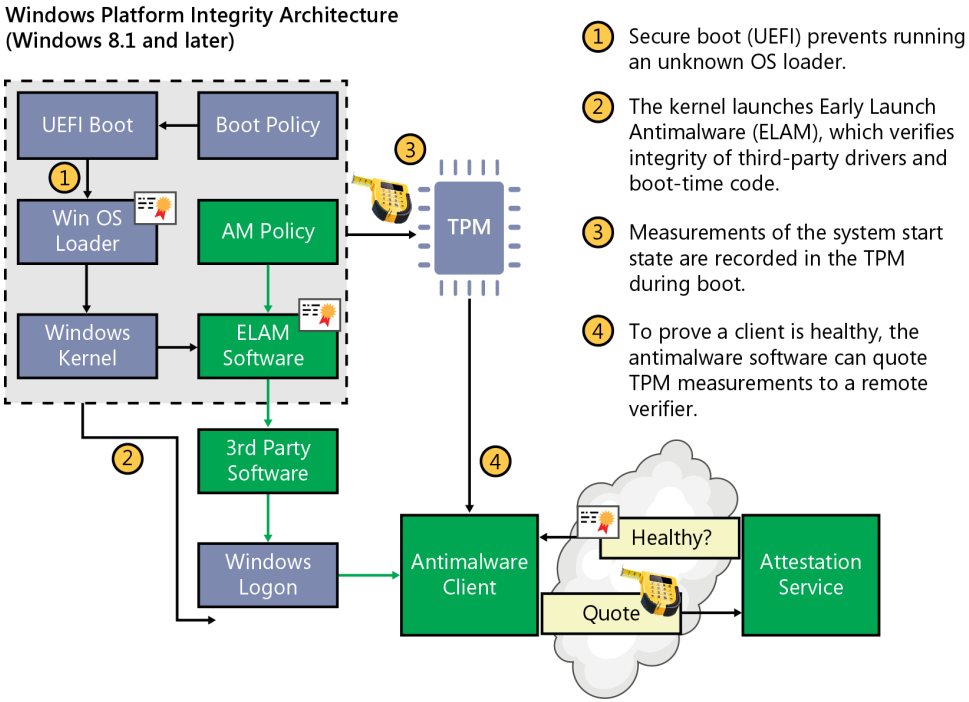


FIGURE 5-1 Security features in Windows 10, enabled on modern hardware, help prevent malicious software from tampering with the boot process.

Here is a description of the four numbered elements shown in Figure 5-1:

- **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 only by using 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 Windows 10 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 Windows 10, 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 has introduced a new public API that allows 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 5-2 shows how PPCH works with the cloud-based Microsoft Intune management service.

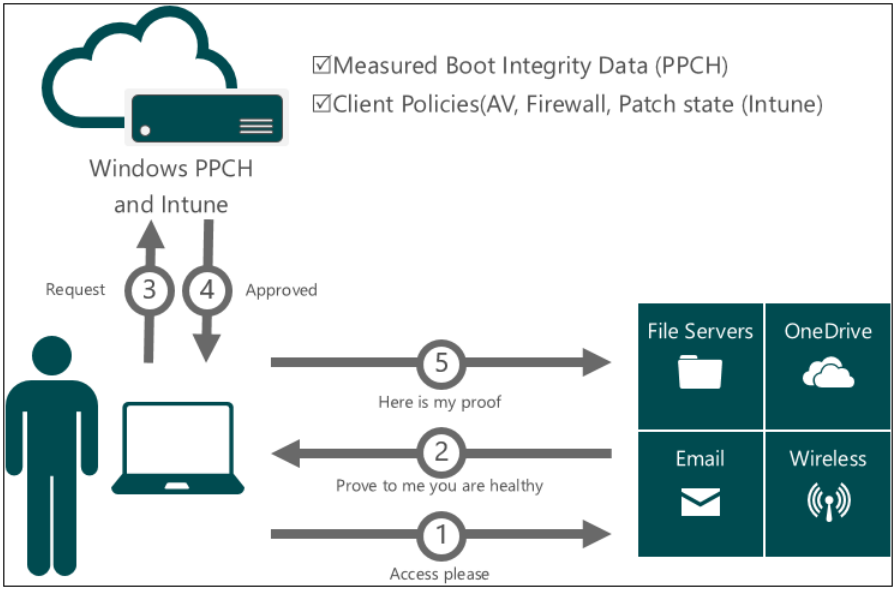


FIGURE 5-2 PPCH can check remote devices for signs of tampering and ensure compliance with policies, controlling access to networks and services based on the results.

Locking down enterprise PCs with Device Guard

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, the only programs allowed to run are those that are trusted, and even programs that bypass other security layers by exploiting a zero-day vulnerability are thwarted.

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 by antitampering features.

To deploy Device Guard, your hardware and software must meet the following requirements:

- The device must be running Windows 10 Enterprise.
- The UEFI firmware must be version 2.3.1 or higher, with Secure Boot enabled and a secure firmware update process. For additional security against physical attacks, Microsoft recommends locking firmware setup to prevent changes in UEFI settings and to block startup using other operating systems.
- Virtualization-based security features require Hyper-V, which runs only on 64-bit PCs that support Intel VT-x or AMD-V virtualization extensions and Second Level Address Translation.
- A VT-d or AMD-Vi input/output memory management unit is required to provide additional protection against memory attacks.
- A Trusted Platform Module is optional, but highly recommended.

In addition to enabling Hyper-V, you must also enable the Isolated User Mode feature, as shown in Figure 5-3.

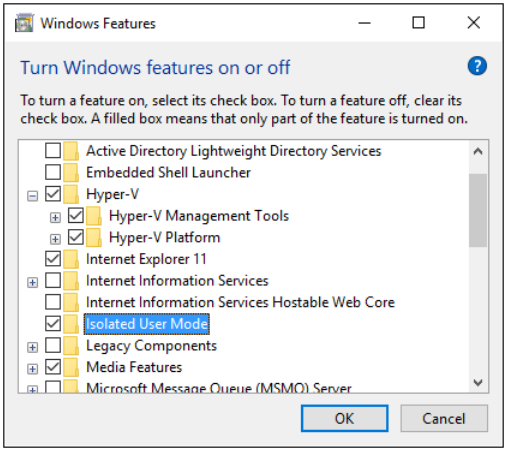


FIGURE 5-3 Enabling the Isolated User Mode feature is a prerequisite to configuring Device Guard mode.

You can also configure these features manually using Windows PowerShell cmdlets or Deployment Image Servicing and Management.

When Configuring Device Guard, you can specify both Universal Windows Platform (UWP) apps and classic Windows desktop programs as trusted. This trust relationship requires that the apps or classic programs be signed using a digital certificate that your organization defines as trustworthy. For UWP apps, the Windows Store publishing process uses compatible signatures that can be verified by Microsoft's certificate authority (CA) or your organization's CA. Independent software vendors can sign Windows desktop apps using certificates, a public key infrastructure, or a non-Microsoft signing authority that is then added to the list of trusted signers.

Microsoft has also announced its intention to introduce a secure Web service that software developers and enterprises can use to sign classic Windows apps.

The final step in Device Guard is to create a Code Integrity policy, which consists of a binary-encoded XML document that includes configuration settings for both the User and Kernel modes of Windows 10 Enterprise, along with restrictions on Windows 10 script hosts. This policy restricts what code can run on a device.

With those configurations and policies enabled, you're ready to deploy Device Guard. For a comprehensive deployment guide, see the detailed write-up at *http://bit.ly/DG-deploy*.

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 (provided that the underlying hardware supports it). That's a significant change from previous versions, which traditionally reserved that feature for business/enterprise editions. Encryption is enabled by default on Windows 10 Home devices that include a TPM. Pro and Enterprise editions can be configured with additional BitLocker protection and management capability.

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 for an unmanaged system is automatically stored in the user's OneDrive storage in case an administrator needs to recover the encrypted data later (in the event of a hardware failure, for example, or a complete reinstall of Windows 10). If you need to reinstall the operating system or mount the drive on 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 store encryption keys using Active Directory (for data recovery 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). 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 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 major 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 Microsoft Passport, bringing identity protection to a new level. This feature replaces passwords with strong two-factor authentication that uses an enrolled device as one factor and biometric information (Windows Hello) or a PIN as the second factor. The associated services are available on all Windows 10 editions, as you can see from Figure 5-4, and are enabled as needed.

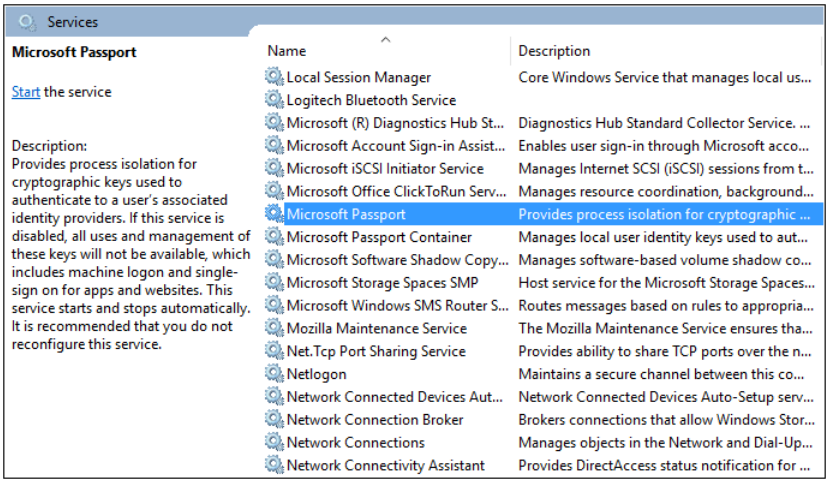


FIGURE 5-4 These two Microsoft Passport services are key to a revolution in identity that eliminates the need for regular entry of passwords on compatible devices.

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 Microsoft account, an Active Directory account, a Microsoft Azure Active Directory (AD) account, or a non-Microsoft service that supports Fast IDentity Online (FIDO) authentication. (The FIDO standard is supported by many banks and existing authentication providers such as RSA.) Once enrolled, the device itself becomes one of the factors required for authentication. The second factor is a PIN (the default option) or, on systems with appropriate hardware support, biometric authentication, such as fingerprint recognition, facial recognition, or an iris scan.

Existing fingerprint readers work with the new authentication measures. For facial recognition, new hardware that includes infrared capabilities (for antispoofing purposes) is required. Microsoft's Surface Pro 4, for example, includes a built-in camera that is compatible with Windows Hello; a Type Cover with integrated fingerprint reader is also available as an option. After the initial setup, you can configure a Surface Pro 4 to unlock automatically when it recognizes the enrolled user's face, as shown in Figure 5-5.

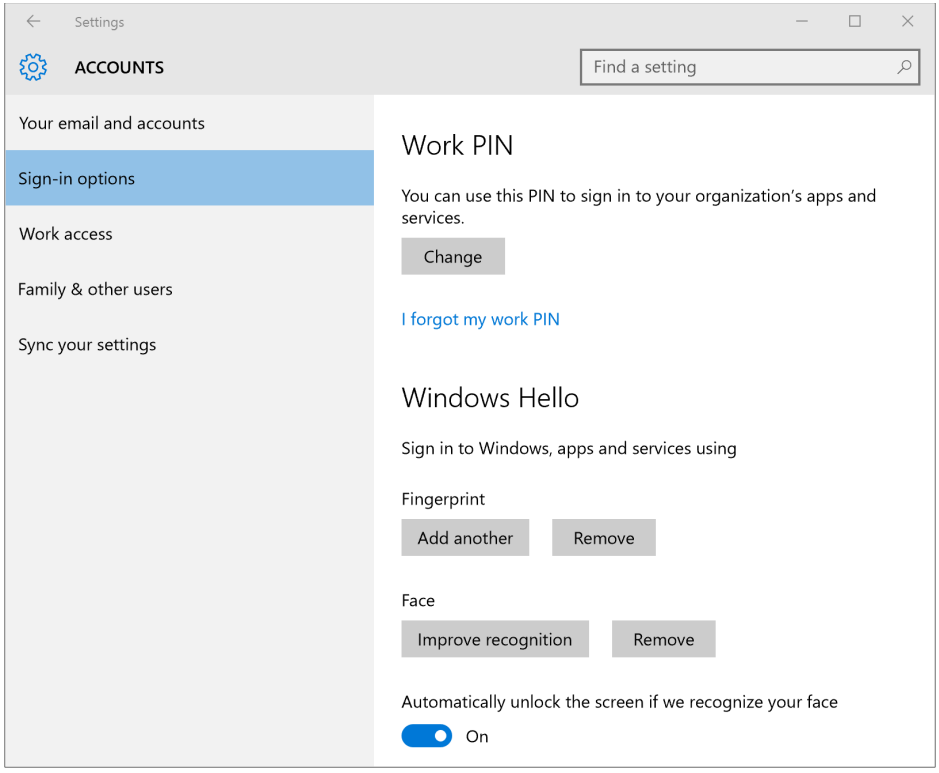


FIGURE 5-5 Biometric authentication is built into Windows 10. On this Surface Pro 4, both a fingerprint reader and facial recognition are set up, with the front-facing camera configured to automatically unlock the device.

Windows 10 supports existing fingerprint readers for authentication. Windows 8.1 introduced a systemwide, end-to-end process for enrolling fingerprints for authentication. This experience is available in Windows 10 as well. After setting up biometric proofs of identity, those methods are available for sign-in and for any activity that requires authentication, as shown in Figure 5-6.

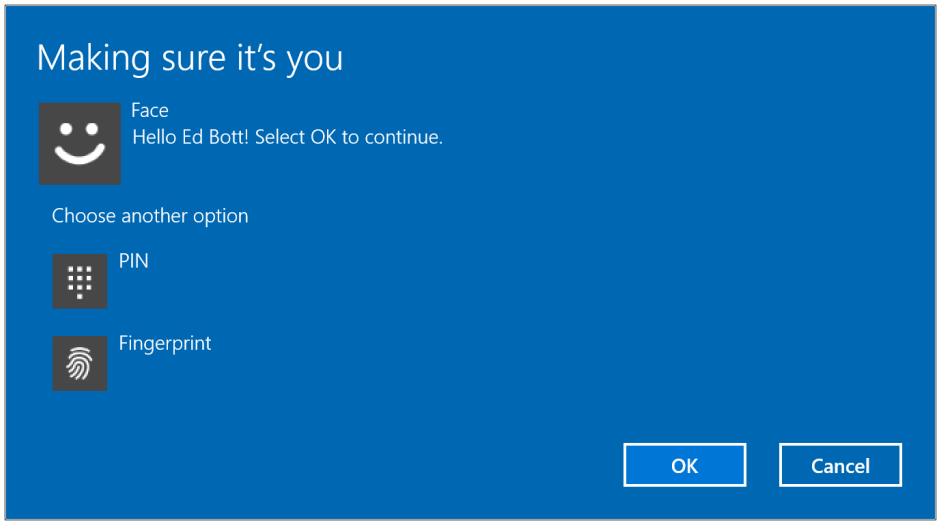


FIGURE 5-6 When Windows Hello biometric authentication is set up, any activity that would require a password can be unlocked using a fingerprint or facial recognition on an enrolled device.

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. The enrollment process doesn't require that the device be domain joined, making this feature especially useful in Bring Your Own Device (BYOD) scenarios.

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.

In domain settings, you can use Group Policy to implement Microsoft Passport in the workplace. The policy settings are available in Computer Configuration > Policies > Administrative Templates > Windows Components > Microsoft Passport for Work. You can use the available settings to enable or disable Passport for Work with domain passwords, to allow or prohibit hardware security devices and biometric authentication, and to define PIN complexity requirements.

You can also enable Passport for Work using mobile device management (MDM) software. These MDM policy settings use the PassportForWork configuration service provider (CSP); a description of this service is available at *http://bit.ly/PassportForWorkCSP*.

Your users can enroll multiple devices with these new credentials. Microsoft Passport also enables Windows 10 Mobile devices to be used as a remote credential when signing into Windows 10 PCs.

During the sign-in process, the Windows 10 PC can connect using Bluetooth to access Microsoft Passport on the user's Windows 10 Mobile device, which is generally in the user's possession. The combination 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, keyloggers, or other attacks.

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 antispyware 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, described earlier in this chapter, 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 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.

Microsoft's technological investment in the SmartScreen technology has been built up over many years. The data comes from various sources, including Microsoft Edge and Internet Explorer, Bing, Windows Defender, and the Enhanced Mitigation Experience Toolkit (EMET). Collectively, this information powers an online service that is able to effectively block many drive-by attacks in the browser. When your users visit a webpage that SmartScreen has identified as having been compromised by an exploit kit, for example, the page contents are blocked with a message like the one shown in Figure 5-7.

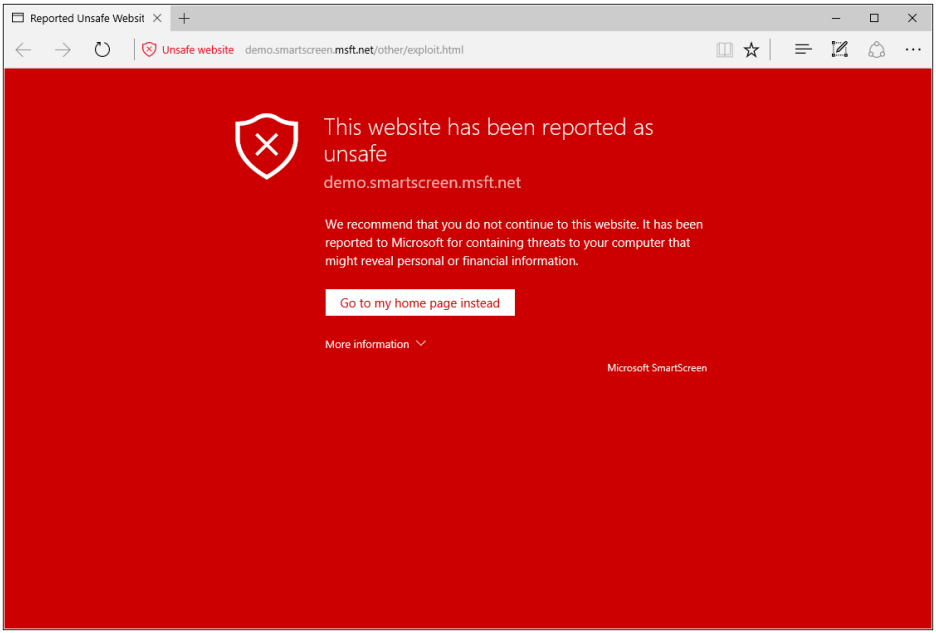


FIGURE 5-7 SmartScreen protection, which is built into both Internet Explorer and the Microsoft Edge browser, is shown here blocking a demo page that mimics a site compromised by malware.

(For live demonstrations of how SmartScreen features work, inside and outside the browser, visit *http://demo.smartscreen.msft.net/*. These demo pages contain no harmful code and are useful for teaching users how to recognize and respond to these important warnings.)

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, similar to the one shown in Figure 5-8.

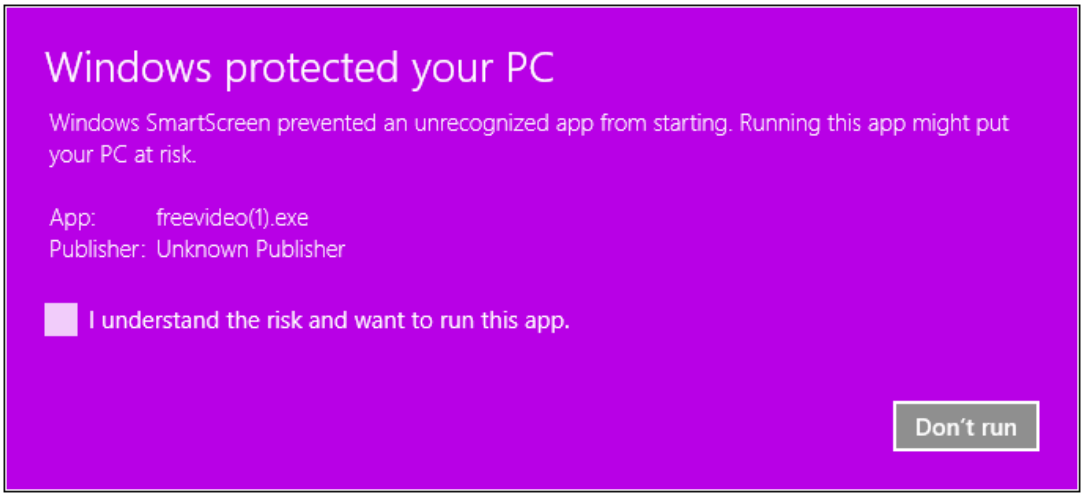


FIGURE 5-8 SmartScreen protection works even with non-Microsoft browsers. This warning message appears when you download and attempt to run an executable program that has been flagged as possibly suspicious.

Local administrators can override SmartScreen blocks 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 settings to do so.

Managing privacy

As Windows has evolved over three decades, its connections to online information sources have grown ever tighter. That information flow works in both directions, with Windows apps able to send and retrieve files, email messages, and other data using systemwide connections to cloud-based services. Windows itself regularly gathers diagnostic information as an essential element of the "Windows as a Service" model.

Windows consumers and small businesses can exercise control over this information flow using options in the Privacy section of the Settings app, as shown in Figure 5-9. Domain administrators can use Group Policy to impose additional controls over privacy settings.

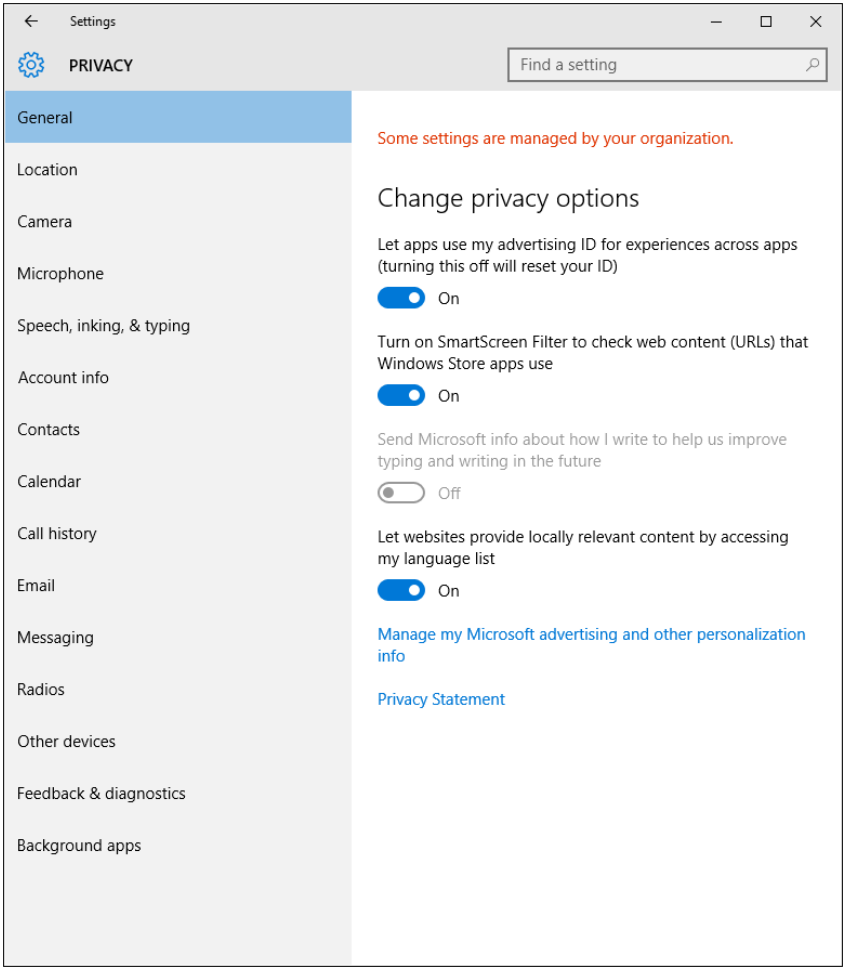


FIGURE 5-9 Privacy options are organized into groups and accessed via the Settings app; note that administrators can manage privacy settings using Group Policy or mobile device management software.

Each category contains a link at the bottom that leads to Microsoft's unified privacy statement, which covers Windows and most Microsoft services. (Office 365, Azure, and other commercial services are covered by separate statements.) Several of the Privacy settings also contain a link to an FAQ page that details the type of data collected and how it is stored and used.

Most of the categories are straightforward, with both general and app-specific options. For example, the Camera section, shown in Figure 5-10, offers a global Let Apps Use My Camera option as well as sliders for allowing individual apps to use a camera.

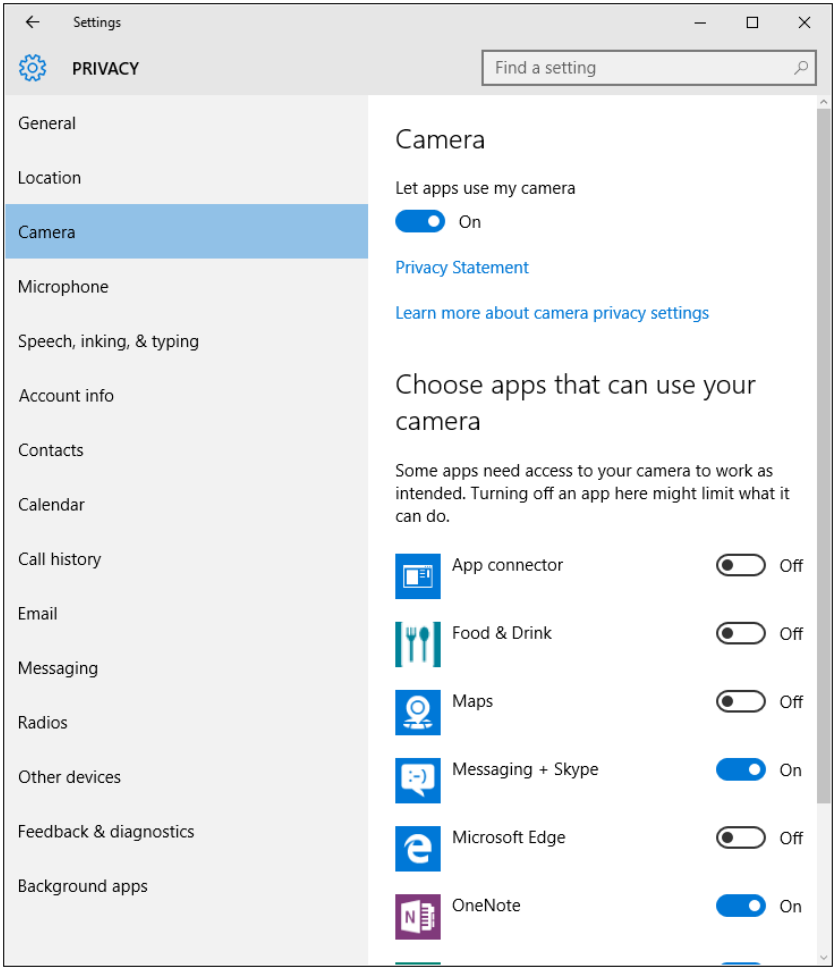


FIGURE 5-10 Many Privacy settings offer both global options and app-specific controls. Using the Camera pane, for example, you can disable camera access for all apps or set access for each app separately.

Historically, enterprise administrators have been especially cautious about settings for error reporting and other diagnostic information. Detailed crash dumps, for example, sometimes include the contents of memory at the time of the crash. Those details are helpful to an engineer trying to find clues as to the cause of the crash, but they can also contain portions of documents that might, in turn, contain confidential information.

The Feedback & Diagnostics section under Privacy settings, shown in Figure 5-11, offers three settings under the Diagnostic And Usage Data heading.

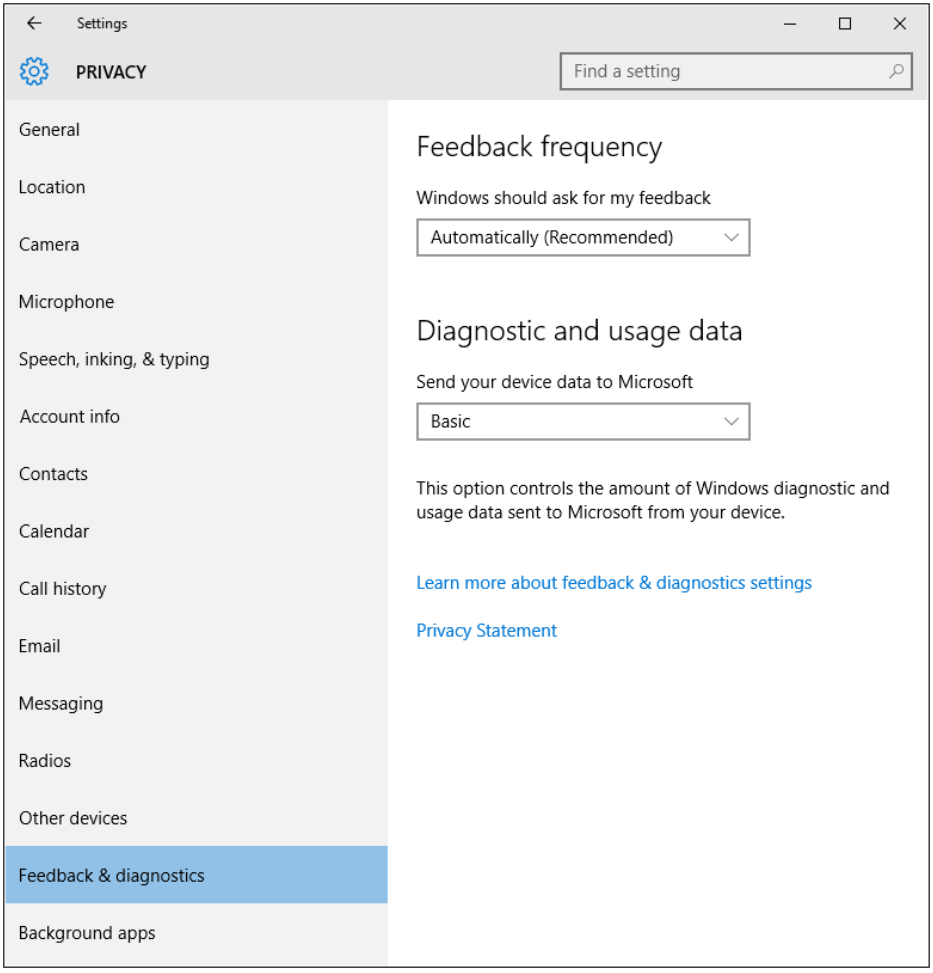


FIGURE 5-11 The Feedback & Diagnostics section of Privacy settings allows you to control the amount of diagnostic data sent to Microsoft. Windows Enterprise and Education editions offer one additional option.

