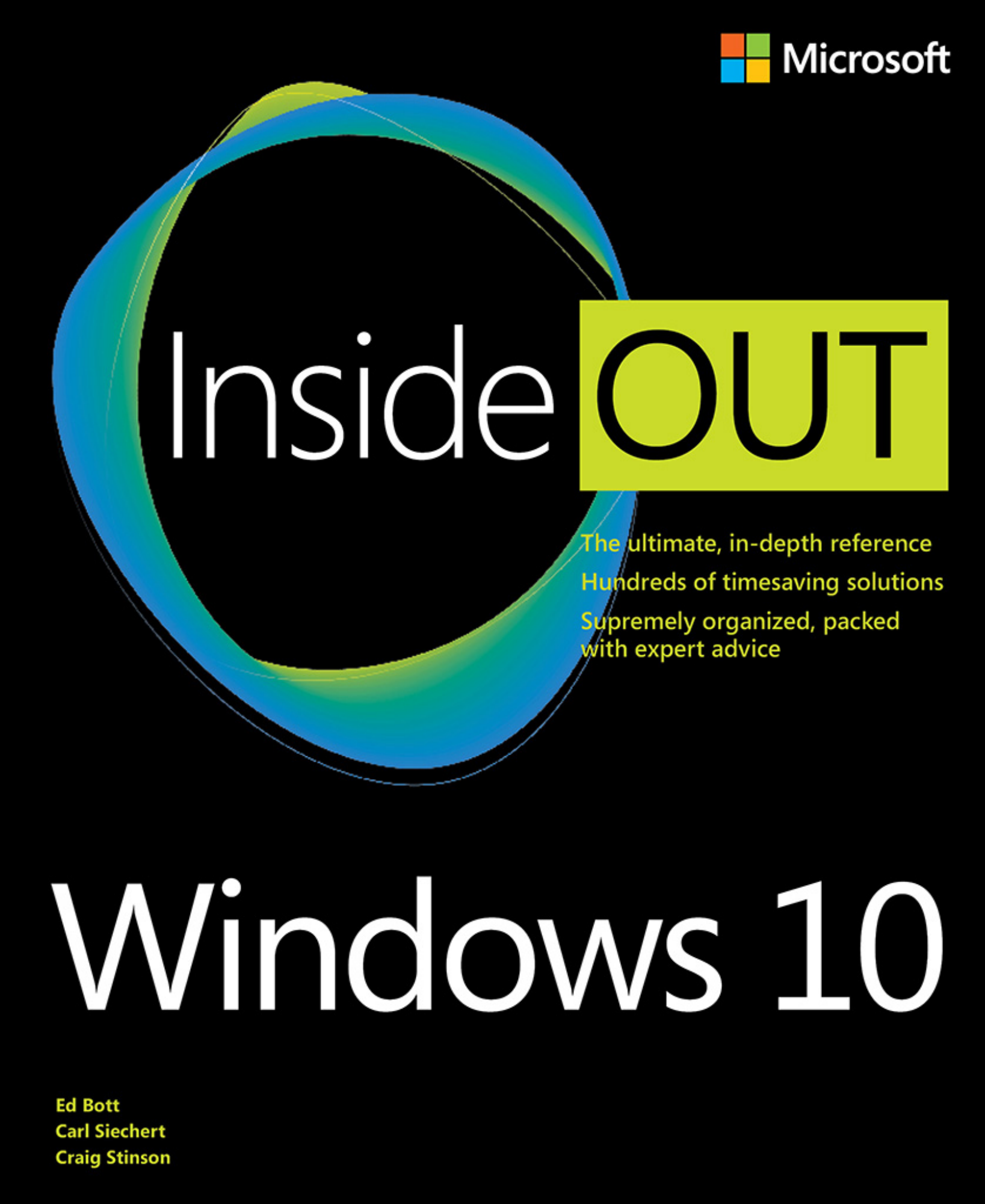

Microsoft
Inside OUT
The ultimate, in-depth reference
Hundreds of timesaving solutions
Supremely organized, packed with expert advice
Windows 10
Ed Bott
Carl Siechert
Craig Stinson

CHAPTER 7

Securing Windows 10 devices

We don't mean to be scaremongers, but they *are* out to get you. Computer attacks continue to increase in number and severity each year. And while the big data breaches—the loss of millions of credit card numbers from a major retailer or the loss of millions of personnel records from the U.S. government—command the most media attention, don't think that the bad guys wouldn't like to get into your computer too. Whether it's to steal your valuable personal data, appropriate your computing resources and bandwidth, or use your PC as a pathway into a bigger target with whom you do business, there are plenty of actors with bad intent.

According to the 2015 Internet Security Threat Report, published by Symantec, 60 percent of all targeted attacks struck small and medium-sized organizations. Like individuals, these organizations often don't have the resources to invest in security—making them juicy targets.

In this chapter, we examine the types of threats you're likely to face at home and at work. More importantly, we describe some of the more significant security improvements made in Windows 10—many of which are in layers you can't see, such as hardware-based protection that operates before Windows loads. Then we explain how to use the more visible security features, including Windows Firewall, User Account Control, BitLocker, and Windows Defender.

Understanding security threats

A decade ago, the threat landscape for Windows users was dominated by viruses and worms. Ah, for the good old days! The modern threat landscape is much more complex and, unfortunately, more insidious. Today, an attacker is likely to be part of an organized crime ring, not an attention-seeking vandal, and attacks are typically designed to go unnoticed for as long as possible.

A rogue program, installed without your knowledge and running without your awareness, can perform malicious tasks and transfer data without your consent. This category of software is often referred to as *malware*.

The goal of the bad guys is to get you to run their software. They might, for example, convince you to install a *Trojan*—a program that appears legitimate but actually performs malicious actions when it's installed. This category of malware doesn't spread on its own but instead uses social engineering (often using popular social networking sites such as Facebook and Twitter) to convince its victims to cooperate in the installation process. As part of its payload, a Trojan can include a downloader that installs additional malicious and unwanted programs. Some Trojans install a "backdoor" that allows an outside attacker to remotely control the infected computer.

What's in it for the bad guys? Money, mostly, gathered in a variety of ways, depending on how the attackers got through your defenses.

A *password stealer* runs in the background, gathers user names and passwords, and forwards them to an outside attacker. The stolen credentials can then be used to make purchases, clean out bank accounts, or commit identity theft.

Bad guys prey on fear with rogue security software (also known as *scareware*), which mimics the actions and appearance of legitimate antivirus software. If you install one of these programs, it inevitably reports the presence of a (nonexistent) virus and offers to remove it—for a fee, of course.

In 2015, the fastest rising star in the malware hall of shame is *ransomware*, a form of digital blackmail in which a program encrypts all your data files and offers to unlock them only upon payment of a ransom.

Phishing attacks, which use social engineering to convince visitors to give away their login credentials, are a separate but potentially devastating avenue to identity theft that can strike in any browser using any operating system.

You can review lists of current malware threats, along with links to details about each one, at the Microsoft Malware Protection Center, *w7io.com/1518*. For a more comprehensive view of the changing threat landscape, the Microsoft Malware Protection Center issues a twice-yearly report, using data from hundreds of millions of Windows users and other sources. You'll find the latest Microsoft Security Intelligence Report at *w7io.com/1501*.

Securing your computer: A defense-in-depth strategy

A multidimensional threat landscape requires a multilayered approach to protecting your PC and your network. The big picture goal is to secure your device, secure your data, secure your identity, and block malware. On a home or small business network, those layers of security include the following:

Use a hardware router to protect your broadband connection. This is an essential part of physical security, even if your network consists of a single PC. We provide an overview of the technology in "Getting started with Windows 10 networking" in Chapter 5, "Networking essentials."

Enable a software firewall and keep it turned on. You can use Windows Firewall, which is included with Windows 10, or a firewall that you obtain elsewhere. To learn more, see "Blocking intruders with Windows Firewall" later in this chapter.

Use biometric sign-in. Biometric sign-in using a fingerprint reader or facial recognition with Windows Hello offers much more than convenience. Because biometric sign-in is linked to a specific device, it provides effective two-factor authentication. If you don't have the necessary hardware, use a PIN or picture password for sign-in—both of which can be more secure than a traditional password. For more information, see "Managing the sign-in process" in Chapter 6, "Managing user accounts, passwords, and credentials."

Set up standard user accounts and keep User Account Control enabled. Standard accounts help to prevent (or at least minimize) the damage that an untrained user can do by installing untrusted programs. User Account Control (UAC) helps in this regard by restricting access to administrative tasks and virtualizing registry and file-system changes. For details, see "Introducing access control in Windows" in Chapter 6 and "Preventing unsafe actions with User Account Control" later in this chapter.

Keep Windows and vulnerable programs up to date. Windows Update handles this chore for Windows, Office, and other Microsoft programs. You're on your own for third-party programs. We provide an overview of security updates in "Staying on top of security updates" later in this chapter.

Use an antimalware program and keep it up to date. Windows Defender, which is included with Windows 10, provides antimalware protection, but many third-party solutions are also available. For details, see "Using Windows Defender to block malware" later in this chapter.

Protect yourself from threats in email messages. At a minimum, your email solution should block or quarantine executable files and other potentially dangerous attachments. In addition, effective antispam features can block scripts and prevent phishing attempts.

Use parental controls to keep kids safe. If you have children who use your computer, family safety features in Windows can help you keep them away from security threats. It also includes options you can use to restrict their computer activities in other ways. For details, see "Controlling your children's computer access" in Chapter 6.

Security And Maintenance, a Control Panel app, monitors many of these areas to be sure you're protected, and it displays an alert if something needs attention. For details, see "Monitoring your computer's security" later in this chapter.

The most important protective layer—and the one that is most easily overlooked—is user education and self-control. Everyone who uses a computer must have the discipline to read and evaluate security warnings when they're presented and to allow the installation only of software that is known to be safe. (Although a user with a standard account can't install or run a program that wipes out the entire computer, he can still inflict enough damage on his own user profile to cause considerable inconvenience.) Countless successful malware attacks worldwide have proven that many users do not have adequate awareness of safe computing methods.

What's new in Windows 10

Because the bad guys are always upping their game, a hallmark of each new version of Windows is a number of new and improved security features. Windows 10 is no exception. Here we enumerate changes available in Windows 10 Home and Windows 10 Pro; several additional features are included with Windows 10 Enterprise on a managed network.

Securing devices

Security features in Windows 10 begin with support for modern hardware designs. Although Windows 10 continues to support legacy hardware, some security features require two elements built in to most newer computers:

- **Unified Extensible Firmware Interface (UEFI).** UEFI is a firmware interface that replaces the BIOS, which has been a part of every PC since the beginning of personal computing. Among other improvements, UEFI enables Secure Boot and Device Encryption, features that are described in the following pages. PCs designed for Windows 8 and later must use UEFI.

