Protecting the Server and Client

LESSON 5

OBJECTIVE DOMAIN MATRIX

Skill/Concept	Exam Objective	Objective Number
Protecting the Client Computer	Understand malware	2.6
	Understand client protection	4.1
Managing Client Security Using Windows Defender	Understand client protection	4.1
Protecting Your Email	Understand email protection	4.2
Securing Internet Explorer	Understand internet security	1.3
Configuring Microsoft Edge	Understand internet security	1.3
Protecting Your Server	Understand server protection	4.3
Using Security Baselines	Understand dedicated firewalls	3.1
Locking Down Devices to Run Only Trusted Applications	Understand encryption	2.5
	Understand client protection	4.1
Managing Windows Store Apps	Understand encryption	2.5
	Understand client protection	4.1

KEY TERMS

AppLocker
backdoor
Bayesian filter
Bring Your Own Device (BYOD) policy
content zone
cookie
Line of Business (LOB) app
malicious software (malware)
Microsoft account
Microsoft Active Protection Service (MAPS)
Microsoft Baseline Security Analyzer (MBSA)
Microsoft Edge
offline file
pharming
phishing
polymorphic virus
pop-up window
ransomware
Read-Only Domain Controller (RODC)
rootkit

rule collection
security baseline
Security Compliance Manager 4.0 (SCM 4.0)
security template
Sender Policy Framework (SPF)
spam
spyware
Trojan horse
Universal Windows Platform (UWP) app
User Account Control (UAC)
virus
virus hoax
Windows Defender
Windows Firewall
Windows Server Update Services (WSUS)
Windows Store
Windows Store for Business
Windows Update
worm
zero-day attack

Lesson 1 introduced using multiple layers of security to protect your resources. Therefore, if the first security layer is compromised, there are other security mechanisms that will protect your resources. You also learned about authentication, permissions, auditing, encryption, malware, and firewalls. This lesson will complete the security picture by focusing on how to implement security on client computers and servers.

■ Protecting the Client Computer

THE BOTTOM LINE

The client computer is the computer that a user would use to connect to the servers and network applications. Because the computer is connected to an organization's network, it is important to protect the client computer. You would like to keep your users productive rather than spend time fixing their computers.

CERTIFICATION READY
What is needed to secure a client computer?
Objective 4.1

After working with computers for a while, you begin to realize that protecting a client computer can become quite complicated when trying to maintain its Windows operating system, its many applications, and the various network applications and services required to make it a productive tool in the face of all the malicious malware to which it's currently exposed.

Protecting Your Computer from Malware

Malicious software, sometimes called ***malware***, is software designed to infiltrate and adversely affect a computer system without the owner's informed consent. It is usually associated with viruses, worms, Trojan horses, spyware, rootkits, and dishonest adware. As a network administrator or computer technician, it is important to know how to identify malware, how to remove malware, and how to protect a computer from malware.

UNDERSTANDING TYPES OF MALWARE

CERTIFICATION READY
How is a buffer overflow exploited?
Objective 2.6

Because it is quite common for a computer to be connected to the internet, there are more opportunities than ever for a computer to be infected by malware. In addition, over the last couple of years, the number of malware attacks perpetrated over the internet is staggering. Also, it is important to ensure that if a computer gets infected on a network, it does not spread to other computers.

Many early forms of malware were written as experiments or practical jokes (known as pranks). Most of the time, these were intended to be harmless or merely annoying. However,

as time goes by, malware has turned more toward vandalism, extortion, and even terrorism, as a tool used to compromise private information, encrypt data for ransom, and generally damage confidence in economic and political systems.

Besides using tools, such as a denial-of-service (DoS) attack, to attack other systems, networks, or websites, causing those systems to have performance problems or otherwise become inaccessible, malware can be identified as one or more of the following:

- Virus
- Worm
- Trojan horse
- Spyware and dishonest adware
- Rootkit
- Backdoor
- Polymorphic virus
- Zero-day attack
- Ransomware

A computer ***virus*** is a program that can copy itself and infect a computer without the user's consent or knowledge. Early viruses were usually some form of executable code that was hidden in the boot sector of a disk or as an executable file (a file name with an .exe or .com extension).

Later, as macro languages were used in software applications such as word processors and spreadsheets to enhance the programs' power and flexibility, malicious macro programs could be embedded within those documents. These documents can further infect other documents, causing a wide range of problems on computer systems as the macro code is executed (when the document is opened).

Today's websites can be written in various programming and scripting languages and can include many executable programs. Therefore, when accessing the internet, a system is placed under constant threat.

A ***worm*** is a self-replicating program that copies itself to other computers over the network without the need for any user intervention. Different from a virus, a worm does not corrupt or modify files on a target computer. Instead, it consumes bandwidth and ties up processor and memory resources, slowing the system down, and causing the system to become unusable. Worms usually spread by using security holes found within the operating system or TCP/IP software implementations.

A ***Trojan horse*** is a program named after the Trojan horse story in Greek mythology. A Trojan horse is an executable program that appears as a desirable or useful program. Because it appears to be a desirable or useful program, users are tricked into loading and executing the program on their system. After the program is loaded, it can cause a computer to become unusable or it can bypass a system's security, allowing private information such as passwords, credit card numbers, and Social Security numbers to be read and copied, as well as executing adware.

Spyware is a type of malware that is installed on computers and collects personal information and browsing habits, often without the user's knowledge. Spyware can also install additional software, which can redirect your web browser to other sites or change your home page.

One type of spyware is the keylogger, which records every key a user presses. Therefore, when typing credit card numbers, Social Security numbers, and passwords, that information gets recorded and is eventually sent to and read by someone without the user's knowledge. It should be noted that not all keyloggers are bad, because some corporations use them to monitor their corporate users.

Adware is any software package that automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. While adware may not necessarily be bad, it is often used with ill intent.

A ***rootkit*** is a software or hardware device designed to gain administrator-level control over a computer system without being detected. Rootkits can target the BIOS, hypervisor, boot loader, kernel or, less commonly, libraries or applications.

A ***backdoor*** is a program that gives some remote user unauthorized control of a system or automatically initiates an unauthorized task. Some backdoors have been installed by viruses or other forms of malware. Other backdoors may be created by programmers within commercial applications or inside a customized application made for an organization.

CERTIFICATION READY
Which type of malware constantly changes in an effort to hide itself?
Objective 2.6

A ***polymorphic virus*** mutates, or changes its code, so that it cannot be as easily detected. Stealth viruses try to hide themselves by monitoring and intercepting a system's call. For example, when the system seeks to open an infected file, the stealth virus disinfects the file and allows the operating system to open it. When the operating system closes the file, the virus re-infects the file.

CERTIFICATION READY
How can a system be protected against zero-day attacks?
Objective 2.6

Viruses and worms often exploit a buffer overflow. In all application programs including Windows itself, there are buffers that hold data. These buffers have a fixed size. If too much data is sent to these buffers, a buffer overflow occurs. Depending on the data sent to the overflow, a hacker uses the overflow to obtain passwords, alter system files, install backdoors, and/or cause errors on the computer. When patches are released to fix a potential buffer overflow, the patch adds code to check the length of data sent to the buffer to make sure that it does not overflow.

Zero-day attacks are attacks based on using unknown or recently announced vulnerabilities. To help prevent these types of attacks, operating systems, network devices, and antivirus software should use the latest security updates and definitions.

CERTIFICATION READY
Which type of malware encrypts data so that the data cannot be accessed?
Objective 2.6

Ransomware is one of the fastest growing forms of malware; it encrypts data files and then demands a ransom to decrypt the files. As the user tries to access the files, the files are unreadable until they are decrypted. Ransomware, also considered a denial-of-service attack, prevents the user from accessing the files. Ransomware attacks are typically carried out using a Trojan horse from a website or through email.

To protect against ransomware, keep in mind the following recommendations:

- Install and use an up-to-date antivirus solution.
- Make sure the operating system and software is up-to-date with the newest security patches.
- Avoid clicking on links or opening attachments or emails from people you don't know or from companies you don't do business with.
- Ensure that SmartScreen Filter (in Microsoft Internet Explorer and Microsoft Edge) is turned on.
- Ensure that a pop-up blocker is enabled in your web browser.
- Back up important files on a regular basis. If your files get encrypted, it may be necessary to pay a ransom to get the files decrypted if you're unable to restore the files from backup.

IDENTIFYING MALWARE

The first step in removing malware is detecting the existence of malware. Sometimes it is easy to see that a system is infected with malware. Other times, you may never know that malware exists on your computer.

Some of the symptoms of malware include the following:

- System performs poorly
- System has less available memory than it should have
- System performs poorly while connected to the internet
- Computer stops responding frequently
- Computer takes longer to start up
- Browser closes unexpectedly or stops responding
- Browser default home or search pages change
- Advertising windows unexpectedly pop up
- Additional toolbars are unexpectedly added to the browser
- Programs start unexpectedly
- Programs cannot start
- Components of Windows or other programs no longer work
- Programs or files are suddenly missing
- Messages or displays on a monitor are unusual
- Sounds or music that are unusual play at random times
- Programs or files that are unknown have been created or installed
- Browser has unknown add-ins
- Files have become corrupted
- File size unexpectedly changes

Of course, to see these symptoms, you may need to actively look for them.

First, to make the most of determining which processes and services are rogue, create a baseline of what processes and services are running on the system under normal conditions, so that you have a basis for comparison. Then, when your machine begins running slow, start Task Manager to view processor and memory utilization. Look at the processes to see which process is using the most processor and/or memory resources. Also, review the processes and services in memory (using Task Manager). In addition, use System Configuration to look for changes in the system. Finally, to detect malware, use an up-to-date antivirus program and an up-to-date antispyware package, which can scan an entire system and look for malware in real time when opening files and accessing websites.

With today's computers generally connecting to the internet and/or other type of network on a continual basis, it's clear that a computer needs to be protected from all types of malware threats. And, as usual, a little common sense can go a long way in protecting a computer and network.

UNDERSTANDING SECURITY UPDATES AND ANTIVIRUS SOFTWARE FOR CLIENTS

Some viruses, worms, rootkits, spyware, and adware are made possible because they exploit a security hole within Windows, Internet Explorer, Microsoft Office, and/or other software packages. Therefore, the first step that should be taken to protect yourself against malware is to keep your system up-to-date with the latest service packs, security patches, and other critical fixes.

The second step to protect your computer from malware is to use an up-to-date antivirus software package. In addition, if your antivirus software does not include an antispyware component, install an antispyware software package. Perform a full system scan with your antivirus software at least once a week and do a quick scan whenever you see any of the symptoms listed in the "Identifying Malware" section of this lesson.

Windows Defender is a software product from Microsoft that prevents, removes, and quarantines spyware in Microsoft Windows. It will help protect a computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software by detecting and removing known spyware from a computer. Windows Defender features real-time protection, a monitoring system that recommends actions against spyware when it's detected, minimizes interruptions, and helps users stay productive. Like an antivirus package, it is necessary to keep Windows Defender up-to-date.

USING COMMON SENSE WITH MALWARE

To avoid malware, be sure to use common sense by following these suggestions:

- Don't install unknown software or software from an unknown source.
- Don't open strange email attachments.
- Don't click hyperlinks from strangers or if it's unclear what the link is supposed to do. This also applies to sources like Yahoo!, AOL, and MSN.
- If your email client supports auto launch, turn it off. Otherwise, you might automatically activate a computer virus just by opening the email.
- Don't visit questionable websites, especially sites that allow downloading software from music and video piracy sites and pornography sites.
- If your web browser alerts you that a site is known for hosting malware, pay attention to these warnings.
- If you surf the internet and browser pop-ups indicate that you need to download the newest driver or check your system for viruses, use caution.
- Don't forget to perform regular backups. So, if a computer does get a virus and data is lost, you can restore from a backup.

TAKE NOTE* While this list may be common knowledge for IT personnel, frequent reminders and awareness training for network users is always a good idea.

REMOVING MALWARE

If some of the malware symptoms listed earlier in this lesson begin to make an appearance, try to detect and remove any malware that is found. The first step in removing malware is to run an antivirus software package and perform a full scan. If an antivirus software package isn't installed, it's time to purchase one. If the package cannot be downloaded directly to the computer, try downloading it from another machine or to an optical disk such as a CD or DVD, or use a thumb drive to transfer it to your system. If it finds malware and removes the malware, reboot your computer and run it again to be sure your system is clean. If it keeps finding different malware, keep running it until your machine is clean.

TAKE NOTE*

Be sure that your antivirus is up-to-date. If it is not up-to-date, it will not know about newer viruses.

If your antivirus software package keeps finding the same malware, make sure you are not accessing a disk or other device that continues infecting the system. Also, it may be necessary to reboot Windows into Safe mode and try another scan. If the option is available, try to boot from a CD or DVD and run the scan.

If a virus cannot be removed, do some research on the internet. Often, step-by-step instructions can be found for removing specific malware, including deleting files and keys in the registry. Of course, be sure that the instructions are from a reliable source and follow the instructions precisely.

TAKE NOTE* If an antivirus software package has trouble removing malware, don't be afraid to contact the company to get assistance.

Remember, that if your antivirus package does not have an antispyware component, install an antispyware package to check for spyware. Also, consider using Windows Defender.

TAKE NOTE* Because some malware includes keylogging capabilities, consider updating logon information for your online accounts using a different computer—if you suspect such malware on your computer.

Microsoft also includes a Microsoft Windows Malicious Software Removal Tool, which checks computers running Windows for infections by specific, prevalent malicious software. Microsoft releases an updated version of this tool on the second Tuesday of each month, and as needed to respond to security incidents. The tool is available from Microsoft Update, Windows Update, and the Microsoft Download Center.

As a reminder, remember to use the following tools when trying to locate and remove possible malware:

- Use Task Manager to view and stop unknown processes and to stop unknown or questionable services.
- Use the Services MMC to stop unknown or questionable services.
- Use System Configuration to disable unknown or questionable services and startup programs.
- Disable unknown or questionable Internet Explorer add-ins.

UNDERSTANDING VIRUS HOAXES

A ***virus hoax*** is a message warning the recipient of a non-existent computer virus threat, usually sent as a chain email that tells the recipient to forward it to everyone they know. This is a form of social engineering that plays on people's ignorance and fear. Some hoaxes may tell people to delete key system files to make the system work properly or they tell people to download software from the internet to clean the virus. But instead, these hoaxes install some form of malware. Antivirus specialists agree that recipients should delete virus hoaxes when they receive them, instead of forwarding them.

Configuring Windows Updates

Windows Update provides Windows 10 users with a way to keep their computers current by checking a designated server. The server provides software that patches security issues, installs updates that make Windows and your applications more stable, fixes issues with existing Windows programs, and provides new features. The server can be hosted by Microsoft or it can be set up and managed in your organization by running the Windows Server Update Services (WSUS) or System Center 2012 R2/2016 Configuration Manager.

Microsoft routinely releases security updates on the second Tuesday of each month on what is known as "Patch Tuesday." Most other updates are released as needed, which are known as "out-of-band" updates. Before immediately installing updates on production systems, test

updates to make sure they will not cause problems. While Microsoft does intensive testing, occasionally problems do occur, either as a bug or a compatibility issue with third-party software. Therefore, always have a good backup of your system and data files before installing patches and have a backout plan, if needed.

Updates are classified as Important, Recommended, or Optional:

- **Important updates:** Offer significant benefits, such as improved security, privacy, and reliability. They should be installed as they become available, and can be installed automatically with Windows Update.
- **Recommended updates:** Address non-critical problems or help enhance your computing experience. While these updates do not address fundamental issues with your computer or Windows software, they can offer meaningful improvements.
- **Optional updates:** Can include updates, drivers, or new software from Microsoft to enhance your computing experience. These optional updates need to be installed manually.

Depending on the type of update, Windows Update can deliver the following:

- **Security updates:** Broadly released fixes for a product-specific security-related vulnerability. Security vulnerabilities are rated based on their severity, which is indicated in the Microsoft security bulletin as critical, important, moderate, or low.
- **Critical updates:** Broadly released fixes for a specific problem, addressing a critical, non-security related bug.
- **Service packs:** A tested, cumulative set of hotfixes, security updates, critical updates, and updates, as well as additional fixes for problems found internally since the release of the product. Service packs might also contain a limited number of customer-requested design changes or features. When an operating system is released, many corporations consider the first service pack as a time when the operating system matures enough to be used throughout the organization.

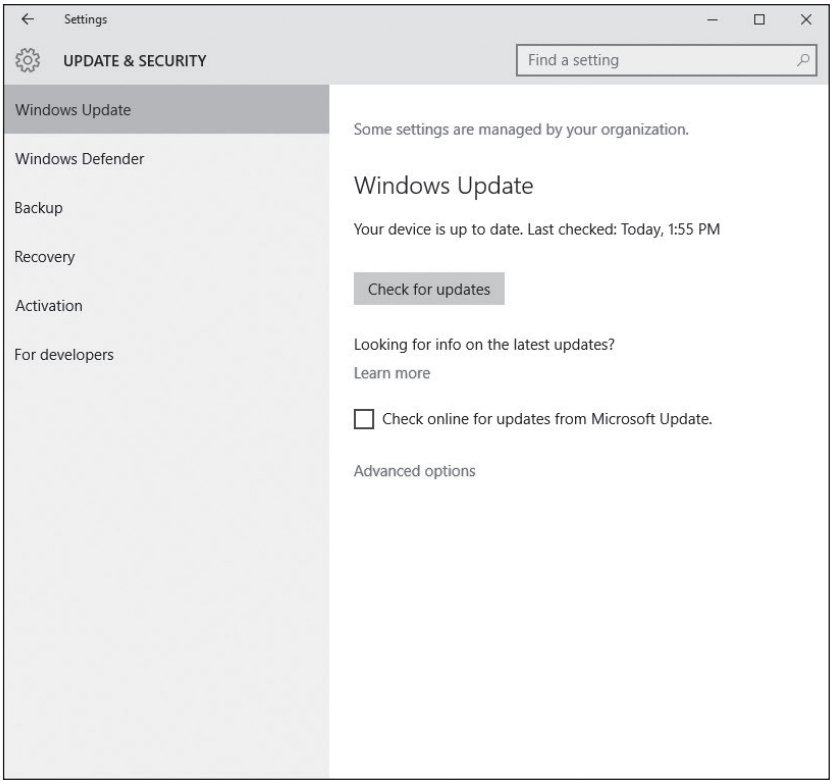
Not all updates can be retrieved through Windows Update. Sometimes, when researching a specific problem, Microsoft may have a fix for the problem by installing a hotfix, or cumulative patch. A hotfix is a single, cumulative package that includes one or more files that are used to address a problem in a software product, such as a software bug. Typically, hotfixes are made to address a specific customer situation and often have not gone through extensive testing as have other patches retrieved through Windows Update.