Microsoft goes to great lengths to anonymize the information sent as part of this program (sometimes referred to internally as *telemetry*), stripping it of personal details and using a unique device ID that allows analysts to determine whether repeated instances of a particular problem report are from multiple devices or instead represent multiple faults in an individual device.

By default, this option is set to Full, allowing Microsoft engineers to see details about how you use Windows features and apps as well as advanced error-reporting options that might include user content. This setting cannot be changed for devices that are enrolled in the Windows Insider program. The Enhanced option contains fewer details but still contains the potential to leak information from personal documents.

Changing this setting to Basic offers minimal diagnostic information to Microsoft, including the capabilities of the device, what is installed, and whether Windows is operating correctly. This option also turns on basic error reporting.

IT pros have one additional option for configuring whether and how telemetry data is collected and shared with Microsoft. The details of this policy are available at *http://go.microsoft.com/fwlink/p/?LinkId=627097*.

This fourth level, called Security, is available on Windows 10 Enterprise, Windows 10 Education, Windows 10 Mobile Enterprise, and IoT Core editions. Setting the telemetry level to Security is accomplished through Group Policy or mobile device management policy or by manually changing a registry setting. Note that enabling this setting disables Windows Update, and this setting should be used only in organizations that use Windows Server Update Services, System Center Configuration Manager, or other alternatives for managing updates.

CHAPTER 6

Microsoft Edge and Internet Explorer 11

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, Microsoft Edge, is brand-new in Windows 10. The other, destined to live on in business settings for years to come, is good old Internet Explorer 11, with the addition of an Enterprise Mode for easing the transition from older Internet Explorer versions.

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 Windows 10—is an excellent competitor. It's fast and generally compliant with web standards.

The trouble is that most enterprise deployments of Windows haven't taken 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 in recent years have pushed out automatic updates for their Windows browsers far more frequently than Internet Explorer.

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 came to an end. On that date, Microsoft changed 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, is 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 isn't the default web browser for new PCs running Windows 10. That honor goes to the new Microsoft Edge. Enterprises can still choose to make Internet Explorer their default browser across all supported Windows versions, but otherwise Internet Explorer will be relegated to a compatibility role.

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:

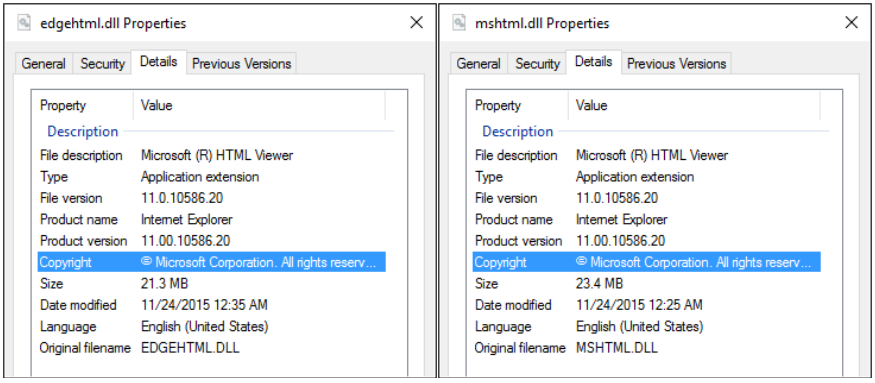
- **EdgeHTML (Edgehtml.dll)** is the new HTML viewer. Although its starting point was the original Trident engine, it has since diverged from that engine significantly. The new engine deliberately eliminates large chunks of legacy code designed to emulate older Internet Explorer versions, including the 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 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. It will not, however, add new features or support for additional web standards; those development efforts are reserved exclusively for the new rendering engine and Microsoft Edge.

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 are currently identified as Preview Release. With a few exceptions, standards that are listed as Under Consideration or In Development (Touch Events, for example) will be available only in EdgeHTML.

For a graphic illustration of the common code that underlies the two browsers, check the properties for each file (as found in C:\Windows\System32). Note that the Product Version is identical for each, as shown here.



Even by the accelerated standards of Windows 10 development, Microsoft Edge is developing at a rapid pace. It was a relatively late addition to the Windows 10 Technical Preview, showing up under the code name "Project Spartan" in publicly available preview builds some five months after the program began.

The first official release of Microsoft Edge coincided with the general availability of Windows 10 in July 2015. In November 2015, Microsoft released a major platform update for Microsoft Edge, bringing the browser to version 25 and the EdgeHTML rendering engine to version 13; this release also adds major improvements to Chakra, the JavaScript engine that powers Microsoft Edge.

Version information is available under the Settings menu in Microsoft Edge.

For those who want to preview features that are still under development and not yet enabled in production releases, type **about:flags** in the address box. That option displays a list of advanced settings and experimental features, as shown in Figure 6-1.

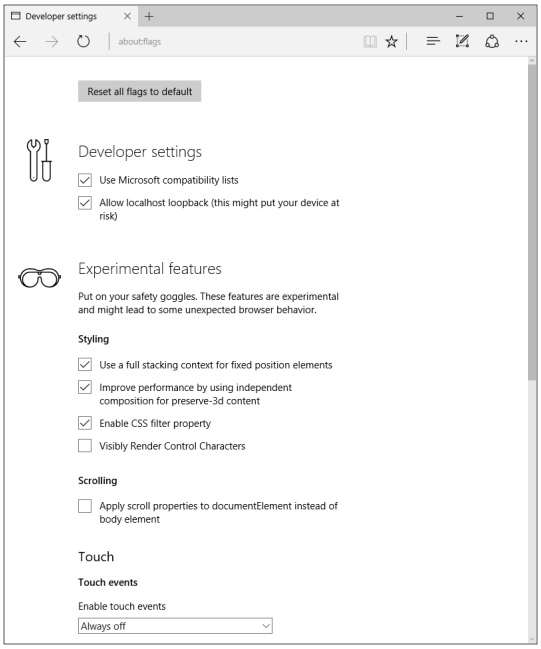


FIGURE 6-1 Entering **about:flags** in the Microsoft Edge address bar unlocks these advanced settings.

One of the most important changes in Microsoft Edge is its user-agent string, 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.

On Windows 10 version 1511, Internet Explorer 11 identifies itself with the following user-agent string:

```
Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
```

In contrast, Microsoft Edge 25 returns this user-agent string with each webpage request:

```
Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0
Safari/537.36 Edge/13.10586
```

The changes in user-agent string make it much more likely that a site will serve up the same standards-compliant page it would serve for other browsers and ignore any Internet Explorer–specific modifications.

Microsoft Edge

As I mentioned earlier in this chapter, Microsoft Edge is a relatively recent arrival in Windows 10 and is still evolving rapidly. In its current incarnation, you can see the deliberately minimalist design shown in Figure 6-2, which probably was a key influence on the Project Spartan code name.

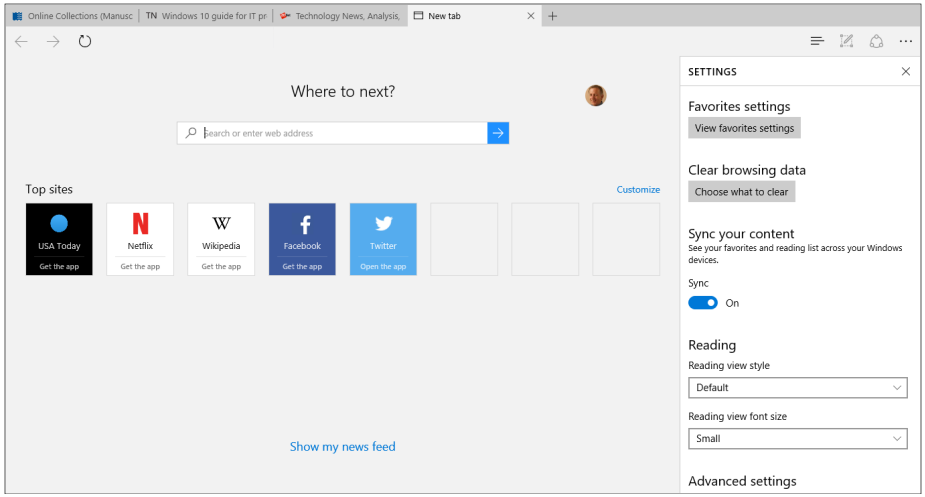


FIGURE 6-2 The minimalist design of the Microsoft Edge browser includes the ability to dock a pane to the right side of the browser window, in this case the Settings menu.

In its default layout, Microsoft Edge is lean indeed. There's no title bar, and only three buttons and an ellipsis that leads to a menu of options and settings. On the new tab page, shown in Figure 6-2, the address bar isn't even visible until you load a page from the search box or click in the space where the address bar would be.

That simplicity of design means there are far fewer settings to tinker with than in Internet Explorer, and some features you might have become accustomed to are missing in action.

The most obvious missing feature in Microsoft Edge 25 is support for any kind of browsing extension. Internet Explorer 11 supports Browser Helper Objects and toolbars, along with a handful of other proprietary extensions. For security reasons, those types of add-ons aren't permitted in Microsoft Edge.

As of Windows 10 version 1511, the only available add-on for Microsoft Edge is Adobe Flash Player, which is built into the browser (and automatically updated) in the same way that it's included with Internet Explorer 11. (Flash capabilities can be disabled in Settings, but the add-on itself cannot be removed.) Microsoft Edge also includes PDF reading capabilities you can use to open PDF documents from websites, email attachments, and local file storage without requiring third-party software.

Microsoft announced plans to allow third-party developers to write add-ons for Microsoft Edge using HTML and JavaScript, a strategy that is consistent with the approach used by competing browsers. This capability should arrive first in preview releases and will probably arrive in the Current Branch

in mid-2016 for consumers and small businesses that accept the default update schedule. (I explain how the Current Branch works in Chapter 1.)

Microsoft Edge includes a handful of signature features that have been part of the product since 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 View 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 tablets running Windows 10, but it's also useful to avoid eye strain when viewing cluttered pages with dense, tiny type.

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.

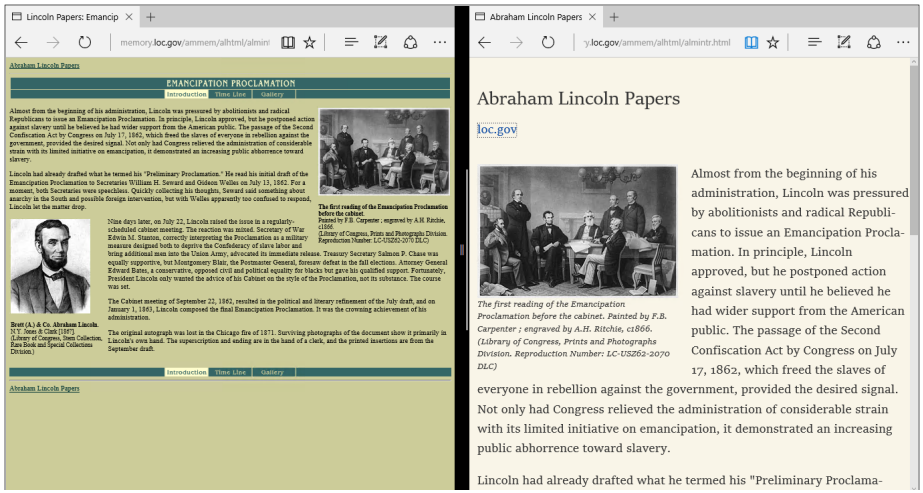


FIGURE 6-3 Enabling Reading View strips away extraneous elements from the original page (left) and reformats text for easier reading (right).

Another signature aspect of Microsoft Edge is its Web Note feature, which you use to annotate a webpage 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 Microsoft Edge toolbar. Figure 6-4 shows this toolbar in action, with a choice of highlighters and pens in multiple colors and sizes, as well as tools that give you the ability to add notes and clip portions of the screen.

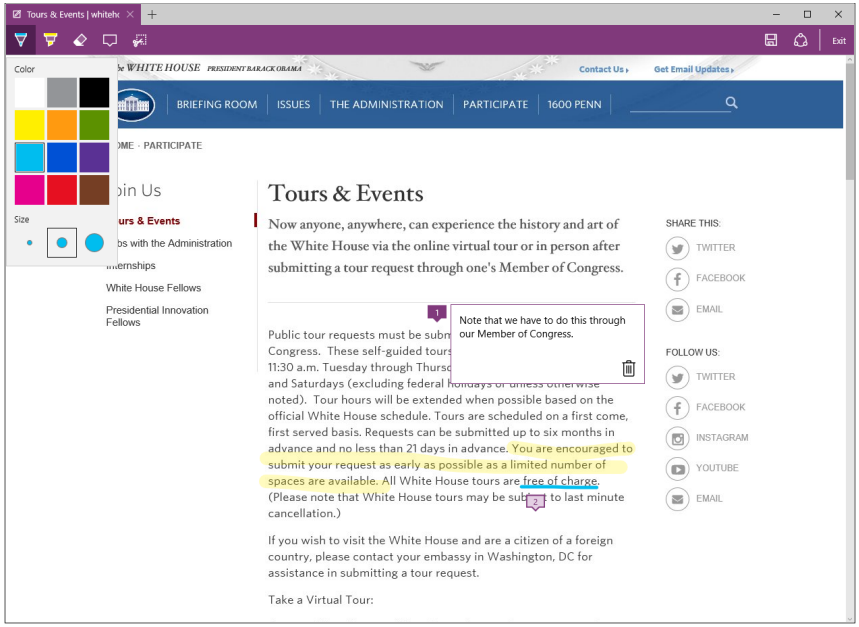


FIGURE 6-4 After you add annotations and markup to a page, you can save or share the results using the two buttons on the right side of the Web Note toolbar.

As with most modern browsers, with Microsoft Edge 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.

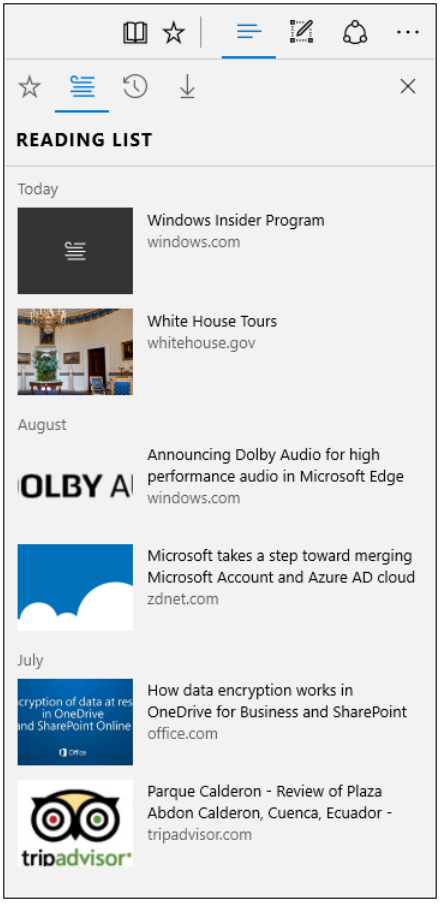


FIGURE 6-5 The Reading List is an alternative to Favorites, sorted and grouped by date saved.

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 Windows 10, but only for backward compatibility with devices running Windows 8.1. Its contents are not linked to the identically named feature in Microsoft Edge.

Microsoft Edge includes direct hooks to Cortana. When you browse to a page that Cortana recognizes, you're given the option to obtain 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.

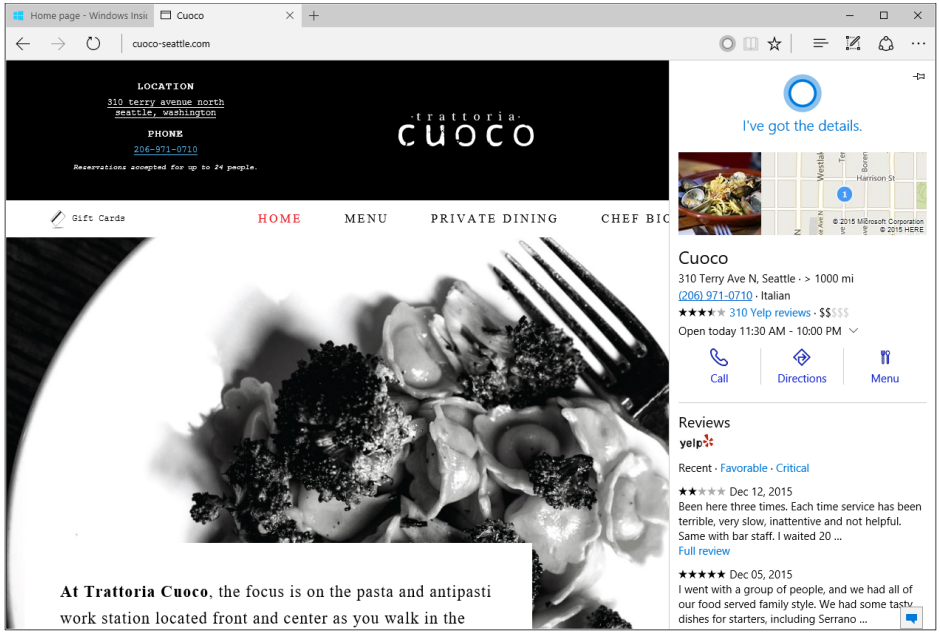


FIGURE 6-6 Cortana is integrated into Microsoft Edge and offers additional information for some webpages.

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

Unlike Internet Explorer, Microsoft Edge 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 to become more feature-rich over time. The November 2015 update to Windows 10, for example, includes the ability to *cast* media to a compatible device such as an Xbox One, the much-requested ability to sync Favorites, and a tab preview option, as shown in Figure 6-7.

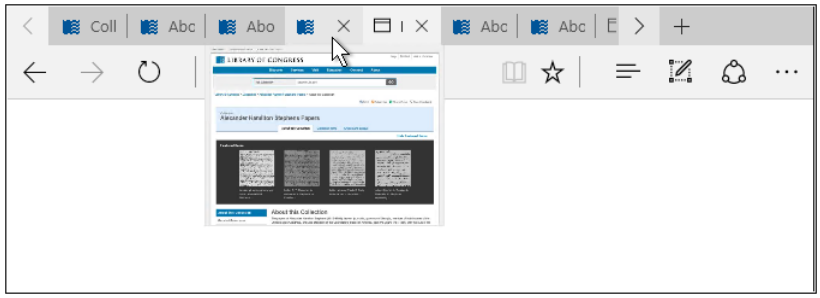


FIGURE 6-7 A new feature in Microsoft Edge version 25 allows you to rest the mouse pointer over a tab to see a preview of its contents.

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 already upgraded to Internet Explorer 11. In enterprise deployments, Microsoft recommends Internet Explorer 11 as a stable, reliable web platform for complex line-of-business (LOB) apps designed to run in a web browser.

Note When you deploy the Long Term Servicing Branch of Windows 10 Enterprise, Microsoft Edge is not available. In that configuration, unless you specifically change the default settings, only Internet Explorer 11 is available.

By comparison, Microsoft Edge 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. Microsoft Edge also can 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 the sites are 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 you turn it 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 uses the specified mode. On Windows 10, Microsoft Edge switches 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 6-8.

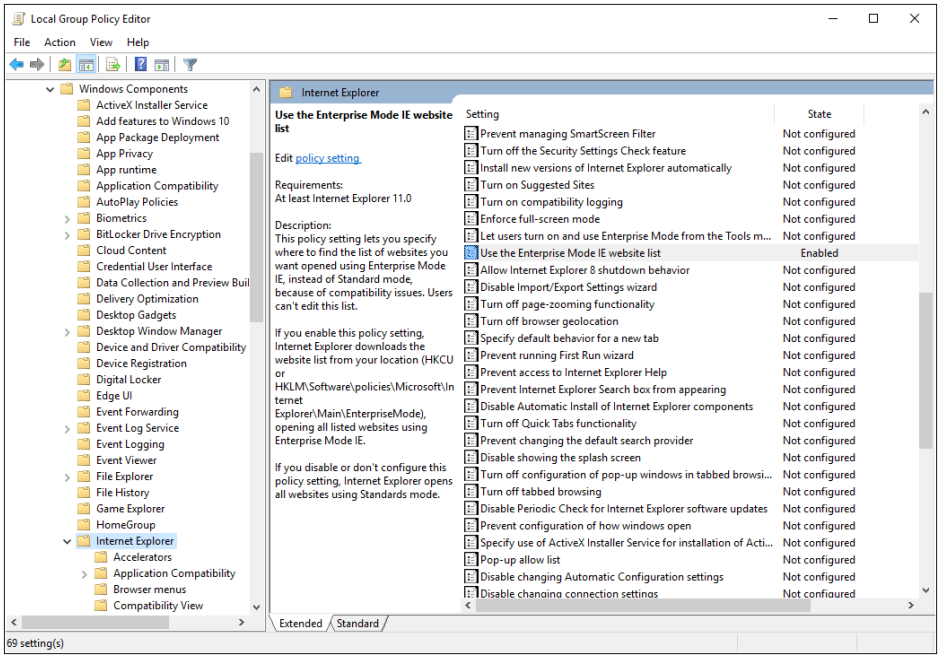


FIGURE 6-8 Turning on Enterprise Mode requires changing this Group Policy setting.

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 might 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. (Note that this value uses the HKLM node rather than HKCU.)

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 6-9 shows the syntax for an Enterprise Mode site list stored in a shared folder on my local network.

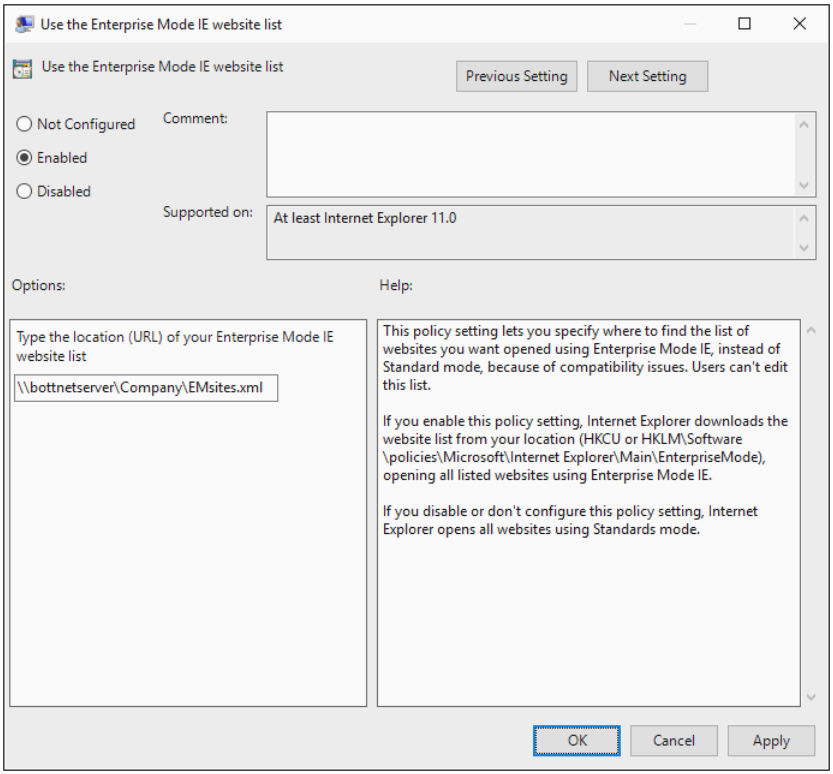


FIGURE 6-9 Enter the file location of the Enterprise Mode site list here or in the appropriate key in Registry Editor.

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 6-10.

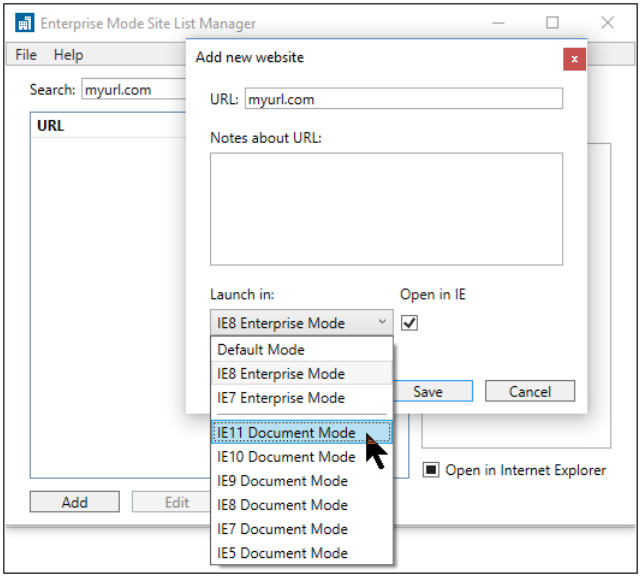


FIGURE 6-10 Use the Enterprise Mode Site List Manager utility to edit the contents of a local or shared list.

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://bit.ly/ie11-enterprise-mode*.

CHAPTER 7

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 especially useful on portable devices, including small tablets and phones.

Some of the features I discuss 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. That allows for easy configuration of metered connections, where you want to avoid large data transfers when possible, and monitoring data usage on a per-connection basis. 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. It also enables tap-to-send apps for quickly sharing small pieces of data, as well as the ability to exchange data using NFC tags.

- **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, shown in Figure 7-1, plugs into the HDMI input on a large television or other display, draws its power from a nearby USB port, and requires no setup.

FIGURE 7-1 The small, unassuming Microsoft Wireless Display Adapter plugs into any HDMI-equipped display and accepts remote connections from any Windows 10 device using Miracast.

Many of these connections can be made by opening Action Center and then tapping the Connect button, at the bottom of the pane beneath any waiting notifications. Figure 7-2 shows Windows 10 ready to connect to a Microsoft Wireless Display Adapter, a Bluetooth-equipped PC, and a Bluetooth-enabled audio headset.

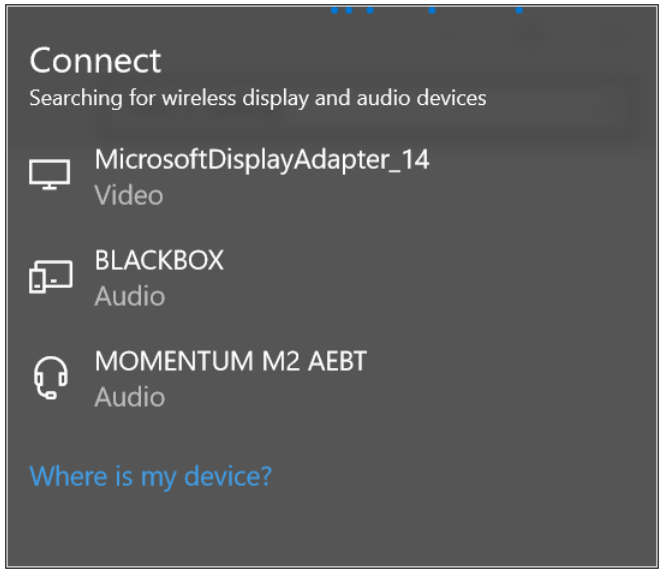


FIGURE 7-2 Tapping the Connect action button in Action Center lists any available Bluetooth, Wi-Fi Direct, or Miracast devices and gives you the ability to make connections with a single tap.

Windows 10 also includes a new feature called Wi-Fi Sense, which allows for automatic connections to known, trusted networks. Type **Wi-Fi** or **Wireless** in the Settings search box to open the Wi-Fi pane, which lists available connections and offers an on-off switch for Wi-Fi connections, as shown in Figure 7-3.

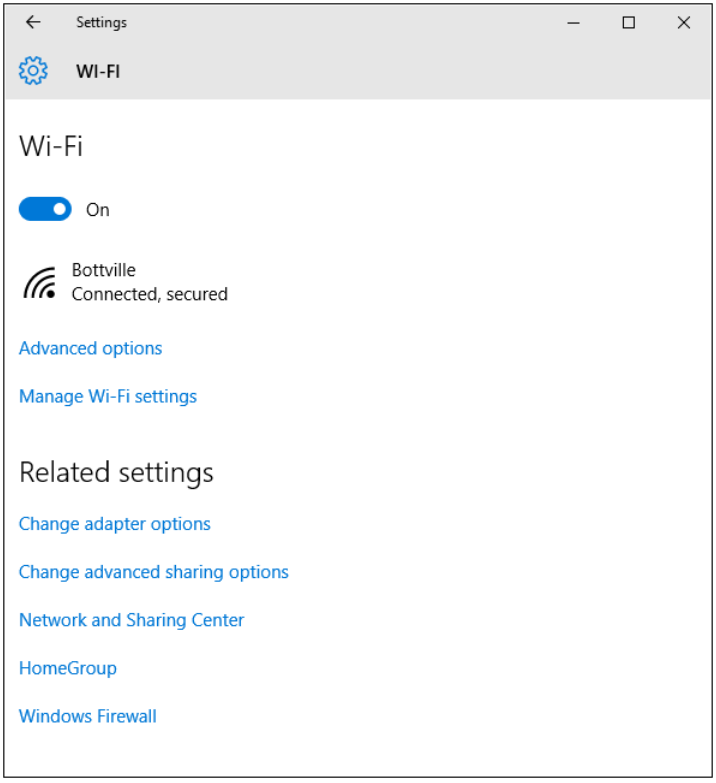


FIGURE 7-3 The Wi-Fi pane offers a simple on-off switch, details about available connections, and a link to several advanced options.

Click or tap Manage Wi-Fi Settings at the bottom of this pane to display the Wi-Fi Sense settings shown in Figure 7-4.