- **Trusted Platform Module (TPM).** A TPM is a hardware chip that facilitates encryption and prevents altering or exporting encryption keys and certificates. With a TPM, BitLocker Drive Encryption (described later in this chapter) is more convenient to use as

well as more secure. Other security features in Windows 10, such as Measured Boot and Device Guard, require the presence of a TPM.

With UEFI and TPM in place, Windows 10 is able to secure the boot process. (Many recent malware attacks take control of the system early in the boot process, before Windows is fully running and before antimalware programs spring into action. This type of malware is called a *rootkit*.) The Windows 10 boot process steps through the following features:

- **Secure Boot.** Secure Boot, a basic feature of UEFI, prevents the use of any alternative operating system (OS) loader. Only an OS loader that is digitally signed using a certificate stored by UEFI is allowed to run. (A conventional BIOS allows interruption of the boot process to use any OS loader, including one that's been corrupted.)

- **Early Launch Antimalware (ELAM).** Antimalware software—including compatible third-party programs as well as Windows Defender—that has been certified and signed by Microsoft loads its drivers before any other third-party drivers or programs. This allows the antimalware software to detect and block attempts to load malicious code.

- **Measured Boot.** Measurements of the UEFI firmware and each Windows component are taken as they load. The measurements are then digitally signed and stored in the TPM, where they can't be changed. During subsequent boots, measurements are compared against the stored measurements.

Securing data

The increased mobility of PCs also increases the risk of theft. Losing a computer is bad enough, but handing over all the data you've stored on the computer is by far the greater loss. Windows 10 includes new features to ensure the thief can't get your data.

- **Device encryption.** On devices that support InstantGo, data on the operating system volume is encrypted by default. (Formerly called Connected Standby, InstantGo is a Microsoft hardware specification that enables advanced power-management capabilities. Among other requirements, InstantGo devices must boot from a solid-state drive.) The encryption initially uses a clear key, but when a local administrator first signs in with a Microsoft account, the volume is automatically encrypted. A recovery key is stored at *onedrive.com/recoverykey*; you'll need it if you reinstall the operating system or move the drive to a new PC.

- **BitLocker Drive Encryption.** BitLocker Drive Encryption offers similar (but stronger) whole-volume encryption, and on corporate networks it allows centralized management. In Windows 10, BitLocker encrypts drives more quickly than in previous Windows versions; additional speed comes from the new ability to encrypt only the part of a volume in use. For more information, see "Encrypting with BitLocker and BitLocker To Go" later in this chapter.

Securing identities

It seems like every week we hear about another data breach where millions of user names and passwords have been stolen. There's a thriving market for this type of information because it enables the thieves to log in anywhere using your credentials. Furthermore, because many people use the same password for different accounts, criminals can often use the stolen information to hack into a theft victim's other accounts. Windows 10 marks the beginning of the end of passwords.

- **Windows Hello.** With Windows 10, enterprise-grade two-factor authentication is built in. After enrolling a device with an authentication service, the device itself becomes one factor; the second factor is a PIN or a biometric, such as a fingerprint, facial recognition, or an iris scan.

- **Microsoft Passport.** After Windows Hello signs you in, Microsoft Passport enables sign-in to networks and web services. Your biometric data remains securely stored in your computer's TPM; it's not sent over the network.

With this combination of authentication methods, an attacker who has a trove of user names and passwords is stymied. To unlock Microsoft Passport (and, by extension, gain the ability to log in to your web services), he needs the enrolled device. And a thief who steals your computer needs your PIN or biometric data. Active Directory, Azure Active Directory, and Microsoft Accounts support this new form of credentials; other services are sure to follow.

For more information about Windows Hello, see "Managing the sign-in process" in Chapter 6.

Blocking malware

Since the days of Windows 7, several features that block malicious software have been beefed up:

- **Address Space Layout Randomization (ASLR).** ASLR is a feature that randomizes the location of program code and other data in memory, making it difficult to execute attacks that write directly to system memory because the malware can't find the memory location it needs. In Windows 10, memory locations are scrambled even more. And because the randomization is unique to each device, a successful attack on one device won't work on another.

- **Data Execution Prevention (DEP).** DEP is a hardware feature that marks blocks of memory so that they can store data but not execute program instructions. Windows 10 can't be installed on a system that doesn't support DEP.

- **Windows Defender.** In Windows 7, Windows Defender is a lightweight antispyware program. But starting with Windows 8 and continuing in Windows 10, Windows Defender includes the well-regarded antimalware capabilities of Windows Security Essentials, a free add-on for Windows 7. Windows Defender supports ELAM, described earlier in this chapter, which means that it can defend against rootkits that attempt to co-opt the boot process. For more information, see "Using Windows Defender to block malware" later in this chapter.

- **SmartScreen.** The goal of SmartScreen, introduced in Windows 7, is similar to that of Windows Defender: stop malicious code from running, which is much better than trying to clean up the damage after the fact. But SmartScreen takes a completely different approach: instead of looking for signatures of known bad programs, it checks a hash of each executable downloaded from an online source against Microsoft's application-reputation database. Files that have established a positive reputation are deemed safe and are allowed to run, whereas files with a negative reputation are blocked.

  In Windows 7, SmartScreen is a feature of Internet Explorer and checks files as they are downloaded. Beginning with Windows 8, SmartScreen is an integral part of Windows (and continues to be a feature of Internet Explorer and, in Windows 10, Microsoft Edge). Therefore, it blocks execution of unknown programs not just as you download them in a browser but any time you attempt to run a program from an online source—including those downloaded with a non-Microsoft browser.

Monitoring your computer's security

In Windows 10, security-related options have been gathered in Security And Maintenance in Control Panel, shown in Figure 7-1. (Veteran users of Windows 7 and Windows 8 will recognize this as the new name for what was called Action Center in those earlier operating systems. In Windows 10, *Action Center* refers to the list of notifications and buttons that can appear on the right side of the screen.) You can open Security And Maintenance from Control Panel or Settings: In the search box of either app, type **security** and then click Security And Maintenance. (No keyboard? Open Control Panel, tap System And Security, and then tap Security And Maintenance.)

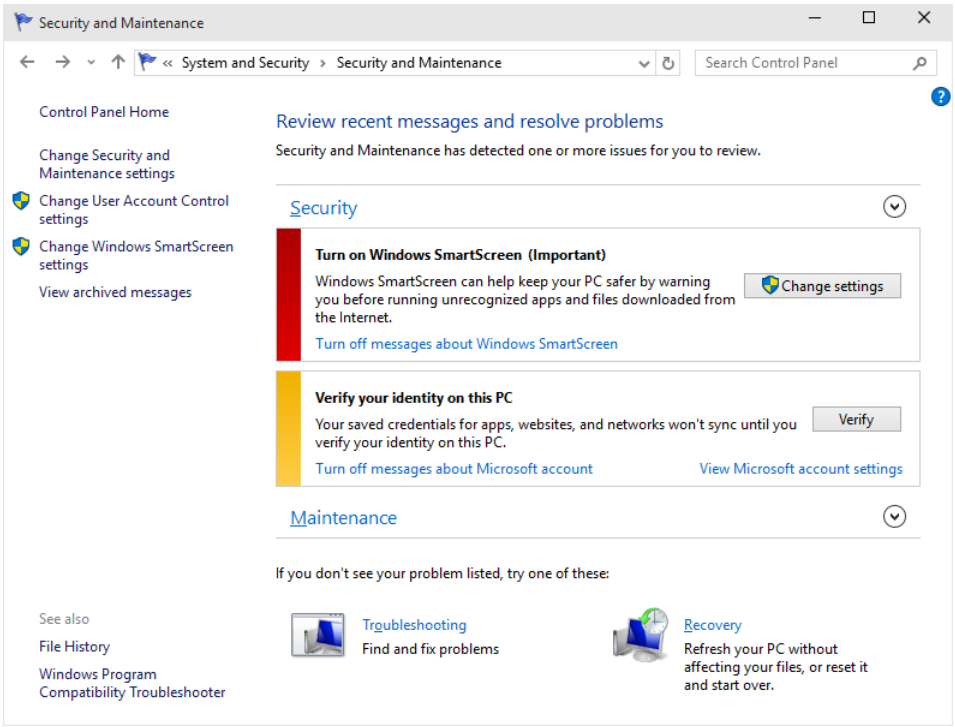


Figure 7-1 Security And Maintenance collects security, maintenance, and troubleshooting information and settings in a single window.

The Security section in Security And Maintenance provides at-a-glance information about your security settings. Items that need your attention have a red or yellow bar, as shown in Figure 7-1. A red bar identifies important items that need immediate attention, such as detection of a virus or spyware or that no firewall is enabled. A yellow bar denotes informational messages about suboptimal, but less critical, settings or status. Next to the bar appear explanatory text and buttons that let you correct the problem (or configure Security And Maintenance so that it won't bother you).

If all is well, the Security category is collapsed and you see nothing in that category when you open Security And Maintenance. Click the arrow to expand the category, and you'll see all the security-related items that Security And Maintenance monitors, as shown in Figure 7-2.

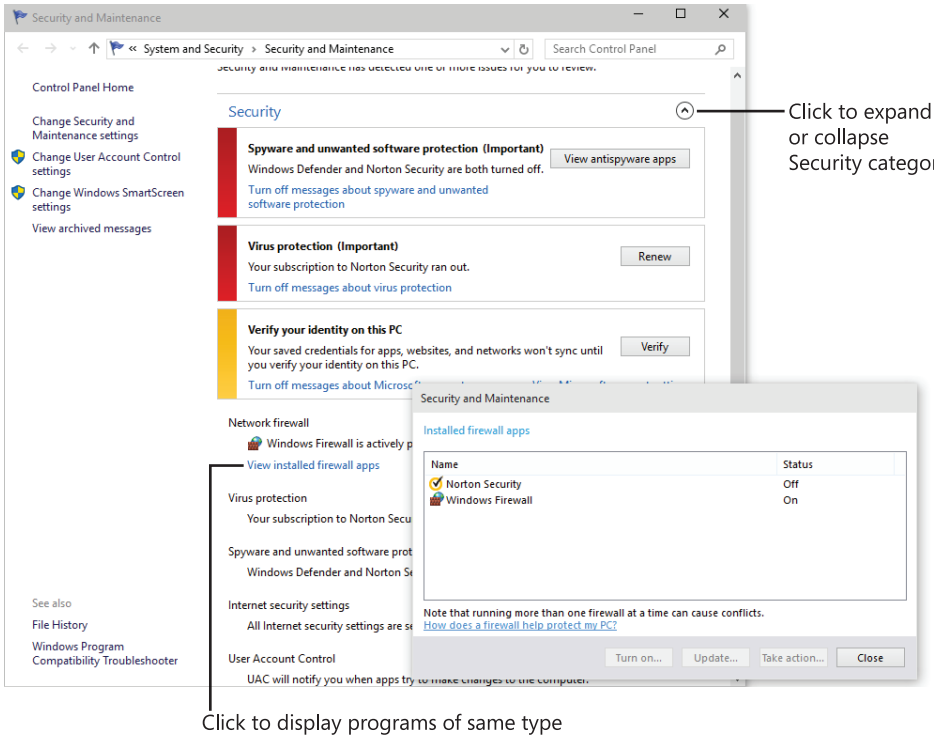


Figure 7-2 When multiple firewall programs are installed, you can click a link to show a list like this one. Use the Turn On button to enable a program that is currently disabled.