For small environments, configure your system to perform automatic updates to ensure that critical, security, and compatibility updates are made available for installation automatically without significantly affecting your regular use of the internet. Automatic updates work in the background when a computer is connected to the internet, to identify when new updates are available, and to download them to your computer. When a download is completed, you will be notified and prompted to install the update. Either install the update then, get more details about what is included in the update, or let Windows send a reminder later. Some updates may require a reboot, but others do not.

When first installing Windows 10, choose how Windows Update should function. On a Windows 10 computer, click the Start button, click Settings, and click Update & security to open the Windows Update page (see Figure 5-1).

Figure 5-1

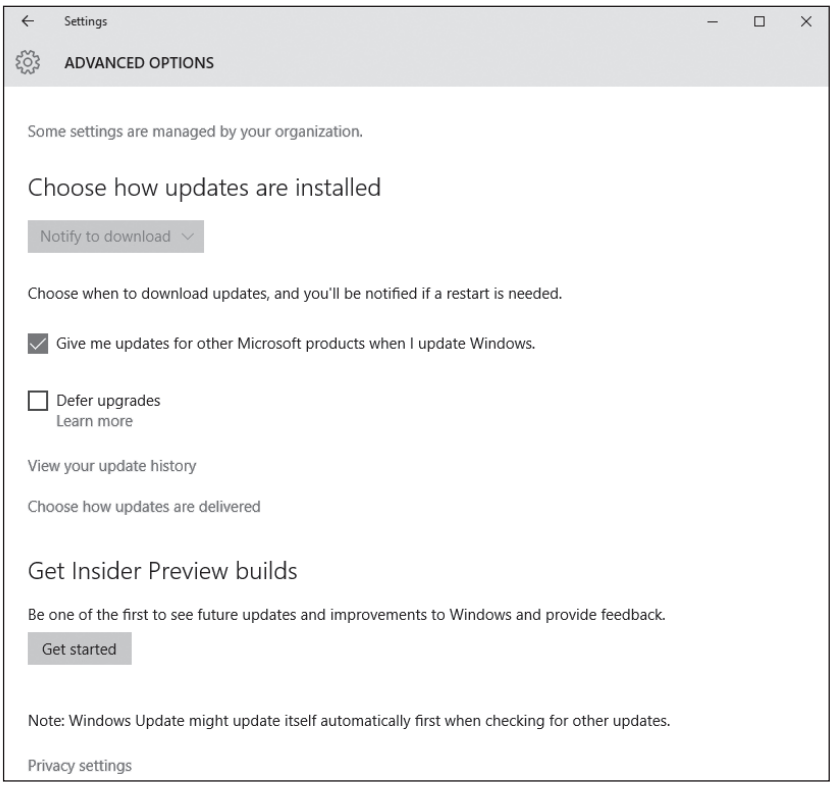
The Windows Update page



Click Advanced options to configure for automatic updates, get updates for other Microsoft products when Windows is updated, defer upgrades, and view the update history (as shown in Figure 5-2).

Figure 5-2

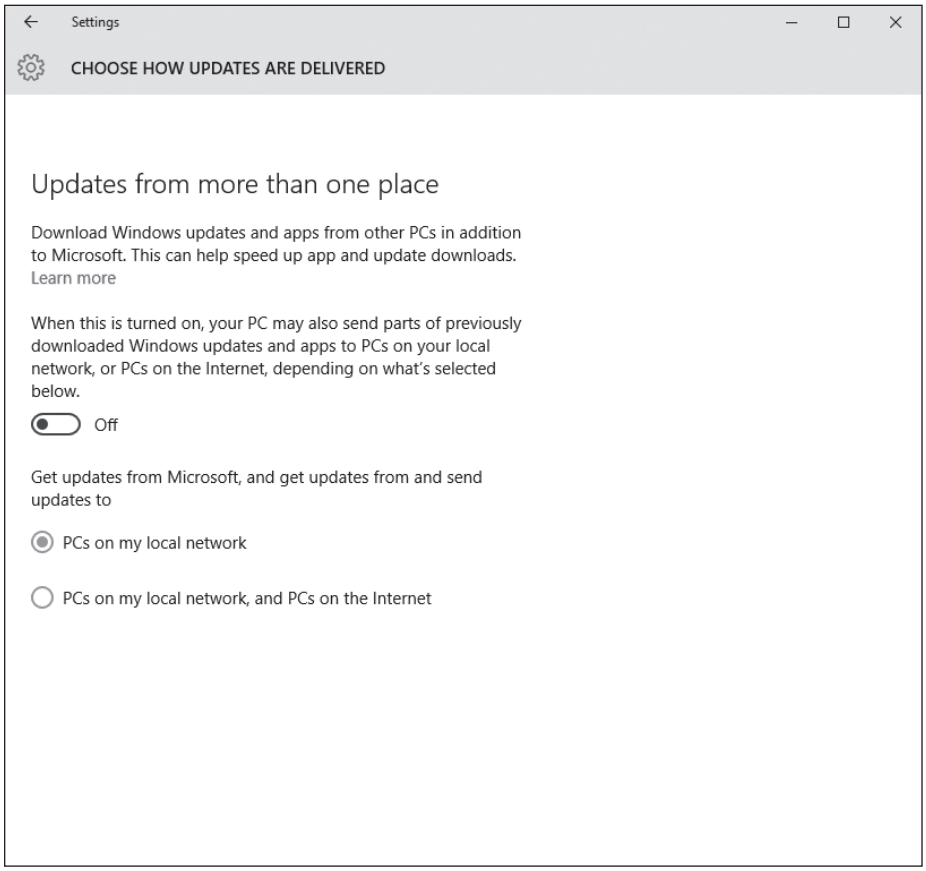
The Windows Update Advanced Options page



Click the Choose how updates are delivered option to see the Updates from more than one place page (see Figure 5-3). Unless your corporation uses WSUS or System Center 2012 R2/2016 Configuration Manager, you must use your internet connection to retrieve updates from Microsoft. Starting with Windows 10, enable the Updates from more than one place option, which also can be used to get updates from other computers on the same network as your local computer and from computers on the internet.

Figure 5-3

The Updates from more than one place page



On the Advanced Options page, customize how updates are installed. By default, the Choose how updates are installed option is set to Automatic (recommended), which means Windows selects a time when a computer is inactive to install the updates and reboot the system. Most organizations would prefer the Notify to schedule restart option so that Windows does not reboot a computer when it is least expected.

Some Windows 10 editions can defer upgrades to your PC. By selecting the Defer upgrades option, new Windows features won't be downloaded or installed for several months. This option is usually used to help avoid problems with an update that might cause problems within your organization.

TAKE NOTE* Deferring upgrades does not affect security updates, but it does prevent you from getting the latest Windows features as soon as they are available.

For corporations, consider using ***Windows Server Update Services (WSUS)*** or System Center Configuration Manager (SCCM) to keep your systems updated. The advantage of using one of these two systems is that it can be used to test the patch, schedule the updates, and prioritize client updates. After determining that the patch is safe to deploy, the patch can be enabled for deployment.

Understanding User Account Control (UAC)

User Account Control (UAC) is a feature that was introduced in Windows Vista and is included with Windows 10. UAC helps prevent unauthorized changes to your computer, thereby helping to protect your system from malware.

If logged on as an administrator, UAC prompts you for permission; and if logged on as a standard user, UAC will prompt for an administrator password before performing actions that could potentially affect your computer's operation or other users' computers. UAC is designed to make sure that unauthorized changes are not made by potentially malicious software that you may not know is running. Be sure to read the warnings carefully, and then ensure that the name of the action or program that's about to start is the one you intended to start.

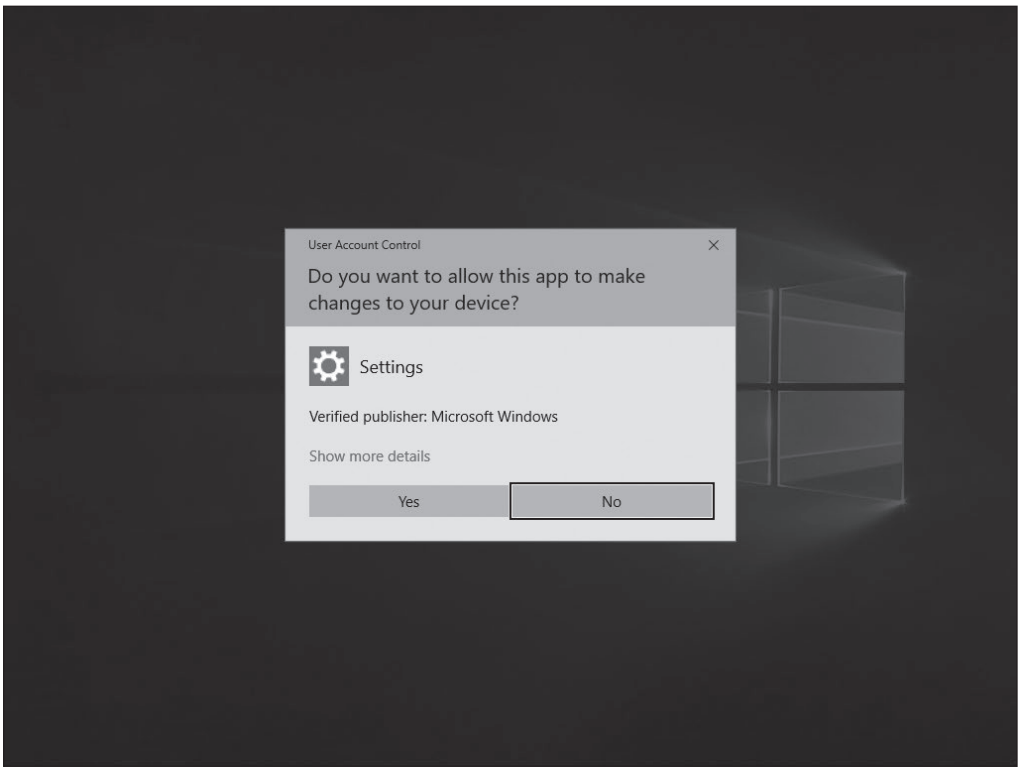
As a standard user in Windows 10, the following actions can be performed without requiring administrative permissions or rights:

- Install updates from Windows Update
- Install drivers from Windows Update or those that are included with the operating system
- View Windows settings
- Pair Bluetooth devices with the computer
- Reset the network adapter and perform other network diagnostic and repair tasks

When an application requests elevation or is run as an administrator, UAC will prompt for confirmation and, if consent is given, allow access as an administrator. See Figure 5-4.

Figure 5-4

UAC confirmation with secure desktop



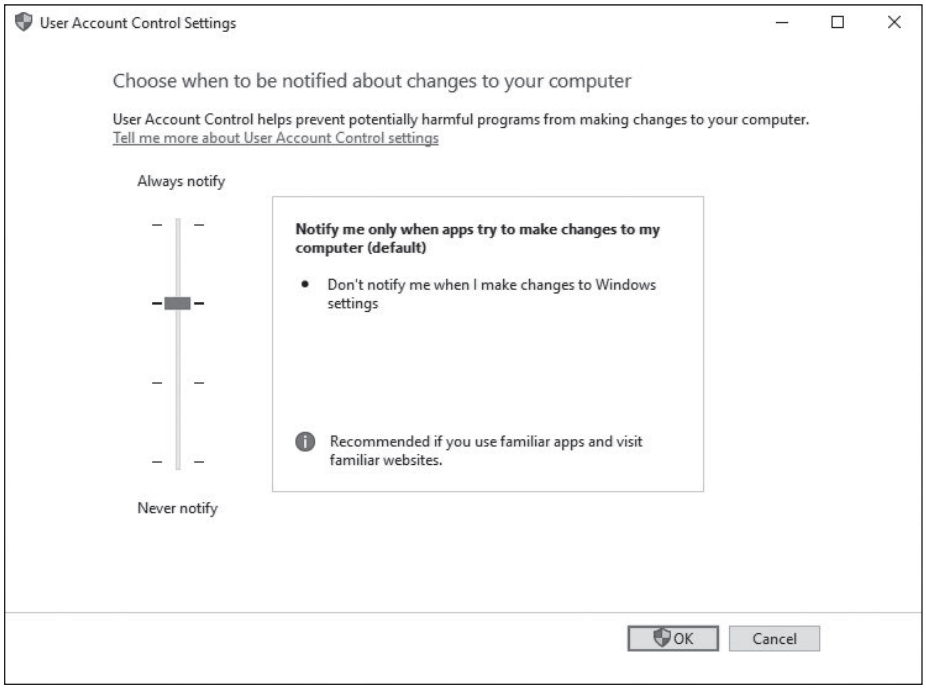
UAC can be enabled or disabled for any individual user account. Of course, if UAC is disabled for a user account, the computer will be at higher risk. However, if you perform a lot of administrative tasks on a computer, the UAC prompts can be annoying and can stop you from doing certain activities, including saving to the root directory of a drive, or using an application that is not compatible with UAC.

ENABLE OR DISABLE UAC

GET READY. To enable or disable UAC, perform the following steps.

1. Open **Control Panel** and click **User Accounts**.
2. On the User Accounts page, click **User Accounts**.
3. Click **Change User Account Control settings**.
4. Drag the slider to the appropriate option, as shown in Table 5-1. See Figure 5-5. Click **OK**.

Figure 5-5
UAC Settings



5. When prompted to restart the computer, click **Restart Now** or **Restart Later** as appropriate for the changes to take effect.

Table 5-1
UAC Settings

Setting	Description	Security Impact
Always notify	You will be notified before apps make changes to your computer or to Windows settings that require the permissions of an administrator. When you're notified, your desktop will be dimmed, and you must either approve or deny the request in the UAC dialog box before you can do anything else on your computer. The dimming of your desktop is referred to as the secure desktop because other apps can't run while it's dimmed.	This is the most secure setting. When notified, carefully read the contents of each dialog box before allowing changes to be made to your computer.

Setting	Description	Security Impact
Notify me only when apps try to make changes to my computer	You will be notified before apps make changes to your computer that require the permissions of an administrator. You will not be notified if you try to make changes to Windows settings that require the permissions of an administrator. You will be notified if an app outside of Windows tries to make changes to a Windows setting.	It's usually safe to allow changes to be made to Windows settings without you being notified. However, certain apps that come with Windows can have commands or data passed to them, and malicious software can take advantage of this by using these apps to install files or change settings on your computer. You should always be careful about which apps you allow to run on your computer.
Notify me only when apps try to make changes to my computer (do not dim my desktop)	You will be notified before apps make changes to your computer that require the permissions of an administrator. You will not be notified if you try to make changes to Windows settings that require the permissions of an administrator. You will be notified if an app outside of Windows tries to make changes to a Windows setting.	This setting is the same as "Notify me only when apps try to make changes to my computer," but you are not notified on the secure desktop. Because the UAC dialog box isn't on the secure desktop with this setting, other apps might be able to interfere with the visual appearance of the dialog box. This is a small security risk if you already have a malicious app running on your computer.
Never notify	You will not be notified before any changes are made to your computer. If you are logged on as an administrator, apps can make changes to your computer without you knowing about it. If you are logged on as a standard user, any changes that require the permissions of an administrator will automatically be denied. If you select this setting, you will need to restart the computer to complete the process of turning off UAC. Once UAC is off, people that log on as administrator will always have the permissions of an administrator.	This is the least secure setting. When you set UAC to never notify, you open up your computer to potential security risks. If you set UAC to never notify, you should be careful about which apps you run, because they will have the same access to the computer as you do. This includes reading and making changes to protected system areas, your personal data, saved files, and anything else stored on the computer. Apps will also be able to communicate and transfer information to and from anything your computer connects with, including the internet.

Using Windows Firewall

Another important client tool is a firewall. As discussed in Lesson 4, a firewall is software or hardware that checks information coming from the internet or a network, and then either blocks it or allows it to pass through to a computer, depending on the firewall settings. A firewall can help prevent hackers or malicious software (such as worms) from gaining access to a computer through a network or the internet. A firewall can also help prevent a computer from sending malicious software to other computers.

Microsoft recommends always using the ***Windows Firewall***. However, because some security packages and antivirus packages include their own firewall, only one firewall should be in use.

TAKE NOTE*

While your network may have a firewall to help protect you from unwanted network traffic from the internet, it is still recommended to have a host firewall on your computer for an extra level of protection. It is especially recommended when the client computer is a mobile computer that may be moved outside of your organization's network.

In addition to the Windows Firewall found in Control Panel, newer versions of Windows include Windows Firewall with Advanced Security. Windows Firewall with Advanced Security combines a host firewall and Internet Protocol security (IPsec). Windows Firewall and Windows Firewall with Advanced Security are tightly coupled together, allowing better control of a firewall. In addition, Windows Firewall with Advanced Security provides computer-to-computer connection security, because it can be used to require authentication and data protection for communications via IPsec.

ENABLE OR DISABLE WINDOWS FIREWALL

GET READY. To enable or disable Windows Firewall, perform the following steps.

1. Open **Control Panel**.
2. If you are in **Category** view, click **System and Security > Windows Firewall**. If you are in icons view, double-click **Windows Firewall**.
3. In the left pane, click **Turn Windows Firewall on or off**. If prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click **Turn on Windows Firewall** under the appropriate network location to enable Windows Firewall or click **Turn off Windows Firewall (not recommended)** under the appropriate network location to disable Windows Firewall. See Figure 5-6. Typically, users should want to block all incoming traffic when connecting to a public network in a hotel or airport, or when a computer worm is spreading over the internet. When blocking all incoming connections, you can still view most web pages, send and receive email, and send and receive instant messages.