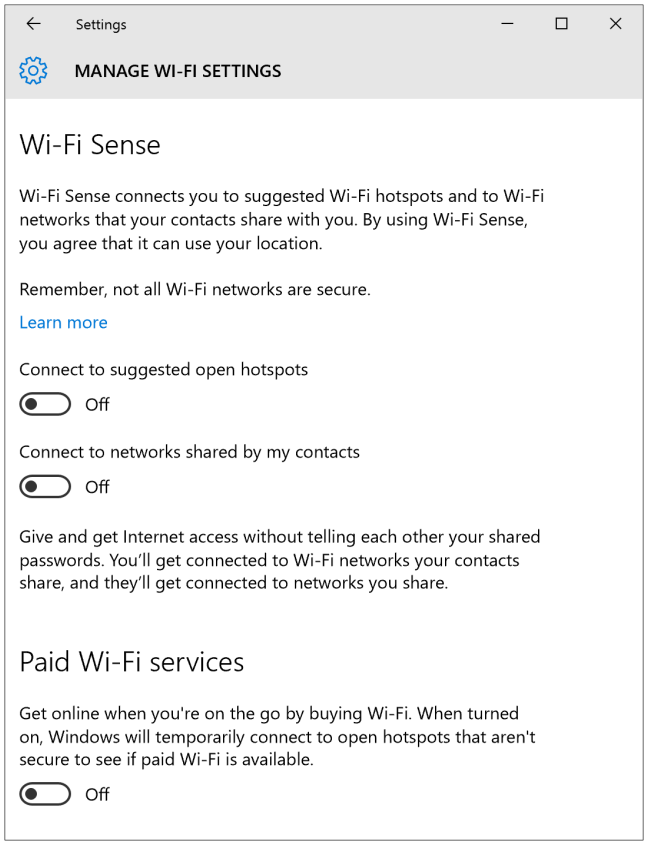


FIGURE 7-4 Wi-Fi Sense allows you to automatically connect to open hotspots that Microsoft has deemed reliable or that your contacts have chosen to share.

All of these settings can be configured using a Group Policy setting that was added in Windows 10 version 1511: Allow Windows To Automatically Connect To Suggested Open Hotspots, To Networks Shared By Contacts, And To Hotspots Offering Paid Services. You'll find this setting under Computer Configuration > Administrative Templates > Network > WLAN Service > WLAN Settings. When this policy is set to Disabled, the Wi-Fi Sense options are visible in Settings but are set to Off and cannot be changed by the user.

One instinctive reaction that longtime Windows users have to Wi-Fi Sense is fear that it will result in unwanted connections to dangerous networks or introduce insecurity on their own home or work network. You certainly should avoid connecting to open networks you know nothing about. But if the only networks to which you automatically connect are those that are known to be safe, the net effect is to improve your security.

With Wi-Fi Sense, Microsoft keeps a list of open networks that are known to be safe and reliable, like the official hotspots found in airports and shopping malls and hotel lobbies and increasingly in public areas in cities. When you or your users visit a new place using a Windows 10 device with Wi-Fi Sense turned on, they'll never see fake hotspots run by criminals; instead, they'll connect automatically to the known network that has established a reputation as safe and reliable.

The Connect To Networks Shared By My Contacts option is designed for use with consumer-grade Wi-Fi access points and routers that use the WPA2 standard for authentication, with a shared key that users enter to gain access. As part of the process of connecting to a WPA2-secured home network on a Windows 10 device, the user has the option to share the connection with contacts and friends.

Sharing a connection this way doesn't allow the person using that shared connection to re-share with their friends. For that, they need the passphrase.

On work networks, of course, you shouldn't be using passphrase-based security. Instead, your network should be secured using 802.11X authentication with a RADIUS server, so that anyone connecting to it has to sign in using credentials that you manage. It's relatively easy to add this setup on a large corporate network. Smaller businesses can look at a service like JumpCloud (*http://jumpcloud.com*) to provide RADIUS-as-a-service at a low cost. (In fact, the service is especially attractive for very small businesses, because it's free for up to 10 users.)

The Paid Wi-Fi Services option is a companion piece to a new Windows Store app from Microsoft, called (naturally) Microsoft Wi-Fi. It uses an industry-standard authentication mechanism to provide secure access to networks, on a pay-as-you-go basis. This program is still in the process of rolling out, so it might be some time before you're able to use this feature in locations you visit regularly.

Making secure connections to corporate networks

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

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

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 7-5 shows this feature in operation.

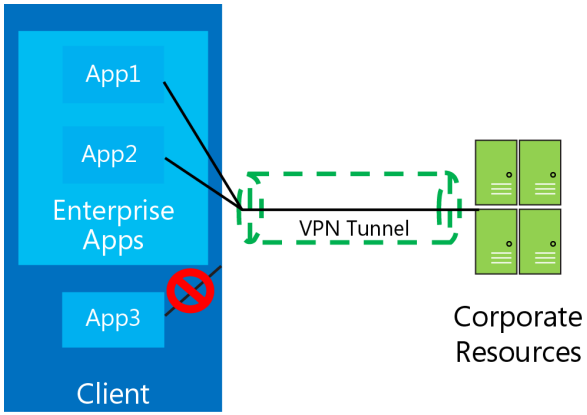


FIGURE 7-5 Administrators can create lists of apps authorized to access corporate servers over a remote network, blocking all other apps.

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 7-6 shows the simple settings for a properly configured DirectAccess connection.

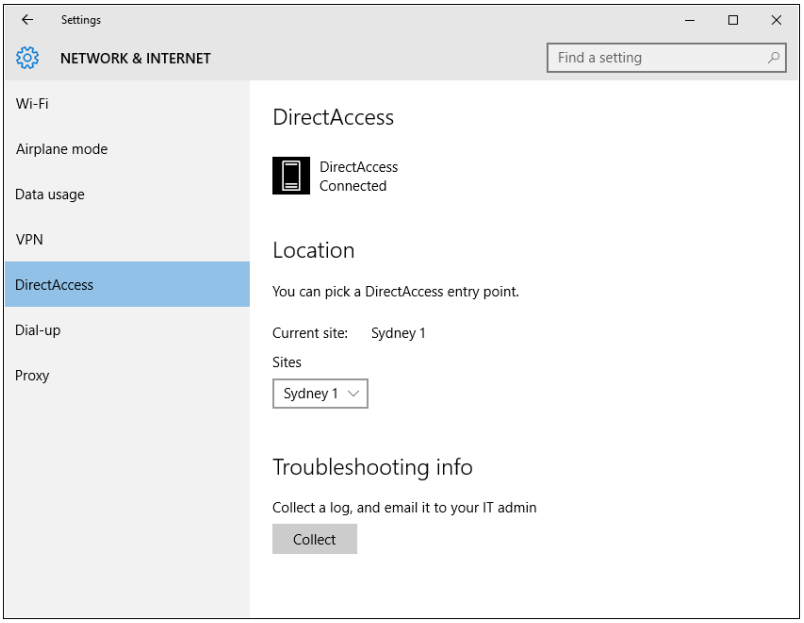


FIGURE 7-6 DirectAccess connections provide the security of a VPN without the hassles of setting up or constantly disconnecting and reconnecting.

Managing network connections

One of the most frustrating aspects of transitioning to a new Windows version is discovering that important features have moved or gone missing. That's especially true with these first Windows 10 releases, where settings are migrating from the classic Control Panel to the new Settings app.

The user-accessible knobs and levers for tweaking network connections are making that transition, which means you'll find significant pieces of functionality in the old-style Network And Sharing Center, with some functions already migrated to the Networking tab of the Windows 10 Settings app. In some cases, that means searching for the location of familiar management tools. A few options from older Windows versions, such as the ability to view a network map or manually name a network, are temporarily unavailable.

This section provides an overview of the tools you'll need.

Figure 7-7 shows the familiar Network And Sharing Center, from which you can enable or disable individual network adapters and inspect or change the properties of existing connections.

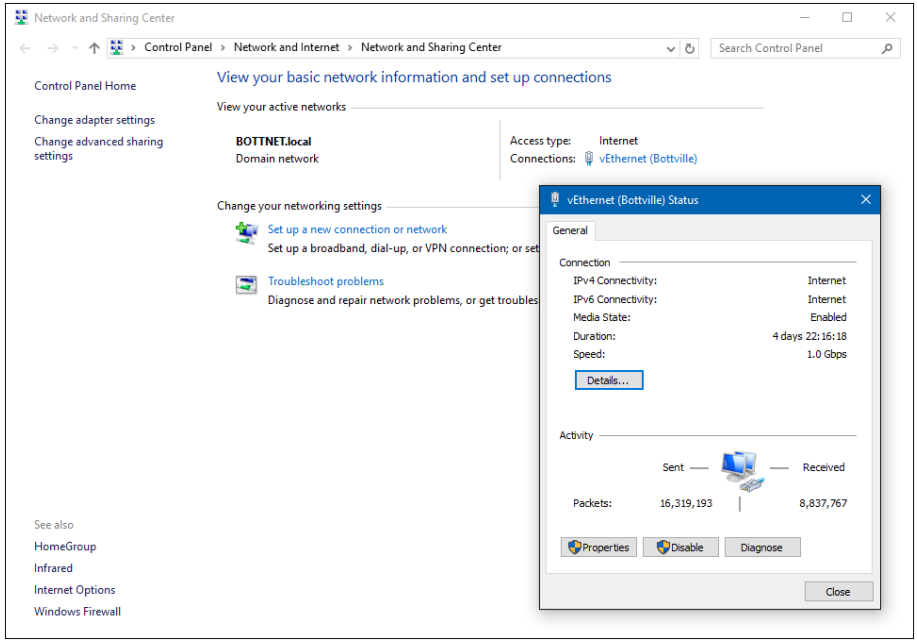


FIGURE 7-7 Your starting point for most network administrative tasks is still the Network And Sharing Center, part of the classic Control Panel.

The Network & Internet page in the new Settings app contains far fewer options, with each pane including multiple links that lead back to the Network And Sharing Center. One feature that's worth digging deeper to find is the list of saved Wi-Fi networks, located at the bottom of the Manage Wi-Fi Settings pane. As Figure 7-8 illustrates, it offers the option to forget a saved network.

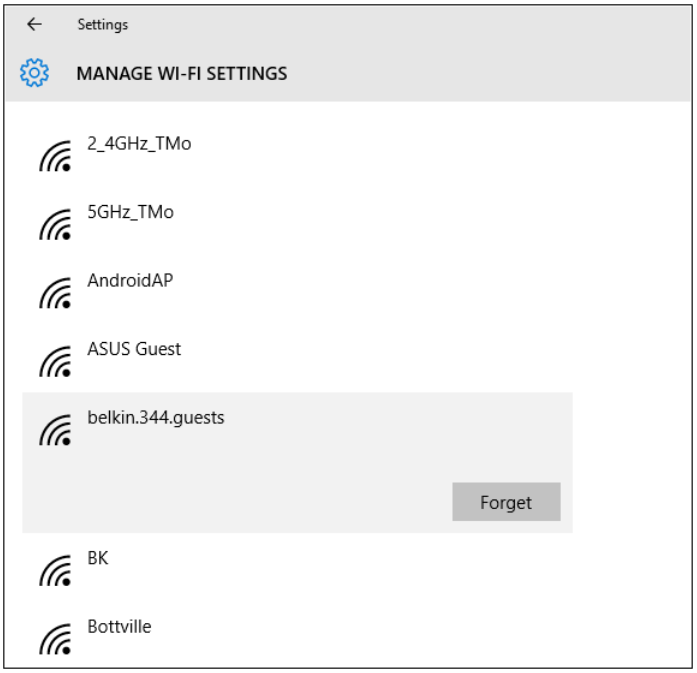


FIGURE 7-8 The list of Wi-Fi networks that have been saved for automatic connection later is one of the few essential features in the new Settings app.

From a management point of view, of course, you'll find the most options available from the command line. 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 7-9 makes clear:

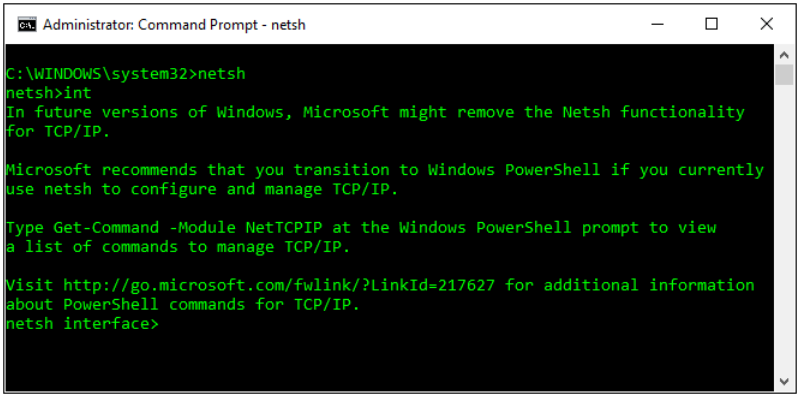


FIGURE 7-9 The venerable Netsh command-line utility is still available in Windows 10, but it's being phased out in favor of PowerShell cmdlets.

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 7-10.

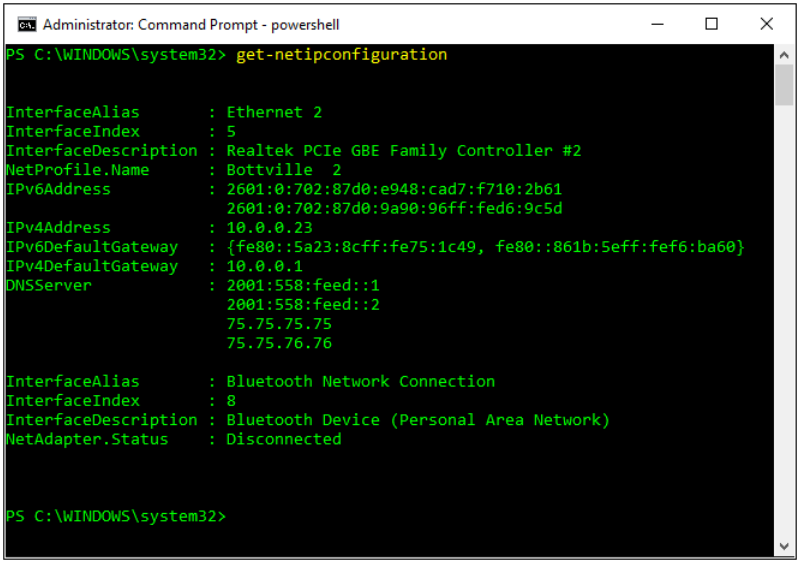


FIGURE 7-10 Simple PowerShell cmdlets provide the ability to view and change network settings in Windows 10.

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.

Note For a full list of network-related PowerShell commands, see *http://bit.ly/powershell-net-tcp*.

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 3.4×10^{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*.

CHAPTER 8

Hyper-V and desktop virtualization options

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 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 familiar if you 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 Windows 10, allows you to set a checkpoint that uses 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 saved the current state of a VM and all running apps and services. Figure 8-1 shows this feature in the configuration settings for a VM.

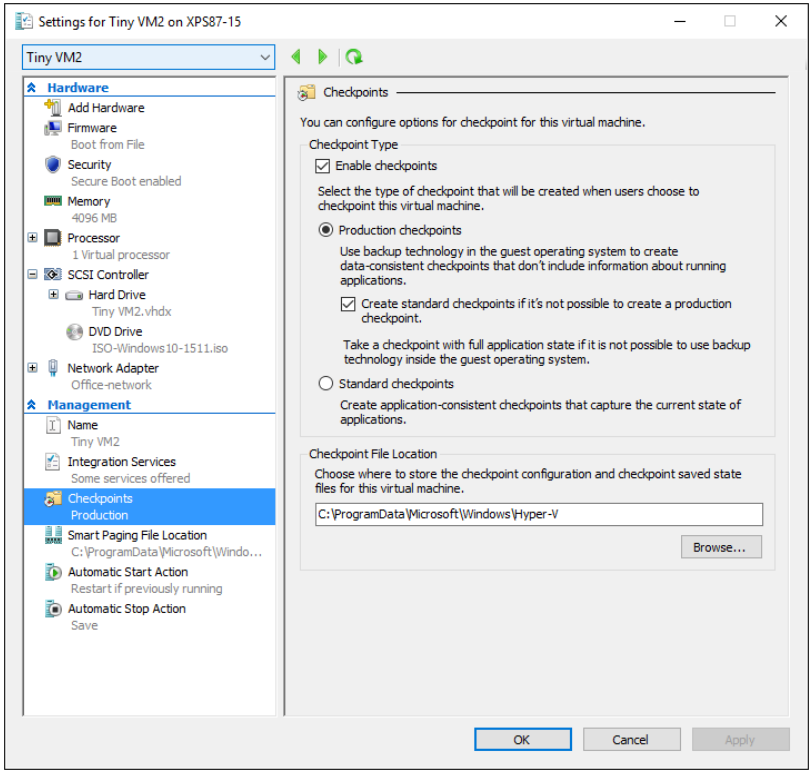


FIGURE 8-1 Production checkpoints, which create a full backup using Volume Snapshot technology, are new in Windows 10.

- **New configuration file format** VMs created in Windows 10 use configuration version 6.2 (available with the July 2015 release) or version 7.0 (introduced in Windows 10 version 1511) 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.
- **New security options** VMs created using the Generation 2 format support Secure Boot. Beginning with version 1511, Hyper-V machines now support a virtual Trusted Platform Module (TPM), which allows for full disk encryption on virtual machines. (Note that you must enable Isolated User Mode for this option to work.)
- **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 or 4 or Surface Book), 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 Windows 10 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 Windows 10. 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 on a PC running 64-bit Windows 10 Pro, Enterprise, or Education:

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.

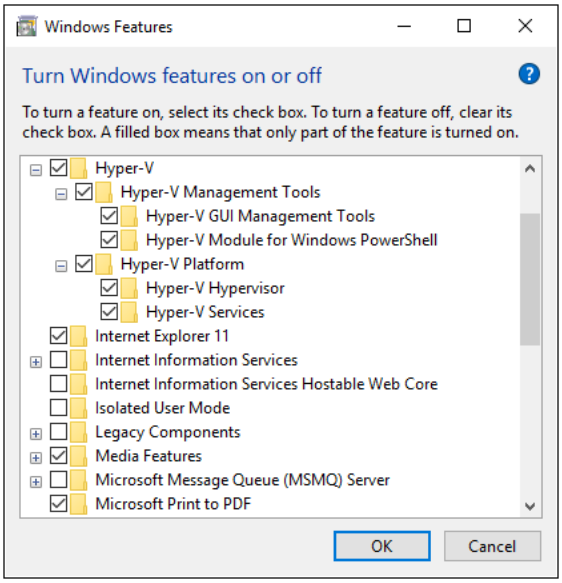


FIGURE 8-2 The Client Hyper-V features in Windows 10 Pro, Enterprise, or Education must be enabled using this dialog box.

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

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

To use a virtual TPM, you need to enable Isolated User Mode. That can be done in the Turn Windows Features On Or Off dialog box or using the following sequence of PowerShell commands:

```
Install-WindowsFeature Isolated-Usermode
New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard -Force
New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard   -Name
EnableVirtualizationBasedSecurity -Value 1 -PropertyType DWord -Force
```

Note For a more detailed discussion of security improvements in the most recent release of Hyper-V, along with details on how to move secure VMs between machines, see the TechNet article "Virtual machine security settings in Hyper-V Manager," at *https://technet.microsoft.com/library/mt403347.aspx*.

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.

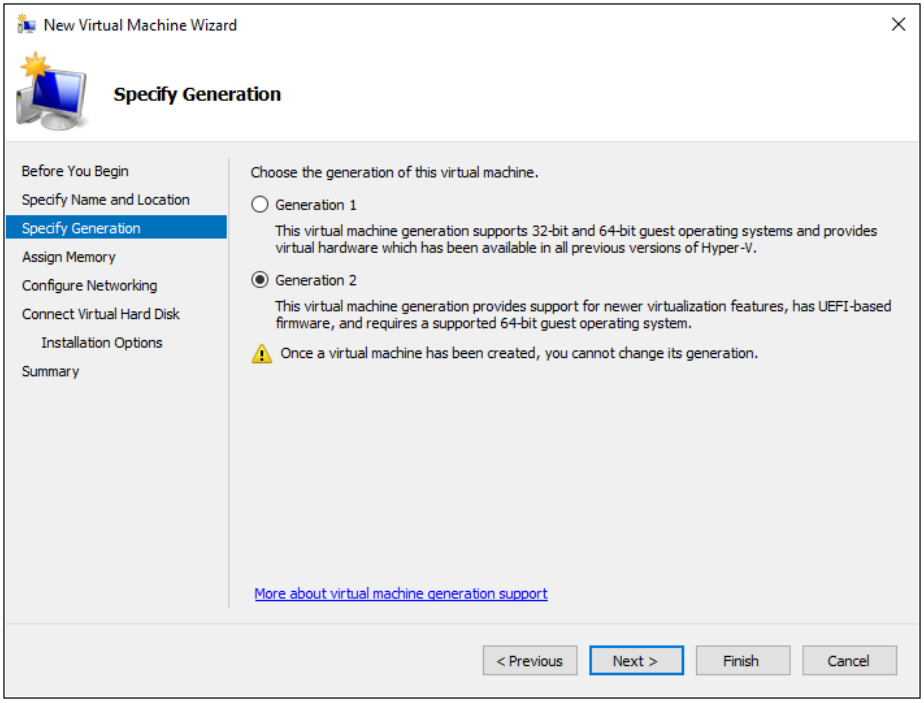


FIGURE 8-3 Client Hyper-V in Windows 10 supports Generation 2 virtual machines, which are based on UEFI and require that you install a 64-bit guest operating system.

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 in an enhanced session.

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 10 offers 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.

Within a few weeks of the release of Windows 10, Microsoft released the Microsoft Desktop Optimization Pack (MDOP) 2015, which is available to Volume License customers with Software Assurance agreements and is also available for testing and evaluation as part of MSDN subscriptions. MDOP enables three virtualization technologies: Microsoft Application Virtualization (App-V), Microsoft User Experience Virtualization (UE-V), and Microsoft Enterprise Desktop Virtualization (MED-V).

Microsoft Azure provides similar virtualization capabilities with Azure RemoteApp, which delivers Windows apps from the cloud to a wide range of client devices, including those running Windows 10.

The engine that powers virtual desktops is Remote Desktop Services (RDS), which debuted in Windows Server 2012 and is also available in Windows Server 2016, which is built on the same code base as Windows 10 and is 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 the throttling of tasks, ensuring a high level of 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 of 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 10 is running in the VM, allowing for the 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 due for improvement when Windows Server 2016 is released).

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.

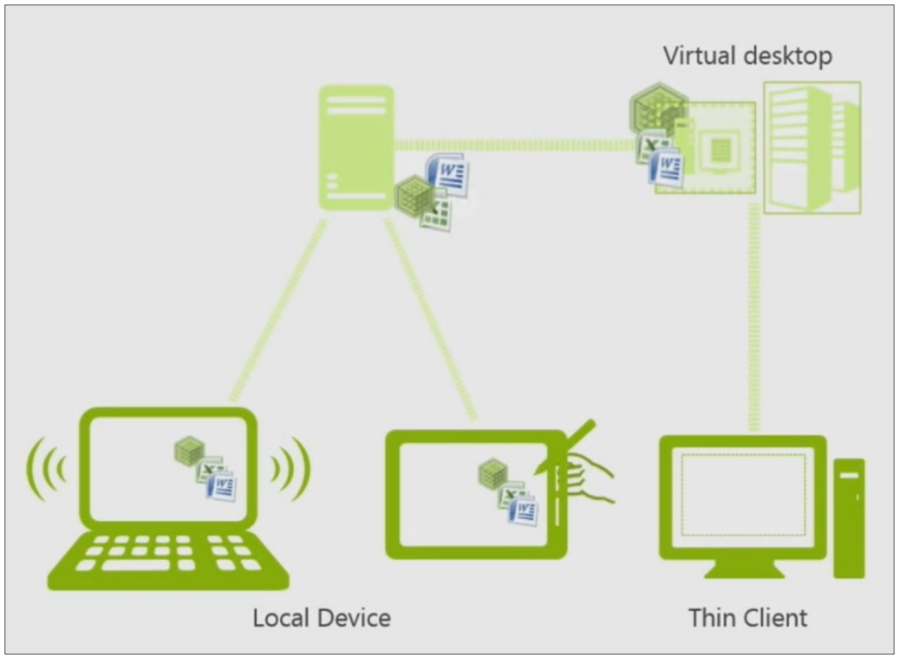


FIGURE 8-4 Virtualized applications can be delivered to local devices using App-V or deployed as part of a virtual desktop using RemoteApp, without requiring local installations.

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 the 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. You can use its dynamic configuration options 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 5.1 is the current release included as part of MDOP 2015, and it is required for Windows 10. (App-V 5.0 and prior versions are not compatible with Windows 10, although App-V packages created with App-V 5.0 are compatible and require no conversion.) It comes in desktop and RDS versions, and it 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 Microsoft Visual C++ libraries.

Note For more details on App-V 5.1, see *http://bit.ly/app-v-51*.

User Experience Virtualization

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 SP1, adds support for Windows 10. It supports 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 and taskbar settings, for example); Microsoft Office 2010 and Microsoft Office 2013 applications; Internet Explorer 11; all preinstalled Windows apps; and a number of Windows desktop applications. New in SP1 is support for roaming network printers.

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.) For more details on Work Folders, see Chapter 13, "Managing mobile devices and enterprise data."

CHAPTER 9

Recovery and troubleshooting tools

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.

This chapter also introduces available troubleshooting tools for Windows, including those that are a part of the operating system as well as some useful external tools. 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 and troubleshooting 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 user-initiated repair and recovery options is Windows Recovery Environment (Windows RE), a feature available since Windows 8, which includes a handful of essential tools for troubleshooting issues and repairing startup problems. On UEFI-based PCs, the Winre.wim image

is copied to the Windows RE Tools partition during the final stage of setup. On BIOS-based PCs, the image is copied to the System partition. In either case, this layout makes it possible to run Windows RE even if the Windows partition has a problem.

Windows RE starts automatically in certain scenarios, including two consecutive failed attempts to start Windows, two consecutive shutdowns that occur within two minutes of boot completion, a Secure Boot error, or a BitLocker error on a touch-only device.

You can start Windows RE manually from Windows 10 installation media, from a recovery drive, or from the recovery partition on a device, if that option is available. You can also start Windows RE manually from Windows 10 by using the Advanced Startup option in Settings, Update & Security; by holding down the Shift key and choosing Restart from the Start menu; or by entering the **Shutdown /r /o** command.

In the initial Choose An Option menu, the user can 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. (On OEM PCs, a Factory Image Restore option might also be available, and organizations that deploy custom images can add an option to this menu as well.)

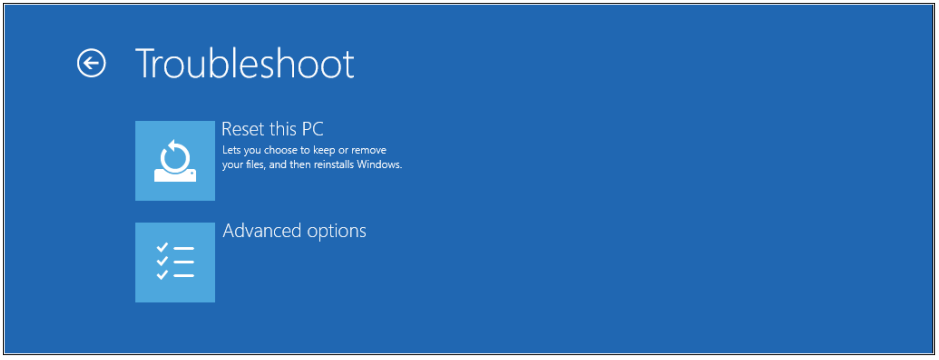


FIGURE 9-1 When you start a Windows 10 device from recovery media, choose Troubleshoot to display these Windows Recovery Environment options.

In Windows 8.1 and in early preview releases of Windows 10, the Troubleshoot menu included separate Refresh and Reset options. These have been consolidated into a single Reset This PC option, which activates the push-button reset feature. This option is also available from the Update & Security page in Settings, for use with systems that are able to start up properly. This option is covered fully later in this chapter.

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

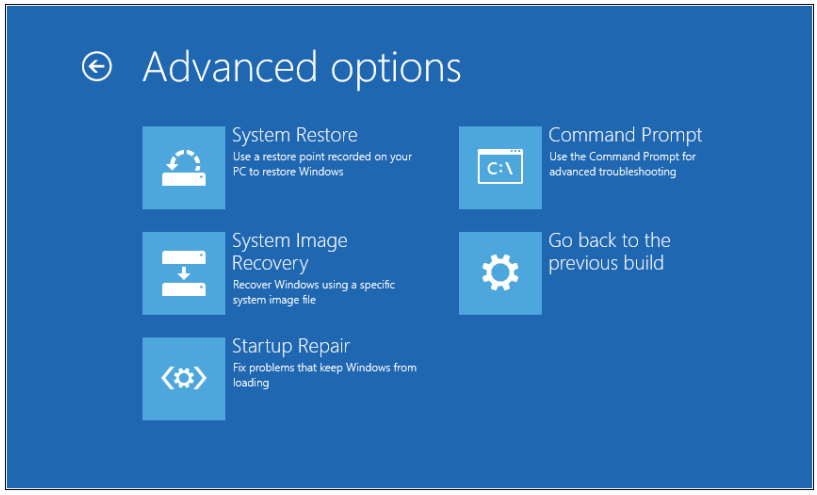


FIGURE 9-2 This Windows RE menu provides access to essential troubleshooting and recovery tools.

Table 9-1 lists the core functions available from the Advanced Options menu, many of which are direct descendants of recovery tools found in previous Windows editions. Note that on some devices you might see additional choices, including the option to access UEFI firmware settings or to roll back to a previous Windows version or preview build.

TABLE 9-1 Advanced options for recovery.

Option	Description
System Restore	You can use this option to choose a restore point created earlier and restore the system configuration.
System Image Recovery	Choosing this option replaces everything on the computer with a system image, including images created using the Windows Backup utility from Windows 7 or later. (In Windows 10, this utility is available in the desktop Control Panel. Under System & Security, choose File History, and then click the System Image Backup link in the lower-left corner.)
Startup Repair	If you choose this option, Windows attempts to diagnose and automatically correct common boot problems.
Command Prompt	This option opens an administrative command prompt, where you can use command-line tools such as Bootrec and Bcdedit.

More Info 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.

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. Although this article was written for Windows 8.1, its instructions apply to Windows 10.

Note that you can customize the Windows Recovery Environment as part of a standard image. For example, you can add a preferred troubleshooting tool to the Windows RE menu or assign a hardware button to invoke Windows RE. These and other how-to topics are documented in the Windows Recovery Technical Reference at *http://bit.ly/win-re-reference*.

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 repeated 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. Windows 10 offers a simplified reset option that is greatly improved compared with its predecessors and generally lives up to the "push button" part of the name.