Security And Maintenance is designed to work with third-party firewall, antivirus, and anti-spyware programs, as well as with the programs built in to Windows (Windows Firewall and Windows Defender). Systems with more than one program installed in any of these categories include a link to show a list of such programs. For example, Figure 7-2 shows a system on which Norton Security is installed. The dialog box that appears when you click the link to view installed programs allows you to turn on any installed program that is currently turned off.

If you don't want to be bothered with alerts from Security And Maintenance about one or more security features, click Change Security And Maintenance Settings. After clearing items you don't want monitored in the dialog box shown in Figure 7-3, you won't receive any further alerts, and thereafter Security And Maintenance passively indicates the status as Currently Not Monitored.

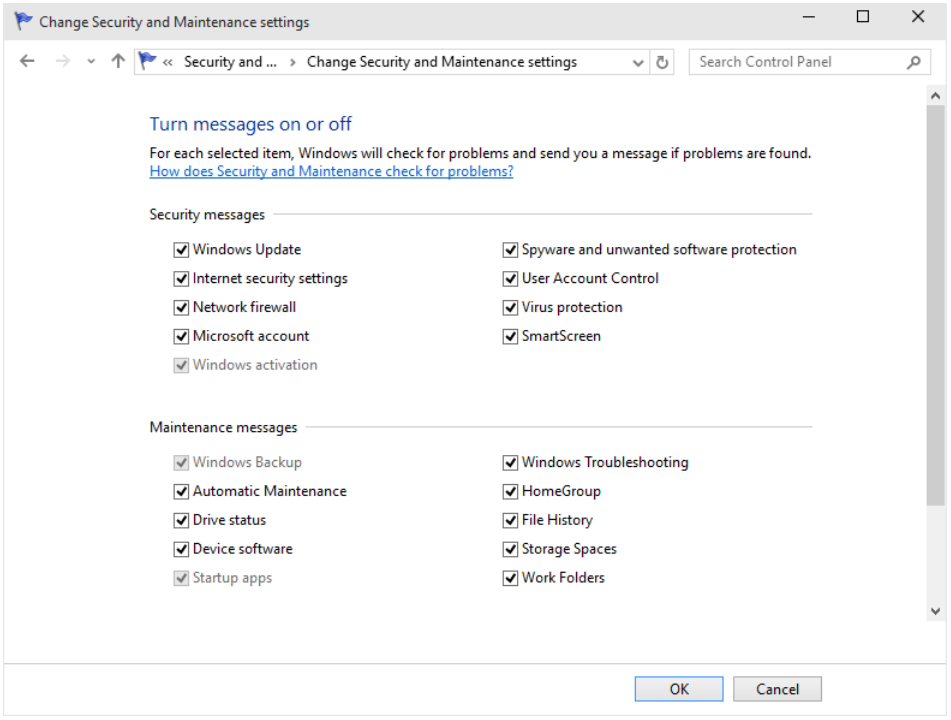


Figure 7-3 You can selectively disable and enable Security And Maintenance monitoring here, or you can manage monitored items individually by clicking links in the main Security And Maintenance window.

Staying on top of security updates

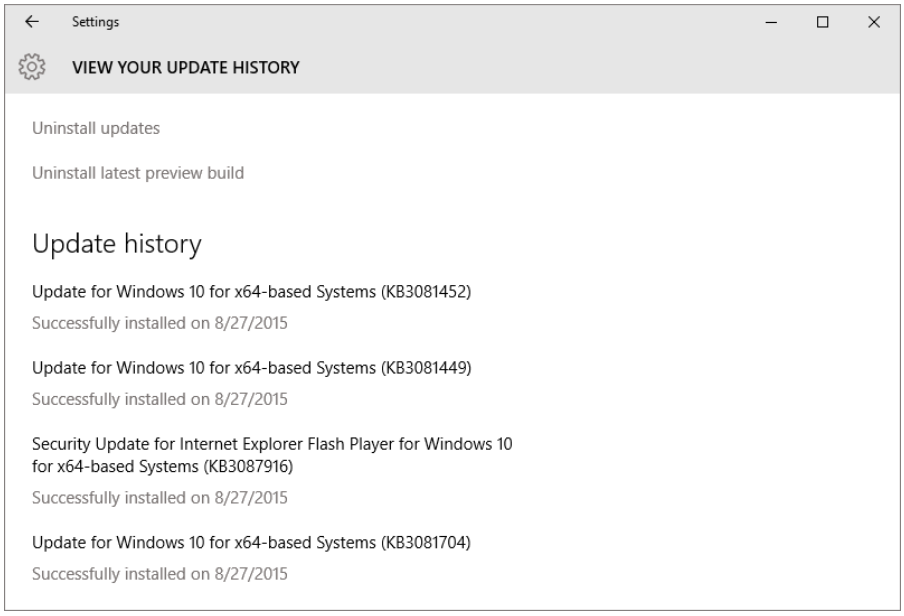
As we noted earlier in this chapter, Microsoft continues to beef up security in Windows. But as new threats emerge, the task is never done, so perhaps the most important step in keeping your system secure is to be sure that you stay current with updates to Windows and other programs. Microsoft issues frequent updates that provide replacements for installed device drivers as well as fixes to code that has been found to be faulty. Some updates provide new features or enhanced performance, while others patch security holes.

To install updates automatically, Windows uses Windows Update. In Windows 10, you'll find Windows Update in Settings under Update & Security. For more information about Windows Update, see "Keeping Windows up to date" in Chapter 15, "System maintenance and performance."

You might be interested in knowing more about current security threats, including those that are addressed by Windows Update: What, exactly, is the threat? How serious is it? What

workarounds are available? Microsoft Security Response Center publishes detailed information, in the form of a *security bulletin*, about the threat and the response. To find this information, you can take either of two routes:

- In Windows Update, click Advanced Options, and then click View Your Update History. Click the link below an item for a brief description, and in the box that pops up click the Support Info link for details. Also notice that each item in the list includes a KB (knowledge base) number. You can get detailed information about the update and the problem it addresses by going to *https://support.microsoft.com/kb/nnnnnnn/*, replacing *nnnnnnn* with the seven-digit number following "KB."



- Visit the Security Advisories and Bulletins page (*w7io.com/0702*). Here you'll find links to chronologically ordered information (most recent first) in the following formats:
  - **Security bulletin summaries.** A single document is published each month containing a complete list of security bulletins published during that month. For each bulletin in the list, you'll find a title and an executive summary, a severity rating (see the following page for more information about these ratings), a list of affected software, and a link to the bulletin.

    You can go directly to a security bulletin summary using this URL: https://technet.microsoft.com/library/security/ms*yy-mmm*/, replacing *yy* with the last two digits of the year (for example, use 15 for 2015) and *mmm* with the standard three-letter abbreviation for the month (for example, use "nov" for November).

- **Security bulletins.** Each bulletin contains detailed information about the issue, including a complete list—with version numbers—of software affected by the threat and, for each affected version, an assessment of the severity. Each security bulletin is assigned a name in the following format: MS*yy-nnn*, where *yy* is the last two digits of the year and *nnn* is a consecutive number that starts with 001 each year. For example, the twenty-seventh security bulletin of 2015 is called MS15-027.

  You can go directly to a security bulletin by appending the bulletin number to this URL: *https://technet.microsoft.com/library/security/*.

- **Security advisories.** Advisories describe security issues that might not require a security bulletin (and with it, a security update) but that can still affect your computer's security.

Each security bulletin includes a rating of the threat's severity. These are the four ratings that are used, listed in order of severity (most severe first):

- **Critical.** A critical vulnerability can lead to code execution with no user interaction.
- **Important.** An important vulnerability is one that can be exploited to compromise the confidentiality or integrity of your data or to cause a denial of service attack.
- **Moderate.** A moderate vulnerability is one that is usually mitigated by default settings and authentication requirements. In other words, you'd have to go a bit out of your way for one of these to damage your system or your data.
- **Low.** A vulnerability identified as low usually requires extensive interaction or an unusual configuration to cause damage.

For more information about these ratings, see "Security Bulletin Severity Rating System" at *w7io.com/0703*.

Blocking intruders with Windows Firewall

Typically, the first line of defense in securing your computer is to protect it from attacks by outsiders. Once your computer is connected to the Internet, it becomes just another node on a huge global network. A firewall provides a barrier between your computer and the network to which it's connected by preventing the entry of unwanted traffic while allowing transparent passage to authorized connections.

Using a firewall is simple, essential, and often overlooked. You'll want to be sure that all network connections are protected by a firewall. You might be comforted by the knowledge that your portable computer is protected by a corporate firewall when you're at work and that you use a firewalled broadband connection at home. But what about the public hotspots you use when you travel?

And it makes sense to run a firewall on your computer even when you're behind a residential router or corporate firewall. Other people on your network might not be as vigilant as you are about defending against viruses, so if someone brings in a portable computer infected with a worm and connects it to the network, you're toast—unless your network connection has its own firewall protection.

Windows includes a two-way, stateful-inspection, packet-filtering firewall called, cleverly enough, Windows Firewall. Windows Firewall is enabled by default for all connections, and it begins protecting your computer as it boots. The following actions take place by default:

- The firewall blocks all inbound traffic, with the exception of traffic sent in response to a request sent by your computer and unsolicited traffic that has been explicitly allowed by creating a rule.
- All outgoing traffic is allowed unless it matches a configured rule.

You notice nothing if a packet is dropped, but you can (at your option) create a log of all such events.

Using Windows Firewall with different network types

Windows Firewall maintains a separate profile (that is, a complete collection of settings, including rules for various programs, services, and ports) for each of three network types:

- **Domain.** Used when your computer is joined to an Active Directory domain. In this environment, firewall settings are typically (but not necessarily) controlled by a network administrator.
- **Private.** Used when your computer is connected to a home or work network in a workgroup configuration.
- **Guest or public.** Used when your computer is connected to a network in a public location, such as an airport or a library. It's common—indeed, recommended—to have fewer allowed programs and more restrictions when you use a public network.

If you're simultaneously connected to more than one network (for example, if you have a Wi-Fi connection to your home network while you're connected to your work domain through a virtual private network, or VPN, connection), Windows uses the appropriate profile for each connection with a feature called multiple active firewall profiles (MAFP).

You make settings in Windows Firewall independently for each network profile. The settings in a profile apply to all networks of the particular type to which you connect. (For example, if you allow a program through the firewall while connected to a public network, that program rule is then enabled whenever you connect to any other public network. It is not enabled when you're connected to a domain or private network unless you allow the program in those profiles.)