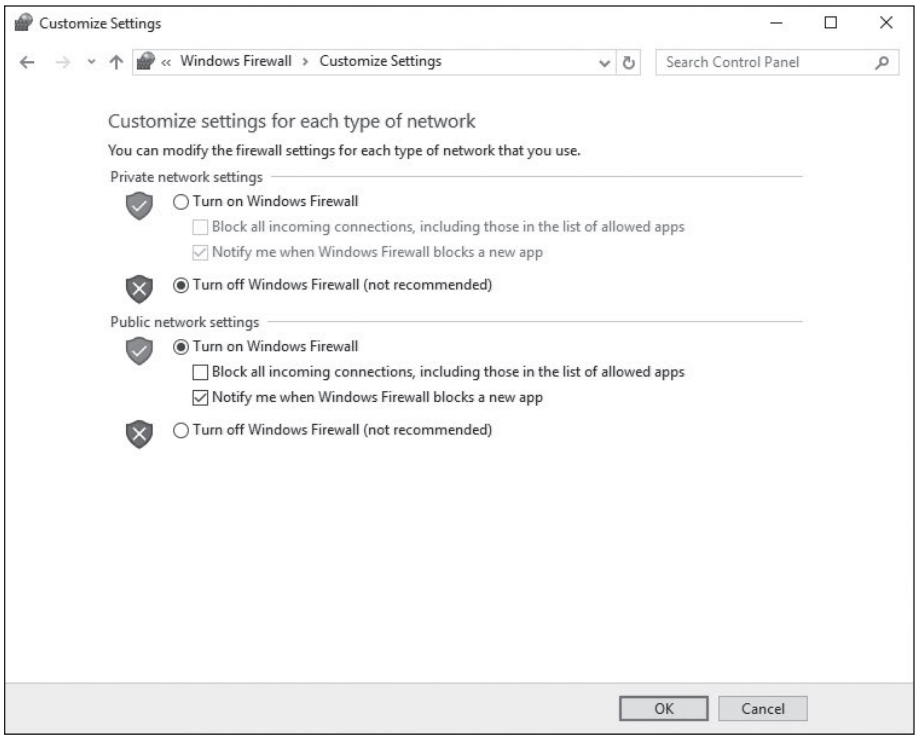


Figure 5-6
Customizing settings for Windows Firewall

5. If desired, select the **Block all incoming connections, including those in the list of allowed apps** check box and the **Notify me when Windows Firewall blocks a new app** check box.
6. Click **OK**.

By default, most programs are blocked by Windows Firewall to help make a computer more secure. To work properly, some programs might require you to allow them to communicate through the firewall.

ALLOW A PROGRAM THROUGH WINDOWS FIREWALL

GET READY. To allow a program to communicate through Windows Firewall, perform the following steps.

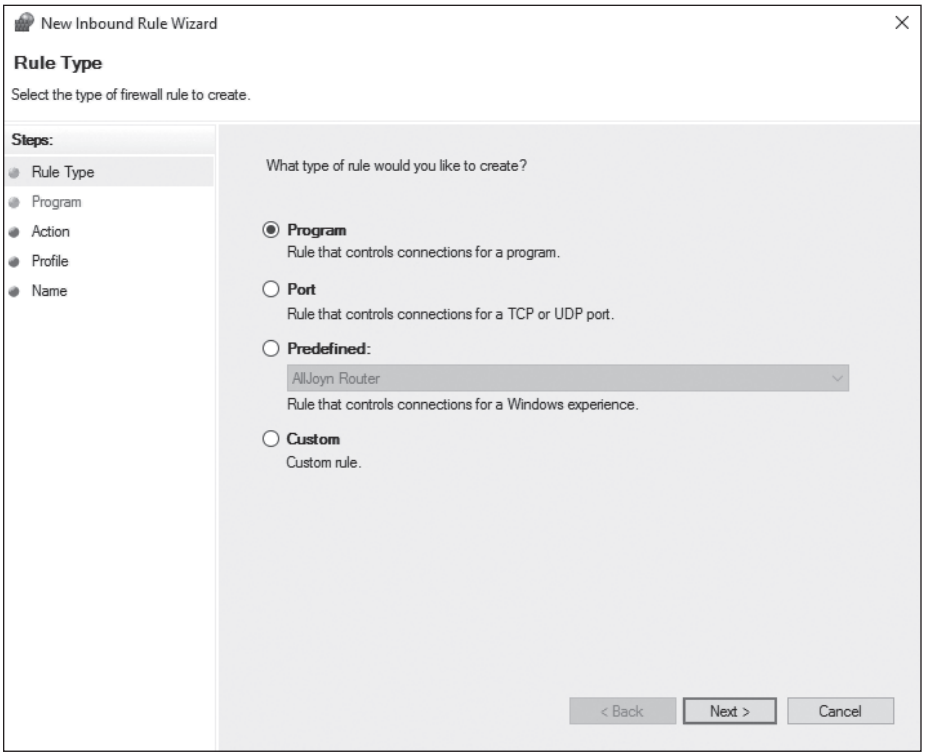
1. Open **Control Panel** and click **Windows Firewall**.
2. In the left pane, click **Allow a program or feature through Windows Firewall**.
3. Click **Change settings**. If prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Select the check box next to the program you want to allow, select the network locations on which you want to allow communication, and then click **OK**.

OPEN A PORT ON WINDOWS FIREWALL

GET READY. If the program isn't listed, you might need to open a port. To open a port on Windows Firewall, perform the following steps.

1. Open **Control Panel** and click **Windows Firewall**.
2. In the left pane, click **Advanced settings**. If prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the Windows Firewall with Advanced Security window, in the left pane, click **Inbound Rules**, and then, in the right pane, click **New Rule**. See Figure 5-7.

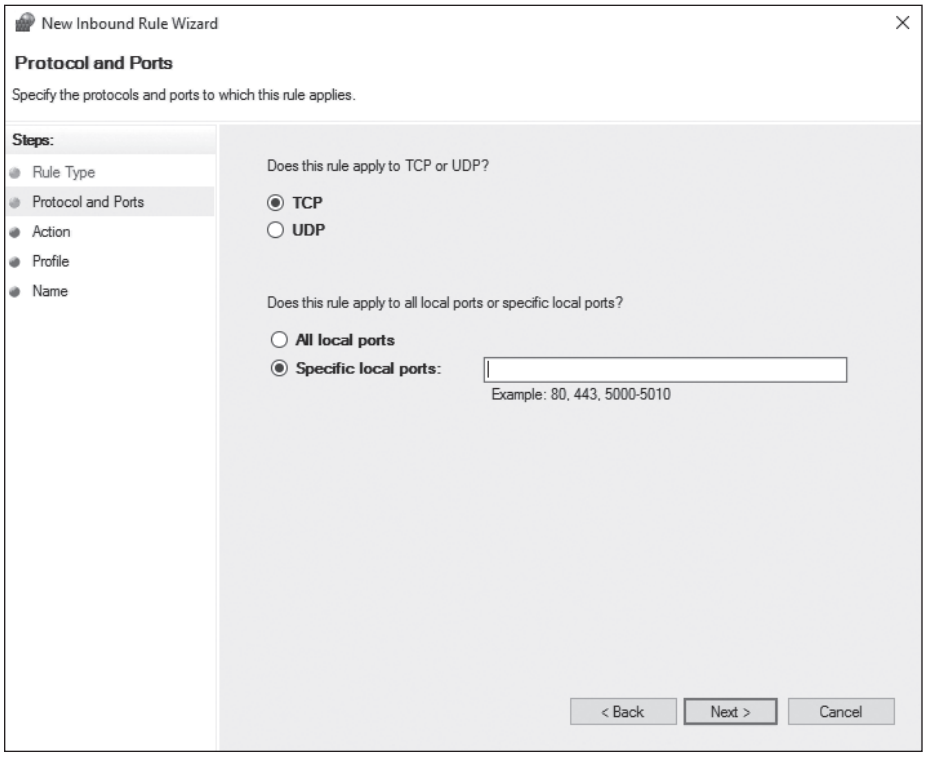
Figure 5-7
Inbound Rules options



4. Click **Port** and click **Next**. See Figure 5-8.

Figure 5-8

Specify a port to open in the firewall



5. Click **TCP** or **UDP** and specify the port numbers. Click **Next**.
6. Click **Allow the connection**, **Allow the connection if it is secure**, or **Block the connection**. Click **Next**.
7. By default, the rule will apply to all domains. If you don't want the rule to apply to a domain, deselect the domain. Click **Next**.
8. Specify a name for the rule and a description, if desired. Click **Finish**.

Using Offline Files

Offline files are copies of network files that are stored on your computer so that they can be accessed when not connected to the network or when the network folder with the files is not connected.

Offline files are not encrypted unless you choose to encrypt them. It might be a good idea to encrypt offline files if they contain sensitive or confidential information and you want to make them more secure by restricting access to them. Encrypting your offline files provides an additional level of access protection that works independently of NTFS file system permissions. This can help safeguard your files in case your computer is ever lost or stolen.

ENABLE OFFLINE FILES

GET READY. To enable offline files, perform the following steps.

1. Right-click the **Start** button and choose **Control Panel**.
2. In the Search Control Panel text box, type **offline**, and click **Manage offline files** in the search results.

3. Click **Enable offline files** and click **OK**.
4. If prompted, reboot the computer.

ENCRYPT OFFLINE FILES

GET READY. To encrypt offline files, perform the following steps.

1. Right-click the **Start** button and choose **Control Panel**.
2. In the Search Control Panel text box, type **offline**, and click **Manage offline files** in the search results.
3. Click the **Encryption** tab.
4. Click **Encrypt** to encrypt your offline files and click **OK**.

When encrypting your offline files, you encrypt only the offline files stored on your computer, and not the network versions of the files. An encrypted file or folder stored on your computer does not need to be decrypted before using it. This is done for you automatically.

Locking Down a Client Computer

When working with end users for an extended period of time, you will soon learn that some users can be their own worst enemy. Therefore, you should consider locking down a computer when necessary, so that users cannot do harm to the computer.

For example, unless a user has a need to be an administrator on their own computer, they should just be a standard user. Therefore, if they are affected by malware, malware will have minimum access to the system. When needed, they could use the runas command options as discussed in Lesson 2.

When working within an organization, it is often advantageous to standardize each company computer. Therefore, when moving from one computer to another, they will be similar. To keep computers standardized, an organization may choose to use group policies so that users cannot access certain features, such as Control Panel, to make changes to the system that may be detrimental.

Allowing users to install software may:

- Introduce malware to a system.
- Bypass safeguards already put in place to protect against malicious viruses and Trojan horse programs.
- Cause conflicts with software already on a baseline computer within an organization.

Limiting your users to standard accounts can limit what software users can install. Group policies can also be used to restrict what software can be executed on a client computer.

Windows 10 supports two mechanisms for restricting applications, both of which are based on group policies:

- Software restriction policies
- AppLocker

■ Managing Client Security Using Windows Defender

THE BOTTOM LINE

Windows Defender is designed to protect a computer against viruses, spyware, and other types of malware. It protects against these threats by providing real-time protection and notifying you of malware attempts or when an application tries to change critical settings.

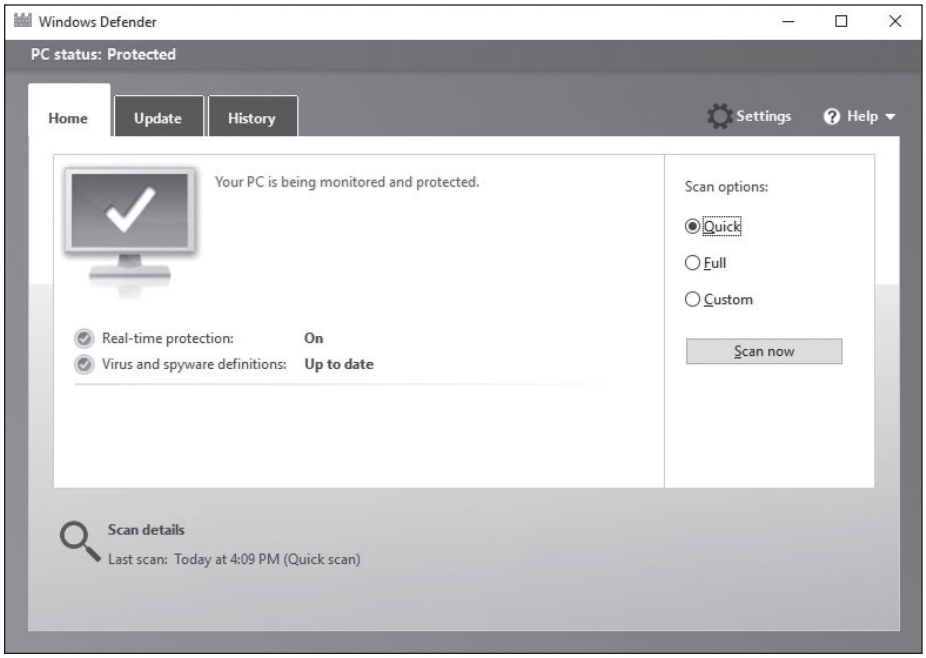
CERTIFICATION READY
Which software is intended to damage, disable, or degrade a computer or computer systems?
Objective 4.1

Windows Defender can also be configured to scan a computer on a regular basis and remove or quarantine any malware it finds.

At the heart of Windows Defender are its definition files, which are downloaded from Windows Update. The definition files, which contain information about potential threats, are used by Windows Defender to notify you of potential threats to your system.

To access Windows Defender from the Windows 10 menu, click Start, type Windows Defender, and click it in the results. Figure 5-9 shows the Windows Defender Home tab.

Figure 5-9
Viewing the Windows Defender Home tab



TAKE NOTE*

Windows Defender automatically disables itself when installing another antivirus product.

The Home tab can be used to check the status of Windows Defender, including whether Windows Defender is up-to-date and whether Windows Defender is protecting your system. It also provides the option to initiate a scan.

When looking at the Home tab, always look for a green message indicating *Your PC is being monitored and protected* and also make sure your system is up-to-date. Other components include:

- **Real-time protection:** Real-time protection uses signature detection methodology and heuristics to monitor and catch malware behavior. Signature detection uses a vendor's definition files to detect malicious programs. If the program contains code that matches the signature, the program most likely contains the virus. This works well when the

threat has already been identified, but what happens between the time the virus is released and the time the definition file is made available? That's where heuristics can help. It is used to monitor for suspicious activity by a program. Suspicious activity includes a program trying to copy itself into another program, a program trying to write to the disk directly, or a program trying to manipulate critical system files required by the operating system. These are indicators of possible malware activity that heuristics can detect.

- **Virus and spyware definitions:** When a new virus is discovered, Microsoft creates a new virus signature/definition update. Each definition file contains a piece of the actual virus code that is used to detect a specific virus or malware. During scans, the content on the computer is compared with information in the definition files. Because new viruses are created every day and existing viruses are modified regularly, it's important to keep your definitions updated.
- **Scan options (Quick, Full, and Custom):** A Quick scan checks the areas that malicious software (including viruses, spyware, and unwanted software) are most likely to infect. A Full scan checks all the files on your disk, including running programs. A Custom scan is designed to check only specified locations and files.
- **Scan details:** This area of the Home tab provides information on when the last scan was performed on the computer.

The Update tab provides information about your virus and spyware definitions. It is important to keep these current to ensure your computer is protected at all times. Windows Defender updates the definition files automatically. Click Update definitions on this tab to manually check for updates.

The History tab provides information about items that have been detected in the past and the actions that were taken with them.

The categories of items are as follows:

- **Quarantined Items:** These items were not allowed to run, and were not removed from your computer.
- **Allowed Items:** These items were allowed to run on your computer.
- **All Detected Items:** These items provide a list of all items detected on your computer.

REMOVE A QUARANTINED ITEM

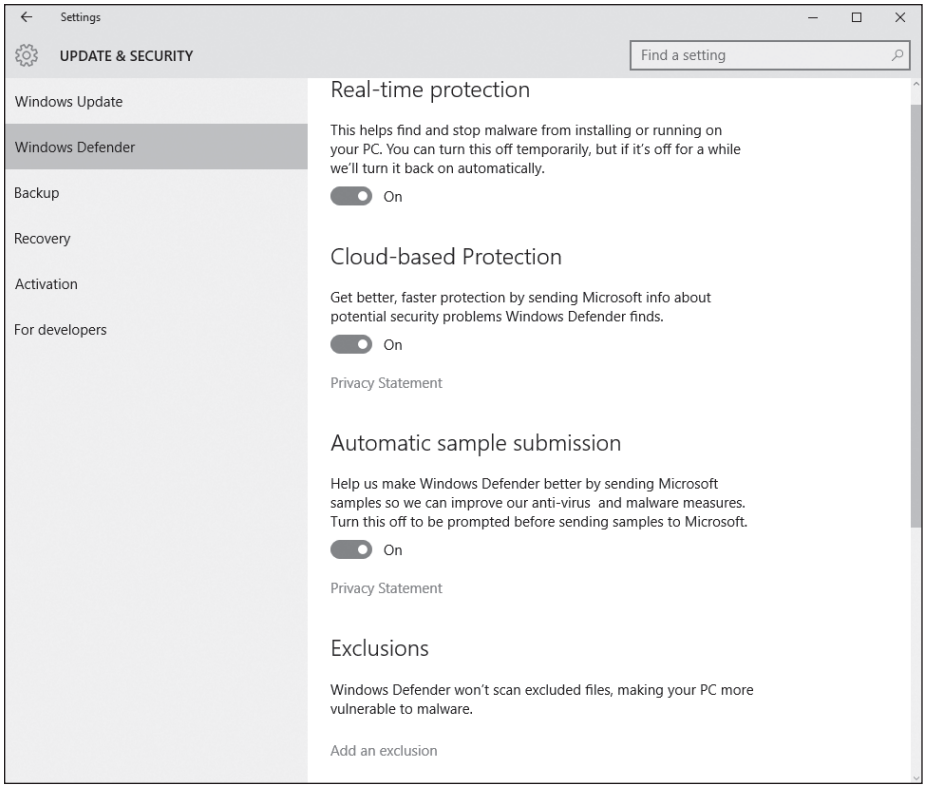
GET READY. To remove a quarantined item, perform the following steps.

1. Open **Windows Defender**.
2. Click the **History** tab.
3. Click **Quarantined Items**.
4. Click **View Details**.
5. Select the detected item and then read the description.
6. Click **Remove**.

Click Windows Defender Settings to open the Windows 10 Settings > Update & security > Windows Defender page, as shown in Figure 5-10. Use the Settings page to fine-tune how Windows Defender works.