On PCs running Windows 8 or later that were built for retail sales and distribution channels, 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, OEMs can still provide this recovery image and its associated partition to allow the system to be rolled back to its state as shipped from the factory. However, this option is no longer required. Instead, Windows 10 is capable of performing a full reset by rebuilding the operating system to a clean state using existing system files from the Windows Component Store (C:\Windows\WinSxS).

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 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 is the modern equivalent of the "last known good configuration" option, allowing recovery to succeed when a recently 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 reset. These customizations are saved in a separate container, which is created as part of the OEM setup process. Note that 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.

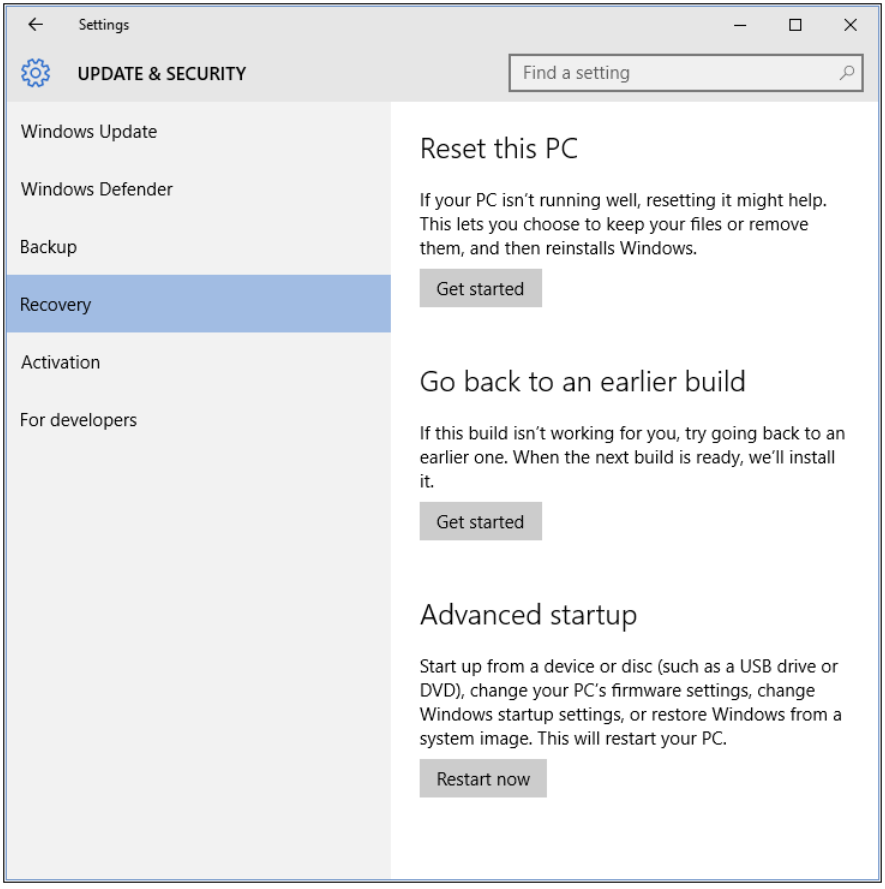


FIGURE 9-3 The options available on this menu vary. On a PC recently upgraded from an earlier version, for example, you'll find an option to go back to that version.

Choosing Reset This PC offers two options, as shown in Figure 9-4.

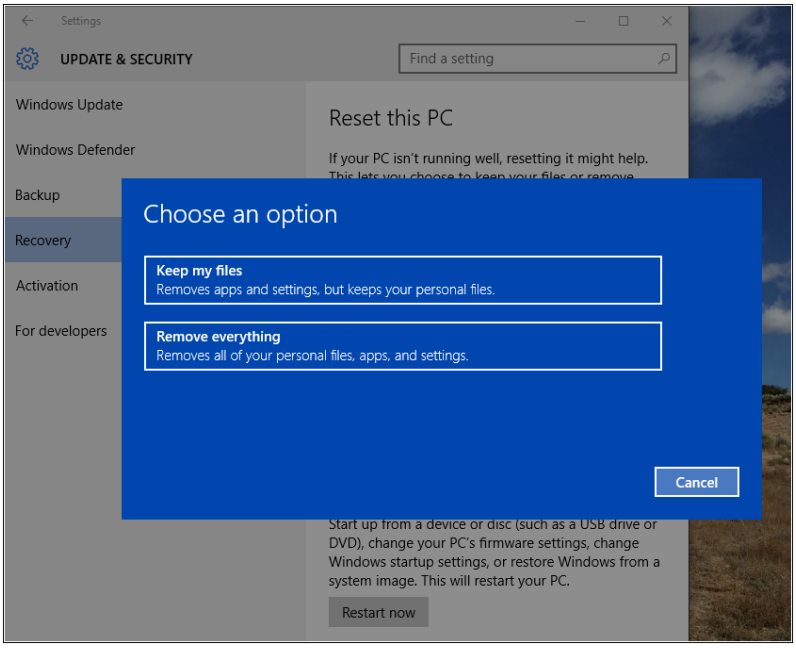


FIGURE 9-4 The Reset This PC feature offers the option to preserve data files (and some settings) or start fresh, removing all files, apps, and settings and effectively doing a clean install.

Both options are equivalent to reinstalling Windows 10 from scratch, with the added ability to preserve files and some settings or to perform a clean install.

The Keep My Files option

This option is the equivalent of the Refresh Your PC feature from Windows 8.1, with the noteworthy difference that it does not preserve apps acquired by the user from the Windows Store. (These need to be restored after the reset is complete.) Choosing Keep My Files retains all data files and preserves the following personalized settings:

- User accounts (local, domain, and Microsoft account) and group memberships
- Domain settings
- Windows Update settings
- Library settings
- Lock screen background
- Desktop themes
- International settings
- Wireless network profiles
- Settings configured in Windows Welcome

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, as well as File History data. All user-installed desktop programs and Windows Store apps are removed, and a list of removed programs is saved on the desktop.

This option boots into Windows RE and gathers user accounts, settings, data, and Windows Store apps. It then uses the most recent system rollup that is at least 28 days old to create a new, clean instance of the following folders, including all subfolders:

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

The reset operation also preserves device drivers, following the same rules as for system files. Drivers are restored to the most recent version that has been on the PC for at least 28 days. Device applets that are installed separately from the driver package are not restored as part of the reset process.

Preinstalled Windows apps are restored to their factory version and state, and will be updated automatically after the reset is complete. 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.

Using the Keep My Files option requires a significant amount of free disk space to function—at least 4 GB plus as much as twice the space occupied by any provisioning packages located in C:\Recovery\Customizations.

The Remove Everything option

This option (called Reset Your PC in Windows 8.1) removes all apps and user data, including user accounts and personalization settings. Choose the Remove Everything option 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 9-5 notes, the Remove Files And 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.

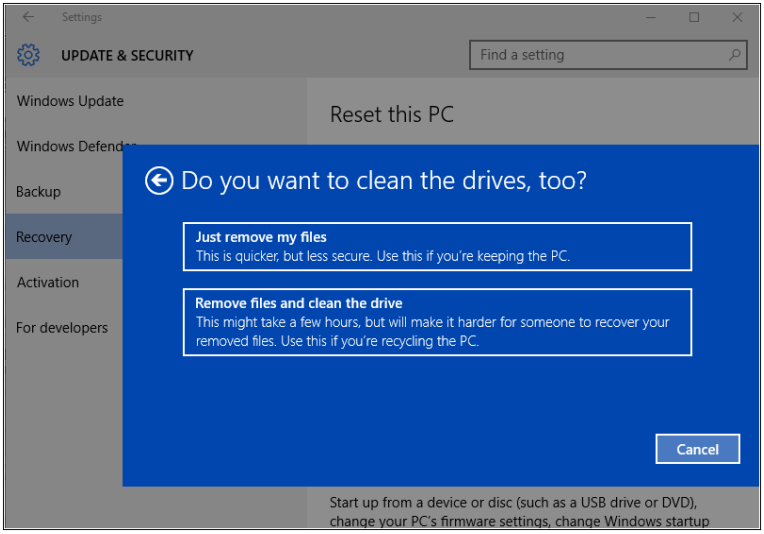


FIGURE 9-5 The Reset This PC procedure includes an option to wipe the drive so that data files from the previous installation can't be recovered easily.

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 cumulative 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.

Troubleshooting tools

Like its predecessors, Windows 10 includes an assortment of diagnostic and troubleshooting tools that can be useful for tracking down the cause of performance problems, crashes, and other unwanted events, especially during pilot testing with a new operating system.

The three utilities in this list should be familiar to every IT pro. I list them here with a quick description of what's new and changed for Windows 10, especially for those upgrading from Windows 7:

- **Task Manager** This venerable Windows utility got a major upgrade beginning with Windows 8, making it significantly more powerful than its predecessor. It's available from the Quick Link menu (by right-clicking on Start or using the Windows logo key + X shortcut), or directly using the keyboard shortcut Ctrl+Shift+Esc. In its expanded view, pay attention to the Startup tab, which offers information about programs that automatically start with Windows. The Performance tab, shown in Figure 9-6, offers details about multiple Windows subsystems, usually with enough information to help you determine the source of a current slowdown.

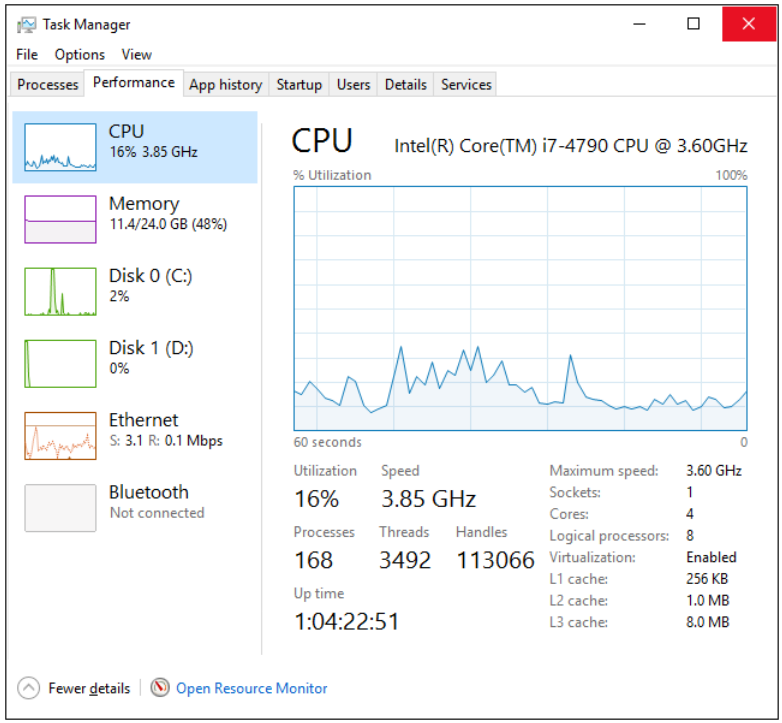


FIGURE 9-6 The Performance tab in Task Manager shows a wealth of information about CPU, memory, disk, and network usage. Note the link at the bottom to open Resource Monitor.

- **Resource Monitor** If you need more details than are available from Task Manager, open this utility, which provides a granular view of file-system and disk activity, processor usage, and network connections.

- **Event Viewer** Virtually every system-related task that Windows does—in the background, in the foreground, or in response to your requests—is logged for posterity. These event logs are available for inspection using the Event Viewer utility (Eventvwr.msc). It has changed little in the past decade.

Sysinternals tools

Windows Sysinternals is one of the most enduring and useful sources of advanced system utilities for any IT pro. The site, available at *http://sysinternals.com*, was created in 1996 by Mark Russinovich, who joined Microsoft in 2006 and is currently Chief Technical Officer of Microsoft Azure.

It would take several pages just to list all the Sysinternals utilities, but a few are essential, especially when troubleshooting in an unfamiliar environment. Process Explorer, for example, offers an amazingly detailed view of currently active processes, whereas AutoRuns allows for pinpoint control over programs that run automatically.

What's remarkable is that these tools are updated regularly, with occasional major releases offering useful new features. What's even more remarkable is that they're free.

Nearly 70 individual Sysinternals troubleshooting utilities are available as part of the Sysinternals Suite. You can also run individual tools from the web-based directory listing at *https://live.sysinternals.com/*.

Microsoft Diagnostics and Recovery Toolset

The Diagnostics and Recovery Toolset (DaRT) is part of the Microsoft Desktop Optimization Pack (MDOP), which is available by subscription for volume-license customers with Software Assurance. It is also available under different licensing terms through Microsoft MSDN subscriptions.

Each version of DaRT is designed to work on a specific version of Windows. For Windows 10, use DaRT 10, which is included with the MDOP 2015 package.

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.

CHAPTER 10

Integrating Azure Active Directory

Every network administrator knows the ins and outs of Active Directory, the service that runs on Microsoft Windows server editions and powers countless Windows domain-based networks worldwide. The Pro, Enterprise, and Education editions of Windows 10 offer full support for traditional Active Directory deployments, of course, but Windows 10 also supports a new, cloud-based alternative called Azure Active Directory, or Azure AD for short.

Like its on-premises counterpart, Azure AD provides identity and access services for businesses. With an Azure AD work or school account, users can sign on to any cloud or on-premises web application, using a wide array of client devices.

Azure AD provides the core directory and identity-management capabilities behind several business-focused Microsoft cloud services, including Microsoft Office 365 and (naturally) Microsoft Azure. You can integrate Azure AD services with a local Active Directory deployment or use it on a standalone basis. In either case, you can configure multifactor authentication to provide secure local and remote access, and you can take advantage of built-in reporting and analytics capabilities that scale to even very large enterprises.

In this chapter, I offer an overview of Azure AD as well as instructions on how to make Azure AD work with Windows 10 devices of all shapes and sizes.

Getting started with Azure AD

You might already be using Azure AD without being aware of it. If you or your organization signed up for a business-focused Microsoft cloud service—such as Azure, Office 365, Microsoft Intune, or Microsoft Dynamics CRM Online—that subscription includes an Azure AD directory. By default, this directory includes a subdomain in the *onmicrosoft.com* domain, but most organizations assign a custom domain name to the directory. For example, Contoso Corporation might start with the default *contoso.onmicrosoft.com* subdomain but add *contoso.com* as a custom domain. This configuration makes it possible for users to sign in and access local or cloud-based resources using a familiar email address.

Each dedicated instance of Azure Active Directory (Azure AD) is called a *tenant*. Although Microsoft hosts the service in its massive and worldwide Azure infrastructure, each Azure AD directory is completely isolated from other directories, as shown in Figure 10-1.

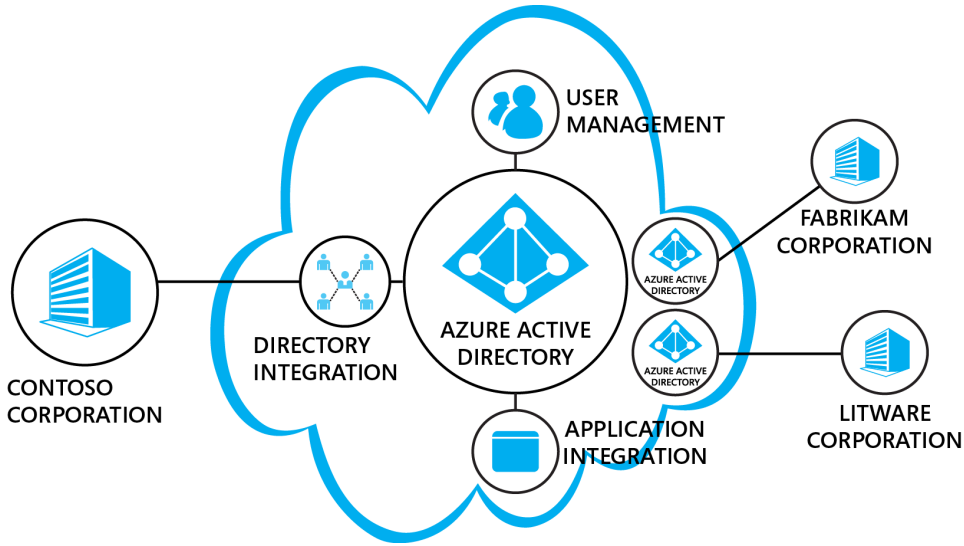


FIGURE 10-1 All Azure Active Directory tenants share the same global infrastructure, but each directory is completely isolated from others for security reasons.

As a convenience, you can consolidate multiple Azure AD directories under a single administrative dashboard. The directories themselves, however, are completely separate and protected from unauthorized access (accidental or malicious).

You can associate the Azure AD directory for an existing Microsoft cloud service, such as Office 365, to a free Microsoft Azure subscription, allowing you to manage that directory within the Azure Management Portal (*https://manage.windowsazure.com*). Figure 10-2 shows what that directory configuration looks like.

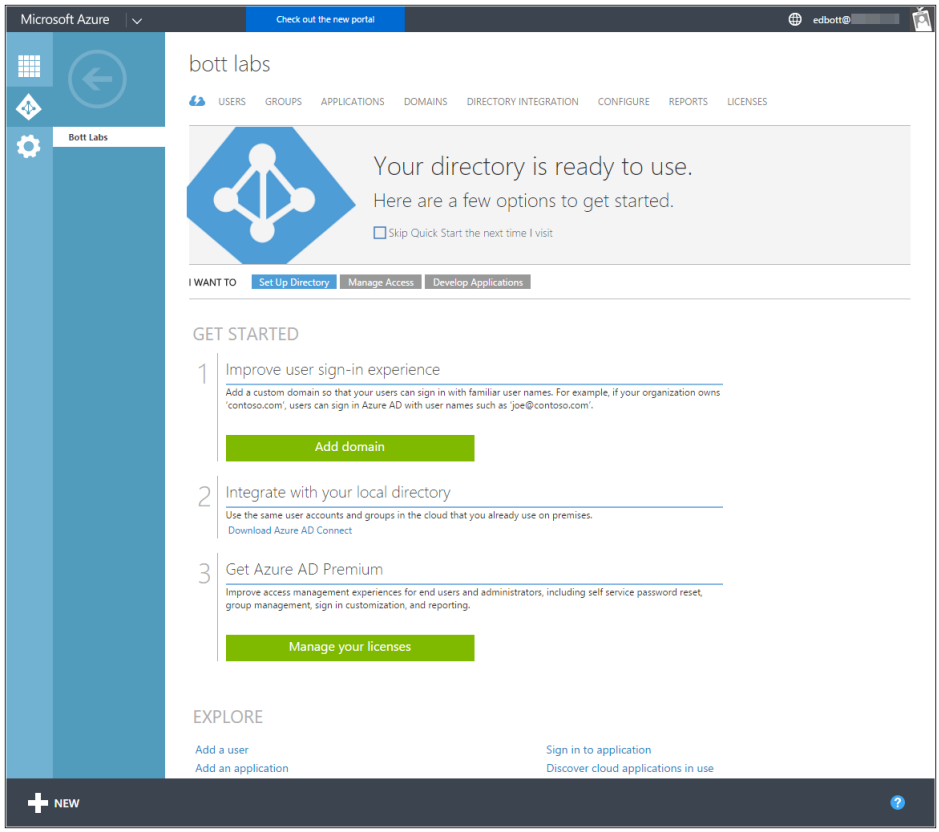


FIGURE 10-2 To configure and extend an Azure AD directory, use this management portal.

Azure AD subscriptions are available at three levels. An Office 365 or Azure subscription includes an Azure AD directory at the Free level. You can upgrade to Basic and Premium editions through a Microsoft Enterprise Agreement, through the Open Volume License Program, or through the Cloud Solution Providers program. Azure and Office 365 subscribers can also purchase Active Directory Premium licenses online.

For details of what's in each Azure AD subscription level, see this article: *https://azure.microsoft.com/en-us/pricing/details/active-directory/*. The following list summarizes the differences:

- **Free** This level allows up to 500,000 directory objects, supports user and group management tools and device registration, and allows self-service password changes for cloud-based users. It also allows up to 10 apps per user to be connected for single sign-on (SSO) use and supports Active Directory Connect, the sync engine for extending on-premises directories to Azure AD.
- **Basic** Along with all the features in the Free level, this tier removes the size limit on directory objects, allows self-service password resets, adds group-based access management and provisioning, and includes a service-level agreement.

- **Premium** At this level, Azure AD subscribers have all the benefits of the Basic tier plus an unlimited number of SSO apps, the ability to configure multifactor authentication, and enhanced self-service password management capabilities. The Cloud App Discovery feature allows network administrators to determine which cloud services (authorized and unauthorized) are in use within the organization and, optionally, integrate them with Azure AD to lessen the risk of data leakage.

Azure AD Premium is also available as part of the Enterprise Mobility Suite, which includes Microsoft Intune and Azure Rights Management.

Azure Active Directory Join is available only on Windows 10 devices. At all subscription levels, including Free, you can join a Windows 10 PC to Azure AD, use desktop SSO features, and recover BitLocker keys with the help of an administrator. At the Premium level, self-service BitLocker key recovery is available, and additional local administrator accounts can join a Windows 10 device using Azure AD Join.

The ability to integrate third-party Software-as-a-Service (SaaS) apps with Azure AD is a key benefit. Hundreds of apps are available via the Application Gallery in Azure AD and available for configuration with a single click. Figure 10-3, for example, shows Amazon Web Services integrated into Azure AD.

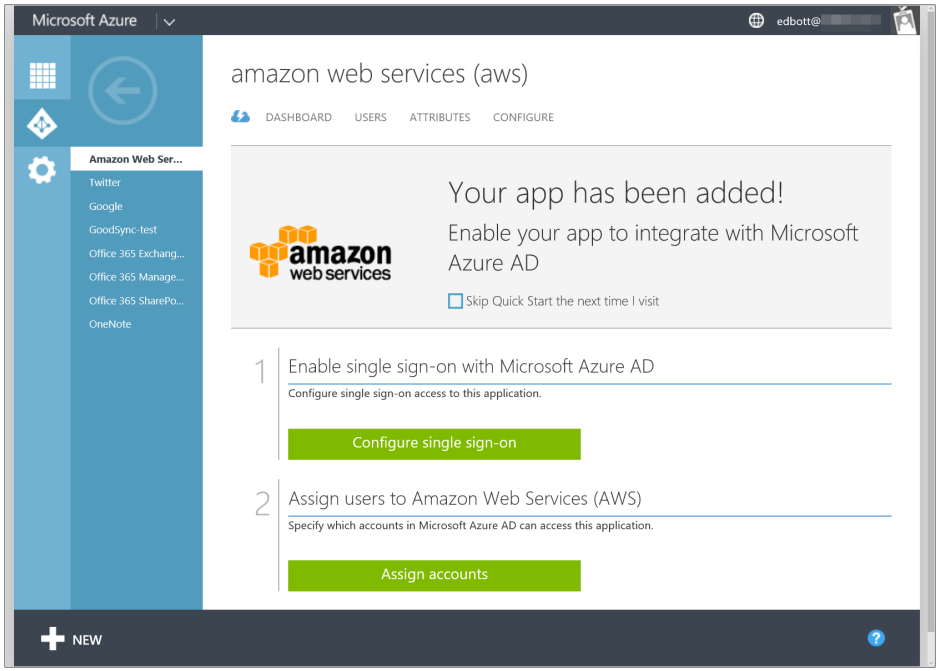


FIGURE 10-3 From the Azure Management Portal, you can integrate third-party web apps and online services and then assign them to users, allowing them to sign on without extra work.

Configuring single sign-on is a straightforward administrative task. You can establish a federation between two services, if that option is supported, or store external credentials for each user directly in Azure AD. You can also connect to a third-party SSO provider. Figure 10-4 shows these options in the Azure Management Portal.

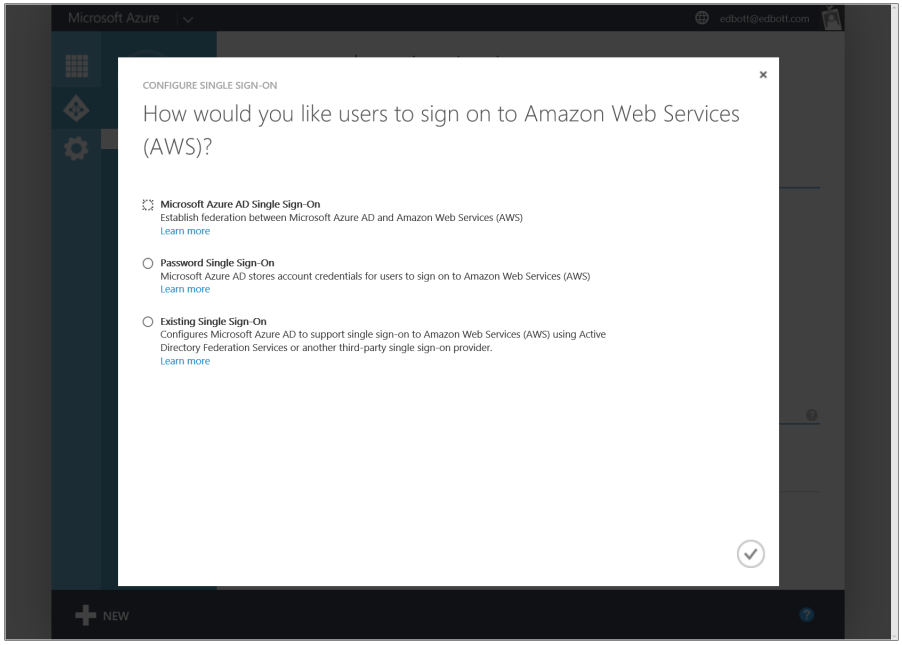


FIGURE 10-4 Configuring single sign-on options is done on a per-app basis and is available even with services that compete with other Microsoft cloud products.

If you choose to store account credentials for users as part of SSO configuration, you enter those details using the Azure Management Portal, as shown in Figure 10-5.

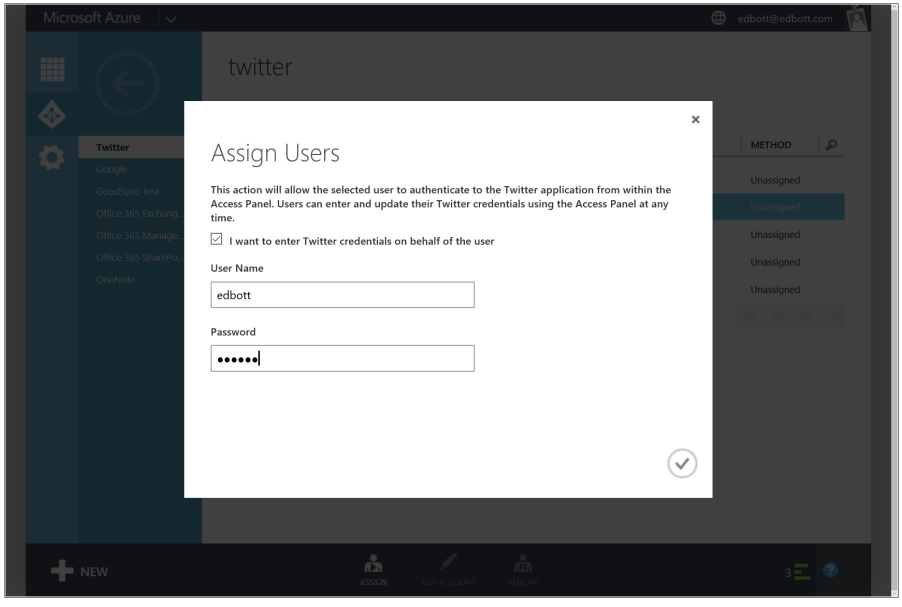


FIGURE 10-5 After integrating an online service like Twitter into Azure AD, you can store user credentials for individual user accounts. Those users can then sign in directly from the Azure AD Access Panel.

Note that even at the Free and Basic levels you can configure SSO and assign user access to as many SaaS apps as you want. Users, however, will see only 10 apps at a time in their Access Panel.

Joining a Windows 10 PC to Azure AD

Just as you can join a Windows 10 Pro or Enterprise PC to an Active Directory domain, you can join a Windows 10 device to Azure AD. This option is most common in scenarios where you plan to use the device to access local resources and cloud services but don't need a full domain join.

The best time to join a PC to Azure AD is during the initial setup of a Windows 10 device. Figure 10-6 shows the page where you begin the process by specifying that you are setting up a company-owned PC.

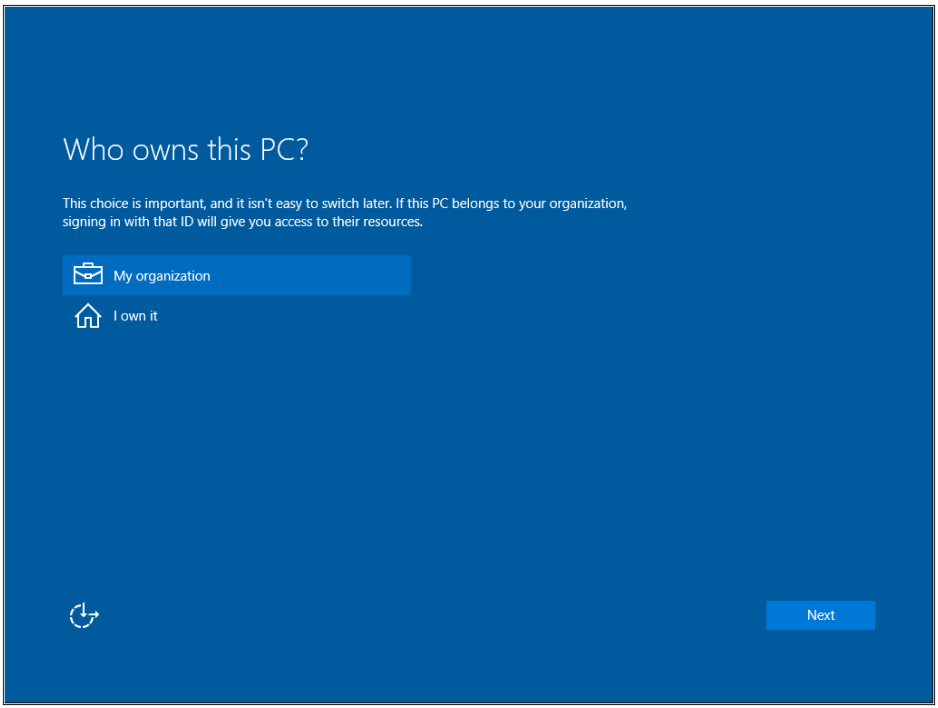


FIGURE 10-6 This step appears in the final stages of setup for a new PC running Windows 10 Pro.