➤ **For more information about network types, see "Setting network locations" in Chapter 5.**

Managing Windows Firewall

Windows Firewall is a Control Panel application that provides a simple interface for monitoring firewall status and performing routine tasks, such as allowing a program through the firewall or blocking all incoming connections. To open Windows Firewall, type **firewall** in the search box or in Control Panel. Click Windows Firewall to display a window similar to the one shown in Figure 7-4.

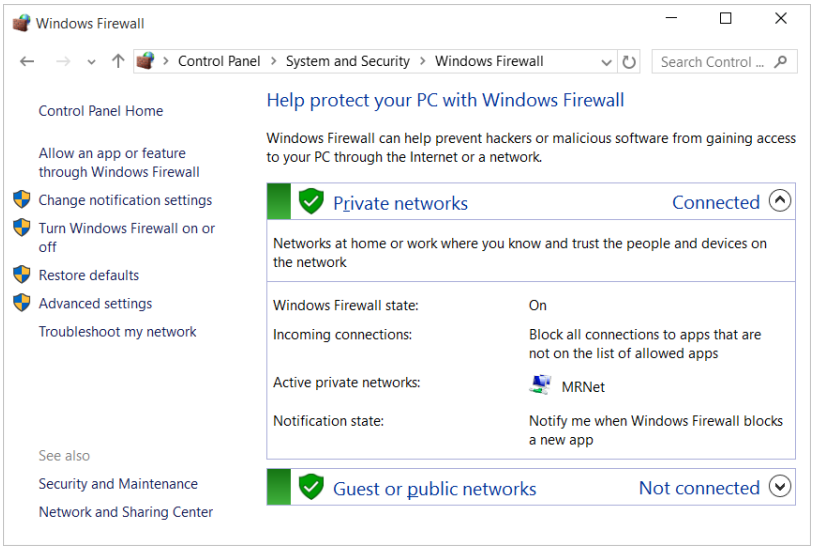
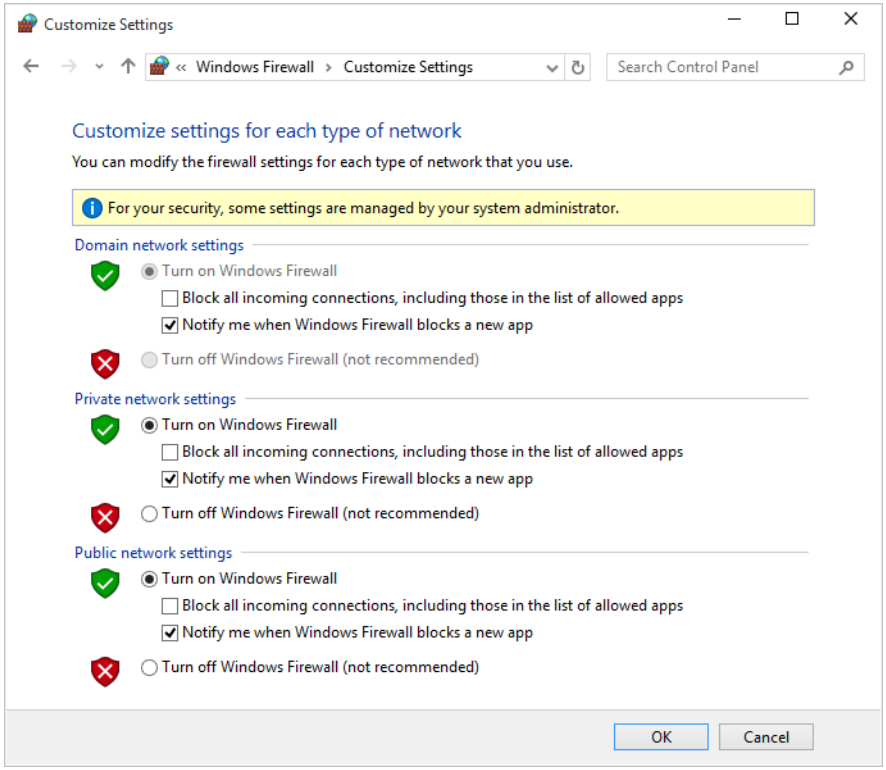


Figure 7-4 Windows Firewall shows status and settings for each currently connected network. The Domain Networks profile appears only on computers that have been joined to a domain.

Enabling or disabling Windows Firewall

The main Windows Firewall application, shown in Figure 7-4, is little more than a status window and launch pad for making various firewall settings. The first setting of interest is to enable or disable Windows Firewall. To do that, click Turn Windows Firewall On Or Off to open the screen shown next. From here you can enable (turn on) or disable (turn off) Windows Firewall for each network type. In general, the only reason to turn off Windows Firewall is if you have installed a third-party firewall that you plan to use instead of Windows Firewall. Most of those, however, perform this task as part of their installation.

As you'll discover throughout Windows Firewall, domain network settings are available only on computers that are joined to a domain. You can make settings for all network types—even those to which you're not currently connected. Settings for the domain profile, however, are often locked down by the network administrator using Group Policy.



The Block All Incoming Connections check box in Customize Settings provides additional safety. When it's selected, Windows Firewall rejects all unsolicited incoming traffic—even traffic from allowed programs or that would ordinarily be permitted by a rule. (For information about firewall rules, see the next section, "Allowing connections through the firewall.") Invoke this mode when extra security against outside attack is needed. For example, you might block all connections when you're using a public wireless hotspot or when you know that your computer is actively under attack by others.

NOTE

Selecting Block All Incoming Connections does not disconnect your computer from the Internet. Even in this mode, you can still use your browser to connect to the Internet. Similarly, other outbound connections—whether they're legitimate services or some sort of spyware—continue unabated. If you really want to sever your ties to the outside world, open Network And Sharing Center and disable each network connection. (Alternatively, use brute force: physically disconnect wired network connections and turn off wireless adapters or access points.)

Allowing connections through the firewall

In some situations, you want to allow other computers to initiate a connection to your computer. For example, you might use Remote Desktop, play multiplayer games, or chat via an instant messaging program; these types of programs typically require inbound connections so that others can contact you.

The simplest way to enable a connection is to click Allow An App Or Feature Through Windows Firewall, a link in the left pane of the main Windows Firewall window. The list of programs and features that initially appears in Allowed Apps, shown in Figure 7-5, depends on which programs and services are installed on your computer; you can add others, as described in the following sections. In addition, program rules are created (but not enabled) when a program tries to set up an incoming connection. To allow connections for a program or service that's already been defined, simply select its check box for each network type on which you want to allow the program. (You'll need to click Change Settings before you can make changes.)

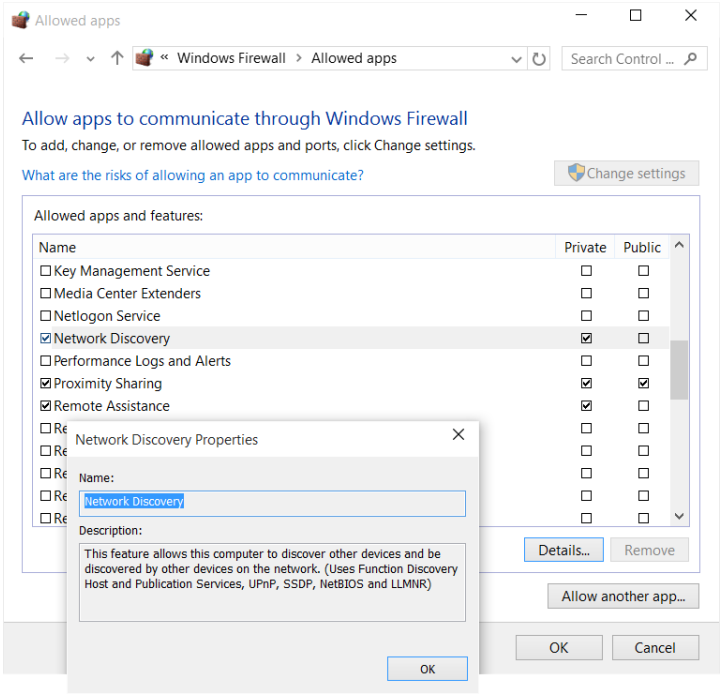


Figure 7-5 Selecting an item and clicking Details displays a description of the program or service.

In each of these cases, you enable a rule in Windows Firewall that pokes a small hole in the firewall and allows a certain type of traffic to pass through it. Each rule of this type increases

your security risk to some degree, so you should clear the check box for all programs you don't need. If you're confident you won't ever need a particular program, you can select it and then click Remove. (Many of the list items included with Windows don't allow deletion, but as long as their check boxes are not selected, these apps present no danger.)

The first time you run a program that tries to set up an incoming connection, Windows Firewall asks for your permission by displaying a dialog box. You can add the program to the allowed programs list by clicking Allow Access.

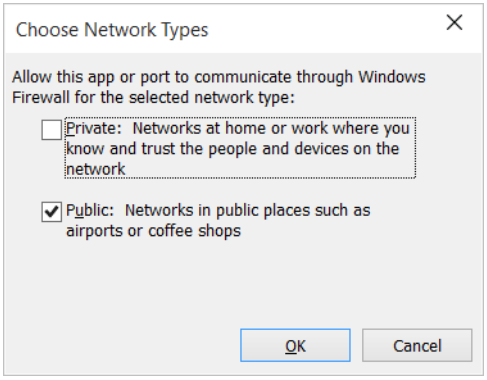
When such a dialog box appears, read it carefully:

- Is the program one that you knowingly installed and ran?
- Is it reasonable for the program to require acceptance of incoming connections?
- Are you currently using a network type where it's okay for this program to accept incoming connections?

If the answer to any of these questions is no—or if you're unsure—click Cancel. If you later find that a needed program isn't working properly, you can open the allowed apps list in Windows Firewall and enable the rule.

Alternatively, you can set up the program from the Allowed Apps window shown in Figure 7-5 without waiting for a Windows Security Alert dialog box to appear. Follow these steps:

1. Click Allow Another App. The Add An App dialog box appears.
2. In Add An App, select the program for which you want to allow incoming connections. Or click Browse and navigate to the program's executable file if it isn't shown in the Apps list.
3. Click Network Types.



4. Select the network types on which you want to allow the program, click OK, and then click Add. (You can also select network types in Allowed Apps after you add the program.)

Restoring default settings

If you've played around a bit with Windows Firewall and perhaps allowed connections that you should not have, you can get back to a known secure state by clicking Restore Defaults in Windows Firewall. Be aware that doing so removes all rules that you've added for all programs. Although this gives you a secure setup, you might find that some of your network-connected programs no longer work properly. As that occurs, you can add again each legitimate program that needs to be allowed, as described on the previous pages.