Figure 5-10

The Windows Defender Settings page



On the Settings page, the following options are available:

- Enable or disable real-time protection
- Select whether you want to use cloud-based protection
- Select the files and locations to be excluded from the scanning process
- Select the file types to exclude from the scan
- Select the processes to exclude
- Display the Windows 10 version information
- Open Windows Defender

Microsoft Active Protection Service (MAPS) is an online community that can help you decide how to respond to certain threat types and it serves as a resource to help stop the spread of new viruses and malware. The information sent helps Microsoft create new definition files. It can be enabled or disabled via the Windows Defender settings. When enabled, information is sent to Microsoft regarding where the software came from, the actions taken, and whether the actions taken were successful.

Windows Defender can also be configured via the Local Group Policy Editor or Group Policy Management Editor (AD domains). The following policies are located in the Computer Configuration\Administrative Templates\Windows Components\Windows Defender node:

- **Scan/Check for the latest virus and spyware definitions before a scheduled scan:** When enabled, Windows Defender checks for new signatures before running the scan.
- **Turn off Windows Defender:** This setting turns Windows Defender on or off.
- **Real-time Protection/Turn off Real-Time Monitoring:** This setting controls whether Windows Defender monitors your system in real time and displays an alert

when malware or potentially unwanted software attempts to install or run on the computer.

- **Threats/Specify threats upon which default action should not be taken when detected:** This setting determines whether Windows Defender automatically takes action on malware that it identifies.
- **MAPS/Join Microsoft MAPS:** This setting determines the type of membership used with MAPS. Options include No Membership, Basic Membership, or Advanced Membership.

To keep your system more secure, schedule a Windows Defender scan.

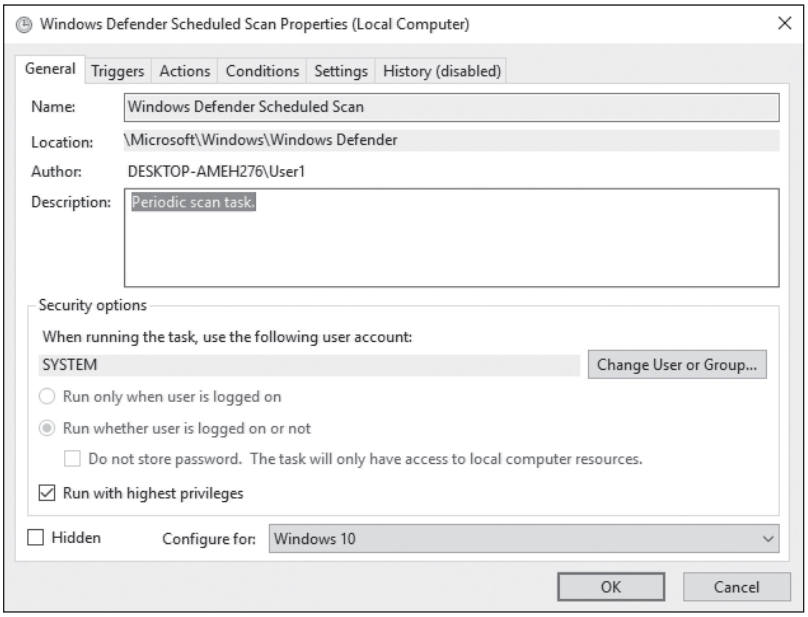
SCHEDULE A WINDOWS DEFENDER SCAN

GET READY. To schedule a Windows Defender scan, log on with administrative privileges and perform the following steps.

1. Click **Start** and type **taskschd.msc**. From the results, click **Task Scheduler**.
2. In the left pane, expand **Task Scheduler Library > Microsoft > Windows > Windows Defender**.
3. Double-click **Windows Defender Scheduled Scan**.
4. In the Windows Defender Scheduled Scan Properties (Local Computer) dialog box (see Figure 5-11), click the **Triggers** tab and click **New**.

Figure 5-11

Scheduling a Windows Defender scan



5. In the Begin the task field, click **On a schedule**.
6. Under Settings, select **One time**. In the Start field, change the time to 5 minutes from your current time.
7. Make sure the **Enabled** check box is selected and click **OK**.
8. To close the Windows Defender Scheduled Scan Properties (Local Computer) dialog box, click **OK**.
9. Open **Windows Defender** to see the status of the scan on the Home tab.

■ Protecting Your Email

THE BOTTOM LINE

Email has become an essential service for virtually every corporation. Unfortunately, most email received will be unsolicited emails called ***spam*** or junk email, some of which can carry malware and may lead to fraud or scams.

CERTIFICATION READY
How can users protect their system from viruses sent through email?
Objective 4.2

The idea behind spam is that it sends lots of unsolicited bulk messages indiscriminately, hoping that a few people will open the email and open a website, purchase a product, or fall for a scam. For spammers, spam has minimal operating costs. Over the last few years, spam grew exponentially, and today composes at least 90% of all the email in the world.

For email recipients, besides the risk of malware and fraud, there is also a loss of productivity as users sort through unsolicited emails. In addition, the IT department will need to install additional storage and provide sufficient bandwidth to accommodate the extra email. Therefore, install a spam blocking device or software that includes antivirus protection. The antivirus will provide another layer to protect your network from viruses.

Managing Spam

To keep your systems running smoothly, it is important for a network administrator put some effort into blocking spam.

The best place to establish an anti-spam filtering system is on a dedicated server or appliance or as part of a firewall device or service. All email will be directed to the anti-spam filter by changing your DNS Mail Exchanger (MX) record to point to the anti-spam server or device. Any email that is not considered to be spam will be forwarded to your internal email servers.

Spam filtering systems will not catch every single spam message. Like an antivirus package, the spam filtering solution needs to be kept up-to-date and needs to be constantly tweaked. Also, consider adding a threatening email address, email domain, IP address range, or keywords into a block list. Any email that is listed in the block list will automatically be blocked. Be sure to take care when using a block list, so the criteria for blocking email isn't so broad that it starts blocking legitimate email.

Many anti-spam solutions will also use Real-time Blackhole Lists (RBLs) or a DNS-based Blackhole List (DNSBL) which can be accessed freely. RBLs and DNSBL are lists of known spammers that are updated frequently. Most mail server software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists. Of course, as spammers look for ways to get around this, it is just one tool that can help reduce the amount of spam that gets through.

Any email identified as spam is usually quarantined or stored temporarily, in case a legitimate email is identified as spam. While this number should be relatively low, train your help desk personnel and possibly your users to access the quarantined email to release legitimate email to its destination. In addition, add the sender's email address or domain to an allow list so that it will not be identified as spam in the future.

Detecting spam can be a daunting task when it must be done manually. Besides the obvious advertisement and keywords, anti-spam systems will also look at the email header to analyze information about the email and its origin. For example, in Outlook 2003, open the email and choose View > Options. Under Internet Headers, the history for an email delivery path is shown. In Outlook 2010, select the message, click the File menu, and then under Info, click Properties.

Sometimes, spammers will try to spoof a legitimate email address or IP address when the message actually comes from one with an email address or IP address that would likely be identified as spam. One way to detect this is via a reverse lookup. For example, if email claims to be sent from a yahoo.com domain, an anti-spam system could do a reverse lookup using the DNS PTR record to find the actual IP address of the yahoo.com domain. If it does not match where the email said it came from, it is considered spam and will be blocked.

Sender Policy Framework (SPF) is an email validation system designed to prevent email spam that uses source address spoofing. SPF allows administrators to specify only those hosts which are allowed to send email from a given domain, as specified in a specific DNS SPF record in the public DNS. If email for a domain is sent from a host not listed in the DNS SPF, it will be considered spam and blocked.

Today, anti-spam packages use special algorithms, such as ***Bayesian filters***, to determine if email is considered spam. These algorithms usually analyze previously received emails and create a database on several attributes based on those previously analyzed emails. When it receives an email, it will compare that email with the attributes it has collected to determine whether it is spam.

Relaying Email

One of the primary email protocols is SMTP. Simple Mail Transfer Protocol (SMTP) is used to transfer email from one server to another and it is responsible for outgoing mail transport. SMTP uses TCP port 25.

Email servers are not only used for your users to send and retrieve email, they are also used to relay email. For example, web and application servers may relay email through their email servers when you order something over the internet and a confirmation email is sent to you.

Usually, only your internal servers should relay email through your mail servers. Unfortunately, spammers look for unprotected SMTP servers to relay their email. As a result, other organizations may flag your server or domain as a spammer and you may be placed on one of the RBLs or DNSBLs. To get off this list, close up your security hole so that other people cannot relay emails through your server, and then contact the organizations that host the RBLs or DNSBLs to remove your server or domain from their list.

■ Securing Internet Explorer

THE BOTTOM LINE

Because browsing a website can expose users to a wide range of hazards, it is important to rely on the browser to help protect systems. Today's browsers include pop-up blockers, security zones, and other built-in security features.

CERTIFICATION READY
What is the source of most malware?
Objective 2.6

Understanding Cookies and Privacy Settings

When using a browser to access the internet, much can be revealed about a user's personality and personal information. Therefore, it is important to take steps to ensure that this information cannot be read or used without your knowledge.

A ***cookie*** is a piece of text stored by a user's web browser. It can be used for a wide range of items including user identification, authentication, storing site preferences, and shopping cart contents. While cookies can give a website a lot of capabilities, they can also be used by

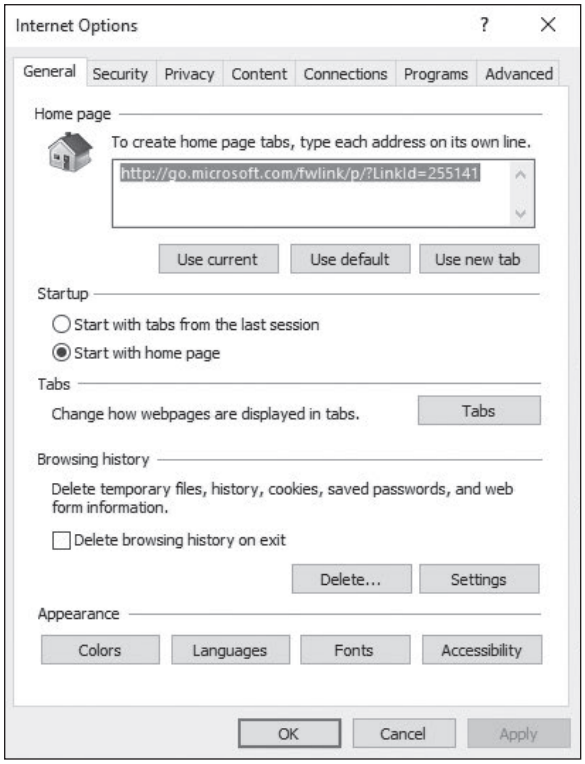
spyware programs and websites to track people. Unfortunately, some websites will not operate without cookies.

DELETE COOKIES IN INTERNET EXPLORER 11

GET READY. To delete cookies in Internet Explorer 11, perform the following steps.

1. Open **Internet Explorer**.
2. Click the **Tools** button and click **Internet options**. See Figure 5-12.

Figure 5-12
Deleting cookies and temporary files



3. On the **General** tab, under Browsing history, click **Delete**.
4. Select the **Cookies and website data** check box if it isn't already selected. Clear or select check boxes for any other options you also want to delete. If you want to keep cookies for your saved favorites, select the **Preserve Favorites website data** check box. Click **Delete**.

Being aware of how your private information is used when browsing the web is important to help prevent targeted advertising, fraud, and identity theft.

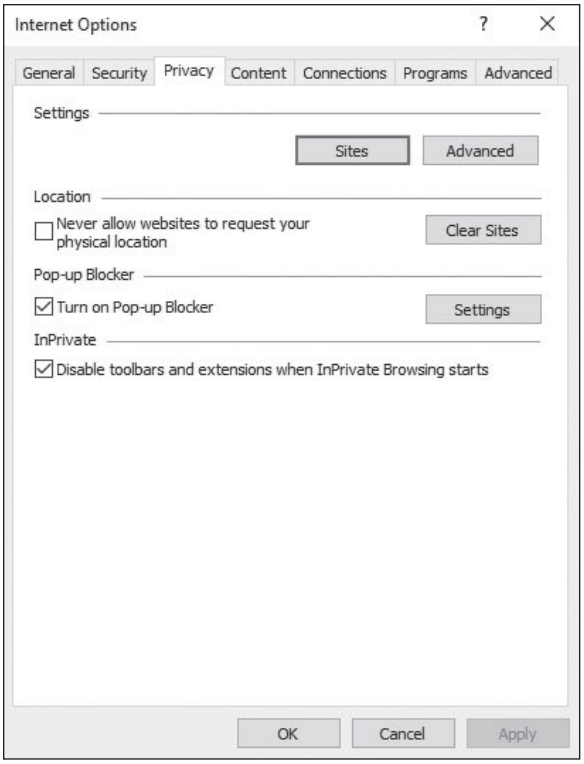
CHANGE PRIVACY SETTINGS

GET READY. To access Internet Explorer privacy settings, perform the following steps.

1. Open **Internet Explorer**.
2. Click the **Tools** button and click **Internet options**.
3. In the Internet Options dialog box, click the **Privacy** tab. See Figure 5-13.

Figure 5-13

The Internet Options Privacy tab



4. To block websites from requesting your physical location, select **Never allow websites to request your physical location**.
5. To choose how cookies are handled, click the **Advanced** button. In the Advanced Privacy Settings dialog box, select **Accept**, **Block**, or **Prompt for first-party and third-party cookies**. Click **OK**.
6. Close the Internet Options dialog box by clicking **OK**.

The rest of this section will discuss the various options available on the Privacy tab.

Use the Advanced button to access and override certain settings.

Pop-up windows are very common. While some pop-up windows are useful website controls, most are simply annoying advertisements, with a few attempting to load spyware or other malicious programs. To help protect your computer, Internet Explorer has the capability to suppress some or all pop-ups. To configure the pop-up blocker, use the following procedure.

CONFIGURE THE POP-UP BLOCKER

GET READY. To configure the Pop-up Blocker settings, perform the following steps.

1. After logging on to a computer running Windows 10, right-click the **Start** button and choose **Control Panel**. The Control Panel window opens.
2. Click **Network and Internet** > **Internet Options**. The Internet Properties dialog box opens.
3. Click the **Privacy** tab. Make sure the **Turn on Pop-up Blocker** check box is selected.
4. Click **Settings**. The Pop-up Blocker Settings dialog box opens.

5. To allow pop-ups from a specific website, type the URL of the site in the Address of website to allow text box and click **Add**. Repeat the process to add additional sites to the Allowed sites list.
6. In the Blocking level drop-down list, select one of the following settings:
   - **High: Block all pop-ups**
   - **Medium: Block most automatic pop-ups**
   - **Low: Allow pop-ups from secure sites**
7. Click **Close** to close the Pop-up Blocker Settings dialog box.
8. Click **OK** to close the Internet Properties dialog box.

Using Content Zones

To help manage Internet Explorer security when visiting websites, Internet Explorer divides your network connection into four ***content zones*** or types. These content zones can be viewed on the Security tab of the Internet Options dialog box. For each of these zones, a security level is assigned.

The security for each content zone is assigned based on dangers associated with the zone. For example, it is assumed that connecting to a server within your own corporation would be safer than connecting to a server on the internet.

The four default content types are:

- **Internet zone:** This zone includes anything that is not assigned to any other zone and anything that is not on your computer, or your organization's network (intranet). The default security level of the Internet zone is Medium.
- **Local intranet zone:** This zone includes computers that are part of the organization's network (intranet) that do not require a proxy server, as defined by the system administrator. These include sites specified on the Connections tab as network paths, such as \\computername\foldername, and local intranet sites, such as http://internal. Sites can be added to this zone. The default security level for the Local intranet zone is Medium-Low, which means Internet Explorer will allow all cookies from websites in this zone to be saved on your computer and read by the website that created them. Lastly, if the website requires NTLM or integrated authentication, it will automatically use your user name and password.
- **Trusted sites zone:** This zone contains sites from which you believe you can download or run files without damaging your system. Sites can be assigned to this zone. The default security level for the Trusted sites zone is Low, which means Internet Explorer will allow all cookies from websites in this zone to be saved on your computer and read by the website that created them.
- **Restricted sites zone:** This zone contains sites that are not trusted and from which downloading or running files may damage your computer or data, or sites that are considered a security risk. Sites can be assigned to this zone. The default security level for the Restricted sites zone is High, which means Internet Explorer will block all cookies from websites in this zone.

To tell which zones the current web page falls into, open the File menu and click Properties. The Properties dialog box also displays the connection, such as DLS 1.2, AES with 128 bit encryption, and the status of Protected Mode. Click the Certificates button to see the SSL digital certificate.

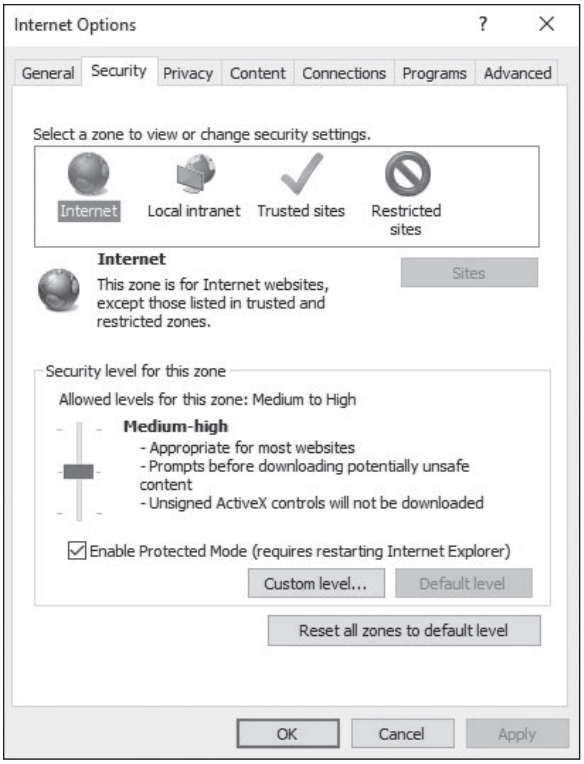
MODIFY THE SECURITY LEVEL FOR A WEB CONTENT ZONE

GET READY. To modify the security level for a web content zone, perform the following steps.

1. Open **Internet Explorer**.
2. Click the **Tools** button and click **Internet options**.
3. In the Internet Options dialog box, click the **Security** tab and click the zone on which you want to set the security level. See Figure 5-14.

Figure 5-14

Configuring the security content zones



4. Drag the slider to set the security level to **High**, **Medium**, or **Low**. Internet Explorer describes each option to help you decide which level to choose. You are prompted to confirm any reduction in security level. Click the **Custom level** button for more detailed control.
5. Click **OK** to close the Internet Options dialog box.