Choosing that option leads to the page shown in Figure 10-7, where you have the option to join Azure AD. (If you choose the option to join a domain, you create a local account and then join it to the domain later.)

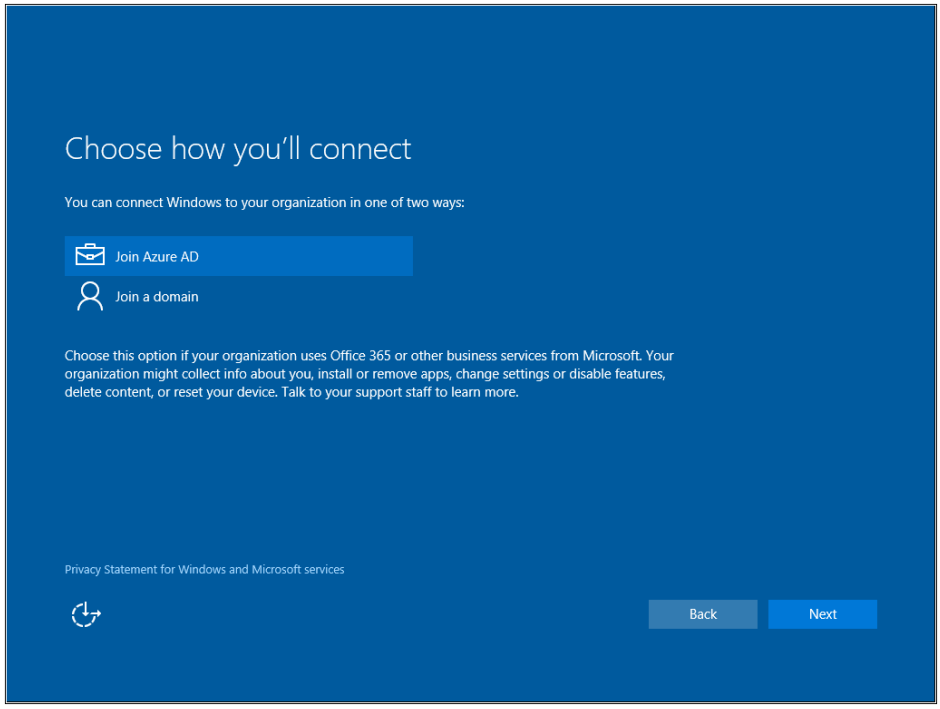


FIGURE 10-7 When setting up a PC for use primarily on a corporate network, you can choose to use your Azure AD credentials or do a more traditional domain join.

After you click or tap this option and enter Azure AD credentials, the process varies depending on how your Azure AD administrator has configured settings. You might be required to verify your identity at this point, using multifactor authentication to enroll the device and set a PIN for access. You're also informed in clear terms that the company's policies will be enforced as part of your ability to sign in on this device.

Figure 10-8 shows the final portion of this setup process, where the user must agree to accept the server policies.

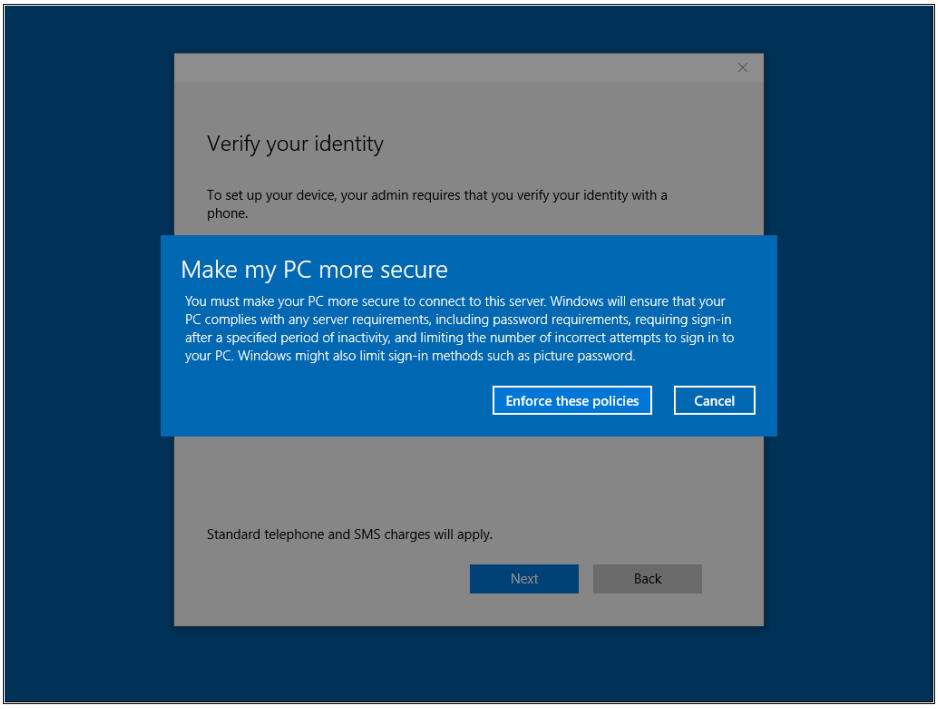


FIGURE 10-8 Joining a Windows 10 PC to Azure AD means that company policies will override some default settings in Windows.

When the process is complete, you can see the current enrollment on the About page in Settings. The Organization name is defined by your organization's settings in Azure AD, and the page includes a button you can click to disconnect from the organization (which also removes your access to the cloud services and organization resources associated with that ID).

This same page is your starting point if you want to join Azure AD on a PC where Windows is already set up. Figure 10-9 shows where you'll find the Join Azure AD button.

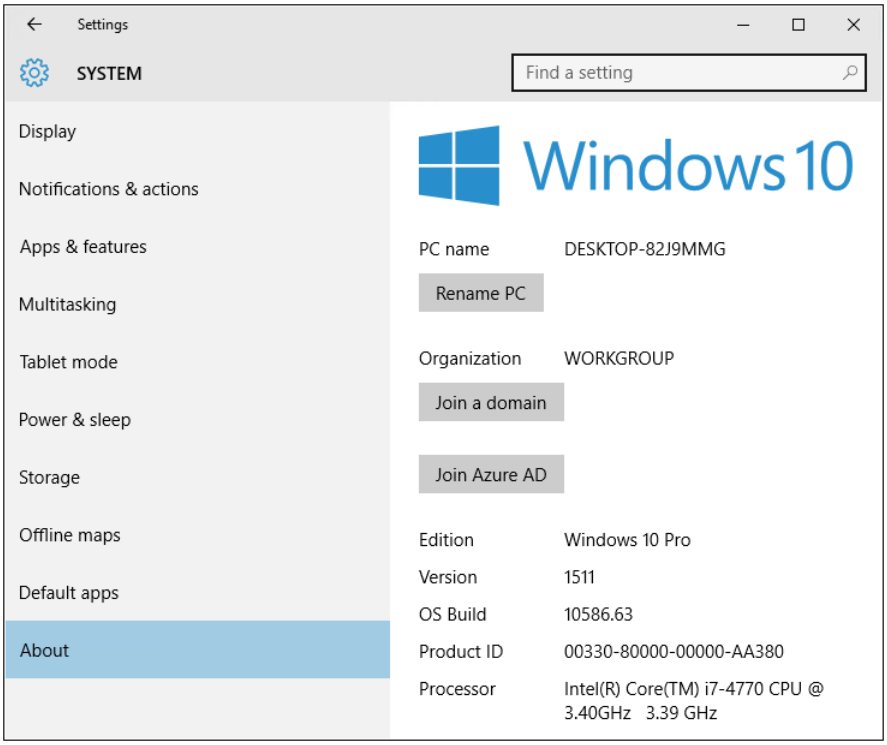


FIGURE 10-9 The System, About page in Settings allows you to join Azure AD on a system that has already been set up with Windows 10.

At any time, users can access their Azure AD accounts, for self-service password changes or for SSO access to apps. You can reach this link by choosing the Azure AD account from the bottom of the Accounts page in settings, or by visiting the account management page in a web browser, at *https://account.activedirectory.windowsazure.com*. Figure 10-10 shows what you see. Note that any apps configured for SSO appear on the Applications pane.

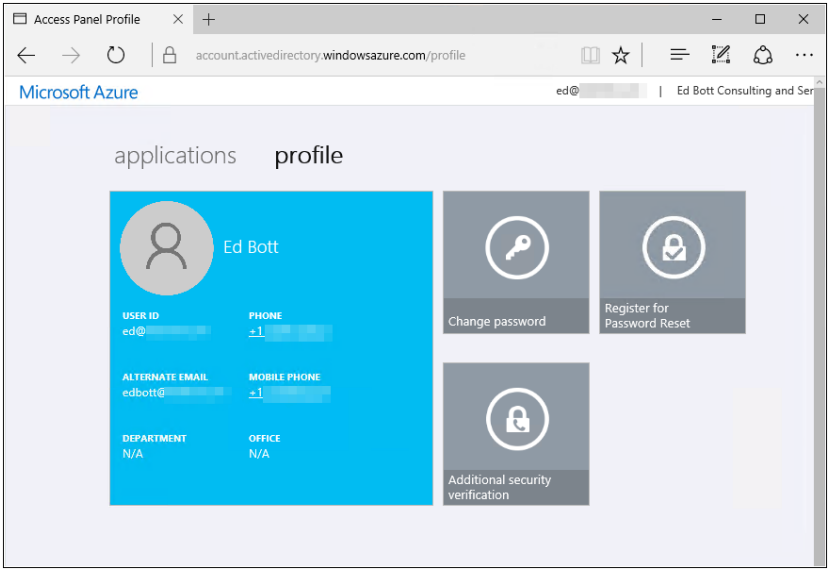


FIGURE 10-10 The Azure AD Access Panel profile allows users to manage information, change or reset passwords, and access preconfigured apps from the App Panel.

Adding work accounts to Windows 10

On personal devices running Windows 10, joining Azure AD isn't always an option, but you can still get some of the benefits of Azure AD by adding a Work or School account using your Azure AD credentials. That step allows you to sign in to Office 365 automatically and use the Azure AD Access Panel.

The process is straightforward. Start from the Accounts page in Settings and then click or tap Work Access to view the options shown in Figure 10-11.

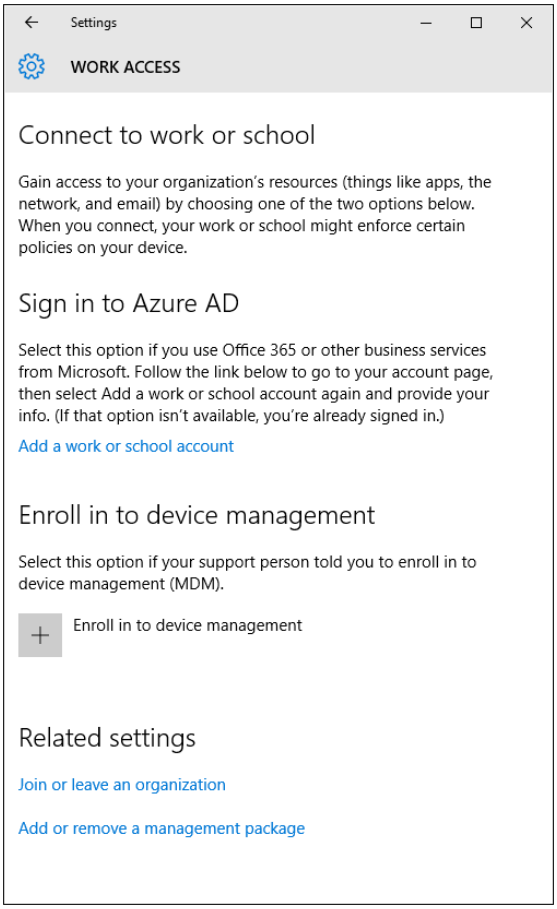


FIGURE 10-11 Adding a work or school account allows you to connect to Office 365 and other services without having a fully managed device.

CHAPTER 11

Universal apps and the new Windows Store

The fundamental dividing line between Microsoft Windows 7 and its successors is the capability of more recent Windows releases to run a new class of apps, informally known as modern apps but formally designated as Trusted Windows Store apps. Windows 10 can still run virtually all classic Windows desktop programs, of course; the new apps add another set of options. Because they're optimized for touch and mobile use, they're easier to use on tablets and hybrid mobile devices. And because they are distributed through the Windows Store, they're inherently more secure and easier to deploy.

This chapter provides an overview of those apps, the new Store common to all Windows 10 editions, and a new set of capabilities called the Windows Store for Business.

The Universal Windows Platform

Apps originally developed for Windows 8 and 8.1 ran only in full-screen mode or snapped to the side of a display. In Windows 10, each modern app, including the built-in Settings app and Microsoft Edge, can run in its own window and can be pinned to the taskbar. This change in behavior makes the new apps first-class citizens alongside their classic Windows desktop counterparts.

The first generation of modern apps, built for Windows 8, used an application architecture called the Windows Runtime (WinRT). With the release of Windows 8.1, that platform was extended to Windows Phone 8.1, allowing developers to build Universal Windows 8 apps that were separate but shared a great deal of common code.

With Windows 10 Microsoft introduced the Universal Windows Platform (UWP), a highly evolved descendant of WinRT that provides a common app platform for every Windows 10 device. Apps built using the UWP don't just share code; they run the same code, targeted to different device families. Some application programming interfaces (APIs) are universal, available on all device families. Child device families have their own APIs in addition to the universal device APIs. A guide to UWP apps, published at the Windows Dev Center (*http://bit.ly/uwp-guide*), is aimed at Windows 10 developers but offers an excellent overview for IT pros as well.

As the authors of that guide note, the addition of the UWP to the Windows 10 unified core makes a huge difference in the capabilities of modern apps:

> *As part of the core, the UWP now provides a common app platform available on every device that runs Windows 10. With this evolution, apps that target the UWP can call not only the WinRT APIs that are common to all devices, but also APIs (including Win32 and .NET APIs) that are specific to the device family the app is running on. The UWP provides a guaranteed core API layer across devices. This means [developers] can create a single app package that can be installed onto a wide range of devices.*

Using the Universal Windows Platform, developers can build apps that are significantly more powerful than their predecessors. These apps can be targeted at any or all those device families, from phones and small tablets to PCs and the Xbox One game console to, ultimately, wearable devices and other nontraditional form factors collectively known as the Internet of Things (IoT), running Windows 10 IoT editions.

Note For more details on the Windows 10 IoT family, see *https://www.microsoft.com/en-us/WindowsForBusiness/windows-iot*.

Most importantly, Windows 10 allows those apps to be delivered through a single store to all those devices. IT pros whose concerns focus on deploying, managing, and securing enterprise apps will want to look carefully at the Windows Store for Business, a new addition in Windows 10 version 1511, which can be extended to deliver universal Windows apps and traditional desktop applications in a managed environment through secure business portals.

Introducing the new Windows Store

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

For starters, the new Store (which is itself a UWP app) offers more than just apps, with games, movies, TV shows, and music available in digital formats for purchase and rent as well. Using a common search box, you can find items in a single category or across the entire Store, as shown in Figure 11-1, with the option to refine your search results.

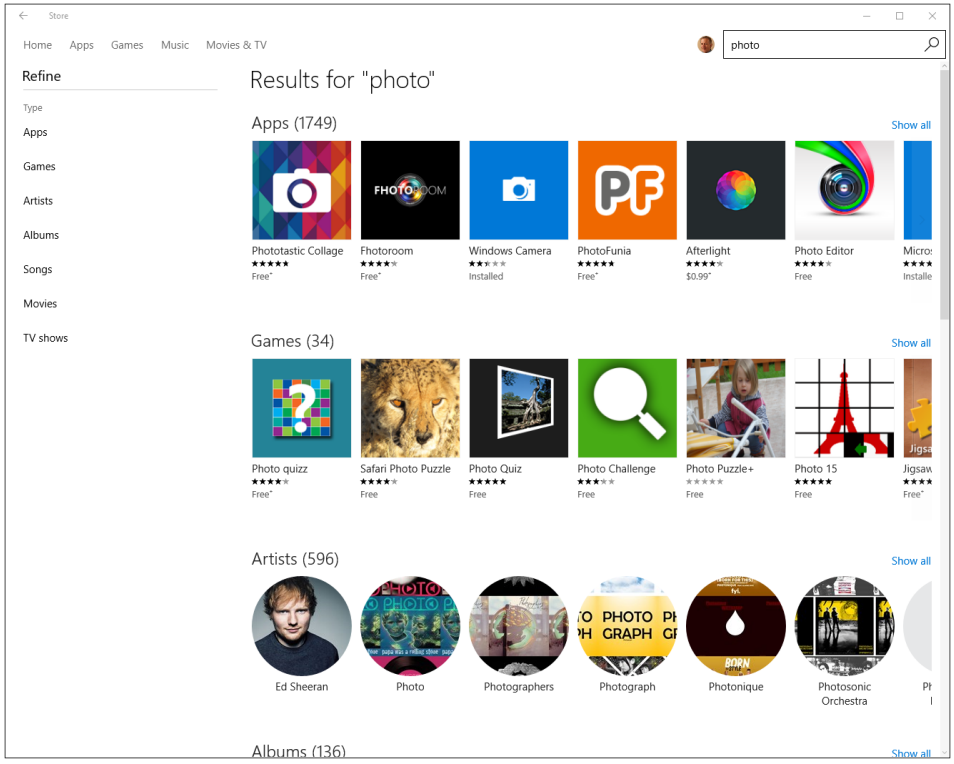


FIGURE 11-1 The Windows 10 Store offers excellent search capabilities and access to more than just apps.

The new Store also includes a more detailed summary of apps you previously installed, with the capability to update apps automatically in the background. When you're signed in to the Store, you can click the current status of downloads and app installs, and you have the capability to pause, resume, and cancel downloads. Figure 11-2 shows this feature in action.

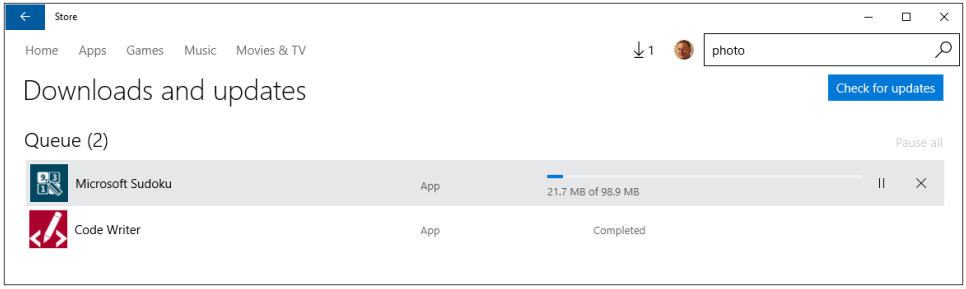


FIGURE 11-2 Clicking your user picture (to the left of the search box) opens a menu that gives you access to settings and account options. You can view and manage current app downloads and updates from this page.

To manage devices associated with a Microsoft account, sign in at *https://account.microsoft.com* and use the Devices tab. You can view all devices that have signed in to the current Microsoft account, and you can see details about that device and its operating system, as shown in Figure 11-3.

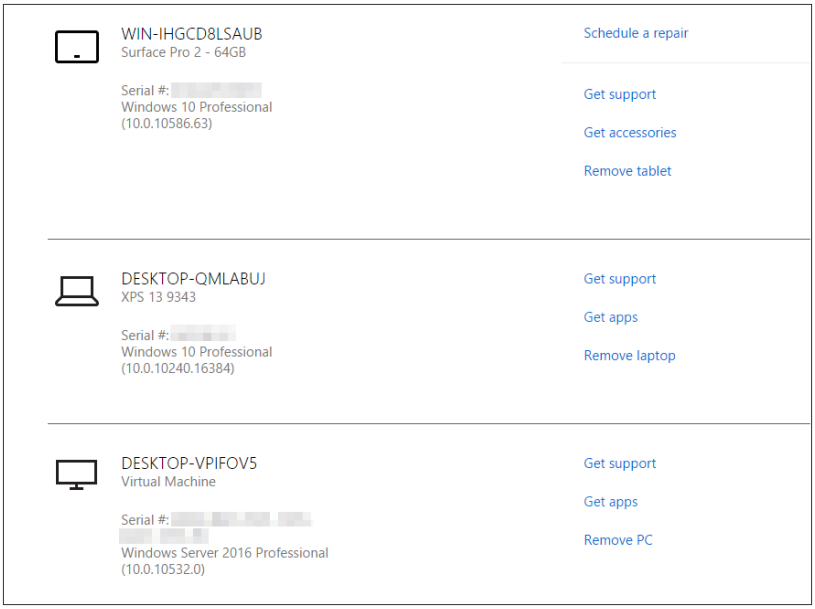


FIGURE 11-3 The Devices tab of the Microsoft account management page lists all devices that have signed in with a particular ID. It supports PCs, laptops, tablets, and phones.

For Microsoft devices, such as Surface tablets, the warranty status and support links are available in this list.

Apps acquired from the Windows 10 Store (free and paid) can be installed on up to 10 devices. A separate list of devices associated with the signed-in user's Store account is available from the Microsoft account page, where you can remove apps if you need to free up a new device for installing an app. Figure 11-4 shows this feature in action.

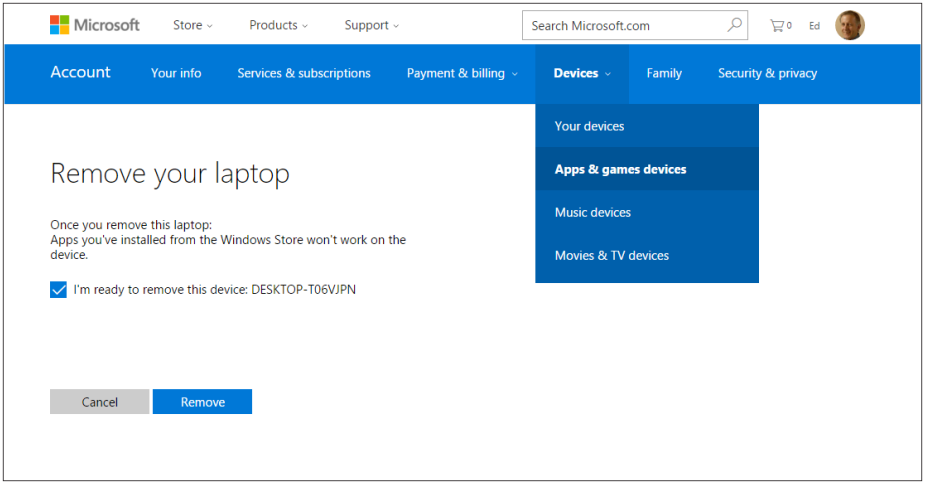


FIGURE 11-4 In Windows 10, apps can be installed on up to 10 devices. Use this page to remove a device from the list of those authorized to install apps from the associated Microsoft account.

For consumer and small-business users of Windows 10, the public Windows Store is the primary means to acquire apps, using a Microsoft account and various payment options. With the new Windows 10 Store, enterprise options are considerably richer.

Before I get to that story, though, it's useful to see the new UWP apps in action.

How Universal Windows Platform apps work

UWP 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.
- Third-party apps can be removed easily, with the exception of a handful of preinstalled apps (also called *provisioned* apps) that can be removed only by using Windows PowerShell commands.
- Every app has an application tile that can be programmed to update dynamically, making it a *live tile*. Apps can also trigger notifications and alerts, using standard APIs. Each user controls the display of information in live tiles and can disable notifications and alerts globally or on a per-app basis.
- 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 benefit is those limitations help ensure the security and reliability of the underlying operating system by blocking the most common attack vectors.

Because UWP 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.

The Groove Music app, included with all editions of Windows 10 except the Long-Term Servicing Branch, offers an excellent illustration. In Figure 11-5, the window is wide enough to display the navigation bar on the left, with full details about the current album on the right.

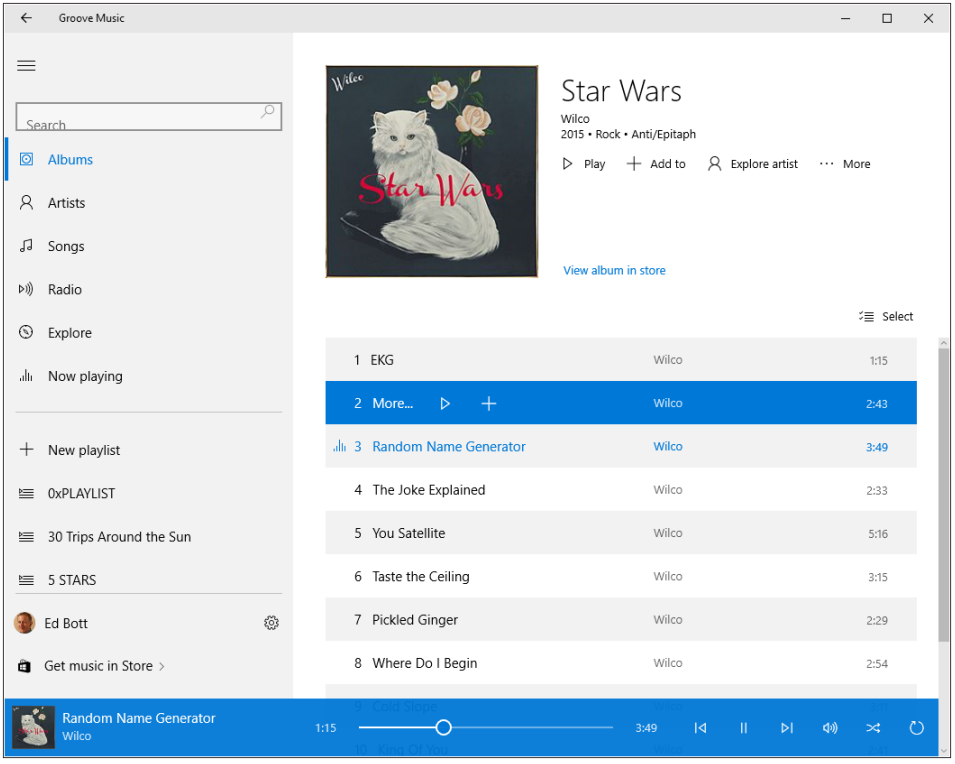


FIGURE 11-5 The adaptive user experience in Windows 10 allows a Universal Windows Platform app like Groove Music to show you more information when screen real estate is available.

As you make that window narrower, the navigation bar first shrinks to a column of icons and then disappears completely, leaving the spare but usable display shown in Figure 11-6.

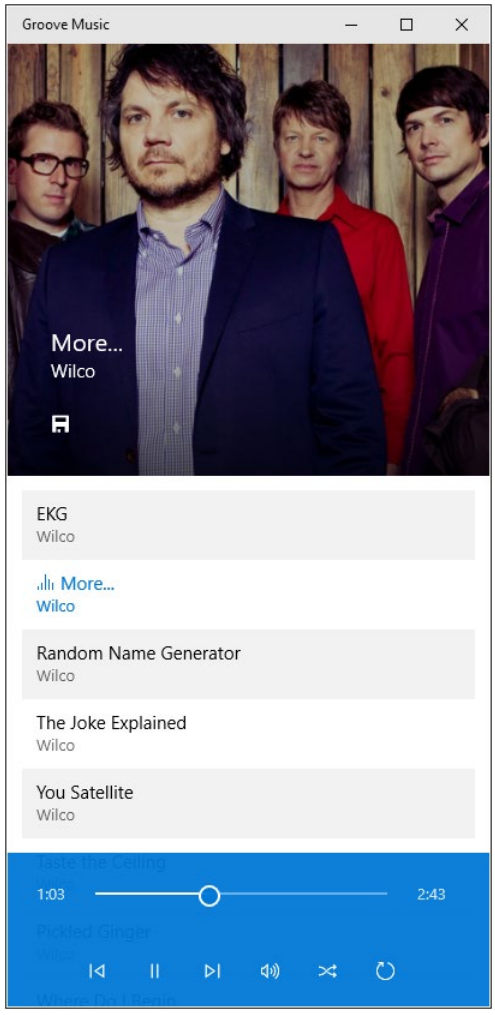


FIGURE 11-6 By contrast, in a smaller window (or on a smaller screen), UWP apps such as Groove Music adapt to the minimal space by hiding navigation elements.

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. Windows 10 also includes News, Sports, Money, and Weather apps, powered by MSN.

As part of a Windows 10 deployment, you might want to remove one or more of these provisioned apps, either manually or as part of the process of preparing a system image for deployment. One technique is to use PowerShell commands, specifically the Get-AppxPackage and Remove-AppxPackage cmdlets, with deployment tools. Microsoft's Ben Hunter documents this process in an article that was written for Windows 8.1 but still applies to Windows 10: *http://bit.ly/remove-built-in-Windows-apps*. An updated version of the script, courtesy of Michael Niehaus, is capable of dynamically determining a list of apps that are removable. That article is available here: *http://bit.ly/remove-windows-10-apps*.

A new feature introduced with Windows 10 version 1511 automatically installs some games and apps from the Windows Store for the signed-in user. These apps vary by region and are aimed primarily at consumers. To prevent them from being installed, enable the Group Policy setting Turn Off Microsoft Consumer Experiences, located under Computer Configuration > Administrative Templates > Windows Components > Cloud Content, as shown in Figure 11-7.

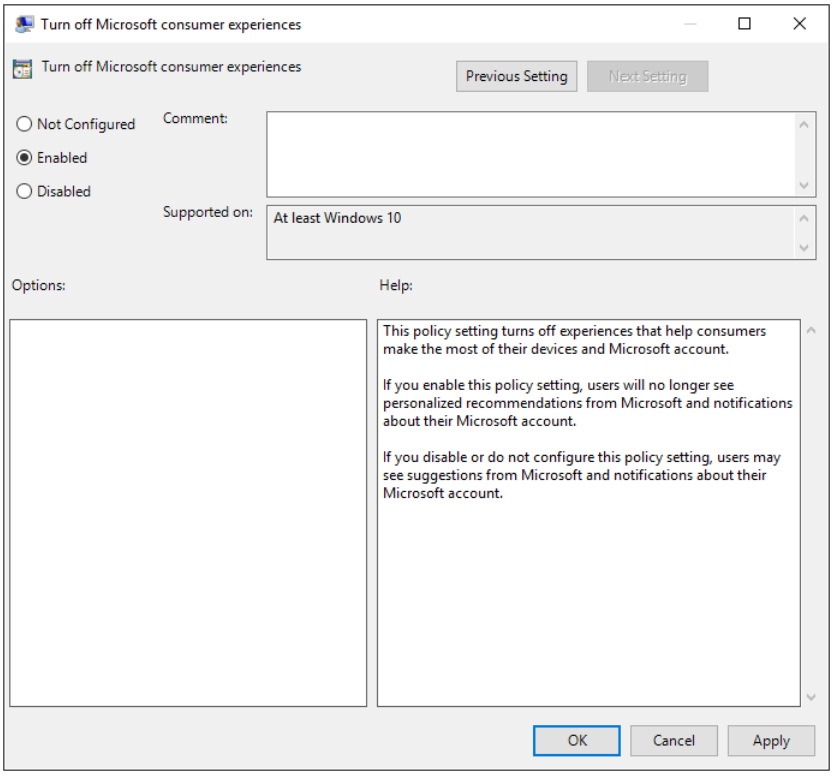


FIGURE 11-7 To prevent games like Candy Crush from being installed on users' machines, enable this setting via Group Policy.