Advanced tools for managing Windows Firewall

If you have any experience at all configuring firewalls, you'll quickly realize that the Windows Firewall application in Control Panel covers only the most basic tasks. Don't take that as an indication that Windows Firewall is underpowered. To the contrary, you can configure all manner of firewall rules, allowing or blocking traffic based on program, port, protocol, IP address, and so on. In addition, you can enable, disable, and monitor rules; configure logging; and much more. With advanced tools, you can also configure Windows Firewall on remote workstations. Because the interface to these advanced features is rather daunting, Windows Firewall provides the simplified interface described earlier. It's adequate not only for less experienced users, but also for performing the routine firewall tasks needed by information technology (IT) professionals and others.

Nonetheless, our tour of security essentials would not be complete without a visit to Windows Firewall With Advanced Security, a snap-in and predefined console for Microsoft Management Console (MMC) that offers granular control over rules, exceptions, and profiles. To open it, in Windows Firewall click Advanced Settings. Windows Firewall With Advanced Security appears, as shown in Figure 7-6.

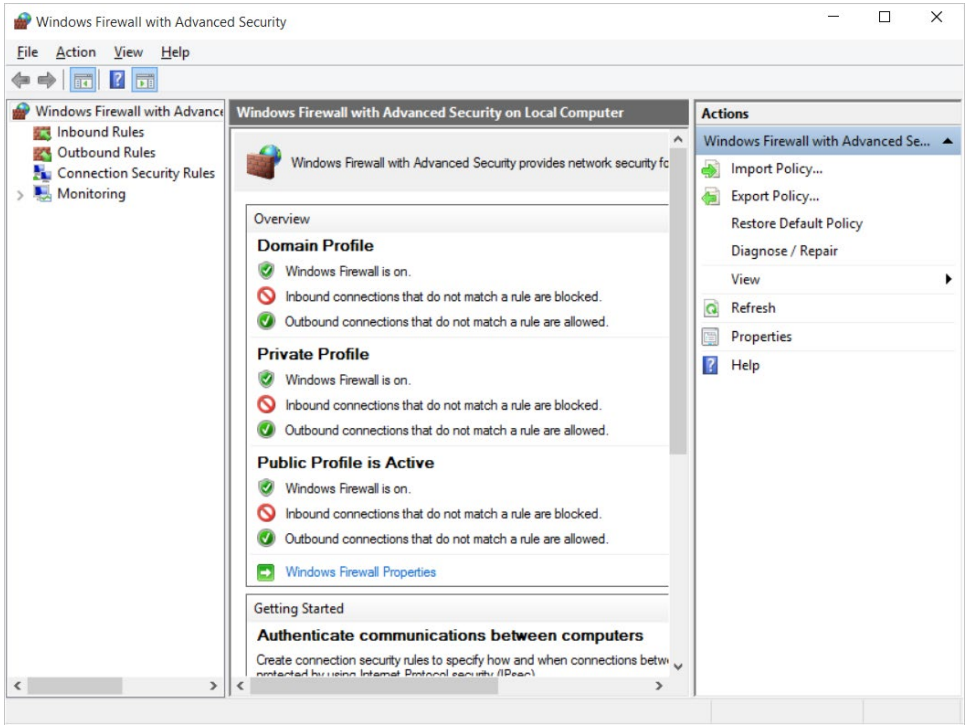


Figure 7-6 In the left pane, click Inbound Rules or Outbound Rules to view, configure, create, and delete firewall rules. The Domain Profile appears even on a computer that is not part of a Windows domain.

The initial view presents information similar to that shown in Windows Firewall. Go just a few steps farther into the cave, however, and you could be lost in no time. The "Windows Firewall with Advanced Security Getting Started Guide" can brighten your path; view it at *w7io.com/1502*. For additional details, see "Using Windows Firewall with Advanced Security" at *w7io.com/0701*.

Inside OUT

Open Windows Firewall With Advanced Security directly

You don't need to open Windows Firewall to get to Windows Firewall With Advanced Security. In the search box, type wf.msc and press Ctrl+Shift+Enter to run it as an administrator.

Preventing unsafe actions with User Account Control

Widely scorned when it was introduced as part of Windows Vista, User Account Control (UAC) intercedes whenever a user or program attempts to perform a system administrative task and asks for the consent of a computer administrator before commencing what could be risky business. Since that rocky start, UAC has been tuned to become an effective security aid—without the annoyance factor that plagued the original implementation.

In Windows 10, user accounts you set up after the first one are standard (nonadministrator) accounts by default; although they can carry out all the usual daily computing tasks, they're prevented from performing potentially harmful operations. These restrictions apply not just to the user; more importantly, they also apply to any programs launched by the user. Even administrator accounts run as "protected administrator" accounts allowed only standard-user privileges except when they need to perform administrative tasks. (This is sometimes called Admin Approval Mode.)

➤ **For information about user accounts, see Chapter 6.**

Most programs are written so that they don't require administrator privileges for performing everyday tasks. Programs that truly need administrative access (such as utility programs that change computer settings) request elevation—and that's where UAC comes in.

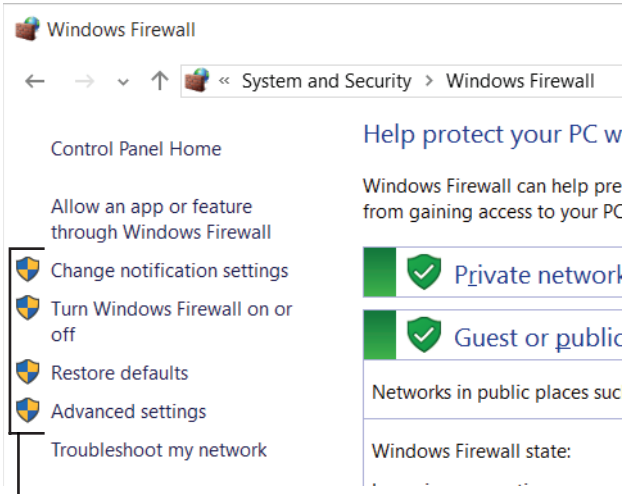
What triggers UAC prompts

The types of actions that require elevation to administrator status (and therefore display a UAC elevation prompt) include those that make changes to system-wide settings or to files in %SystemRoot% or %ProgramFiles%. (On a default Windows installation, these environment variables represent C:\Windows and C:\Program Files, respectively.) Among the actions that require elevation are the following:

- Installing and uninstalling desktop applications
- Installing device drivers that are not included in Windows or provided through Windows Update
- Installing ActiveX controls
- Changing settings for Windows Firewall
- Changing UAC settings
- Configuring Windows Update

- Adding or removing user accounts
- Changing a user's account type
- Running Task Scheduler
- Restoring backed-up system files
- Viewing or changing another user's folders and files

Within Windows, you can identify in advance many actions that require elevation. A shield icon next to a button or link indicates that a UAC prompt will appear if you're using a standard account.



Shield icons identify links that require UAC elevation

If you sign in with an administrator account (and if you leave the default UAC settings unchanged), you'll see fewer consent prompts than if you use a standard account. That's because the default setting prompts only when a program tries to install software or make other changes to the computer, but not when you make changes to Windows settings—even those that would trigger a prompt for a standard user with default UAC settings. Windows uses autoelevation to elevate without prompting certain programs that are part of Windows. Programs that are elevated automatically are from a predefined list, they must be digitally signed by the Windows publisher, and they must be stored in certain secure folders.

Limitations of User Account Control

User Account Control isn't a security silver bullet. It's one layer of a defense-in-depth strategy.

Some Windows users assume that UAC consent dialog boxes represent a security boundary. They don't. They simply represent a place for an administrator to make a trust decision. If a bad guy uses social engineering to convince you that you need his program, you've already made a trust decision. You'll click at least a half-dozen times to download, save, and launch the bad guy's program. A UAC consent request is perfectly normal in this sequence, so why wouldn't you click one more time?

If this scenario bothers you, the obvious solution is to adjust UAC to its highest level. Among other changes, this setting disables the autoelevation behavior. (For details on how to do this, see "Modifying UAC settings" later in this chapter.) If a program tries to use this subterfuge to sneak system changes past you, you'll see an unexpected consent dialog box from the system. But as soon as you provide those elevated credentials, the code can do anything it wants.

A better alternative is to sign in using a standard account, which provides a real security boundary. A standard user who does not have the administrator password can make changes only in her own user profile, protecting the system from unintended tampering.

Even running as a standard user doesn't provide complete protection. Malware can be installed in your user profile without triggering any system alarms. It can log your keystrokes, steal your passwords, and send out email using your identity. Even if you reset UAC to its highest level, you could fall victim to malware that lies in wait for you to elevate your privileges and then does its own dirty work alongside you.

As we said, enabling UAC is only one part of a multilayered security strategy. It works best when supplemented by a healthy skepticism and up-to-date antimalware software.

Dealing with UAC prompts

At sign-in, Windows creates a token that is used to identify the privilege levels of your account. Standard users get a standard token, but administrators actually get two: a standard token and an administrator token. The standard token is used to open Explorer.exe (the Windows shell), from which all subsequent programs are launched. Child processes inherit the token of the process that launches them, so by default all applications run as a standard user—even when you're signed in with an administrator account. Certain programs request elevation to administrator privileges; that's when the UAC prompt is displayed. If you provide administrator

credentials, Windows then uses the administrator token to open the program. Note that any processes that the successfully elevated program opens also run as an administrator.

As an elevation-requesting application attempts to open, UAC evaluates the application and the request and then displays an appropriate prompt. As an administrator, the most common prompt you're likely to see is the consent prompt, which is shown in Figure 7-7. Read it, check the name of the program, click Yes if you're confident that it's safe to proceed, and carry on.

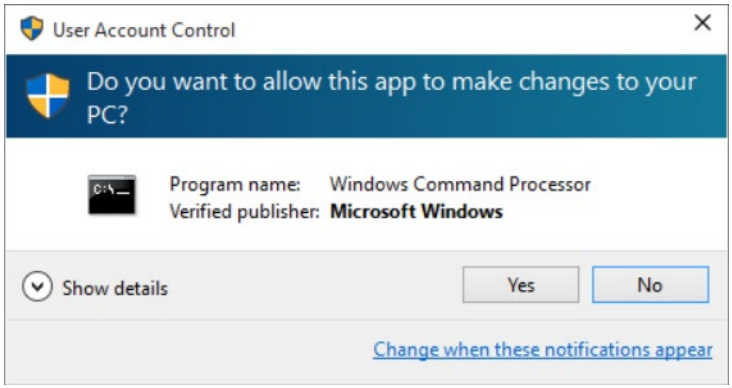


Figure 7-7 Clicking Show Details displays a link to the program's certificate.

If you use a standard account, when a program requires elevation you'll see the credentials prompt, which is shown in Figure 7-8. If the user is able to provide the credentials (that is, user name and password, smart card, or fingerprint, depending on how sign-in authentication is configured on the computer) of an administrator, the application opens using the administrator's access token.