For each of the web content zones, there is a default security level. The security levels available in Internet Explorer are:

- **High:** Excludes any content that can damage your computer by maximizing safeguards and disabling less secure features.
- **Medium-high:** Appropriate for most websites; prompts before downloading potential unsafe content.
- **Medium:** Warns you before running potentially damaging content.
- **Medium-low:** Appropriate for local network\intranet websites; allows most content to be run without prompting.
- **Low:** Does not warn you before running potentially damaging content.
- **Custom:** Creates a security setting of your own design.

The easiest way to modify the security settings that Internet Explorer imposes on a specific website is to manually add the site to a security zone. The typical procedure is to add a site to the Trusted sites zone, to increase its privileges, or add it to the Restricted sites zone, to reduce its privileges. To do this, use the following procedure.

ADD A SITE TO A SECURITY ZONE

GET READY. Log on to Windows 10. To add a site to a security zone, perform the following steps.

1. Right-click **Start** and choose **Control Panel**.
2. Click **Network and Internet** > **Internet Options**. The Internet Properties dialog box opens.
3. Click the **Security** tab.
4. Click either the **Trusted sites** or **Restricted sites** zone to which you want to add a site.
5. Click **Sites**. The Trusted sites dialog box or Restricted sites dialog box opens.
6. Type the URL of the website you want to add to the zone into the **Add this website to the zone** text box and click **Add**. The URL appears in the Websites list.
7. Click **Close** to close the Trusted sites or Restricted sites dialog box.
8. Click **OK** to close the Internet Properties dialog box.

To modify the security properties of a zone, use the following procedure.

MODIFY SECURITY ZONE SETTINGS

GET READY. Log on to Windows 10. To modify security zone settings, perform the following steps.

1. Right-click **Start** and choose **Control Panel**.
2. Click **Network and Internet** > **Internet Options**. The Internet Properties dialog box opens.
3. Click the **Security** tab.
4. Select the zone for which you want to modify the security settings.
5. In the **Security level for this zone** box, drag the slider to increase or decrease the security level for the zone. Moving the slider up increases the protection for the zone and moving the slider down decreases the protection.
6. Select or clear the **Enable Protected Mode** check box, if desired.
7. To exercise more precise control over the zone's security settings, click **Custom level**. The Security Settings dialog box for the zone opens.
8. Select radio buttons for the individual settings in each of the security categories. The radio buttons typically make it possible to enable a setting, disable it, or prompt the user before enabling it.
9. Click **OK** to close the Security Settings dialog box.
10. Click **OK** to close the Internet Properties dialog box.

Understanding Phishing and Pharming

Phishing and pharming are forms of attacks to get users to access a bogus website so the phisher or pharmer can spread malware and/or collect personal information.

Phishing is a technique based on social engineering. With phishing, users are requested (usually through email or other websites) to supply personal information by:

- Receiving an email that requests your user name, password, and other personal information such as account numbers, PINs, and Social Security numbers.
- Redirecting a user to a convincing-looking website that requires users to supply personal information, such as passwords and account numbers.

For example, an email states that your account has just expired or that you may need to validate your information. Within the email, there is a link to click. When you click the link, the fake website appears. However, just by logging on, you provide the user name and password to the hacker, which can then be used to access your account.

To help protect against Phishing, Internet Explorer 8 introduced SmartScreen Filter that examines traffic for evidence of phishing activity and displays a warning to the user if it finds any. It also sends the address back to the Microsoft SmartScreen service to be compared against lists of known phishing and malware sites. If SmartScreen Filter discovers that a website you're visiting is on the list of known malware or phishing sites, Internet Explorer will display a blocking webpage and the address bar will appear in red. From the blocking page, choose to bypass the blocked website and go to your home page instead, or continue to the blocked website (this is not recommended). If you decide to continue to the blocked website, the address bar will continue to appear in red.

One of the best ways to avoid such ploys is to know that they exist. When an email requests personal information, look for signs that the email is fake and that the actual links may go to bogus websites (for example, instead of going to ebay.com, it goes to ebay.com.com or ebay_ws.com). Don't trust hyperlinks. Never supply a password or any other confidential information to a website unless you type the URL yourself and are sure that it is correct.

Pharming is an attack aimed at redirecting a website's traffic to a bogus website. This is usually accomplished by changing the hosts file (text that provides name resolution for host or domain names to IP addresses) on a computer or by exploiting a vulnerability on a DNS server.

Understanding Secure Sockets Layer (SSL) and Certificates

When surfing the internet, there are times when it is necessary to transmit private data over the internet such as credit card numbers, Social Security numbers, and so on. During these times, it is important to use http over SSL (https) to encrypt the data sent over the internet. By convention, URLs that require an SSL connection start with https: instead of http:.

SSL is short for Secure Sockets Layer. It's a cryptographic system that uses two keys to encrypt data—a public key known to everyone, and a private or secret key known only to the recipient of the message. The public key is published in a digital certificate, which also confirms the identity of the web server.

When connecting to a site that is secured using SSL, a lock appears in the address bar, along with the name of the organization to which the CA issued the certificate. Clicking the lock icon displays more information about the site, including the identity of the CA that issued the certificate. For even more information, click the View Certificate link to open the Certificate dialog box.

When visiting certain websites, Internet Explorer may find problems with the digital certificate such as that the certificate has expired, it is corrupted, it has been revoked, or it does not match the name of the website. When this happens, IE will block access to the site and display a warning stating that there is a problem with the certificate. At this point, close the

browser window or ignore the warning and continue on to the site. Of course, the warning should be ignored only if you trust the website and believe that you are communicating with the correct server.

■ Configuring Microsoft Edge

THE BOTTOM LINE

Microsoft Edge is the new Microsoft lightweight web browser with a layout engine built around web standards designed to replace Internet Explorer as the default web browser. It integrates with Cortana, annotation tools, Adobe Flash Player, a PDF reader, and a reading mode. Extension support was developed and added to the Windows 10 Anniversary Update in July 2016.

CERTIFICATION READY
Which security settings are available in Microsoft Edge that are also available in Microsoft Explorer?
Objective 1.3

The following buttons display at the top of the Microsoft Edge window:

- Reading view
- Add to Favorites or Reading List
- Hub (Favorites, reading lists, history, and downloads)
- Make a web note
- Feedback
- Settings

To open Microsoft Edge settings (as shown in Figure 5-15), click the Settings (. . .) button and click the Settings option.

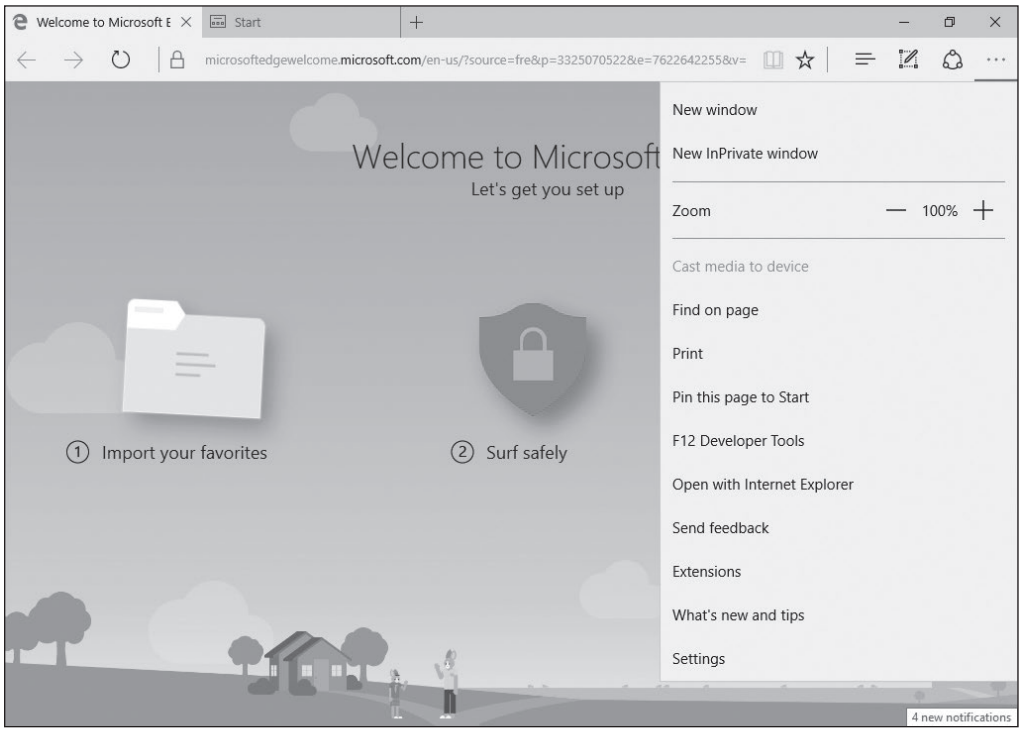


Figure 5-15
Configuring Microsoft Edge

Under Settings, the following tasks can be performed:

- Enable or disable the favorites bar
- Set Microsoft Edge to start with a New tab page, My previous tabs, or a specified web page

- Set whether new tabs will be top sites and suggested content or a blank page
- Set the search engine to Bing, Google, or any search engine of your choice
- Clear browsing history and delete media licenses, pop-up exceptions, and location permissions
- Set the Reading style to Default, Light, Medium, or Dark, and specify the Reading font size

Clicking the Advanced Settings option provides access to these additional tasks:

- Enable or disable Flash Player
- Opt to use caret browsing
- Set privacy options
- Manage saved passwords
- Opt to save form entries
- Choose to block pop-ups and cookies
- Manage protected media licenses
- Send Do Not Track requests
- Enable or disable page prediction
- Enable or disable SmartScreen Filter
- Turn on or off Cortana integration

■ Protecting Your Server

THE BOTTOM LINE

When looking at security, it is important to consider securing everything—the network, the clients, and the servers. Securing all three forms a layered approach that makes it more difficult for hackers and malware to breach your organization. Previous lessons discussed how to keep your network secure, and earlier in this lesson, you learned how to keep your clients secure. This section covers how to secure the server.

CERTIFICATION READY
How can servers be protected so that they are always up and running?
Objective 4.3

Servers are computers that are meant to provide network services and applications for your organization. Different from workstations, if a server fails, it will affect multiple users. Therefore, it is more important to keep a server secure than a workstation.

Separating Services

The first step in securing a server is deciding where to physically place the server. Of course, the server should be kept in a secure location. In addition, the servers should be in their own subnet to reduce the amount of traffic to the servers, especially broadcasts.

To minimize one service or application from interfering with and affecting another service or network application, it is recommended that services or network applications should be run on their own server. This allows you to customize access to the individual service or network application. With today's virtual machine technology, it is easy to allow a separation between services while keeping costs to a minimum.

Using a Read-Only Domain Controller (RODC)

Windows Server 2008 introduced the ***Read-Only Domain Controller (RODC)***, which contains a full replication of the domain database. It was created to be used in places where a domain controller is needed but where the physical security of the domain controller could not be guaranteed. For example, it might be placed in a remote site that is not very secure and which provides a slower WAN link. Also, because a site may have a slow WAN link, a local domain controller would benefit the users at that site.

An RODC does not perform any outbound replication and accepts only inbound replication connections from writable domain controllers. Because the RODC has only a read-only copy of the Active Directory database, the administrator needs to connect to a separate, writable, domain controller to make changes to Active Directory.

To deploy an RODC, do the following:

- Ensure that the forest functional level is Windows Server 2003 or higher.
- Deploy at least one writable domain controller running Windows Server 2008 or higher.

Hardening Servers

The next step in securing a server is to harden the server by reducing its surface of attack and thereby reducing the server's vulnerabilities. To harden a server, look for security guides/guidelines and best practices for Windows servers and for the specific network services that are being installed, such as Microsoft Exchange or Microsoft SQL Server.

One of the most important steps in securing a server is to make sure that Windows, Microsoft applications, and other network applications are kept up-to-date with the newest security patches. As with clients, you use Windows updates, WSUS, and SCCM to provide updates to servers. Of course, before applying patches to a production system, be sure to test the security updates.

To reduce the surface of attack, disable any service that is not necessary so that those services cannot be exploited in the future. In addition, consider using the host firewalls (such as Windows firewalls) that will block all ports that are not being used.

To reduce the effect of losing a server, it's a good idea to separate the services—do not install all your services on one server. Also, plan for the rest and hope for the best. In other words, anticipate that a server will eventually fail. Therefore, consider using redundant power supplies, RAID disks, redundant network cards, and clusters.

Also, disable or delete any unnecessary accounts. For example, although the administrator account cannot be deleted, it can be renamed to something else so that it would be more difficult for a hacker to guess what it is. And, of course, the guest account should be disabled. In addition, you should not use the administrator account for everything. For example, if a service is required, create a service account for that service and give the account the minimum rights and permissions needed to run the service.

Besides disabling or deleting any unnecessary accounts and assigning only the minimum rights and permissions for users to do their jobs, you should also restrict who can log on locally to the server.

In addition, disable any unsecure authentication protocols. For example, you should not use Password Authentication Protocol (PAP) when using remote access protocols. You should not use FTP with passwords. Instead, use anonymous, which does not require passwords (assuming it uses only content that does not need to be secure), or use secure FTP, which

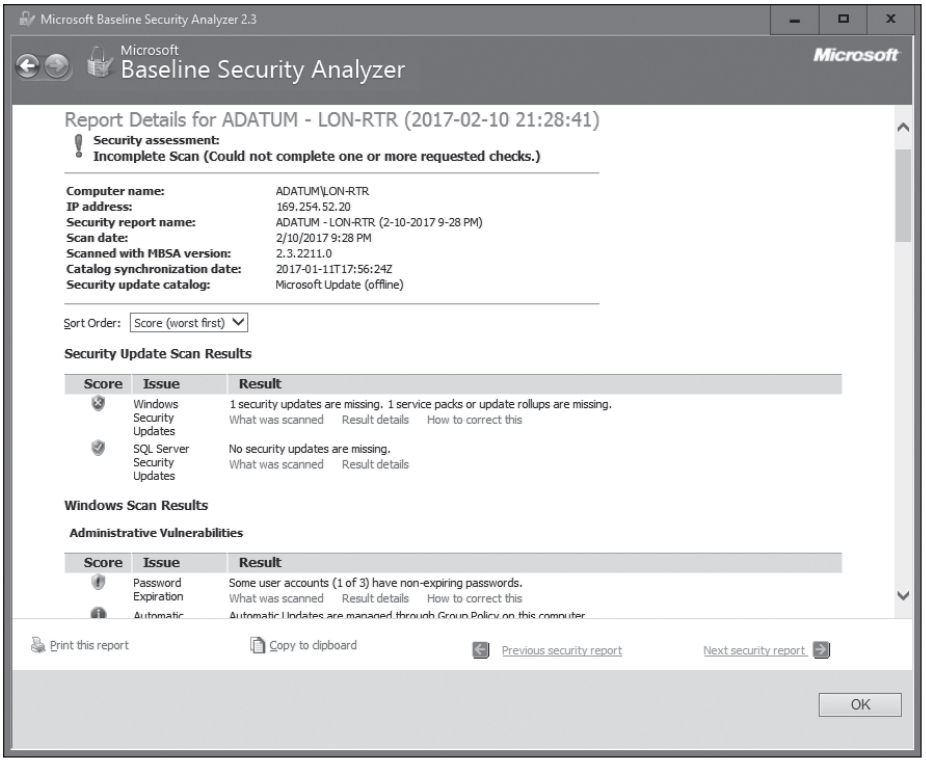
will encrypt the password and content when being transmitted over the network. For similar reasons, use SSH instead of telnet.

Lastly, enable a strong audit and logging policy and review these logs on a regular basis. Then, if someone tries to hack a server or do something they should not be doing, there will be a record of his or her activities. This should include being alerted to both successful and failed account logons.

Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to determine the security state of a system by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products such as Microsoft SQL Server and Microsoft Office macro settings. See Figure 5-16.

Figure 5-16

Using Microsoft Baseline Security Analyzer (MBSA)



Microsoft often publishes security guides and best practices guides for their various products. Go to the http://technet.microsoft.com website and search for security guides or security guidance.

Understanding Secure Dynamic DNS

Since Windows Server 2003, Windows servers have provided support for the dynamic DNS update functionality. Dynamic DNS lets client computers dynamically update their resource records in DNS. When using this functionality, DNS administration is improved by reducing the time that it takes to manually manage DNS zone records. Use the DNS update functionality with DHCP to update resource records when a computer's IP address is changed.

With typical unsecured dynamic updates, any computer can create records on your DNS server which leaves your system open to malicious activity. To keep your DNS server secure,

secure DNS makes it so that only members of an Active Directory domain can create records on the DNS server.

■ Using Security Baselines

THE BOTTOM LINE

As has been made very clear, one of the biggest concerns of any organization is security. To secure systems, it is necessary to configure a wide range of settings. Windows 10 includes more than 3,000 Group Policy settings and more than 1,800 settings for Internet Explorer. Many of these settings are security-related settings that must be managed within an organization.

CERTIFICATION READY
How can the current security settings in Windows be collected to determine which settings are not compliant?
Objective 3.1

A ***security baseline*** is a collection of security settings. Security baselines should include Microsoft's recommendations for configuring those settings. To help with faster deployments, and to ease the managing of Windows, Microsoft provides customers with security baselines that can be used with Group Policy Objects (GPOs).

Using Security Templates

Group policies are often used to make a computer more secure. Use security templates to implement security settings quickly and efficiently, copy and apply security settings from one computer to another, and check the security settings based on a security template.

A ***security template*** is a collection of configuration settings stored in a text file with the .inf extension. They can be used for the following tasks:

- Save the security configuration to a file
- Deploy the security settings to a computer or group policy
- Analyze compliance of a computer's current configuration against the desired configuration

Use a security template to configure the following policies and settings:

- **Account Policies:** Configure password restrictions, account lockout policies, and Kerberos policies
- **Local Policies:** Configure audit policies, user rights assignments, and security options policies
- **Event Log Policies:** Configure maximum event log sizes and rollover policies
- **Restricted Groups:** Specify users who are allowed to be added to a specific group such as domain administrators
- **System Services:** Specify the startup types and permissions for system services
- **Registry Permissions:** Set access control permissions for specific registry keys
- **File System Permissions:** Specify access control permissions for NTFS files and folders

Security templates can be deployed using the following:

- Active Directory group policy objects
- Security Configuration and Analysis snap-in

To manage security templates, use the Security Templates snap-in. This snap-in is not included in Administrative Tools—you need to open Microsoft Management Console (MMC) to manually add the snap-in.