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.

Using the Windows Store for Business

Enterprises running Windows 10 can develop universal line-of-business (LOB) apps and make them available to users inside their organization. They can also purchase licenses for Windows 10 apps and allow their employees to install those apps without requiring a Microsoft account. These apps can be deployed in either of two ways: through a private store, managed and deployed by the Windows Store, or through a process called *sideloading*.

The Windows Store for Business debuted with Windows 10 version 1511. Organizations with an Azure Active Directory infrastructure can use this capability to allow users to sign in with their Azure AD accounts and view, download, and install apps. Licenses are managed and tracked by the Windows Store for Business.

To begin building a custom Windows Store for Business, sign in at *http://businessstore.microsoft.com* using Azure AD administrative credentials. Figure 11-8 shows the inventory-management page for one such store, with a handful of apps available for use within the organization.

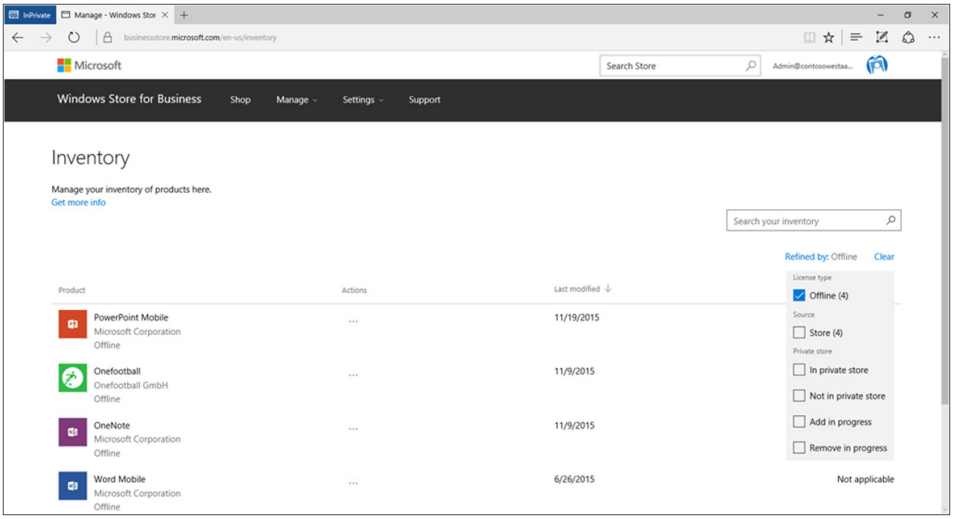


FIGURE 11-8 The Windows Store for Business has a look and feel similar to the public Store but is restricted to members of your organization who sign in with an Azure AD account.

Admins can add apps to the private store, which appears as a tab in the Windows Store for Business for members of the Azure AD organization. Only apps with online licenses can be added to the private store, either when you as administrator acquire the app or by assigning it from inventory later. Once the app is in your private store, employees can claim and install the app.

Figure 11-9 shows the process of adding an app to the inventory in a private store.

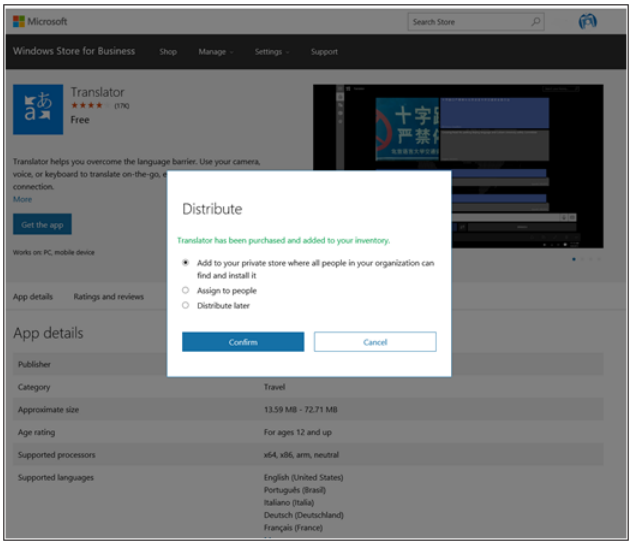


FIGURE 11-9 As a Windows Store for Business administrator, you can select apps from the public Store and make them available privately to members of your organization.

Updates are delivered via normal update channels—Windows Update or Windows Server Update Services (WSUS).

LOB apps can be distributed within an organization using mobile device management (MDM) software or deployment tools, such as System Center Configuration Manager or Microsoft Deployment Toolkit, without any connection to the Windows Store. This process, called *sideloading*, doesn't require that the apps be signed by Microsoft, nor are Azure AD accounts necessary. The apps must, however, 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 individually using deployment tools or MDM software.

This feature is still new and is evolving quickly. For a walkthrough of one scenario, see the article "Using the Windows Store for Business with MDT 2013," at *http://bit.ly/Windows-Store-for-Business-with-MDT2013*.

CHAPTER 12

Storage

One absolute constant in every version of Microsoft Windows since its earliest days is the need for built-in storage to accommodate the operating system, settings, apps, data files, and digital media. But the details of storage subsystems have changed dramatically since the early days.

Just a few years ago, for example, a solid-state drive (SSD) was a luxury reserved for only the priciest of systems. Today, SSD prices have dropped to affordable levels, with flash storage as an alternative for low-cost devices and traditional hard drives often used as secondary storage or accelerated with an SSD cache.

At the same time, the move to solid-state storage on portable devices has dramatically reduced the average size of the default drive. Manufacturers of some portable PCs in early 2016 now offer a choice of SSD (typically 128 GB at the low end) or a much larger conventional hard drive. That means buyers have to choose between fast but limited storage and larger drives that are slower and less reliable.

Over the years, PC makers steadily increased the size of the primary system drive. As the SSD era began, that trend reversed. For tablets and inexpensive portables, the primary system drive can shrink to very small sizes indeed, with a new Compact OS mode enabling Windows 10 to work with primary storage devices that would have been too small to run some earlier versions of Windows comfortably.

DVDs are increasingly an endangered species, but thanks to the USB standard, removable drives that use other form factors are more common than ever.

This chapter offers a high-level overview of the many storage options available across the ecosystem of devices running Windows 10, starting with a look at the tools for managing fixed and removable storage.

Storage Tools

As an IT pro evaluating Windows 10, you have an eclectic selection of tools to examine, configure, manage, and troubleshoot storage devices. Some of these tools will be familiar even to the oldest of old-time Windows users. Others are new in Windows 10 and presage a slow but steady migration of core functions such as these to the modern Windows 10 user interface.

Disk Management

The most important of all storage tools is the Disk Management console, Diskmgmt.msc, shown in Figure 12-1. (The fastest way to open this console is to right-click Start or press Windows key + X to open the Quick Links menu, and then click or tap Disk Management.)

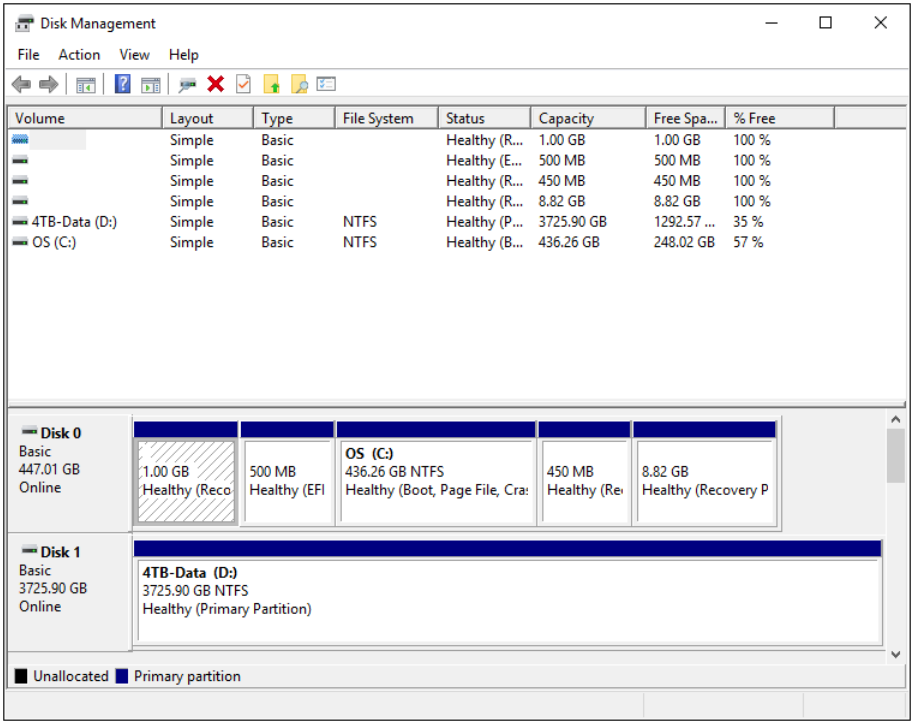


FIGURE 12-1 The Disk Management console should look familiar to even the most grizzled IT pro.

DiskPart

For more advanced disk-management tools, the DiskPart utility is available. As shown in Figure 12-2, it runs in an elevated Command Prompt window, with its own command-line-driven environment you can use to enumerate, select, and manage disks, volumes, and other storage objects.

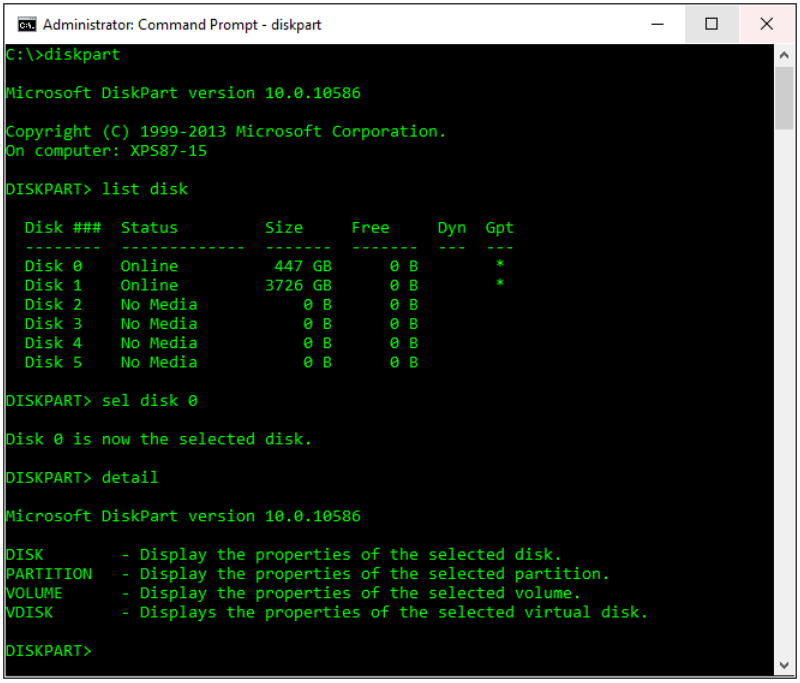


FIGURE 12-2 To see a full list of DiskPart commands, type Help. Type any command with no arguments to see the available syntax for that command.

One of the most powerful DiskPart commands is Clean, which immediately removes every bit of partition or volume formatting from the currently selected disk. This command sets every byte and every sector on the disk to zero, which completely deletes all data contained on the disk and erases any disk formatting that had been previously applied to the disk. (Technically, it might be possible for an expert with advanced technology to recover data from a drive that had been erased in this way, but that would involve a tremendous amount of effort.)

Storage Sense

The Storage Sense display is completely new in Windows 10 and can be found by choosing System and then Storage from the new Settings app. As Figure 12-3 shows, the initial display lists available fixed storage devices, with a graphical display of used and free storage, followed by a list of default storage locations for standard data folders.

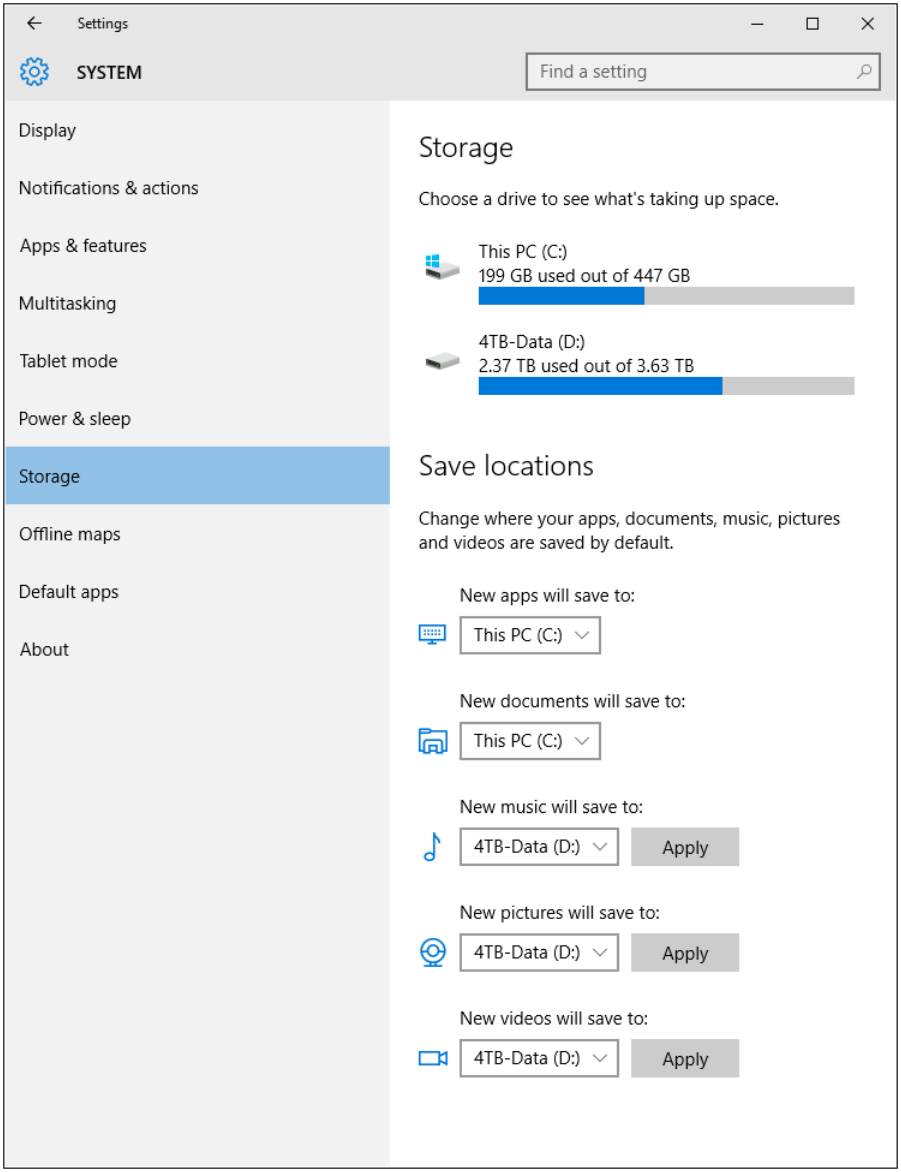


FIGURE 12-3 The Storage interface offers an overview of available storage and includes the option to move the location of default data folders.

Clicking the entry for any drive in the Storage pane displays a listing of usage organized by file categories, as shown in Figure 12-4. (In case you're wondering, the very large Other category in that figure includes virtual hard disk files for Hyper-V virtual machines.)

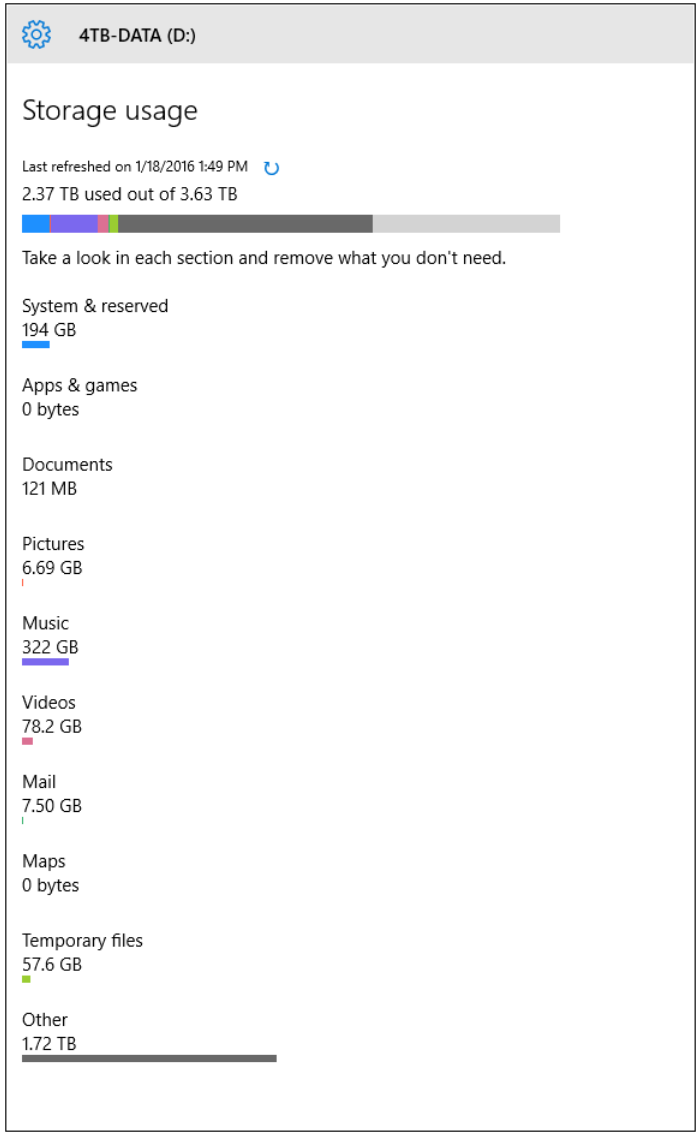


FIGURE 12-4 Clicking any drive in the Storage pane displays a detailed list of how its space is being used, as broken down by file categories.

File History

The File History feature was introduced in Windows 8 as the latest in a long line of backup solutions for individual Windows PCs. It continues in Windows 10 with only minor modifications.

File History (which is the direct descendant of the Previous Versions feature from older Windows versions) requires either an external drive or a compatible network location as the backup drive.

After you choose a File History drive and enable the feature, Windows begins saving copies of all files at regular intervals, giving you a backup from which you can recover older versions of individual files or entire folders or drives. In conjunction with the ability to restore saved settings and Windows Store apps using a Microsoft account, it allows a very quick transfer from one primary computing device to another.

As is common with many such features, you can configure File History from either of two entry points. One is in the Windows 10 Settings app, where a search for File History turns up a simple page with an on-off switch and a More Options link that opens a Settings pane like the one shown in Figure 12-5.

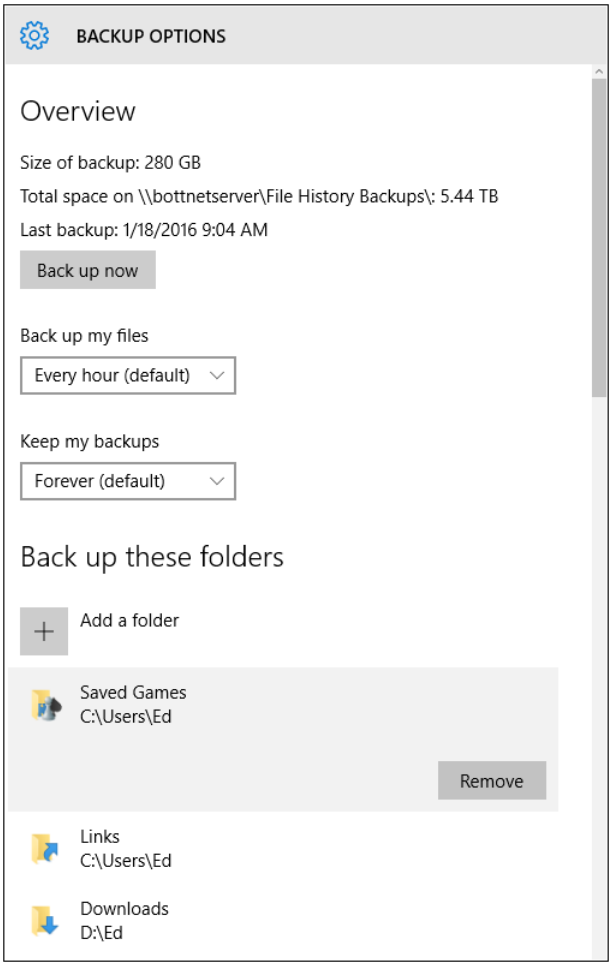


FIGURE 12-5 The list of folders to be backed up using File History extends far beyond the three folders shown here.

The alternative entry point, with many duplicated controls and a few unique options, is in the classic Control Panel, as shown in Figure 12-6.

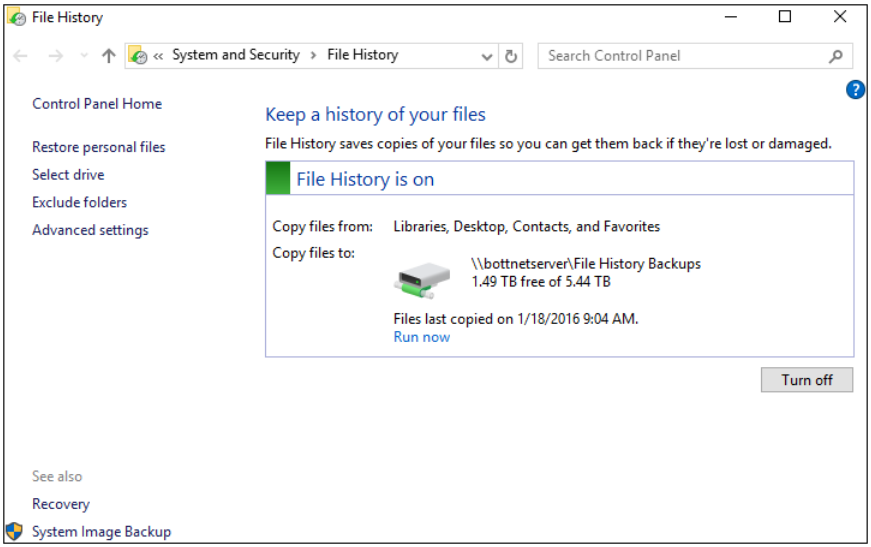


FIGURE 12-6 The classic Control Panel view of File History offers options to restore backed-up files from a File History drive. Note in this case that the backup target is a shared network drive.

Over time, most of these functions should migrate to the newer Settings app.

Advanced Storage Options

Up until this point, most of the features I've been describing have been applicable to standard desktop or laptop PCs, with a single system drive and possibly some external data storage. In this section, I discuss two esoteric features that are worth exploring, especially if you're migrating from Windows 7.

Storage Spaces offers a software-based way to combine multiple physical storage devices into a single virtual device without relying on hardware-based features such as Redundant Array of Inexpensive (or Independent) Disks (RAID).

You use the Storage Spaces console to turn two or more storage devices into a single virtual device, called a Storage Space, which has its own drive letter and acts for all practical purposes as if it were a physical drive. Figure 12-7 shows one example, with a 512-GB drive and 256-GB drive combined into a virtual drive accessible via File Explorer as drive F.

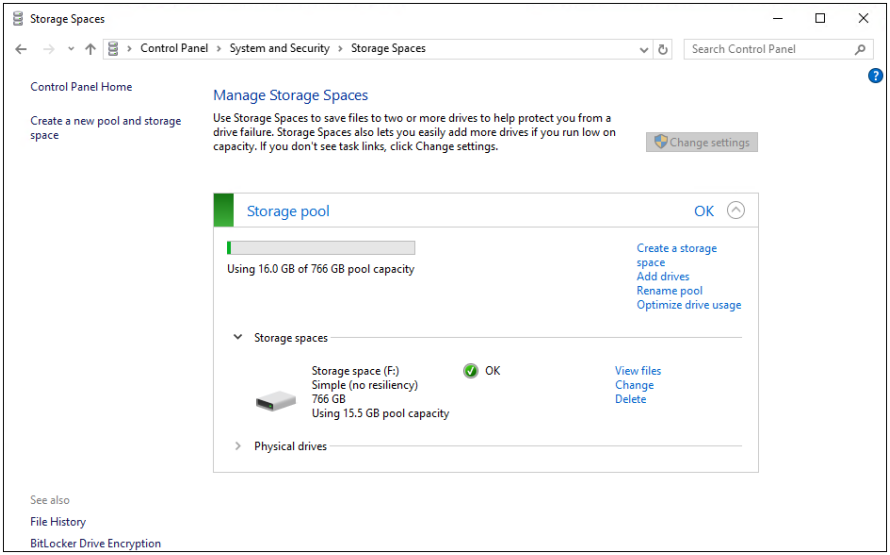


FIGURE 12-7 The Storage Spaces feature lets you combine multiple physical drives into a single virtual drive. This example simply combines the space into a single pool.

The process of creating a Storage Space allows you to choose from four types of spaces. A space created using the Simple option just combines the multiple capacities to give a virtual drive whose capacity is literally the sum of its parts. But with the right number of physical devices, you can also choose resilient options to protect your data from the failure of a physical drive. Figure 12-8 shows the options available under the Resiliency heading when creating a new Storage Space.

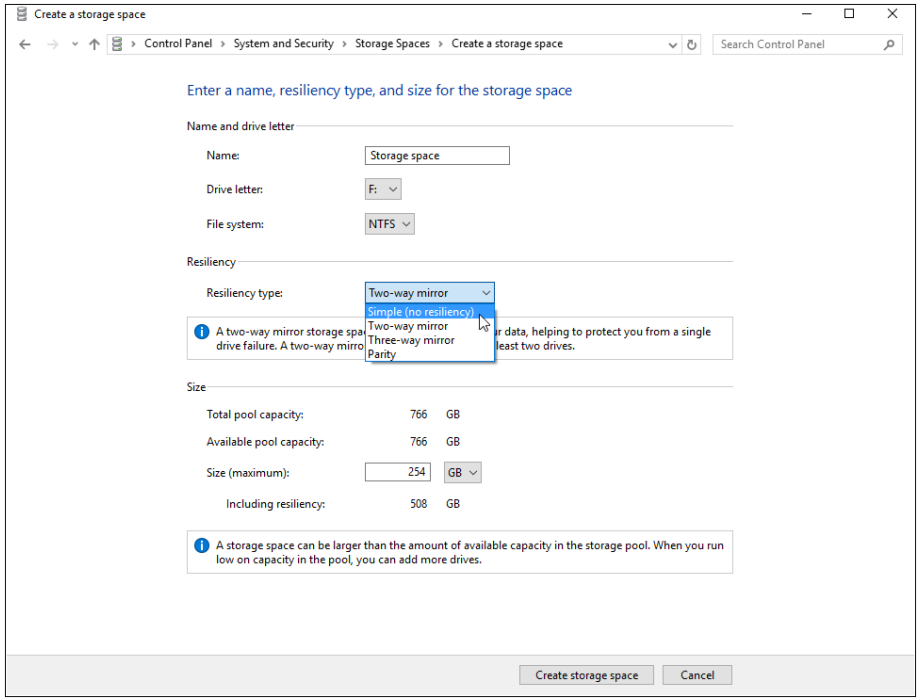


FIGURE 12-8 With enough physical drives, you can create Storage Spaces that add resiliency so that you can recover data even when a physical drive fails.

The other advanced option that every IT pro should know about is the option to create and mount a Virtual Hard Disk (VHD) file as if it were a physical drive. The advantage of VHDs is that they can be moved easily from machine to machine and mount directly when double-clicked in Windows 10. (The ability to mount a VHD was introduced in Windows 8; on Windows 7 PCs, this action requires third-party software.)

In the Disk Management console, you have two very obscure but useful options, for creating a new VHD that acts as if it were a separate hard drive or for attaching an existing VHD file using its own drive letter. If you routinely save software files and templates in a standard location, the option for creating a new VHD might make it easier to migrate to a new PC, by simply copying a single VHD file instead of locating an entire folder of files. Figure 12-9 shows this feature in action, after clicking the Create VHD option from the Action menu in the Disk Management console.

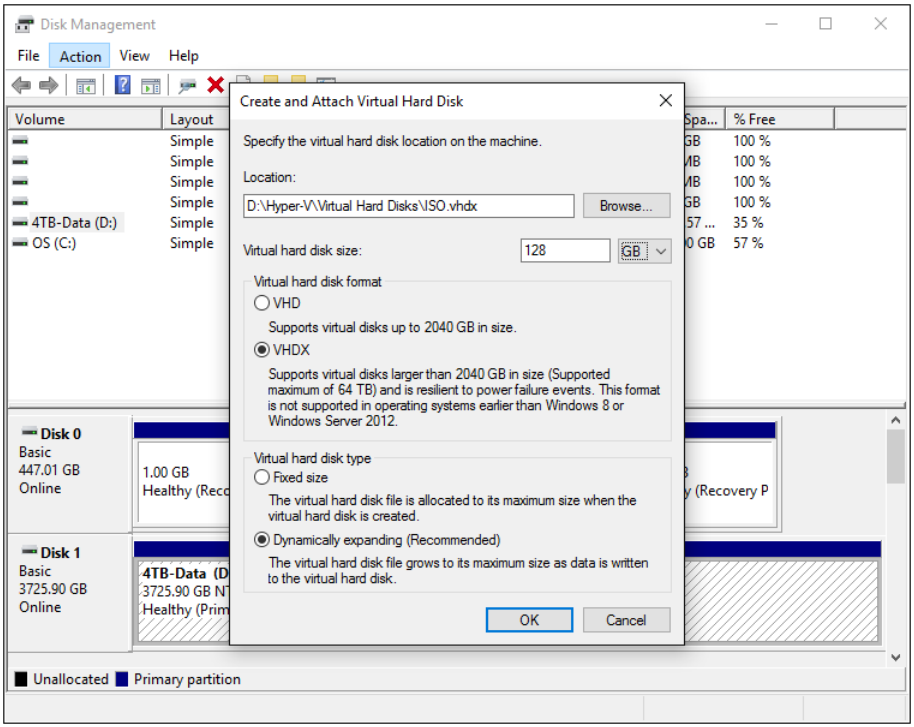


FIGURE 12-9 Click the Action menu in Disk Management and then choose Create VHD to open this dialog box. Choose a location and a file name to create a virtual hard disk that acts like a separate physical drive.