By default, the UAC dialog box sits atop the secure desktop, a darkened representation of your desktop that runs in a separate process that no other application can interfere with. (If the secure desktop wasn't secure, a malicious program could put another dialog box in front of the UAC dialog box, perhaps with a message encouraging you to let the program proceed. Or a malicious program could grab your keystrokes, thereby learning your administrator sign-in password.) When the secure desktop is displayed, you can't switch tasks or click the windows on the desktop. (In fact, they're not really windows. When UAC invokes the secure desktop, it snaps a picture of the desktop, darkens it, and then displays that image behind the dialog box.)

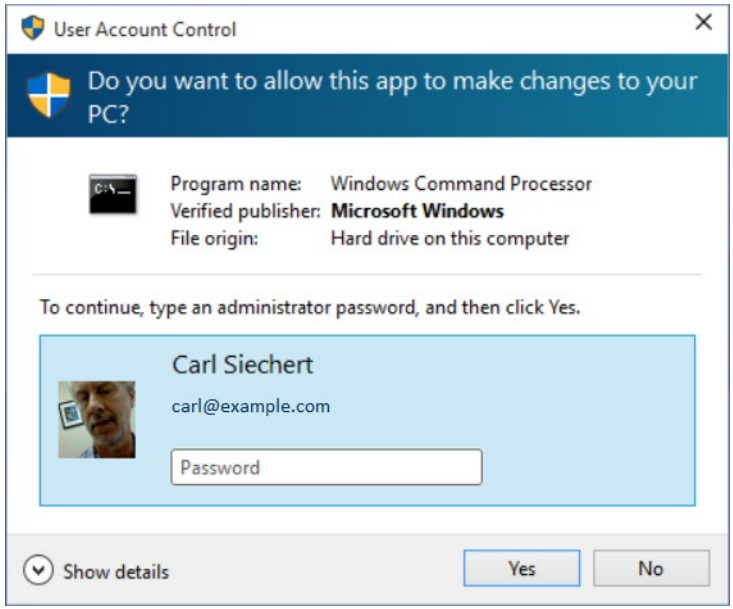


Figure 7-8 To perform an administrative task, a standard user must enter the password for an administrator account.

TROUBLESHOOTING

There's a delay before the secure desktop appears

On some systems, you have to wait a few seconds before the screen darkens and the UAC prompt appears on the secure desktop. There's no easy way to solve the slow-down, but you can easily work around it. In User Account Control Settings (described in the next section, "Modifying UAC settings"), you can take the protection level down a notch. The setting below the default provides the same level of UAC protection (albeit with a slight risk that malware could hijack the desktop), except that it does not dim the desktop.

NOTE

If an application other than the foreground application requests elevation, instead of interrupting your work (the foreground task) with a prompt, UAC signals its request with a flashing taskbar button. Click the taskbar button to see the prompt.

It becomes natural to click through dialog boxes without reading them or giving them a second thought. But it's important to recognize that security risks to your computer are real and that actions that trigger a UAC prompt are potentially dangerous. Clearly, if you know what you're doing and you click a button to, say, change Windows Update settings, you can blow

past that security dialog box with no more than a quick glance to be sure it was raised by the expected application. But if a UAC prompt appears when you're not expecting it—stop, read it carefully, and think before you click.

Modifying UAC settings

To review your User Account Control options and make changes to the way it works, in the search box or in Control Panel, type **uac** and then click Change User Account Control Settings. A window similar to the one shown in Figure 7-9 appears.

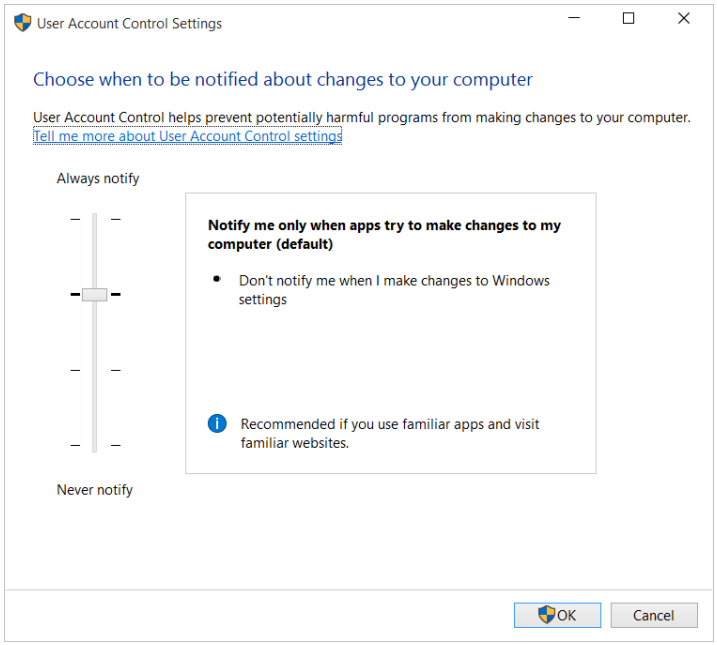


Figure 7-9 The topmost setting might overwhelm you with UAC prompts; the bottom setting turns off UAC.

Your choices in this window vary slightly depending on whether you use an administrator account or a standard account. For standard accounts, the top setting is the default; for administrator accounts, the second setting from the top is the default. Table 7-1 summarizes the available options.

To make changes, move the slider to the position you want. Be sure to take note of the advisory message in the bottom of the box as you move the slider. Click OK when you're done—and then respond to the UAC prompt that appears! Note that when you're signed in with a standard account, you can't select one of the bottom two options, even if you have the

password for an administrator account. To select one of those options, you must sign in as an administrator and then make the change.

Table 7-1 User Account Control settings

Slider position	Prompts when a program tries to install software or make changes to the computer	Prompts when you make changes to Windows settings	Displays prompts on a secure desktop
Standard user account			
Top (default)	✔	✔	✔
Second	✔	✔	
Third	✔		
Bottom (off)			
Administrator account			
Top	✔	✔	✔
Second (default)	✔		✔
Third	✔		
Bottom (off)			

TROUBLESHOOTING

User Account Control settings don't stick

If you find that nothing happens when you make a change to User Account Control settings, be sure that you're the only one signed in to your computer. Simultaneous sign-ins that use Fast User Switching can cause this problem.

Inside OUT

Use Local Security Policy to customize UAC behavior

Users of the Pro and Enterprise editions of Windows 10 can use the Local Security Policy console to modify the behavior of UAC. Start Local Security Policy (Secpol.msc), and open Security Settings\Local Policies\Security Options. In the details pane, scroll down to the policies whose names begin with "User Account Control." For each policy, double-click it and then click the Explain tab for information before you decide on a setting. With these policies, you can make several refinements in the way UAC works—including some that are not possible in the User Account Control Settings window. (Administrators on Windows-based enterprise networks can also configure these options using Group Policy management tools.) For details about each of these policies, see "UAC Group Policy Settings" at *w7io.com/1523*.

Regardless of your UAC setting, the shield icons still appear throughout Control Panel, but you won't see UAC prompts if you've lowered the UAC protection level. Clicking a button or link identified with a shield immediately begins the action. Administrators run with full administrator privileges; standard users, of course, still have only standard privileges.

CAUTION

Don't forget that UAC is more than annoying prompts. Only when UAC is enabled does an administrator run with a standard token. Only when UAC is enabled does Internet Explorer run in a low-privilege Protected Mode. Only when UAC is enabled does it warn you when a rogue application attempts to perform a task with system-wide impact. And, of course, disabling UAC also disables file and registry virtualization, which can cause compatibility problems with applications that use fixes provided by the UAC feature. For these reasons, we urge you not to select the bottom option in User Account Control Settings, which turns off UAC completely.

Encrypting information

Windows provides the following encryption tools for preventing the loss of confidential data:

- Encrypting File System (EFS) encodes your files so that even if someone is able to obtain the files, he or she won't be able to read them. The files are readable only when you sign in to the computer using your user account.
- BitLocker Drive Encryption provides another layer of protection by encrypting entire hard-disk volumes. By linking this encryption to a key stored in a Trusted Platform Module (TPM) or USB flash drive, BitLocker reduces the risk of data being lost when a computer is stolen or when a hard disk is stolen and placed in another computer. A thief's standard approach in these situations is to boot into an alternate operating system and then try to retrieve data from the stolen computer or drive. With BitLocker, that type of offline attack is effectively neutered.
- BitLocker To Go extends BitLocker encryption to removable media, such as USB flash drives.

NOTE

Encrypting File System and BitLocker Drive Encryption are not available in Windows 10 Home. Encrypting a removable drive with BitLocker To Go requires Windows 10 Pro or Windows 10 Enterprise; the resulting encrypted drive can be opened and used on a device running Windows 10 Home.

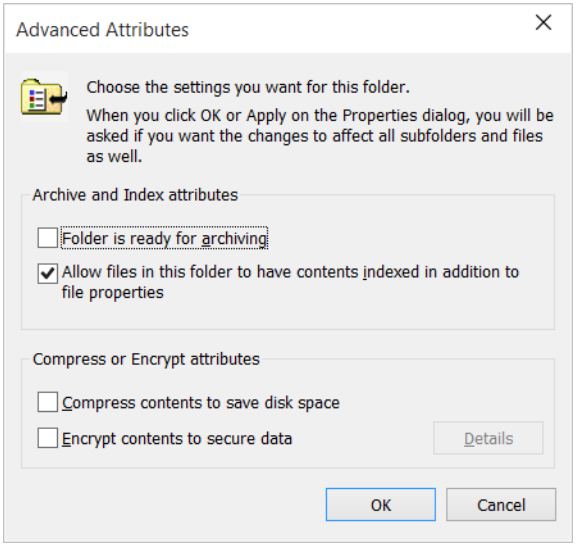
Using the Encrypting File System

The Encrypting File System (EFS) provides a secure way to store your sensitive data. Windows creates a randomly generated file encryption key (FEK) and then transparently encrypts the data, using this FEK, as the data is being written to disk. Windows then encrypts the FEK using your public key. (Windows creates a personal encryption certificate with a public/private key pair for you the first time you use EFS.) The FEK, and therefore the data it encrypts, can be decrypted only with your certificate and its associated private key, which are available only when you sign in with your user account. (Designated data recovery agents can also decrypt your data.) Other users who attempt to use your encrypted files receive an "access denied" message. Even administrators and others who have permission to take ownership of files are unable to open your encrypted files.

You can encrypt individual files, folders, or entire drives. (You cannot encrypt the boot volume—the one with the Windows operating system files—using EFS, however. For that, you must use BitLocker.) We recommend that you encrypt folders or drives instead of individual files. When you encrypt a folder or drive, the files it contains are encrypted, and new files that you create in that folder or drive are encrypted automatically.