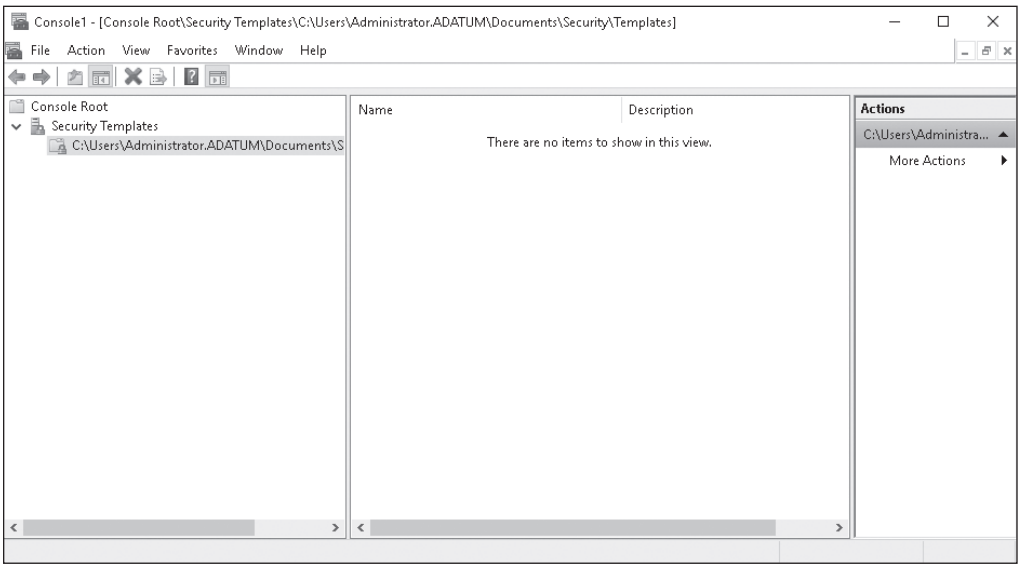
OPEN THE SECURITY TEMPLATES SNAP-IN

GET READY. To open the Security Templates snap-in, perform the following steps.

1. Right-click **Start** and choose **Command Prompt (Admin)**.
2. At the command prompt, execute the **mmc** command. An empty console opens.
3. Click **File** > **Add/Remove Snap-in**.
4. In the Add or Remove Snap-ins dialog box, scroll down to and click **Security Templates**. Click **Add**. Click **OK**. The Security Templates snap-in is available (see Figure 5-17).

Figure 5-17

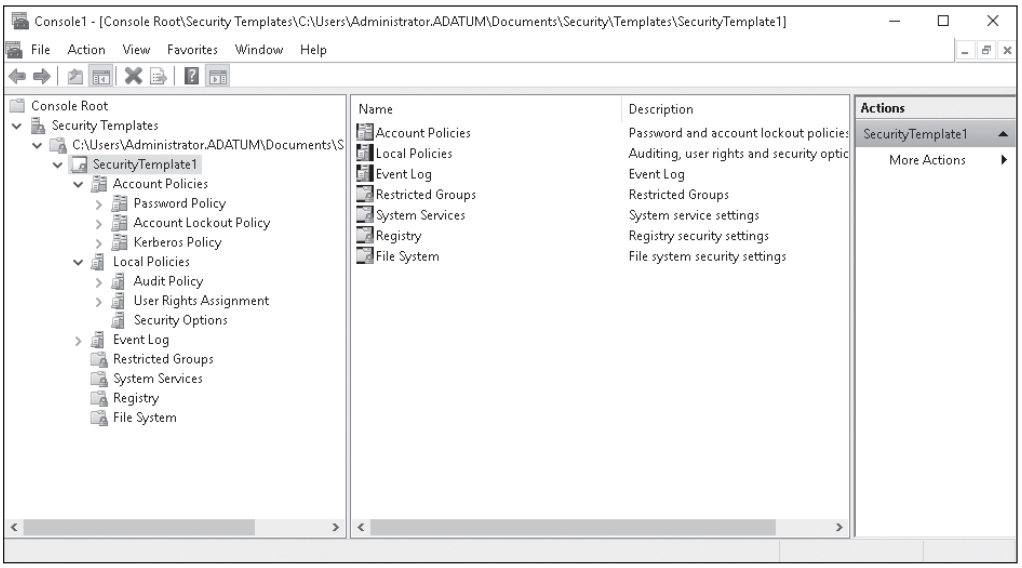
Adding the Security Templates snap-in to MMC



5. To create a new security template, right-click the node where you want to store the security template and choose **New Template**.
6. In the dialog box, in the Template name text box, type a descriptive name. Click **OK**. The security template is added in the console. Figure 5-18 shows the security templates.

Figure 5-18

Viewing a security template



Settings are configured the same way a GPO is configured. The only exception is when adding registry settings that are not already listed in the Local Policies\Security Options portion of the template. After making your changes, right-click the template and choose Save. For an updated security baseline for Windows 10 and Server 2016 computers, search the www.microsoft.com website and download the Windows 10 RS2 and Server 2016 Security Baseline.

After a security template is created and saved, deploy those settings by importing the security template into the GPO for a domain, site, organization unit object, or a local computer. To import a security template into a GPO, open the GPO, right-click the Security Settings node, and choose Import Policy. If you select the Clear This Database Before Importing check box, all security settings in the GPO will be erased prior to importing the template settings, so the GPO's security settings will match the template's settings.

COMPARE SETTINGS WITH A SECURITY TEMPLATE

GET READY. To compare settings with a security template, perform the following steps.

1. Right-click the **Start** menu and choose **Command Prompt (Admin)**.
2. At the command prompt, execute the **mmc** command. An empty console opens.
3. Click **File** > **Add/Remove Snap-in**.
4. In the Add or Remove Snap-ins dialog box, scroll down and then click **Security Configuration and Analysis**. Click **Add**. Click **OK**. The Security Configuration and Analysis console is available (see Figure 5-19).

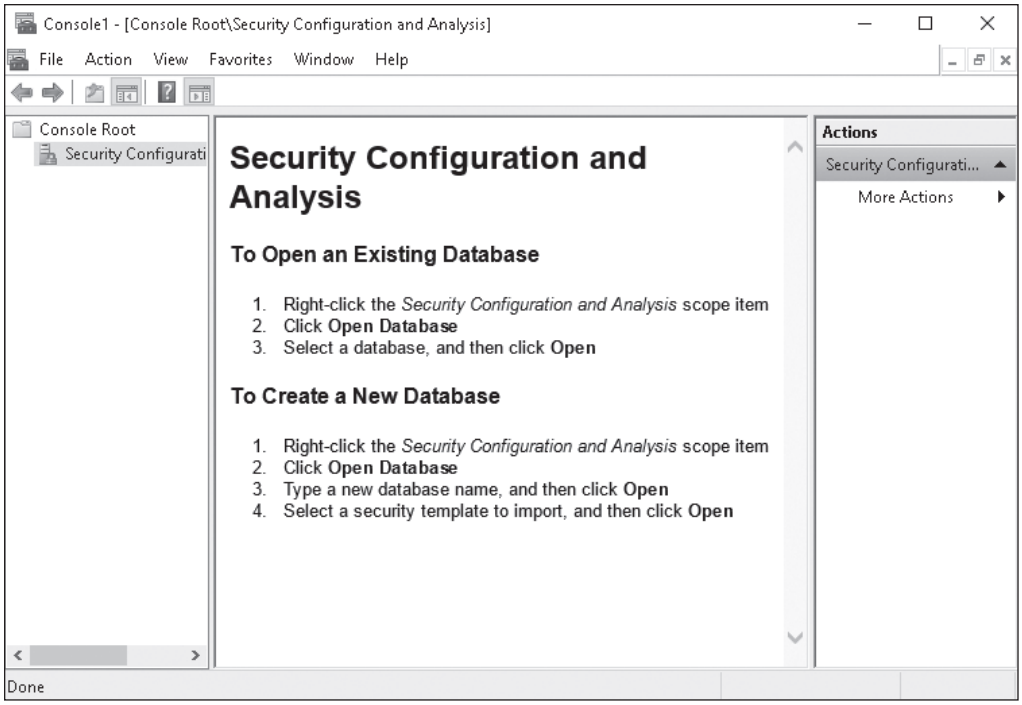


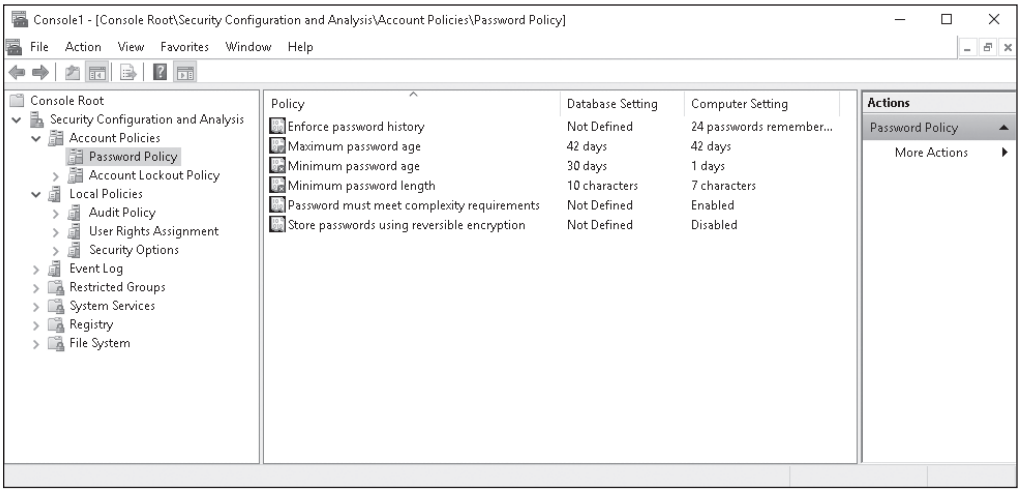
Figure 5-19
Viewing the Security Configuration and Analysis console

5. Right-click **Security Configuration and Analysis** and choose **Open Database**.
6. In the Open database dialog box, in the File name text box, type **SecDB** and click **Open**.
7. In the Import Template dialog box, click **SecurityTemplate1.inf** and click **Open**.

8. To analyze a computer based on the security template, click **Analyze Computer Now**.
9. In the Perform Analysis dialog box, click **OK**.
10. When the analysis is done, look for settings that are not compliant. For example, Figure 5-20 shows that the Minimum password age and Minimum password length settings are not compliant.
11. Close the Security Configuration and Analysis console.

Figure 5-20

Comparing a security template with actual settings



Using Security Compliance Manager

Security Compliance Manager 4.0 (SCM 4.0) is a free tool from Microsoft that can be used to quickly configure and manage your desktops, traditional data center, and private cloud using Group Policy and System Center Configuration Manager. It includes creating new baselines for Windows Server 2016, Windows 10, and Internet Explorer 11. To install Security Compliance Manager, .NET Framework 3.5 must be installed.

CERTIFICATION READY
Which free tool can help to quickly configure and manage your desktops?
Objective 3.1

SCM provides ready-to-deploy policies and configuration packages that are based on Microsoft Security guide recommendations and industry best practices. When deployed as a GPO, you can manage configuration drift, address compliance requirements, and reduce security threats.

INSTALL SECURITY COMPLIANCE MANAGER

GET READY. To install Security Compliance Manager 4.0, perform the following steps.

1. Double-click the **Security_Compliance_Manager_Setup.exe** file. When you are prompted to confirm that you want to run the executable program, click **Run**.
2. In the Microsoft Visual C++ 2010 x86 Redistributable Setup dialog box, click the **I have read and accept the license terms** option and click **Install**.
3. After the Visual C++ 2010 x86 Redistributable is installed, click **Finish**.
4. In the Microsoft Security Compliance Manager Setup window, on the Welcome screen, click **Next**.

5. On the License Agreement page, click the **I accept the terms of the license agreement** option and click **Next**.
6. On the Installation Folder page, click **Next.**
7. On the Microsoft SQL Server 2008 Express page, click **Next**.
8. On the SQL Server 2008 Express License Agreement page, click the **I accept the terms in the license agreement** option and click **Next**.
9. On the Ready to Install page, click **Install**.
10. When the SQL Server Express and Microsoft Security Compliance Manager is installed, click **Finish**. Microsoft Security Compliance Manager (SCM) 4.0 opens.
11. Click **File > Check for Updates**.
12. In the Downloads Updates dialog box, click **Download**.
13. When you are prompted to confirm that you want to run this software, click **More options**. Then click the **Always run software from "Microsoft Corporation"** option and click **Run**. Repeat the process until all there are no more security warnings.
14. In the Import Baselines Wizard, on the Select packages file page, click **Next**.
15. On the Baseline details page, click **Import**.
16. On the Results page, click **Finish**.

Expand the Windows Server 2016 category in the left pane to see a list of baseline templates for several different server roles, such as Domain Controller Security Compliance 1.0, Domain Security Compliance 1.0, and Member Server Security Compliance. Microsoft recommends that organizations only apply Domain Controller, Domain Security, and Member Server security templates to servers.

Figure 5-21 shows the Windows 10 Computer Security Compliance Manager. As shown in the figure, there are 765 unique settings, and the Authentication Types group has 43 settings. However, when you click a setting—because this is a baseline template that's provided by Microsoft—you need to duplicate it before you can make changes. The settings can then be modified, as shown in Figure 5-22.

Figure 5-21

Viewing Windows 10 settings with Computer Security Compliance Manager

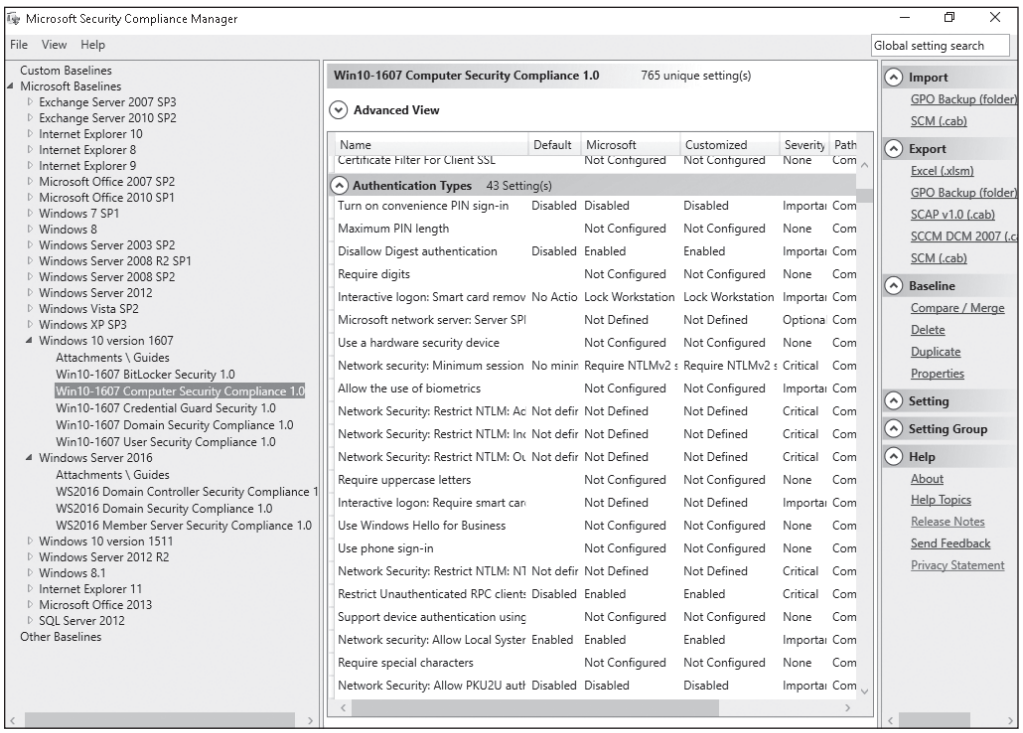
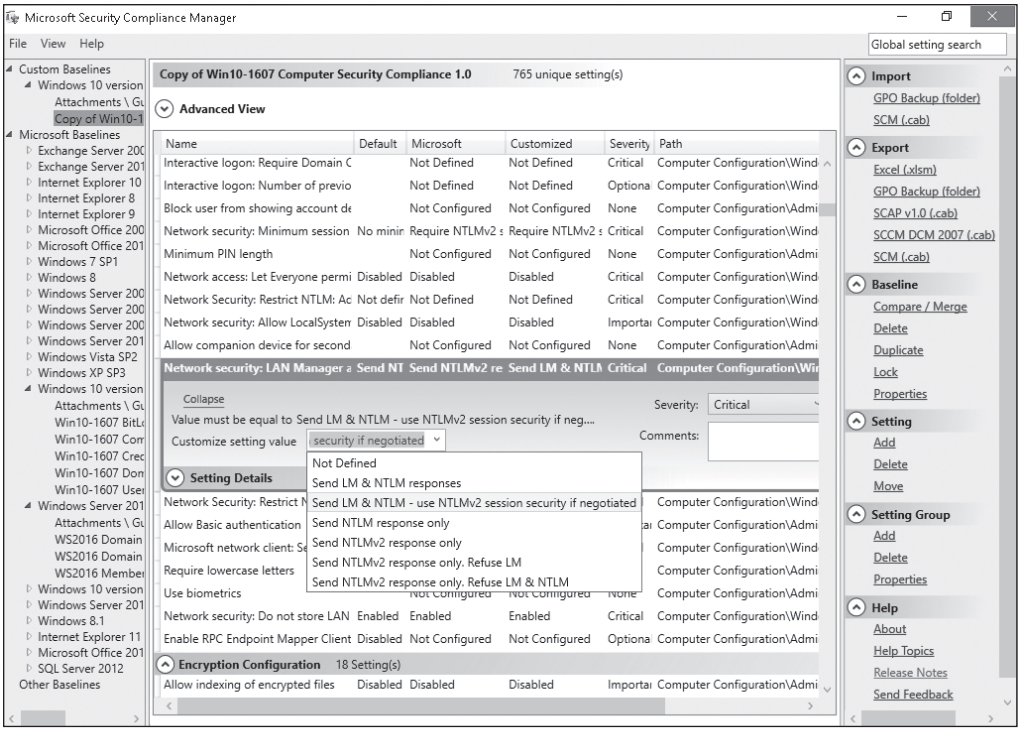


Figure 5-22

Changing a Windows 10 setting with Computer Security Compliance Manager



After configuring the desired settings, export the SCM Template Settings as a GPO Backup. Then, use the backup to create a new GPO and link it to an organizational unit or domain.