Finally, for fixed and removable storage devices, Windows 10 Pro, Enterprise, and Education editions offer a full range of BitLocker and BitLocker To Go encryption features. A long list of improvements makes these features far easier to work with than their Windows 7 predecessors. Figure 12-10 shows a portable PC with an encrypted system drive and a removable SD card containing an encrypted volume.

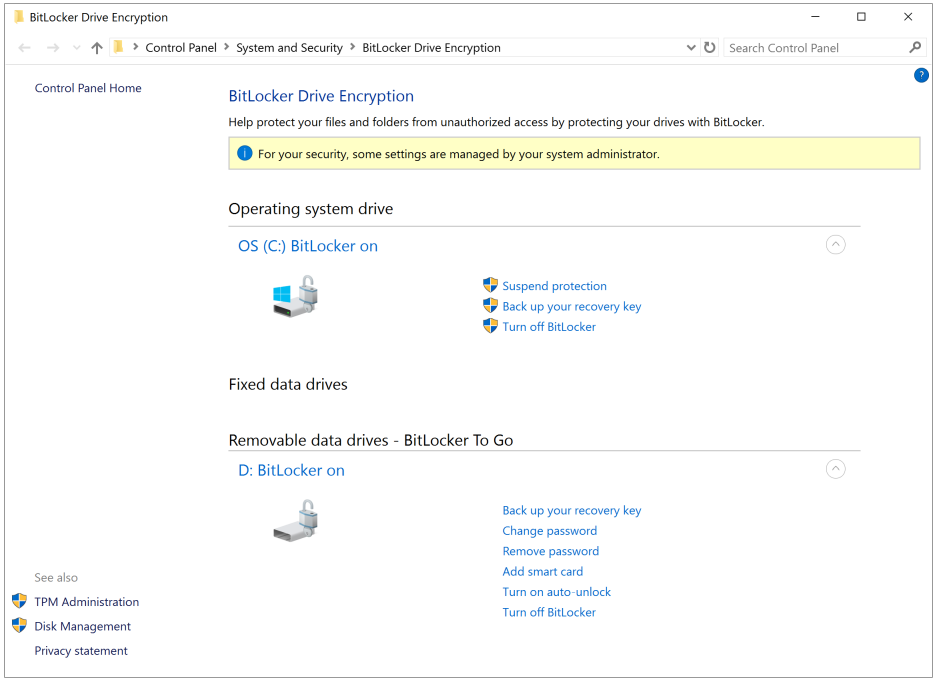


FIGURE 12-10 BitLocker capabilities are faster and easier to manage in Windows 10 than in previous versions.

CHAPTER 13

Managing mobile devices and enterprise data

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

Today, that's all changed.

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

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

Mobile device management strategies

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

- System Center Configuration Manager offers full management capabilities over traditional domain-joined Windows PCs, including those running Windows To Go and Windows Embedded. It also works with Apple-branded devices running OS X. Using the most recent release, System Center Configuration Manager (SCCM) and Endpoint Protection (Version 1511), you can manage Windows 10 devices via MDM directly.
- Microsoft Intune is a cloud-based service that can manage PCs running Windows 10, as well as mobile devices running Windows 10 Mobile, iOS, and Android. You don't have the same control as with a fully managed, domain-joined PC, but you can effectively exercise light control over predictable scenarios. Microsoft Intune can also be integrated into SCCM.

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

This management agent is available on most mobile devices, and it is included by default with all editions of Windows 10, with no additional software required. For PCs owned and managed by your organization, you can deploy the full Configuration Manager client. For personal devices that employees bring in as part of a BYOD strategy, joining the domain as a fully managed device is either impractical or impossible—personal devices running the Core edition of Windows 10 or Windows 10 Mobile lack domain-join capabilities. In that case, you can use Microsoft Intune to perform light management capabilities.

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

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

Two additional features also can be used as part of a BYOD strategy. Using Azure Active Directory (Azure AD), you can authenticate a personal device and allow the user to access corporate resources and applications. (I cover this feature in more detail in Chapter 10, "Integrating Azure Active Directory.") Work Folders is a simplified file-synchronization feature, introduced in Windows 8.1, that personal devices running Windows 10 can use to securely store and access files from a corporate network.

This chapter looks at all of the above strategies.

System Center Configuration Manager

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

Note If you've used previous versions of System Center Configuration Manager, you might notice the absence of a year in the name of the current release. That's a deliberate decision, one that reflects the strategy of releasing updates more frequently. As with Windows 10, Configuration Manager versions are now identified with a four-digit numeric string in *yydd* format, with version 1511 (and a Technical Preview version 1512) being current at the time of this writing. For an overview of version 1511, see the announcement at *http://bit.ly/system-center-1511*.

Configuration Manager is a user-centric tool designed to work with your organization's Active Directory infrastructure. This means that it associates hardware assets with specific users, allowing fine-tuned management of exactly which software and features are available to users. Configuration Manager also provides IT pros with a comprehensive reporting platform and deployment options.

Using Configuration Manager, you can perform the following functions:

- **Operating-system deployment/upgrades** The latest Configuration Manager release supports a wide range of deployment scenarios, including in-place upgrades to move systems directly from Windows 7 and Windows 8.1 to Windows 10. (I cover these scenarios more fully in Chapter 4, "Deploying Windows 10 in the enterprise.")
- **Application management** Configuration Manager includes a set of tools and resources you can use to package, manage, deploy, and monitor applications in the enterprise.
- **Endpoint protection** Security, antimalware, and Windows Firewall management features are included.
- **Compliance settings** Use built-in tools to assess and, if necessary, adjust the configuration of client devices to meet compliance requirements.
- **Company-resource access** Grant remote access to resources by setting up Wi-Fi profiles, virtual private network (VPN) profiles, and certificate profiles. For example, you can install trusted root CA certificates for your enterprise to authenticate Windows 10 devices on corporate Wi-Fi hotspots and VPNs.
- **Remote-connection profiles** Create and deploy remote-connection settings to devices, and thus make it easier for users to connect to their computer on the corporate network.
- **Inventory** As an administrator, you can collect detailed information about hardware, software, data files, and license usage on managed devices.

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

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

You can use Microsoft Intune (described in the next section) to manage Windows 10 devices that are not joined to the domain and do not have the Configuration Manager client installed.

Microsoft Intune

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

One of the unique features found in Microsoft Intune is its customizable company portal. The company portal is an interface customized with downloadable applications that IT administrators can make available for an organization. The company portal also allows users to directly contact IT and request remote assistance. Figure 13-1 shows the dashboard ready to begin managing mobile devices.

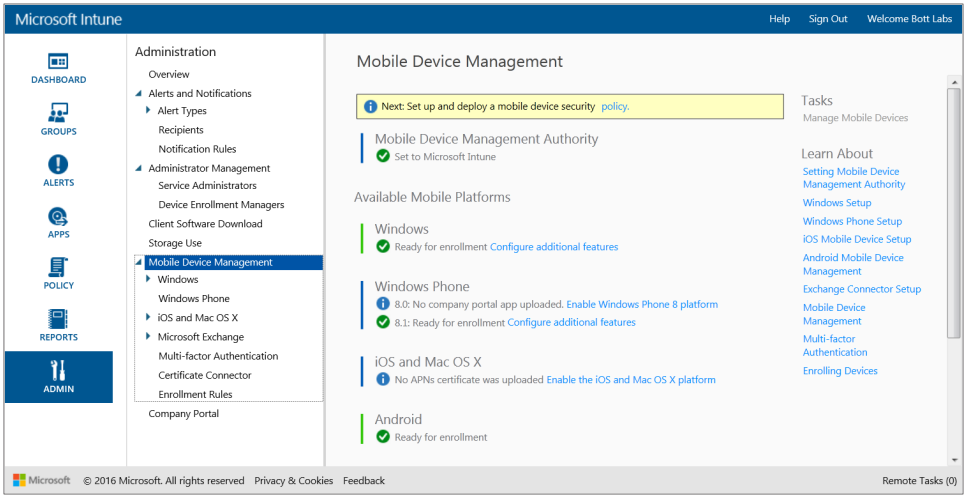


FIGURE 13-1 You can manage mobile devices, including those running Windows 10, from the Intune dashboard.

Managing a Windows 10 PC in Microsoft Intune (or on a third-party MDM server) involves installing a piece of client software, which can be manually deployed, automatically deployed using Group Policy, or installed as part of an image. (For details, see *https://technet.microsoft.com/en-us/library/dn646969.aspx*.) This client handles enrollment, a process that installs one or more certificates on the mobile device to manage authentication, and then periodically synchronizes with the management server to check for updates and apply new policies.

Microsoft Intune includes the capability to deploy apps automatically during enrollment, and users can install additional apps from a self-service company portal. Users can securely access corporate information using Microsoft Office mobile apps and line-of business apps, with management having the capability to restrict actions that can leak sensitive data, like copy and paste or save as, to only apps managed by Intune.

For Windows 10 PCs, you can configure and deploy classic Windows apps using the Intune Software Publisher, shown in Figure 13-2.

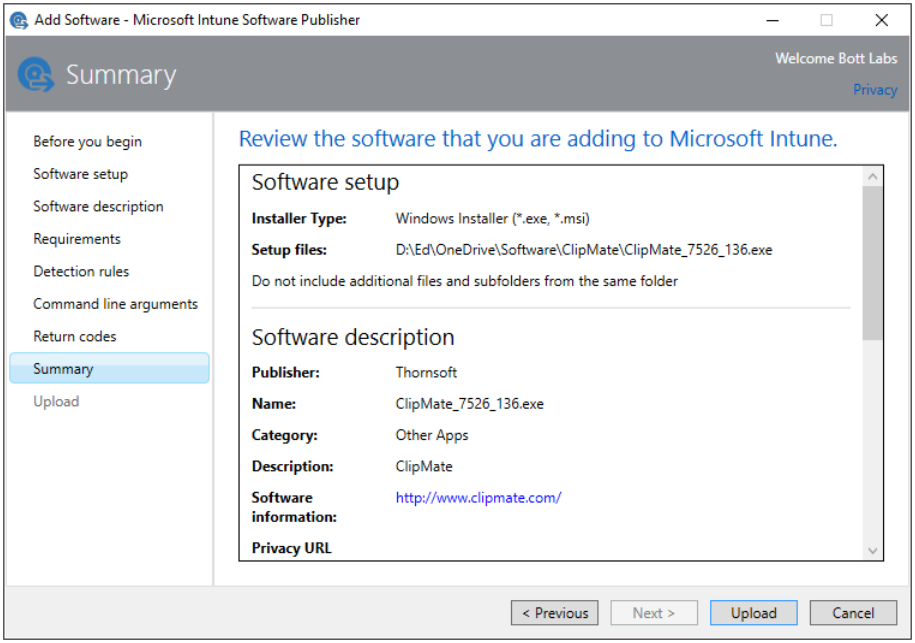


FIGURE 13-2 Microsoft Intune includes a software library where you can publish and deploy apps, including classic Windows desktop programs, for managed PCs.

Intune also can be used to remove corporate data and applications when a device is unenrolled, when it is determined to be out of compliance, or if it's lost, stolen, or retired from use.

Work Folders

Work Folders is another relatively new feature, supported on Windows 10 devices (and earlier versions) as well as mobile devices that connect to Windows Server 2012 R2 or later. With Work Folders enabled, a user can securely sync data to her device from a user folder located in the corporate data center, allowing the user to work with it offline. Files created or modified in the local copy of the folder sync back to the file server in the corporate environment. You can set up Work Folders on a multitude of devices running Windows, iOS, or another supported platform. If you store all your personal work files in the Work Folders location (with as many subfolders as you want to create), they'll roam with you to all your devices.

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

Windows 10 devices do not need to be domain joined for synchronization with personal files stored on the server. Your domain credentials unlock access to Work Folders, maintaining secure offline access to files.

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

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

On the client side, syncing is natively integrated into the file system. To connect to Work Folders, you start in the desktop Control Panel by clicking the Set Up Work Folders option shown in Figure 13-3.

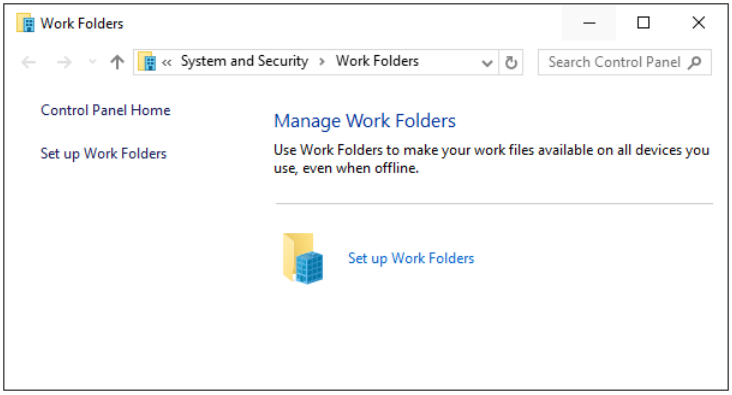


FIGURE 13-3 The Work Folders capability is built into the desktop Control Panel in all editions of Windows 10.

That, in turn, leads to a straightforward wizard where you enter either your email address or the URL that the administrator established and then accept the security policies associated with the data files in the Work Folders share, which includes the right to remotely delete them. Some device capabilities, such as encryption of the synced folder and a password-protected screen lock, might be required.

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

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

OneDrive for Business provides access to Microsoft SharePoint resources and personal files stored in the Office 365 cloud. It is designed primarily for data collaboration in teams, with strong workflow-related features. It can be securely managed, but its extensive feature set means it's unnecessarily complex for simple file storage and synchronization between devices.

Work Folders doesn't have any file-sharing features, but it's incredibly easy to use. It happens outside the firewall, so it doesn't require a VPN connection. The administrator can require that Workplace Join be enabled, preventing a potential attacker (or a careless employee) from accessing files using untrusted devices. It doesn't require the installation of a sync utility, and no additional configuration beyond the initial setup is necessary.

For Windows 10, the Work Folders feature has been enhanced for faster synchronization of changes. (In Windows 8.1, sync operations could be delayed by up to 10 minutes.) Windows 10 version 1511 adds integration with Enterprise Data Protection; using this feature, an administrator can require encryption on the remote device using a key associated with the Enterprise ID and can, in turn, wipe the data remotely using MDM software such as Microsoft Intune.

CHAPTER 14

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 unification of the Windows 10 platform means that the operating system and the new universal Windows apps are 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 traditional desktop and laptop PCs, and it runs the same universal apps, delivered through the same Windows Store, as its desktop counterpart.

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 Insider 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.)

The signature feature of Windows 10 Mobile, called *Continuum*, allows you to connect a mobile device to an external monitor, mouse, and keyboard to create an experience that is much like Windows 10 on a PC. Continuum leverages the Universal Windows Platform: Built-in apps such as Mail, as well as the Office Mobile apps, work exactly as they do on a Windows 10 PC.

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

The evolution of Windows on mobile devices

In its roughly six 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 apps capable of sharing data and licensing between desktop and mobile platforms.

The first public release of Windows 10 for phones arrived as a Technical Preview in February 2015, a few months after the first desktop Windows 10 Technical Preview. That initial release supported only a handful of phones. Further preview releases, targeting a wider population of phones, arrived throughout the rest of the year.

In late 2015, several months after the release of Windows 10 for PCs, Microsoft released two flagship phones, the Lumia 950 and Lumia 950XL (shown in Figure 14-1), with Windows 10 preinstalled. Several other manufacturers have announced support for the platform. The official release for other supported devices will be in early 2016.

FIGURE 14-1 Microsoft's Lumia 950XL was one of the first devices to ship with Windows 10 Mobile.

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 (with screen sizes under 8 inches measured diagonally), including models based on the same ARM processors used in phones and small tablets that run other operating systems. As of this writing, in early 2016, no such devices have been released.

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.

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 are not upgradeable to Windows 10.

Installing Windows 10 Mobile

The simplest way to evaluate or deploy Windows 10 Mobile is on new hardware that ships with Windows 10 preinstalled by the device manufacturer. To evaluate Windows 10 Mobile on older hardware, be sure the device meets Microsoft's requirements.

The device must have at least 8 GB of storage, must be running Windows Phone 8.1, and must be on the list of supported devices here: *http://windows.microsoft.com/en-us/windows/preview-supported-phones*. (To check which operating system version is installed on a Windows phone, go to Settings, About, More Info.)

If the device passes that check, you can install Windows 10 Mobile manually. If your mobile carrier offers Windows 10 Mobile as an over-the-air update, use that option. If not, you'll need to bypass the carrier by joining the Windows Insider program. Start by enrolling at *https://insider.windows.com* using the same Microsoft account you plan to use with the phone. (If you previously enrolled in the desktop preview program with that account, you can skip this step.)

Then, on the supported mobile device, install the Windows Insider app from the Store and sign in using your Microsoft account. Choose the Get Preview Builds option, shown in Figure 14-2, to allow the device to download and install preview builds.

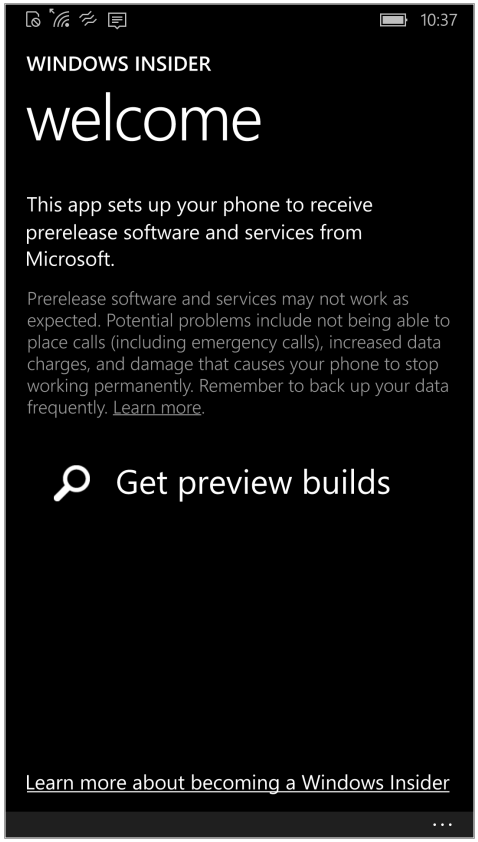


FIGURE 14-2 Install this Windows Insider app on a supported phone to bypass the normal carrier update process and enable access to Windows 10 Mobile.

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 14-3.

FIGURE 14-3 Enrolling in the Insider releases for Windows 10 Mobile require that you choose whether to be part of the Fast or Slow ring, just as in the preview program for desktop Windows 10 releases.

To see which ring your device is currently enrolled in, or to leave the Insider program, 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.

Restoring the original operating system to a Windows 10 Mobile device (including the option to restore Windows Phone 8.1 if you're leaving the Insider program) requires a separate utility, the Windows Device Recovery Tool. Information about the tool, including a download link, is available at *http://windows.microsoft.com/en-us/windows-10/windows-device-recovery-tool-faq*. 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 14-4, is an excellent illustration. The iconography is similar to what appears in the Settings app on a desktop PC running Windows 10, with just a few subtle changes.

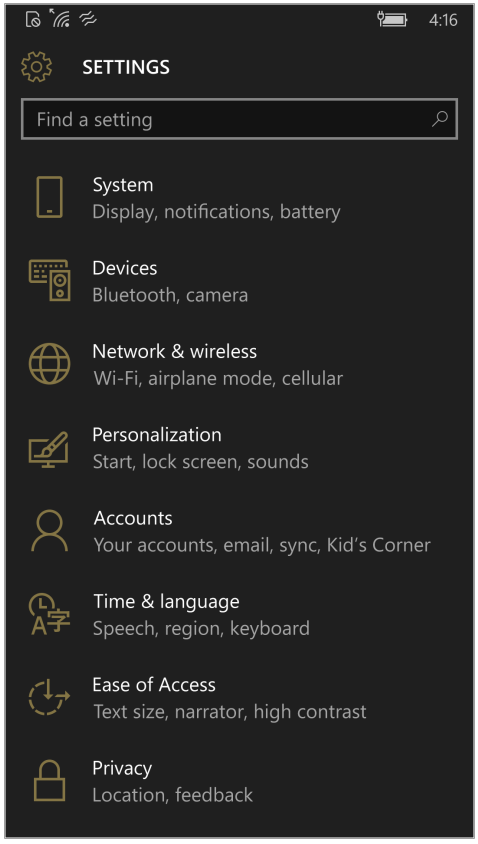


FIGURE 14-4 The Settings app on a mobile device looks nearly identical to its desktop counterpart, with only minor differences, such as the System icon.

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 14-5 shows the mobile Notifications center, which you summon with a downward swipe.

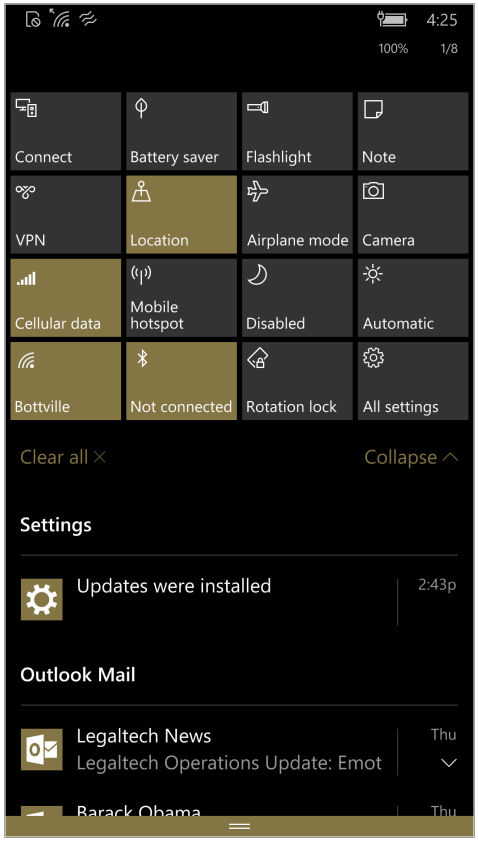


FIGURE 14-5 Just as in Windows 10 on the desktop, the Notifications center contains action buttons for one-tap access to common settings.

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.

Windows 10 Mobile and apps

Much of the usefulness of Windows 10 Mobile is delivered by its apps, of course—specifically, the first-party apps developed by Microsoft and delivered as part of Windows 10.

The elegance of the Universal Windows Platform means that developers can write a single app that runs on dramatically different devices, with displays and capabilities adjusting automatically, as

needed. Figure 14-6 shows Cortana's Notebook on Windows 10 Mobile, for example, which shares the same settings as the desktop version. Any personalization you perform in Windows 10, using either device, automatically syncs to the other.

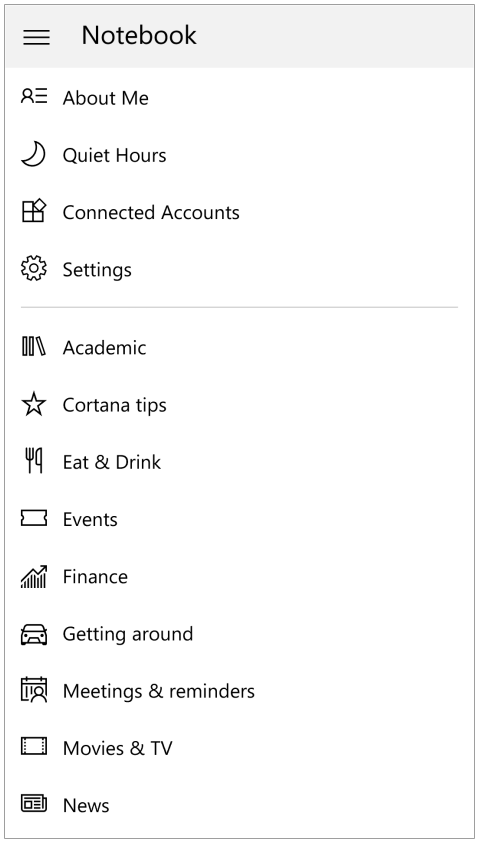


FIGURE 14-6 The Cortana app on a mobile device is identical to its desktop counterpart, with Notebook settings synced between them.

Another difference between the behavior of apps on a mobile device compared to a conventional desktop or portable PC is that the display can rotate 90 degrees. That means an app can intelligently adjust the layout of the display depending on whether it's in portrait or landscape orientation. Figures 14-7, for example, demonstrates the difference between these two orientations for the built-in Weather app.

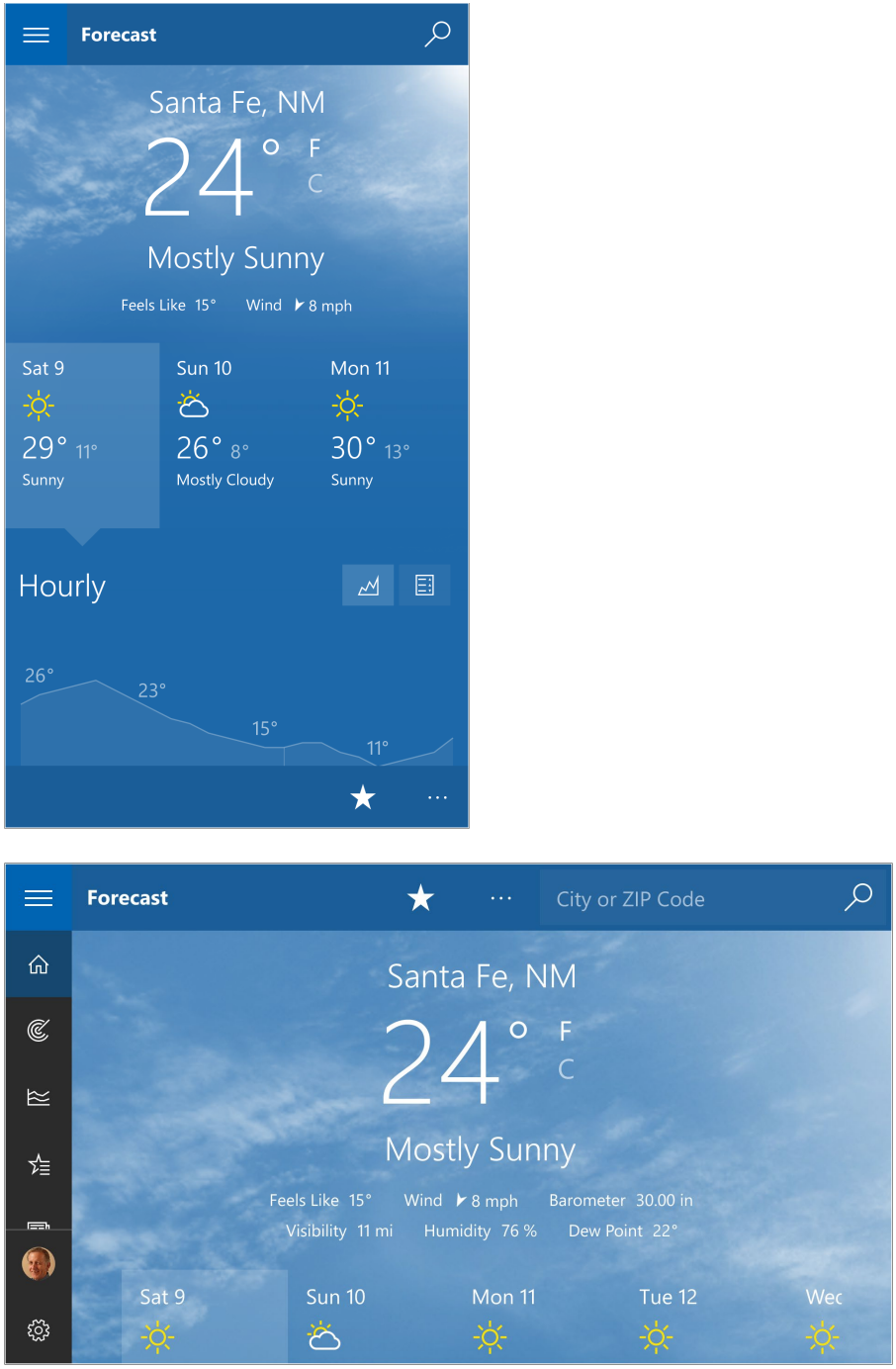


FIGURE 14-7 Switching the built-in Weather app from portrait orientation (top) to landscape (bottom) rearranges navigation elements. The hamburger menu, however, always remains in the upper-left corner.

The built-in Mail and Calendar apps have the same capabilities as on the desktop, offering connections to standard account types. Likewise, the Photos and Groove Music apps integrate neatly with OneDrive to offer access to pictures and music stored in the cloud.

More Info For a more detailed discussion of Windows 10 apps, see Chapter 11, "Universal apps and the new Windows Store."

Universal Office apps for Word, Excel, PowerPoint, and OneNote are included by default with Windows 10 Mobile.

Continuum

A 5-inch mobile screen is handy for portability, but that small screen is far from optimal for many productivity tasks, such as writing a lengthy document or building a spreadsheet.

For those tasks, Windows 10 Mobile offers a feature called Continuum. Connecting the phone to a TV or external monitor requires new hardware specifically built for Windows 10 Mobile; the feature is not available on older devices that have been upgraded from Windows Phone 8.1. To make the connection, you need specialized hardware:

- A wired dock, such as the Microsoft Display Dock (shown in Figure 14-8), connects to the external monitor using an HDMI or DVI cable or an active DisplayPort to DVI cable. (Passive DisplayPort cables will not work, and VGA cables won't work with video content.)

FIGURE 14-8 The Continuum feature requires a device built specifically for Windows 10 Mobile, along with hardware such as the Microsoft Display Dock shown here.