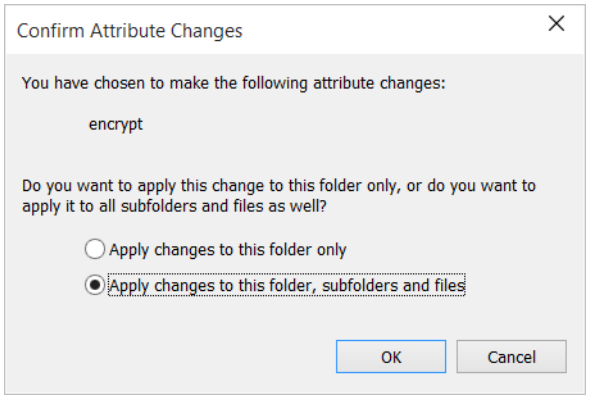
To encrypt a folder, follow these steps:

1. In File Explorer, right-click the folder, choose Properties, click the General tab, and then click Advanced, which displays the dialog box shown next. (If the properties dialog box doesn't have an Advanced button, the folder is not on an NTFS-formatted volume and you can't use EFS.)



2. Select Encrypt Contents To Secure Data. (Note that you can't encrypt compressed files. If the files are already compressed, Windows clears the compressed attribute.)

3. Click OK twice. If the folder contains any files or subfolders, Windows then displays a confirmation message.



NOTE

If you select Apply Changes To This Folder Only, Windows doesn't encrypt any of the files currently in the folder. Any new files that you create in the folder, however, including files that you copy or move to the folder, will be encrypted.

After a file or folder has been encrypted, File Explorer displays its name in green. This minor cosmetic detail is the only change you are likely to notice. Windows decrypts your files on the fly as you use them and reencrypts them when you save.

CAUTION

Before you encrypt anything important, you should back up your file recovery certificate and your personal encryption certificate (with their associated private keys), as well as the data recovery agent certificate, to a USB flash drive or to your OneDrive. Store the flash drive in a secure location. To do this, open User Accounts in Control Panel, and then click Manage Your File Encryption Certificates. If you ever lose the certificate stored on your hard drive (because of a disk failure, for example), you can restore the backup copy and regain access to your files. If you lose all copies of your certificate (and no data recovery agent certificates exist), you won't be able to use your encrypted files. No backdoor exists (none that we know of, at any rate), nor is there any practical way to hack these files. (If there were, it wouldn't be very good encryption.)

To encrypt one or more files, follow the same procedure as for folders. You'll see a different confirmation message to remind you that the file's folder is not encrypted and to give you an opportunity to encrypt it. You generally don't want to encrypt individual files because the information you intend to protect can too easily become decrypted without your knowledge. For example, with some applications, when you open a document for editing, the application creates a copy of the original document. When you save the document after editing, the application saves the copy—which is not encrypted—and deletes the original encrypted document. Static files that you use for reference only—but never for editing—can safely be encrypted without encrypting the parent folder. Even in that situation, however, you'll probably find it simpler to encrypt the whole folder.

Encrypting with BitLocker and BitLocker To Go

BitLocker Drive Encryption can be used to encrypt entire NTFS volumes, which provides excellent protection against data theft. BitLocker can secure a drive against attacks that involve circumventing the operating system or removing the drive and placing it in another computer. BitLocker provides the greatest protection on a computer that has TPM version 1.2 or later; on these systems, the TPM stores the key and ensures that a computer has not been tampered with while offline. If your computer does not have TPM, you can still use BitLocker on your operating system volume, but you must insert a USB startup key or enter a password each time you start the computer or resume from hibernation. Non-TPM systems do not get the system integrity check at startup.

BitLocker To Go, a feature introduced in Windows 7, allows you to encrypt the entire contents of a USB flash drive or other removable device. If it's lost or stolen, the thief will be unable to access the data without the password.

To apply BitLocker Drive Encryption or BitLocker To Go, right-click the drive in File Explorer and then click Turn On BitLocker. BitLocker asks how you want to unlock the encrypted drive—with a password, a smart card, or both. After you have made your selections and confirmed your intentions, the software gives you the opportunity to save and print your recovery key, as shown in Figure 7-10.

Your recovery key is a system-generated, 48-character, numeric backup password. If you lose the password you assign to the encrypted disk, you can recover your data with the recovery key. BitLocker offers to save that key in a plain text file; you should accept the offer and store the file in a secure location.

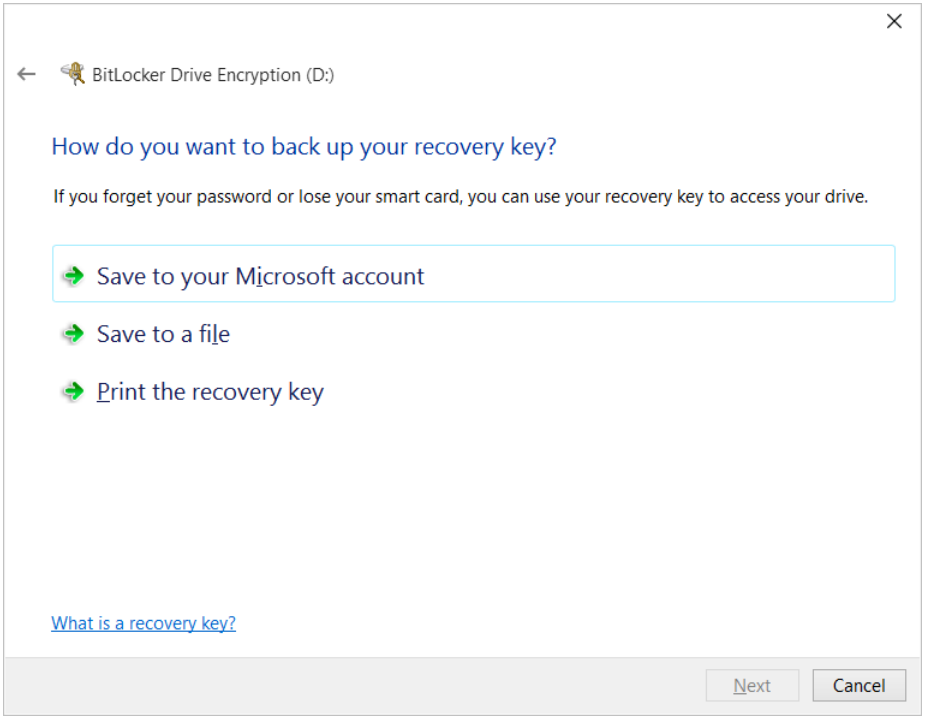


Figure 7-10 The option of saving the recovery key to your Microsoft account—that is, to your OneDrive—is new with Windows 10.

Inside OUT

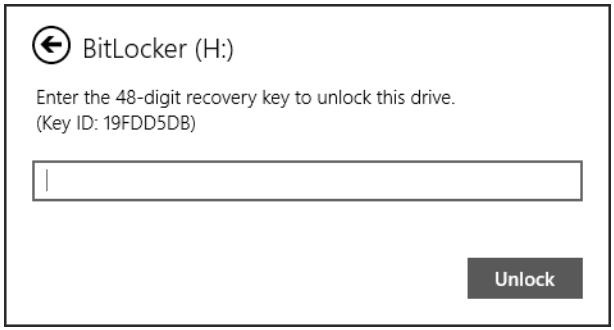
Store your recovery keys on OneDrive

Clicking Save To Your Microsoft Account saves the recovery key on your OneDrive, making it accessible anywhere you have an Internet connection. But the trick is finding that key on OneDrive: Go to *onedrive.com/recoverykey*.

With all preliminaries out of the way, BitLocker begins encrypting your media. This process takes a few minutes, even if the disk is freshly formatted. However, if you are in a hurry, you can opt to encrypt only the used space on the drive. This choice can save you a considerable amount of time if your disk contains only a small number of files.

To read a BitLocker-encrypted removable disk, you need to unlock it by using whatever method you have stipulated. If you're prompted for a password that you have lost or

forgotten, click More Options and then click Enter Recovery Key. In case you have several recovery-key text files, BitLocker To Go gives you the key's identification code:



Find the entry on OneDrive (*onedrive.com/recoverykey*) or the text file whose name matches the identification code, copy the recovery key from this text file to the BitLocker dialog box, and you'll be granted temporary access to the files, which is good until you remove the disk or restart the computer. At this point, you might want to change the password; open BitLocker Drive Encryption in the System And Security section of Control Panel and click Change Password.

To remove BitLocker encryption from a disk, open BitLocker Drive Encryption in Control Panel and click Turn Off BitLocker. The software will decrypt the disk; allow some time for this process.

➤ **For more information about BitLocker, see *http://bit.ly/bitlocker-overview*.**

Using Windows Defender to block malware

The best way to fight unwanted and malicious software is to keep it from being installed on any PC that is part of your network. Over the years, malicious hackers have found a variety of ways to install malware: floppy disks, document files, email attachments, instant messaging attachments, AutoPlay on USB flash drives, scripts, browser add-ons . . . and the list goes on. Many of these transmission methods rely on social-engineering techniques designed to lure inattentive or gullible users into opening an infected attachment, visiting an infected website, and so on. Not satisfied with being able to pick off the inattentive and gullible, authors of hostile software are always on the lookout for techniques they can use to spread infections automatically.

Any program that tries to sneak onto your PC without your full knowledge and consent should be blocked. An important layer in a basic PC protection strategy, therefore, is to use

up-to-date antimalware software. Into the breach steps Windows Defender, the antimalware program included in Windows 10.

Windows Defender runs as a system service and uses a scanning engine to compare files against a database of virus and spyware definitions. It also uses heuristic analysis of the behavior of programs to flag suspicious activity from a file that isn't included in the list of known threats. It scans each file that you access in any way, including downloads from the Internet and email attachments you receive. (This feature is called *real-time protection*—not to be confused with scheduled *scans*, which periodically inspect all files stored on your computer to root out malware.)

Using Windows Defender

In general, you don't need to "use" Windows Defender at all. As a system service, it works quietly in the background. The only time you'll know it's there is if it finds an infected file; one or more notifications will pop up to alert you to the fact.

Nonetheless, you might want to poke around a bit. To open Windows Defender, type **defender** in the search box, and click the program's shortcut. If a shortcut to Windows Defender doesn't appear or if you don't have a keyboard, open Settings, tap Update & Security, tap Windows Defender, scroll all the way to the bottom, and tap Use Windows Defender.

The Home tab, shown in Figure 7-11, shows the current status and the results of the most recent scan. This tab also tells you whether real-time protection is enabled.