■ Locking Down Devices to Run Only Trusted Applications

THE BOTTOM LINE

Removing users from the administrative role on computers can reduce the number of applications they can install, but it does not prevent them from loading apps that do not require administrative privileges to run. Use AppLocker to establish rules that determine which programs your users are allowed to run.

CERTIFICATION READY
How can you ensure that only authorized applications run on your company computers?
Objective 2.5

Use ***AppLocker*** to control how users access and use programs and files, and extend the functionality originally provided by the Software Restriction policy found in earlier versions of Windows operating systems. In Windows 10, AppLocker is located in the Local Group Policy Editor.

ACCESS APPLOCKER

CERTIFICATION READY
How can you ensure that users do not install software that they download from the internet?
Objective 4.1

GET READY. To access AppLocker using the Local Group Policy editor (gpedit.msc), perform the following steps.

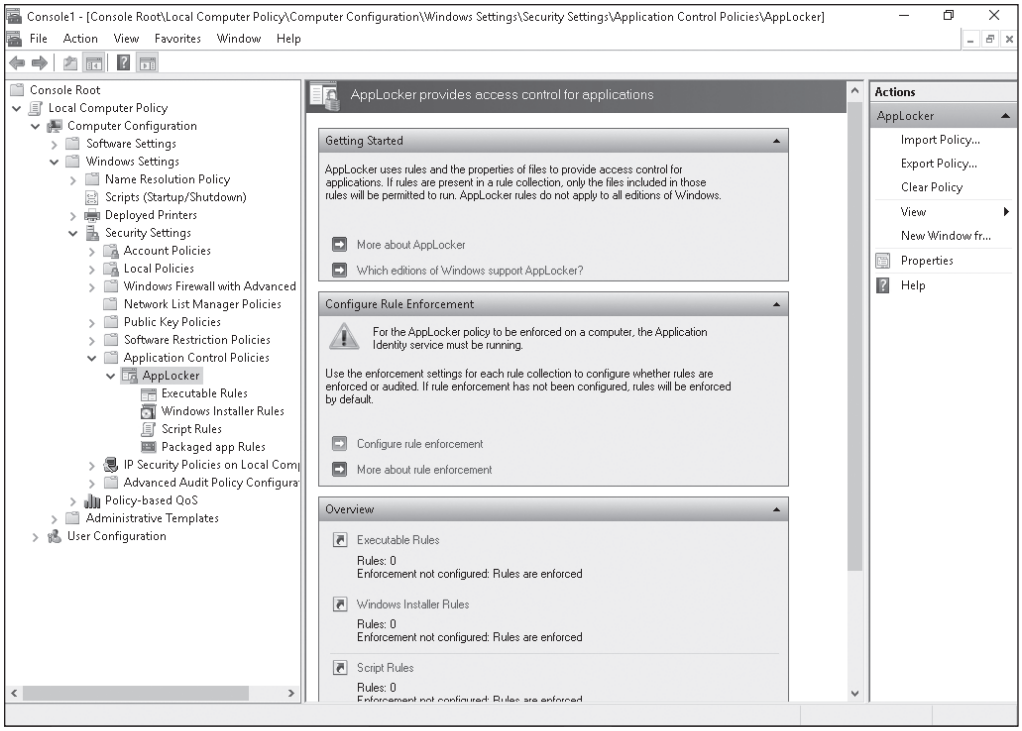
1. Press **Windows logo key+r**.
2. In the Run box, type **gpedit.msc** and click **OK.** The Local Group Policy Editor displays.
3. Click **Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker**.

AppLocker uses rules and file properties to determine which programs and files are allowed to run on the computer. As shown in Figure 5-23, AppLocker includes four ***rule collections***:

- Executable Rules
- Windows Installer Rules
- Script Rules
- Packaged app Rules

Figure 5-23

The AppLocker rule collections



These rule collections can be used to differentiate the rules for different types of applications. AppLocker uses rules and a file's properties to determine which applications are allowed to run.

A traditional app consists of several components (.exe files, scripts, and so on). These components might not share the same publisher, product, or product version attribute. In order to manage traditional apps, AppLocker needs to control them using different rule collections. On the other hand, a Windows app (packaged app) shares the same attributes; therefore, a single rule can be created to control the entire application.

Rule collections include the following:

- Executable files (.exe, .com)
- Scripts (.ps2, .bat, .js, .cmd, vbs)
- Windows Installer files (.msi, .mst, .msp)
- Packaged apps and Packaged app installers (.appx)

By default, there are no rules in any of the rule collections; therefore, AppLocker will allow every file covered in each collection to run.

When creating rules with AppLocker, the following options are available:

- **Create New Rule:** Use this wizard to walk through the process of creating one AppLocker rule at a time—setting permissions, publishers, exceptions, and providing a name for the rule.

- **Automatically Generate Rules:** This wizard creates rules for multiple packaged apps in a single step. Select a folder and let the wizard create the applicable rules for the files in the folder or for packaged apps.
- **Create Default Rules:** This wizard creates rules that are meant to ensure that some key Windows paths are allowed for execution (C:\Windows files or C:\Program files). If the default rules are not in place, when creating a new rule, AppLocker will prompt you to create them.

Prior to configuring a rule, install the application for which you want to create the rule. After it is installed, perform the following steps to configure the rule:

1. Set permissions. AppLocker uses three rule types:

   Allow: Programs on the list are allowed to run; all other programs are blocked.

   Deny: Programs on the list are not allowed to run; all other programs are allowed.

   Exceptions: Used for both allow and deny rules to provide exceptions to the rule.
2. Set the primary condition (publisher, path, or file hash):

   Publisher: This option identifies an application based on the manufacturer's digital signature. The digital signature contains information about the company that created the program (publisher). If you use this option, the rule can survive an update of the application as well as a change in the location of its files. This allows you to push out the updated version of the application without having to build another rule.

   Path: This option identifies an application based on its location in the file system. For example, if the application is installed in the Windows directory, the AppLocker path is %WINDIR%.

   File hash: This option causes the system to compute a hash on the file. Each time the file is updated (via an upgrade or patch), the hash must be updated.
3. Add an exception (optional). In this step, you can add an exception to the rule (if applicable). For example, you might have enabled access for a suite (such as Microsoft Office) but do not want selected users to be able to use Microsoft Access because there are a limited number of licenses.
4. Type a name for the rule. In this step, give the rule a name and add an optional description.

TAKE NOTE* Rules created for a packaged app can use only the Publisher condition. Windows does not support unsigned packaged apps or installers.

CREATE AND TEST AN APPLOCKER RULE

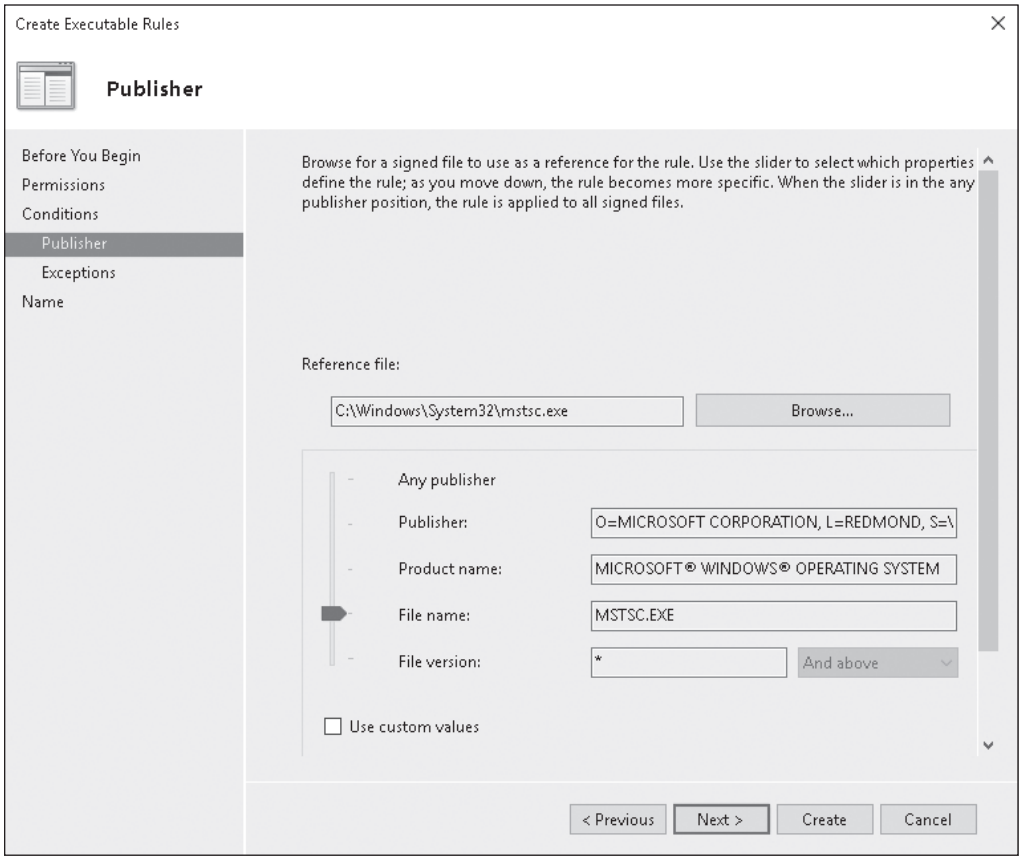
GET READY. To create and test an AppLocker rule that blocks the use of the Remote Desktop Connection client (mstsc.exe), log on to a Windows 10 computer as an administrator, and then perform the following steps.

1. Press **Windows logo key+r** and in the Run box, type **services.msc** and click **OK**. The Services console displays.
2. Right-click the **Application Identity** service and choose **Start**. Close the Services console after confirming that the service is running.
3. Press **Windows logo key+r** and in the Run box, type **gpedit.msc** and click **OK**. The Local Group Policy Editor displays.
4. Click **Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker**.
5. Right-click **Executable Rules** and choose **Create New Rule**.
6. Read the Before You Begin screen and click **Next**.

7. Select **Deny**.
8. Click **Select** and in the Enter the object name to select box, type **Users** and click **OK**.
9. Click **Next** to continue.
10. Select **Publisher** and click **Next**.
11. Click **Browse** and navigate to the C:\Windows\System32 directory. Click the **mstsc .exe** file and click **Open.**
12. Drag the slider to **File name** (see Figure 5-24) and click **Next**. This setting ensures the rule will block all instances of the Remote Desktop Connection client (mstsc .exe), regardless of the version.

Figure 5-24

Viewing the executable rules/ publisher information for the AppLocker rule



13. Click **Next**. You do not set an exception to this rule.
14. Type a name for the rule and a description (optional). For example, you might type Disallow Remote Desktop Connection client on Company Systems.
15. Click **Create**.
16. When you are prompted to create the default rules, click **Yes**. This ensures important rules are allowed to run.
17. Close the Local Group Policy Editor.
18. To force Group Policy to update, press **Windows logo key+r** and in the Run box, type **`Gpupdate /force`** and then click **OK**.
19. Log on with any non-administrative account and test the policy.
20. Press **Windows logo key+r** and in the Run box, type **mstsc.exe** and click **OK**. The user will see the Your system administrator has blocked this program message.

When creating a policy using the Local Group Policy Editor, you are applying the policy to the local computer and the users who log on to it. If you decide later that you want to use the same policy, but apply it to multiple computers across your Active Directory domain, export the policy and then import it into a Group Policy Object linked to a container in the Active Directory hierarchy (site, domain, or organizational unit). This eliminates the need to re-create the policy settings.

EXPORT THE LOCAL POLICY

GET READY. To export the local policy, log on to the Windows 10 client computer as an administrator, and then perform the following steps.

1. Press **Windows logo key+r** and in the Run box, type **gpedit.msc** and click **OK**. The Local Group Policy Editor displays.
2. Click **Computer Configuration > Windows Settings > Security Settings > Application Control Policies**.
3. Right-click **AppLocker** and choose **Export Policy**.
4. In the File name field, type a name for the policy and click **Save**. For example, you might type Remote Desktop Connection client on Company Systems. Make a note of the location where you are saving the policy. This location must be accessible from your domain controller.
5. When the 4 rules were exported from the policy message displays, click **OK**.

IMPORT THE LOCAL POLICY

GET READY. To import the local policy settings into a Group Policy Object in Active Directory and apply it to all computers in your domain, perform the following steps.

1. Log on to a domain controller or a Windows 10 client computer that is a member of a domain with an administrative account that has access to the Group Policy Management console.
2. Press **Windows logo key+r** and in the Run box, type **gpmc.msc** and click **OK**. The Group Policy Management Editor window opens.
3. Right-click the **Group Policy Objects** folder and choose **New**.
4. Type a name for the new GPO and click **OK**.

   For example, you might type Disallow Remote Desktop Connection client on Company Systems.
5. Right-click the GPO and choose **Edit**.
6. Click **Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies**.
7. Right-click **AppLocker** and choose **Import Policy**.
8. Browse to the local policy file you exported earlier, select the policy file, and then click **Open**.
9. When prompted to import the policy now, click **Yes**.
10. When the 4 rules were imported from the policy message displays, click **OK**.
11. Close the Group Policy Management Editor.
12. In the Group Policy Management console, right-click the domain name (contoso) and choose **Link an Existing GPO**.
13. In the Group Policy objects section, click **Disallow Remote Desktop Connection client on Company Systems** and click **OK**.

    Now, no computer in your domain will be allowed to use the Remote Desktop Connection program.

Managing Windows Store Apps

THE BOTTOM LINE

Windows Store apps are a class of applications for Windows devices, including PCs, tablets, phones, Xbox One, Microsoft Hololens, and the Internet of Things. They are typically distributed and updated through the Windows Store.

CERTIFICATION READY
How can users find and install only applications that an administrator approves from the Windows Store?
Objective 2.5

Universal Windows Platform (UWP) apps are a special type of Windows Store app that can be installed on multiple hardware platforms, such as an Intel tablet that is running Windows 10 Pro, an Xbox One, or a Windows 10 Phone. Windows Store apps differ from traditional applications in that they are designed to run in a single, full window display across multiple form factor devices (for example, desktops, laptops, or tablets). These devices can be touch-based or they can use a standard mouse and keyboard.

Configuring the Windows Store

CERTIFICATION READY
How can access to the Windows Store be disabled?
Objective 4.1

The ***Windows Store*** provides a central location for purchasing and downloading Windows apps that run on Windows 8 and higher operating systems. Windows Store apps are special types of apps that work on computers that are running Windows 8 and higher operating systems. Windows Store apps do not run on Windows 7 or earlier versions of Windows. Windows Store apps tend to be smaller and faster than desktop apps.

Windows 10 includes the Windows Store app, which can be accessed directly from the taskbar. In Windows 10, the Windows Store enables users to deploy both Windows Store apps and desktop apps. To browse the Windows Store, it is not necessary to sign in with a Microsoft account. However, to download and install apps from the Windows Store, you do have to sign in with a Microsoft account.

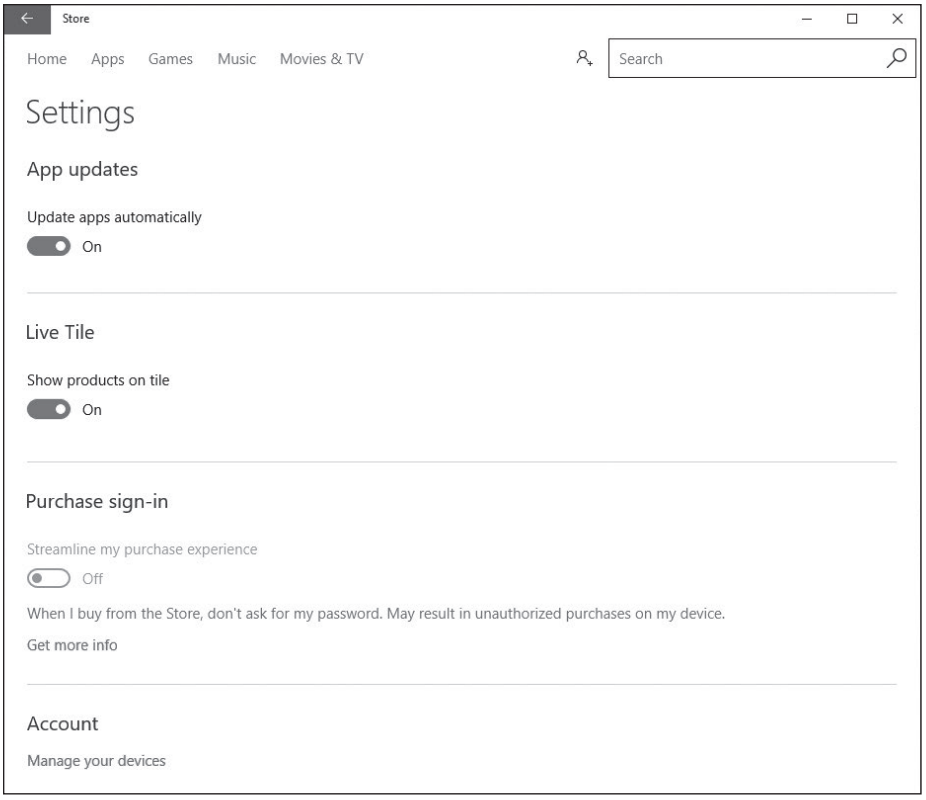
A ***Microsoft account***, previously called Windows Live ID, is a unique account that is the combination of an email address and a password that you use to sign in to services like Outlook.com, MSN.com, Hotmail.com, OneDrive, Windows Phone, or Xbox Live. When setting up a computer running Windows 10 for the first time, create a Microsoft account using an email address that you provide. The email address can come from any provider. After the account is set up, Microsoft will use it, along with your password, to help manage your settings across all your PCs that run Windows 10. Microsoft accounts can be used to synchronize your desktop across multiple Windows 10 devices and provide a consistent experience when working with Windows Store apps. Purchased apps will be available from each device, feeds will be synced across all devices, and state information will be maintained, so you can start a game or read a book and pick it up later on another device. You can create a Microsoft account during the initial installation of the operating system or after the system is running.