- For a wireless connection, you can use a Miracast adapter connected to the HDMI port on the TV or monitor.

At this stage of development, only a few apps work with Continuum, including Microsoft Edge, Word, Excel, Photos, and Mail. An Office 365 subscription is required to access some features in the Office Mobile apps. A handful of third-party apps, including USA Today and Audible, also support the feature. The list of compatible apps should grow over time.

Windows 10 Mobile in the enterprise

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. To check the current status of device encryption and enable or disable it, look in Settings under System, Device Encryption.

Windows 10 Mobile also supports connections to Work accounts and allows signing in to Azure Active Directory. For organizations that use mobile device management (MDM) software, the option to enroll in device management is available under Settings, Accounts, Work Access.

Other options under Settings, Accounts include Provisioning (for automatically adding configuration packages created by an organization's IT department), and the Kid's Corner and Apps Corner features, which allow another person to use specific apps on your device while safeguarding your personal information and organizational apps and data files.

CHAPTER 15

What's new in Group Policy in Windows 10

For IT pros, the ability to manage PCs using Group Policy is one of the primary reasons to choose Microsoft Windows as the computing platform for an organization. In combination with Active Directory, Group Policy offers a way to enforce security policies, to manage content and apps on company-owned devices, and to reduce support costs by keeping users from inadvertently messing up a properly configured system.

This chapter presents an interesting selection of policies that are new in Windows 10. It's not a complete list, but rather is here to point you in the direction of potentially useful new capabilities in your administrative toolkit.

For the sake of convenience, most of the examples in this chapter are illustrated using the Local Group Policy Editor (Gpedit.msc). This utility is your first choice when you're evaluating Windows 10 and don't have access to a domain controller or don't need the power and complexity of Active Directory. Of course, all the policies listed in this chapter can be set using Group Policy in an Active Directory domain as well.

For a reasonably complete list of policy settings that are included with the administrative template files (.admx) delivered with current Windows versions, download the latest update of "Group Policy Settings Reference for Windows and Windows Server" from the Microsoft Download Center: *http://bit.ly/group-policy-settings*. (All downloads on this page are in Microsoft Excel spreadsheet format.)

Windows Update for Business

For many IT pros, the most interesting new Windows 10 policy settings are those that control how and when updates and upgrades are installed from Windows Update. Collectively, these Windows Update for Business features allow administrators to delay the installation of individual and cumulative updates in one-week intervals, up to a total of four weeks, and to defer major features upgrades by up to eight months.

You'll find these two policies in a single Defer Upgrades and Updates setting, located under Computer Configuration > Administrative Templates > Windows Components > Windows Update. When this policy is enabled, as shown in Figure 15-1, you can set separate values for each policy. If you discover that a current update is causing problems within your organization, you can select the Pause Upgrades And Updates check box to immediately suspend delivery of updates until the next month's scheduled delivery.

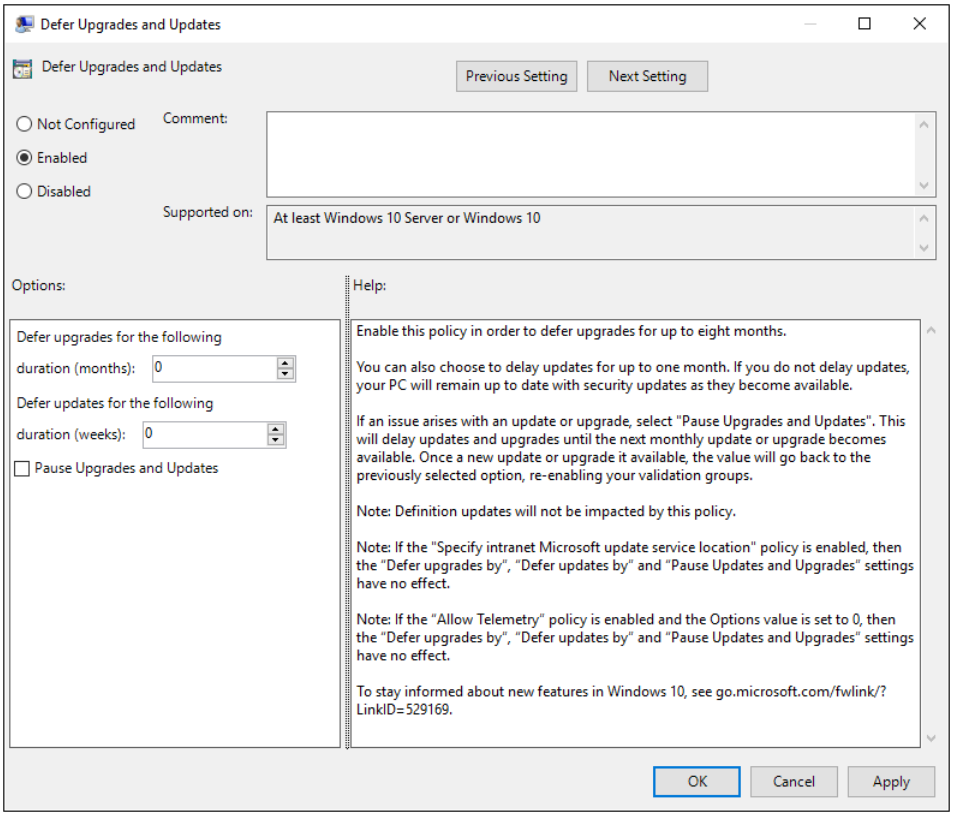


FIGURE 15-1 Use Group Policy to enable the Windows Update for Business features, which you can use to delay the installation of updates and full upgrades.

Note that these settings don't apply if you deliver updates using a tool other than the public Windows Update servers, such as a Windows Server Update Services (WSUS) server on your network. In addition, if the Allow Telemetry policy is enabled and set to 0 on a PC running Windows 10 Enterprise, Windows Update is effectively disabled and the Windows Update for Business settings have no effect.

Device Guard

Device Guard, another new feature available only in Windows 10 Enterprise, offers IT pros the capability to lock down a device so that it runs only applications from an approved list. Credential Guard, a related enterprise-security feature, uses hardware virtualization to secure credentials.

Deploying Device Guard, with or without Credential Guard, is a complex process that involves enabling hardware-security features, creating a code-integrity policy, and then applying that policy to individual devices. Two Group Policy settings represent a small but critical part of this deployment process. These settings, shown in Figures 15-2 and 15-3, are located under Computer Configuration > Administrative Templates > System > Device Guard.

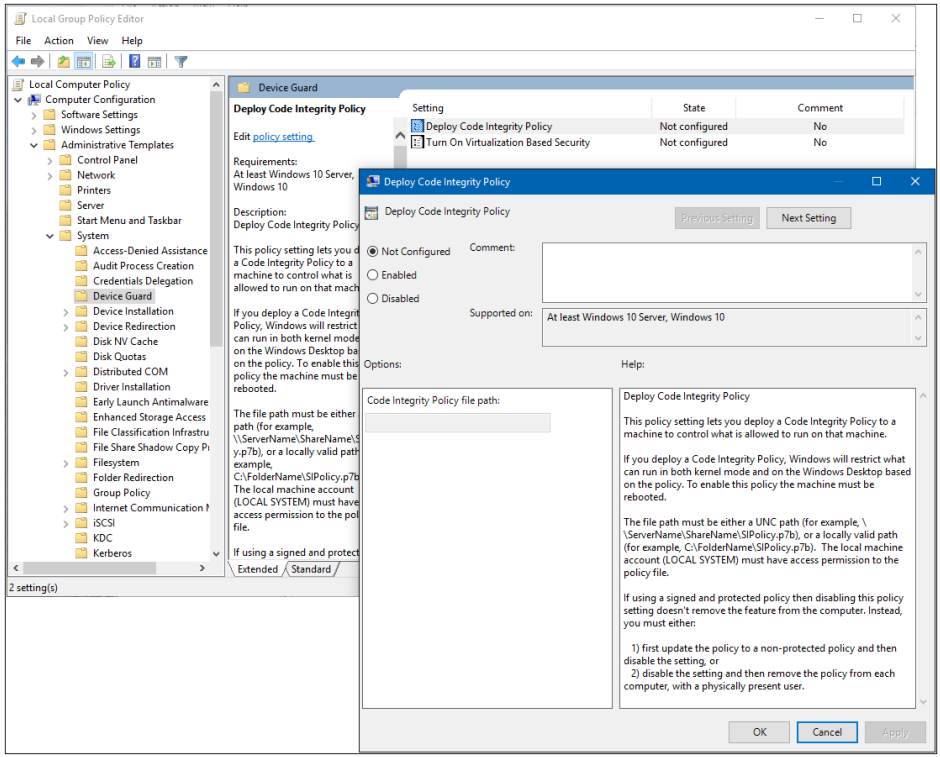


FIGURE 15-2 Device Guard is a new feature you can use to lock down a Windows 10 device so that it runs only trusted programs. These policy settings are just a small part of the deployment process.

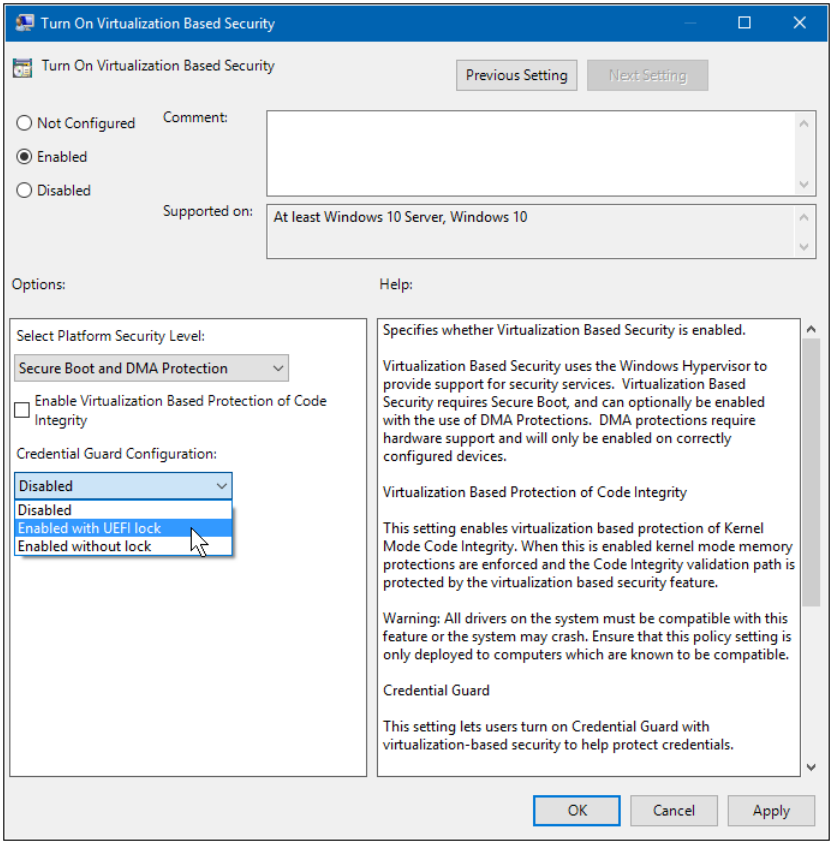


FIGURE 15-3 On systems running Windows 10 Enterprise, Credential Guard can offer enhanced protection for domain credentials.

Note For a more detailed discussion of Device Guard, see "Locking down enterprise PCs with Device Guard," in Chapter 5, "Security and privacy in Windows 10." The official (and very detailed) deployment guide for Device Guard is available at *http://bit.ly/DG-deploy*.

Microsoft Passport for Work

Windows 10 domain-joined devices can use the new Microsoft Passport for Work feature to exchange credentials securely without requiring passwords. After enrolling the device by authenticating to a service such as Azure AD or Active Directory, the user can sign in with a gesture, such as a biometric device (Windows Hello) or a PIN.

As an administrator, you can control the configuration of Microsoft Passport for Work by requiring a hardware security device (TPM) or biometric authentication, for example, and setting strict complexity requirements for the PIN. All these settings are located under Computer Configuration > Administrative Templates > Windows Components > Microsoft Passport for Work.

Microsoft Edge and Internet Explorer

The introduction of the Microsoft Edge browser in Windows 10 brings the need for new Group Policy Objects to manage its behavior and configuration. In addition, Internet Explorer 11 now supports Enterprise Mode, which is configured through Group Policy as well.

Windows 10 version 1511 includes more than a dozen settings for Microsoft Edge, all accessible from the new Microsoftedge.admx administrative template. Figure 15-4 shows this group of settings, available under Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge.

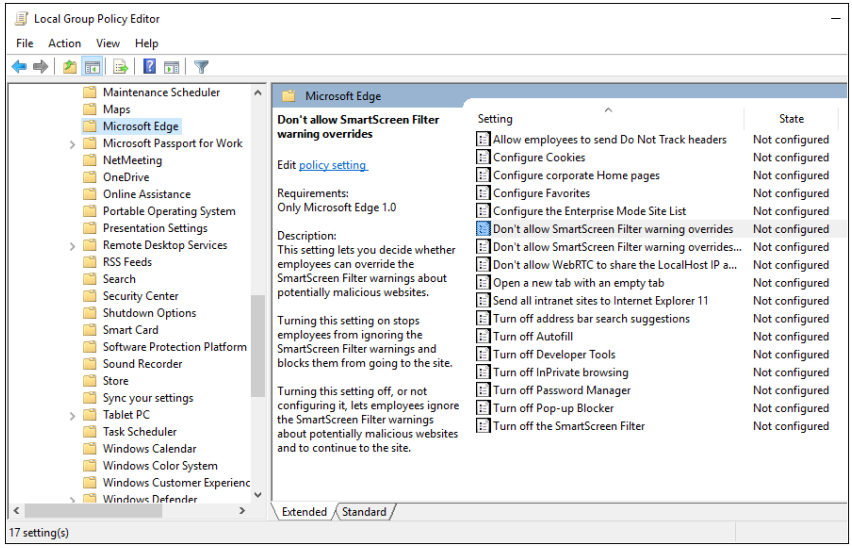


FIGURE 15-4 The new default browser in Windows 10, Microsoft Edge, comes with its own set of Group Policy settings.

Configuring Enterprise Mode involves a Group Policy setting under Microsoft Edge as well as two settings under Computer Configuration > Administrative Templates > Windows Components > Internet Explorer. You use those settings to control whether users can turn on and use Enterprise Mode from the Tools menu and also to specify the location of the Enterprise Mode IE website list, as shown in Figure 15-5.

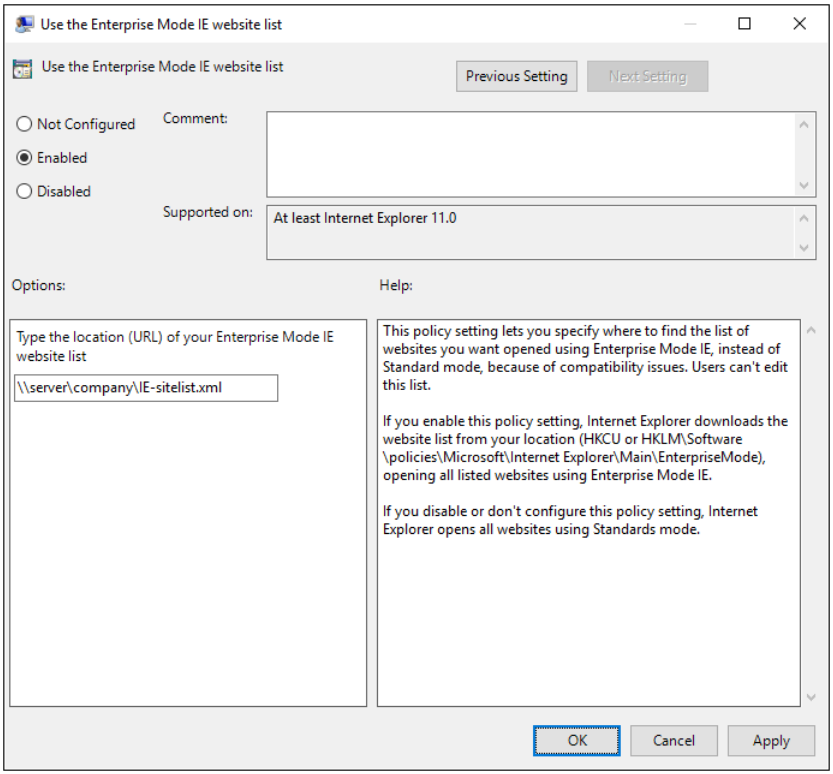


FIGURE 15-5 Configuring Enterprise Mode for Internet Explorer 11 makes it possible for users to continue using sites that don't work properly under modern web standards.

One additional setting of note for Internet Explorer 11 in Windows 10 is a policy to control the use of the HTTP2 network protocol.

Controlling access to preview builds and telemetry data

An essential part of the continuous development of Windows 10 involves the voluntary participation of members of the Windows Insider program, who receive preview builds ahead of their public release. Preview builds are, by definition, unfinished; using a preview build entails a risk of instability or data loss.

You can restrict access to preview builds using policy settings under Computer Configuration > Administrative Templates > Windows Components > Data Collection And Preview Builds, as shown in Figure 15-6.

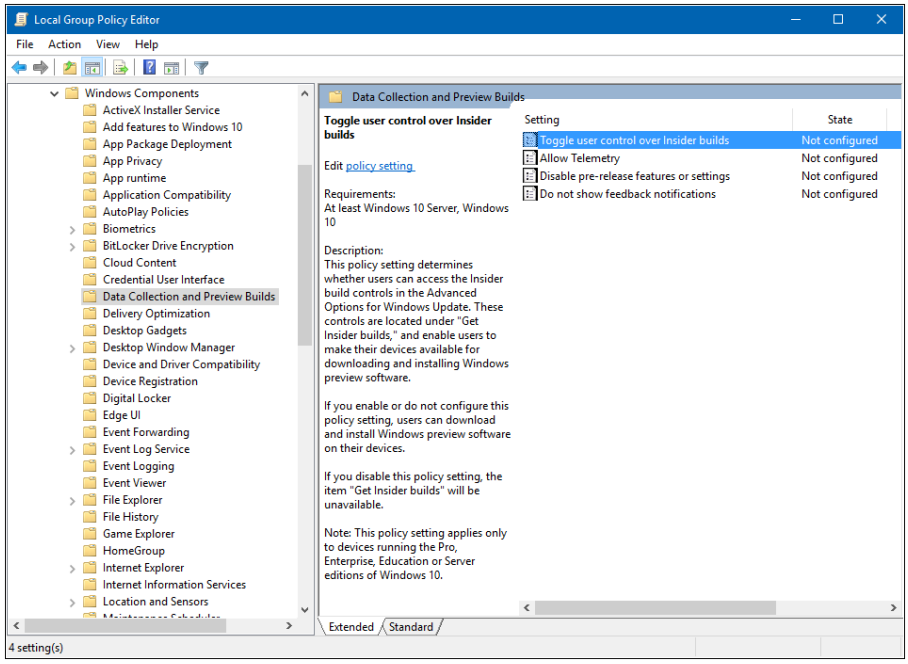


FIGURE 15-6 If you don't want your users installing preview builds of Windows 10, set this policy.

Setting Toggle User Control Over Insider Builds to Disabled removes the option for users to get preview builds. Note that this policy setting applies only to devices running the Pro, Enterprise, and Education editions of Windows 10.

The Allow Telemetry setting, also in this group, creates a fourth option that minimizes the amount of data sent to Microsoft as part of its normal diagnostic and usage data-collection policy. (The other three options are located in Settings, Privacy, Feedback & Diagnostics.) This minimal setting sends only data from the Malicious Software Removal Tool and Windows Defender (if enabled), as well as settings for the telemetry client.

Managing Windows Update Delivery Optimization

By design, Windows 10 creates a peer-to-peer delivery system that helps spread the load of delivering Windows apps and updates. In a managed environment, you might prefer to restrict this peer sharing to devices that are on the same local network or domain. You might also want to exercise control over the amount of upload bandwidth this feature can use.

These and other policy settings are available under Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization. Confusingly, the Help text for this setting specifies numeric values (0 through 3, with a setting of 0 disabling the feature), while the actual interface for changing this setting in the Group Policy editor uses a drop-down list whose entries correspond to those numeric values, as shown in Figure 15-7.

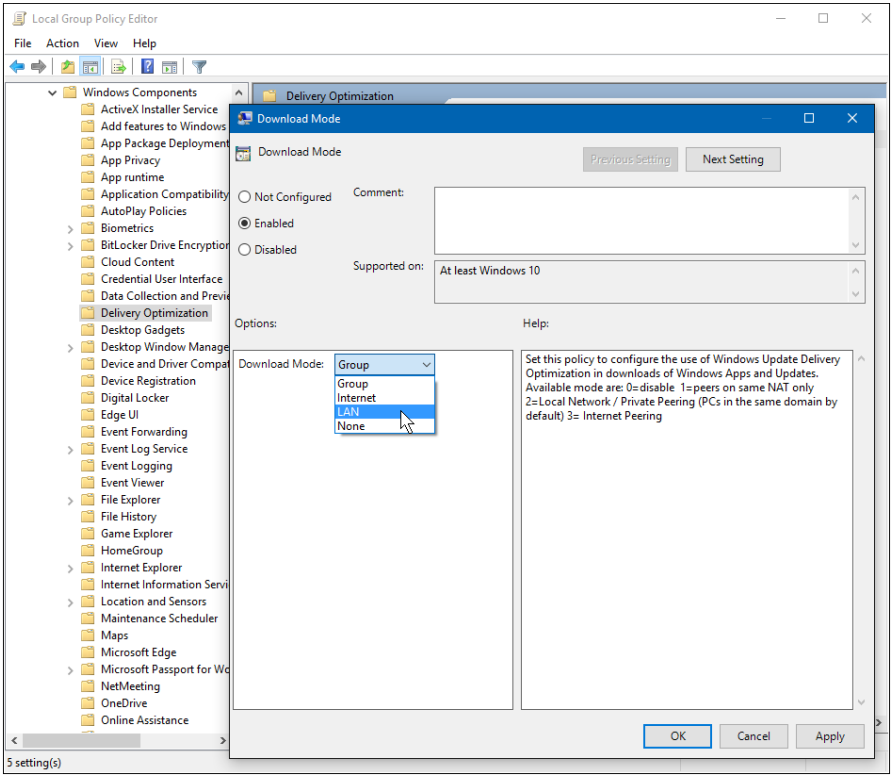


FIGURE 15-7 By using Delivery Optimization policies, you can control peer-to-peer delivery of Windows apps and updates on your corporate network.

Security policies

The list of security policies available for a Windows 10 PC goes on for many pages, with administrators having fine-grained control over every aspect of the system. Most of these policies in Windows 10 are extensions of previously available policies, including many that were first made available in the Windows 8 and 8.1 releases.

The few new policies in this group for Windows 10 are esoteric but interesting.

Under Computer Configuration > Administrative Templates > System > Mitigation Options, for example, you'll find a new Untrusted Font Blocking setting, which prevents users from loading any font files except those that are properly installed in the secured Fonts folder.

Another new policy is located under Computer Configuration > Administrative Templates > Windows Components\BitLocker Drive Encryption\Operating System Drives. By enabling the Configure Pre-boot Recovery Message And URL policy setting, you can supply a custom recovery message or replace the existing URL displayed on the pre-boot key recovery screen when the OS drive is locked.

Finally, an option added to Windows 10 version 1511 offers new choices for the encryption algorithm and key cipher strength used with BitLocker drives. The new support for XTS-AES encryption is appropriate for fixed drives; however, it should be used with caution for removable data drives, which might need to be unlocked using BitLocker on older Windows versions that don't support this encryption type.

Figure 15-8 shows these settings.

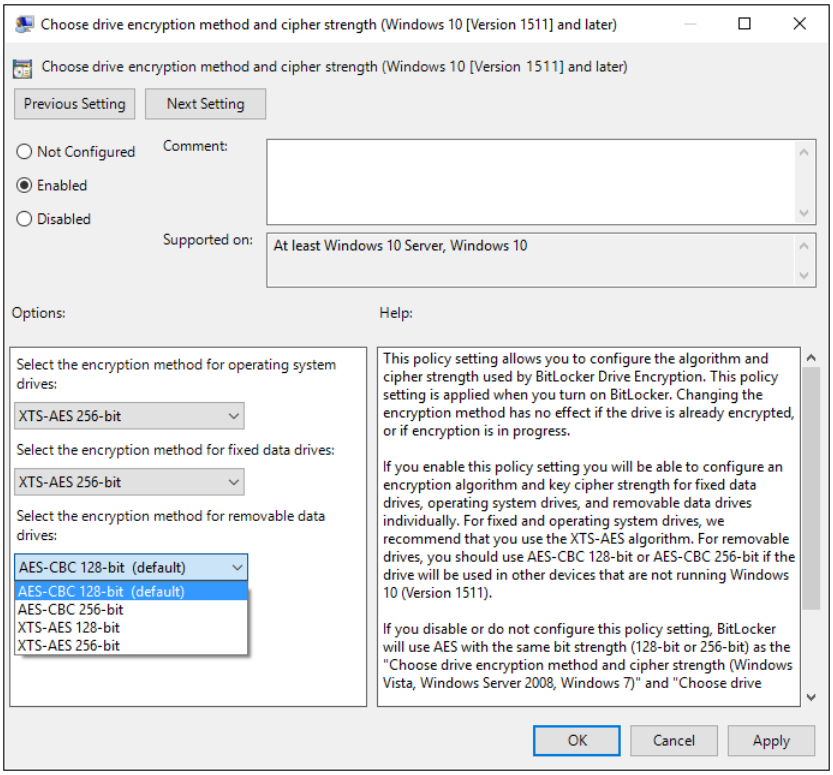


FIGURE 15-8 Effective with Windows 10 version 1511, you can specify the XTS-AES encryption algorithm with a cipher strength of 256-bit. Avoid setting this option on removable drives that might be used with incompatible operating systems.

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

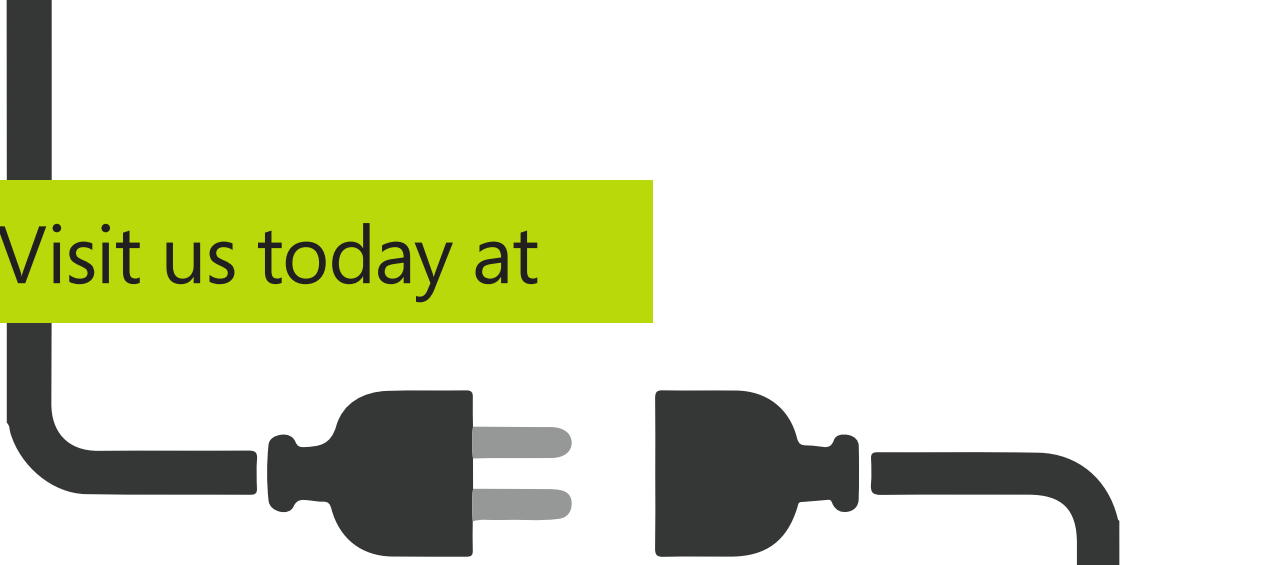
www.microsoftvirtualacademy.com/ebooks

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

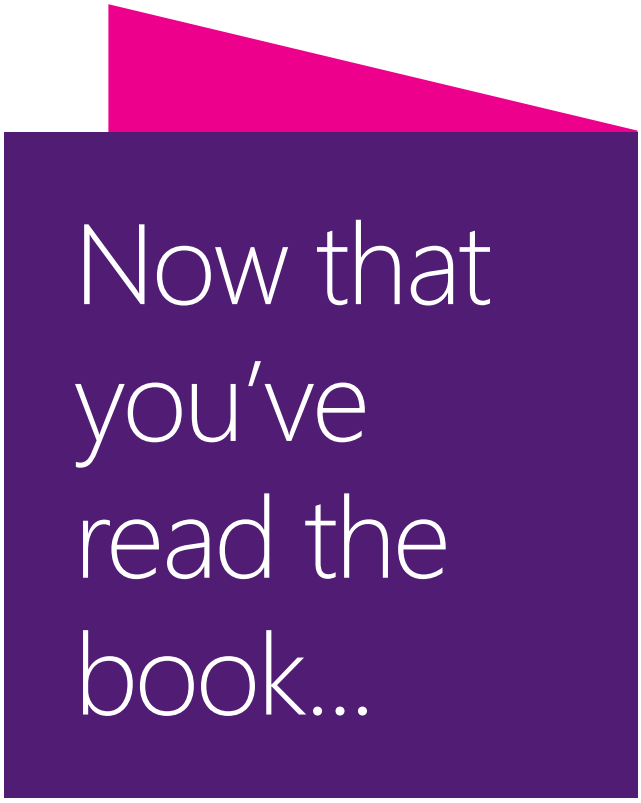
Visit us today at



microsoftpressstore.com

- **Hundreds of titles available** – Books, eBooks, and online resources from industry experts
- **Free U.S. shipping**
- **eBooks in multiple formats** – Read on your computer, tablet, mobile device, or e-reader
- **Print & eBook Best Value Packs**
- **eBook Deal of the Week** – Save up to 60% on featured titles
- **Newsletter and special offers** – Be the first to hear about new releases, specials, and more
- **Register your book** – Get additional benefits

Microsoft



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