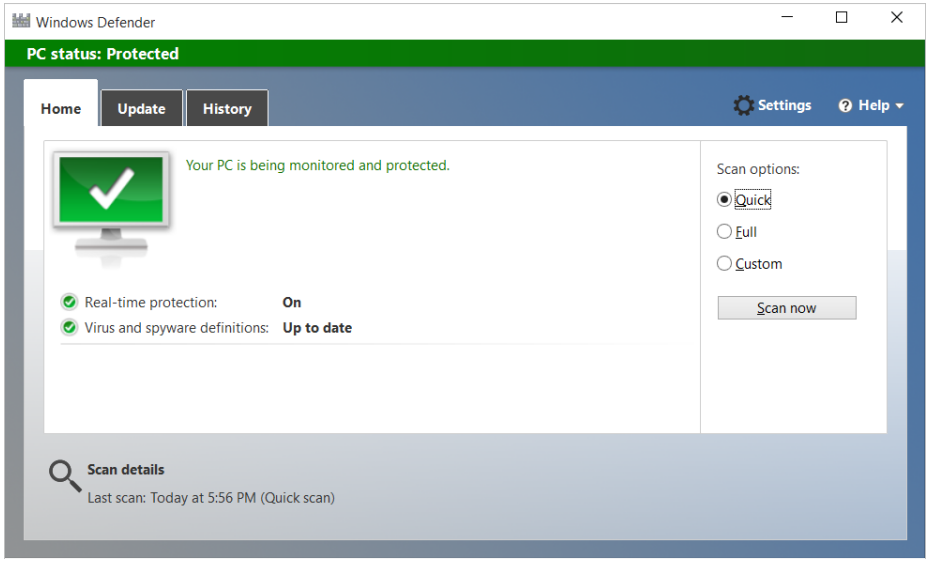


Figure 7-11 The Home tab provides status and a launch pad for manual scans.

To temporarily disable real-time protection (if it is interfering with the installation of a legitimate program, for example), click Settings to open a window in which you can turn off real-time protection. Doing so causes the PC Status banner at the top of the program window to glow red and change from Protected to At Risk; a large Turn On button dominates the Home tab. Windows Defender is so anxious to restore real-time protection, in fact, that it automatically turns it back on when you restart your computer or after some time elapses.

Windows Defender uses Windows Update to retrieve definition files and periodic updates to the detection engine. The Update tab in Windows Defender shows when the definitions were last updated and also features an Update button in case you want to get the latest definitions immediately instead of waiting for Windows Update.

Manually scanning for malware

The combination of real-time protection and periodic scheduled scanning is normally sufficient for identifying and resolving problems with malware and spyware. However, if you suspect that you've been infected, you can initiate a scan on demand. To immediately scan for problems, on the Home tab (see Figure 7-11) under Scan Options, select the type of scan you want to perform and click Scan Now.

The Quick option kicks off a scan that checks only the places on your computer that malware and spyware are most likely to infect, and it is the recommended setting for frequent regular scans. Choose Full if you suspect infection (or you just want reassurance that your system is clean) and want to inspect all running programs and the complete contents of all local volumes. Click Custom if you want to restrict the scan to any combination of drives, folders, and files.

Inside OUT

Run a scan from a script or a scheduled task

Windows Defender includes a command-line utility that you can use to automate scans with a script or a scheduled task. You'll find MpCmdRun.exe in %ProgramFiles%\Windows Defender. For details about using the utility, open an elevated Command Prompt window and run the program with no parameters.

A full scan can be burdensome, especially if you have hundreds of thousands of files scattered around local disks. To minimize the time and system resources, you can specify that Windows Defender skip over locations and file types that you know are safe and haven't been tampered with. To do that, begin by clicking Settings. On the Windows Defender tab in Settings, click Add An Exclusion (under Exclusions) to display a window like the one shown in Figure 7-12.

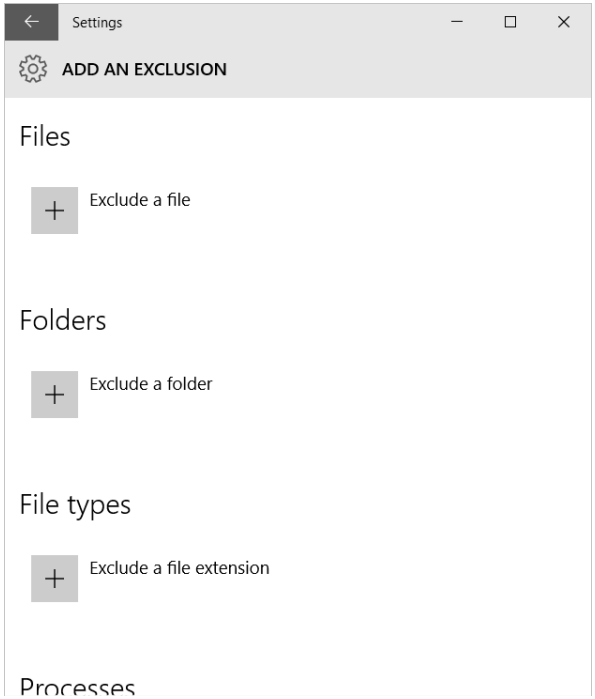


Figure 7-12 Files, folders, file types, and processes that are excluded are ignored during scans. Click the plus icon to add items to the exclusion list.

There you'll find four options that affect scanning:

- **Exclude A File.** Specify files that you know to be safe.
- **Exclude A Folder.** Specify folders that you know to be safe. This is an appropriate option if you have a folder full of previously downloaded system utilities that routinely trigger alerts. Do not use this option with folders where you normally download new files.
- **Exclude A File Extension.** Similarly, you can exclude from scans all files with the file name extensions (such as common scripts) that you specify.
- **Exclude A .Exe, .Com Or .Scr Process.** If you find that a program is routinely detected as a potential threat despite your telling Windows Defender to allow it, consider adding the program to this list. Be sure to specify the process name (Myprogram.exe) and not the program name. This strategy is less risky than excluding the containing folder;

if you grant blanket approval for files in the containing folder, and later some real spyware ends up in the folder, you risk allowing malware to sneak onto your system with no warning.

To delete an exclusion (so it will no longer be excluded from scans), return to Add An Exclusion, click or tap the name of the exclusion you want to delete, and click Remove.

Dealing with detected threats

If Windows Defender detects the presence of malware or spyware as part of its real-time protection, it displays a warning above the notification area and, in most cases, resolves the problem without you lifting a finger.

To learn more about its findings, in Windows Defender click the History tab. Select Quarantined Items, and then click View Details. As Figure 7-13 shows, Windows Defender shows the name, alert level, and detection date of the quarantined item or items.

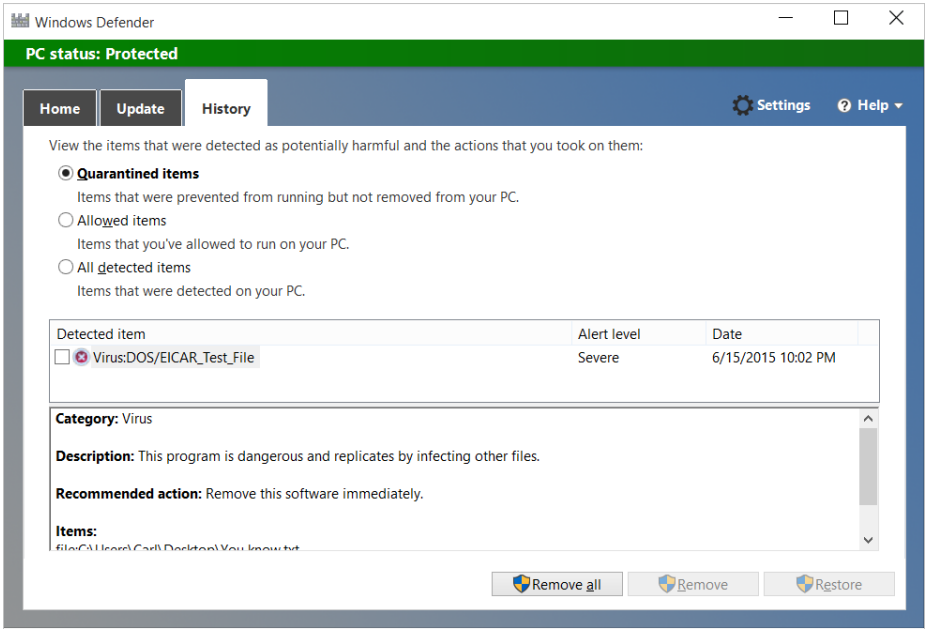


Figure 7-13 The box below the list shows details about the selected item; a link at the bottom of that box (not shown) leads to online information about the particular infection.

Detected items are moved to a restricted folder (%ProgramData%\Microsoft\Windows Defender\Quarantine) whose permissions include a Deny access control entry that locks out the built-in Users and Everyone groups. Executable files in this folder cannot be run, nor can

the folder's contents be accessed from File Explorer. Items moved here can be managed only from the Windows Defender console (preferred) or an elevated Command Prompt window.

Stopping unknown or malicious programs with SmartScreen

SmartScreen, which began as a feature in Internet Explorer in Windows 7, is used to identify programs that other users have run safely. It does so by comparing a hash of a downloaded program with Microsoft's application-reputation database. This occurs when you download a program using Microsoft Edge or Internet Explorer, and when you attempt to run a program that you have downloaded from the Internet—regardless of what browser you use.

Programs with a positive reputation run without any ado. Programs that are known to be bad or that have not yet developed a reputation are blocked. A message similar to the one shown in Figure 7-14 appears.

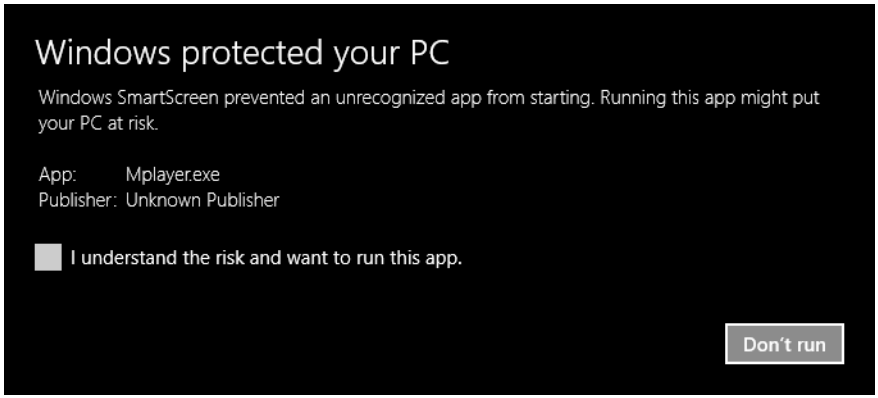


Figure 7-14 When you attempt to run a downloaded program that doesn't match one in Microsoft's database, a message like this appears.

If you're certain that a program is safe, you can override the block by selecting the check box, which adds a Run Anyway button you can then click. With default settings in place, you'll then need the approval of someone with an administrator account before the program runs. Don't say you weren't warned.

You can adjust the level of SmartScreen protection by going to Security And Maintenance (see Figure 7-1 earlier in this chapter) and clicking Change Windows SmartScreen Settings. Besides

the default setting, you can remove the requirement for administrator approval or you can disable SmartScreen altogether.