When you open the Windows Store, click the Sign in icon (the icon next to the Search text box). If you click the Sign up button, you can also configure the following:

- **Downloads and updates:** View the current downloads and check for updates for the Windows Store apps.
- **Settings:** Enable automatic updates, show products on the Live Tile, streamline purchases, and manage your devices that are connected to the Microsoft account. Figure 5-25 shows the Windows Store Settings page.

Figure 5-25

Managing Windows Store settings



CONFIGURE THE WINDOWS STORE

GET READY. To configure the Windows Store, perform the following steps.

1. On the taskbar, click the **Windows Store** button.
2. To sign in to the Windows Store, click the **Sign In** button and click **Sign In**.
3. When you are prompted to choose an account, click **Microsoft account**.
4. Specify the proper credentials in the Email or phone dialog box and click **Sign in**.
5. Click the user icon and click **Settings**.
6. To update apps automatically, ensure that the Update apps automatically option is set to **On**.
7. To streamline your purchases so that you will not be prompted for a password, ensure that the Streamline my purchase experience option is set to **On**.
8. To view your downloads and updates, click the user icon again and click **Downloads and updates**.

Implementing Windows Store Apps

Searching for a Windows Store app is quite easy. Type the search term (a specific name or a desired category) and Microsoft provides a list of available apps. After you select apps, they install in the background. When the installation is done, the app appears in a tile on the Start menu.

The applications available through the Windows Store must be certified by Microsoft for compatibility and content. Certified apps cannot contain adult content and cannot advocate discrimination, illegal activity, alcohol, tobacco products, drugs, weapons, profanity, or extreme violence.

Although the Windows Store can provide a wide variety of apps and tools to enhance Windows 10, it might be necessary to restrict access for your users. This restriction would ensure that users are working with only authorized applications within your organization.

To deny access, set up a policy for a single computer/user or for multiple computers and users. The tool that should be used depends upon where you want to use the policy. For example, to configure the policy and test it, use the Local Group Policy Editor on a Windows 10 client machine. To deploy the policy settings across your domain, use the Group Policy Management Console. In either case, the settings are located under the Administrative Templates\Windows Components\Store under the Computer Configuration and User Configuration nodes.

TAKE NOTE*

If you create the policy using the Local Group Policy Editor, you can export and import it into a GPO at the domain level. It does not have to be re-created.

When configuring the policy using the Local Group Policy Editor for a user (User Configuration\Administrative Templates\Windows Components\Store), there is only one option to set within the policy:

- Turn off the Store application:
  - **Not Configured (default):** Access to the Store is allowed.
  - **Enabled:** Access to the Store is denied.
  - **Disabled:** Access to the Store application is allowed.

When setting the policy for a computer (Computer Configuration\Administrative Templates\Windows Components\Store), the following options are available:

- Turn off Automatic Download of updates:
  - **Not Configured (default):** Download of updates is allowed.
  - **Enabled:** Automatic downloads are turned off.
  - **Disabled:** Automatic downloads of updates are allowed.
- Allow Store to install apps on Windows To Go workspaces:
  - **Not Configured (default):** Access to the Store is not allowed.
  - **Enabled:** Access to the Store is allowed on the Windows To Go Workspace. Use this option only when the device is used with a single PC.
  - **Disabled:** Access to the Store is denied.
- Turn off the Store application:
  - **Not Configured (default):** Access to the Store is allowed.
  - **Enabled:** Access to the Store is denied.
  - **Disabled:** Access to the Store application is allowed.

RESTRICT ACCESS TO THE WINDOWS STORE USING A LOCAL GROUP POLICY

GET READY. To restrict access to the Windows Store using a Local Group Policy, log on to a Windows 10 computer with administrative credentials, and then perform the following steps.

1. Click the **Start** button, type **gpedit.msc**, and press **Enter**. The Local Group Policy Editor opens.
2. Expand **Computer Configuration > Administrative Templates > Windows Components** and click **Store**.
3. Double-click the **Turn off the Store application** setting. In the Turn off the Store application dialog box, click **Enabled**.

4. Attempt to access the Windows Store. Click the **Store** tile located on the Windows 10 Start menu. The Windows Store isn't available on this PC message appears.
5. Return to the group policy setting you enabled in Step 3 and click **Not Configured** to regain access to the Windows Store.

In some situations, you might administer a computer in a public area (such as a library or kiosk) that needs to run just a single Windows app. In these situations, configure Windows 10 settings to restrict access to a single application.

When you assign access to a single Windows Store app, you restrict the application to a user account. When the user logs on to the computer, that user can only access the assigned app.

RESTRICT A USER ACCOUNT TO RUN A SINGLE WINDOWS STORE APP

GET READY. To restrict a user account to run a single Windows Store app, perform the following steps.

1. Click the **Start** button and click **Settings**.
2. Click **Accounts** and click **Family & other users**.
3. In the right pane, click **Set up assigned access**.
4. Click **Choose an account** and select the account that you want to restrict.
5. Click **Choose an app** and select the installed app to which you want to restrict the account.
6. Sign out of the computer to make the changes effective.

Implementing Windows Store for Business

To support larger organizations that need to control which apps are installed on the organization's computers, Microsoft developed the Windows Store for Business. The ***Windows Store for Business*** supports volume purchases of Windows apps, flexible distribution options, and the ability to reclaim or re-use licenses. You can also create a private store for your employees that includes apps from the Windows Store as well as the organization's private apps.

Many organizations enforce policies that are designed to standardize the apps used on company-supplied computers. They do not want their users installing just any application they find, even if those apps are certified to work with Windows 10. ***Bring Your Own Device (BYOD) policies*** might also be in place, requiring you to control access to the Windows Store. A BYOD policy defines the standards, restrictions, and procedures for end users who have authorized access to company data from their personal devices (tablets, laptops, or smartphones). The policy also includes hardware and related software that is not approved, owned, nor supplied by the company. In either case, as the administrator, ensure that your strategy for accessing the Windows Store aligns with your company's policies.

In addition to determining your strategy for controlling access to Windows apps and the Windows Store, consider the deployment of ***Line of Business (LOB) apps***. LOB apps include apps that are critical to running the company business as well as apps that are unique to the company's main business. To use the new Windows Apps format for your LOB apps, deploy them via the Windows Store or a process called sideloading. To deploy your LOB apps via the Windows Store, they must go through a certification process with Microsoft to ensure they are compatible with Windows 10 and meet the criteria for apps being deployed from the Windows Store. The apps will also be available to the public, which may not be desirable. To bypass the Windows Store requirements and make the apps available to your internal users only, consider sideloading them as part of the overall design strategy.

The general steps for using the Windows Store for Business include:

1. Sign up for Windows Store for Business.
2. Assign roles.
3. Get apps and content.
4. Distribute apps and content.

SIGN UP FOR WINDOWS STORE FOR BUSINESS

GET READY. To sign up for Windows Store for Business, perform the following steps.

1. Open Internet Explorer and go to **https://www.microsoft.com/en-us/business-store**.
2. Click the **SIGN UP NOW** link.
3. In the Sign up dialog box, in the Enter an email address text box, type the desired Microsoft Azure Active Directory (AD) account email address and click **Next**.
4. If the account is not a Microsoft Azure Active Directory (AD) account, you are prompted to create the Azure AD account by clicking **Sign up**.
5. On the Welcome page, enter all of the following information and then click **Next**:
   Country or region: Specify the appropriate country or region
   First name: ***<Your first name>***
   Last name: ***<Your last name>***
   Business email address: Same email address that you used in Step 3
   Business phone number: ***<Your cell phone number>***
   Company name: ***<Your Last Name>*** **Corporation**
   Size of organization: **25-49 people**
6. On the Create your user ID page, enter the following information and then click **Next**:
   Enter a user name: ***<FirstInitial><LastName>***
   Your company: ***<Your Last Name>*** **Corporation**
7. On the Prove. You're. Not. A. Robot. page, in the Phone number text box, type your cell phone number and click **Text me**.
8. In the Enter your verification code text box, type the code that you received on your cell phone. Click **Create my account**.
9. Click **You're ready to go**.
10. When the Terms of Use are displayed, scroll down to the bottom. Select **I accept this agreement and certify that I have the authority to bind my organization to its terms** and click **Accept**.
11. In the Welcome to the Windows Store for Business dialog box, click **OK**.

After signing up for Windows Store for Business, you can assign roles to other employees in your organization. To add more people, click Settings > Permissions, and click Add people. You will be prompted to type the names or email addresses and to choose one of the following roles:

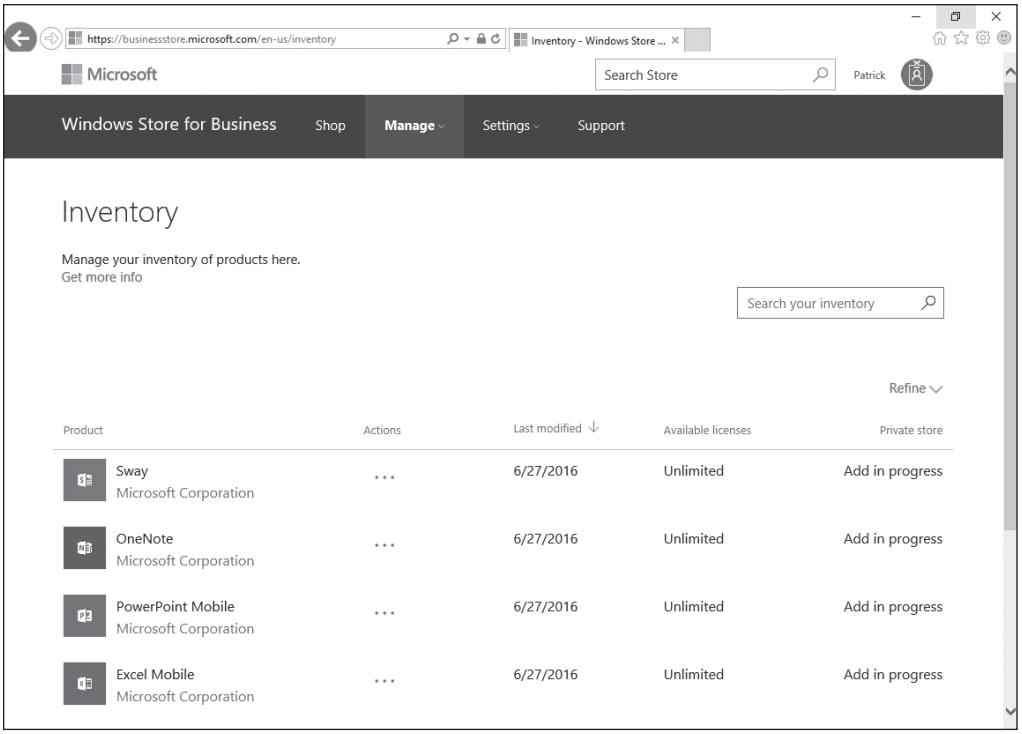
- **Admin:** Can configure account settings, acquire apps, distribute apps, and sign policies and catalogs
- **Purchaser:** Can acquire apps and distribute apps
- **Device Guard signer:** Can sign policies and catalogs

To manage your applications:

- To see your inventory, click Manage > Inventory, as shown in Figure 5-26.
- To add your own LOB apps, click Manage > New LOB apps.
- To show your order history, click Manage > Order history.

Figure 5-26

Managing inventory settings



To distribute apps and content, use the following distribution options:

- After purchasing an app, email employees a link they can click to install the app.
- Curate a private store for all employees. Add the app to the private store and users can install the app when needed.
- Distribute the app with a mobile device management (MDM) tool that can synchronize your Store for Business inventory; this tool is installed and configured in Azure Active Directory (AD).
- Organizations that use an MDM to manage apps can use a policy to show only the private store.

SKILL SUMMARY

IN THIS LESSON, YOU LEARNED:

- Because a client computer is connected to an organization's network, which may have direct and indirect access to servers and the network resources, it is important to protect the client computer.
- A computer virus is a program that can copy itself and infect a computer without the user's consent or knowledge.
- A backdoor is a program that gives some remote, unauthorized control of a system or initiates an unauthorized task.
- Some viruses, worms, rootkits, spyware, and adware are made possible because they exploit some security hole within Windows, Internet Explorer, or Microsoft Office.
- The first step that should be taken to protect yourself against malware is to keep your system up-to-date with the latest service packs, security patches, and other critical fixes for Windows (as well as other Microsoft products, such as Internet Explorer and Microsoft Office).

- A virus hoax is a message warning the recipient of a non-existent computer virus threat, usually sent as a chain email that tells the recipient to forward it to everyone they know. It is a form of social engineering that plays on people's ignorance and fear and may include emotive language and encouragement to forward the message to other people.
- User Account Control (UAC) is a feature that was introduced in Windows Vista and is included with Windows 10 that helps guard against malware.
- Microsoft recommends always using the Windows Firewall.
- Offline files are copies of network files that are stored on your computer so that they can be accessed when not connected to the network or when the network folder with the files is not connected.
- Offline files are not encrypted unless you choose to encrypt them. Consider encrypting your offline files if they contain sensitive or confidential information, and you want to make them more secure by restricting access to them.
- By restricting users to standard user accounts, you can limit what software those users can install.
- Use group policies to restrict what software can be executed on a client computer.
- Most of the email will be unsolicited emails called spam or junk email.
- The best place to establish an anti-spam filtering system is on your email relay, on a dedicated server or appliance, or as part of a firewall device or service.
- Many anti-spam solutions will also use Real-time Blackhole Lists (RBLs) or a DNS-based Blackhole List (DNSBL), which can be accessed freely. RBLs and DNSBL are lists of known spammers that are updated frequently.
- Sometimes, spammers will try to spoof a legitimate email address or IP address when the message actually comes from one with an email address or IP address that would likely be identified as spam.
- Simple Mail Transfer Protocol (SMTP) is used to transfer email from one server to another and it is also responsible for outgoing mail transport.
- Spammers look for unprotected SMTP servers through which they can relay their email.
- A cookie is a piece of text stored by a user's web browser. It can be used for a wide range of items, including user identification, authentication, storing site preferences, and shopping cart contents.
- While some pop-up windows are useful website controls, most are simply annoying advertisements, with some attempting to load spyware or other malicious programs.
- To help manage Internet Explorer security when visiting sites, Internet Explorer divides a network connection into four content zones or types. For each of these zones, a security level is assigned.
- Phishing and pharming are forms of attacks to get users to a bogus website in an attempt to spread malware or collect personal information.
- When surfing the internet, there are times when it is necessary to transmit private data such as credit card numbers, Social Security numbers, and so on. During these times, it is important to use http over SSL (https) to encrypt the data sent over the internet.
- The server should be kept in a secure location. In addition, the servers should be in their own subnet to reduce the amount of traffic to the servers, especially broadcasts.

- To secure a server is to harden the server by reducing its surface of attack and thereby reducing the server's vulnerabilities. To harden a server, look for security guides and best practices for Windows servers and for the specific network services that you are installing.
- Windows servers provide support for the dynamic update functionality. Dynamic DNS lets client computers dynamically update their resource records in DNS.
- To keep your DNS server secure, secure DNS makes it so that only members of an Active Directory domain can create records on the DNS server.

■ Knowledge Assessment

Multiple Choice

Select the correct answer(s) for each of the following questions.

1. Which type of malware copies itself onto other computers without the owner's consent and will often delete or corrupt files?

a. Virus
b. Worm
c. Trojan horse
d. Spyware

2. Which type of malware collects personal information or browsing history, often without the user's knowledge?

a. Virus
b. Worm
c. Trojan horse
d. Spyware

3. Which of the following is most likely the problem when a computer seems to be slow and a different default web page displays?

a. The ISP has slowed the network connection.
b. The computer has been infected with malware.
c. The computer has not been updated.
d. The user accidentally clicked the turbo button.

4. Which of the following is the best thing to do to protect a computer against malware, besides installing an antivirus software package? (Choose the best answer.)

a. Keep the computer up-to-date with the latest security patches.
b. Reboot the computer on a regular basis.
c. Change the password on a regular basis.
d. Spoof the IP address.

5. Which of the following refers to a thoroughly tested, cumulative set of hotfixes and other patches?

a. Recommended update
b. Hotfix pack
c. Service pack
d. Critical update

6. Which technology is used by Windows to prevent unauthorized changes to your system?
   a. UAC
   b. Protected mode
   c. Windows Defender
   d. ProtectGuard

7. When using UAC, which of the following tasks requires administrative permissions or rights?
   a. Install updates from Windows Update.
   b. Change the date and time.
   c. Reset the network adapter.
   d. Install drivers from Windows Update.

8. When attempting to change the display settings, which of the following causes a pop-up that prompts if a user wants to continue?
   a. Windows Firewall
   b. Protected Mode
   c. Windows Update
   d. UAC

9. Which host-based firewall software comes with Windows 10?
   a. Windows Firewall
   b. Windows Protected Mode
   c. UAC
   d. Windows GuardIt

10. Which program can be used to configure IPsec on a computer running Windows Server 2016?
    a. Windows Firewall with IPsec Plugin
    b. IPsec Monitor
    c. Windows Firewall with Advanced Security
    d. IPsec Configuration console

11. Which of the following tasks is recommended if sensitive or confidential information is stored in offline files?
    a. Clear the cache.
    b. Encrypt the offline files.
    c. Clear the cookies.
    d. Execute `ipconfig /renewip`.

12. Which of the following tasks should be performed if legitimate emails are being blocked at a spam-blocking device?
    a. Flush out the quarantined items.
    b. Reboot the spam-blocking device.
    c. Add the email address or domain to the allow list.
    d. Add the email address or domain to the block list.

13. SMTP uses which of the following TCP ports?
    a. 43
    b. 25
    c. 80
    d. 443

14. When using IE, how many content zones are there?
    a. 1
    b. 2
    c. 4
    d. 8

15. Which of the following refers to a social engineering technique in which a user receives an email stating that his account has just expired and he should log on to a legitimate-looking website to fix the problem?
    a. Phishing
    b. Pharming
    c. Phaking
    d. Spoofing the IP address

16. Which of the following is used to stop a program from running on a Windows 10 system?
    a. AppLocker
    b. Windows Defender
    c. Microsoft Passport
    d. Smart card

17. Which type of account is used with outlook.com and OneDrive and can be used to synchronize a desktop across multiple computers?
    a. Domain account
    b. Microsoft account
    c. Local account
    d. Virtual account

18. Which of the following is a collection of security settings that can be used to configure client settings?
    a. Biometrics
    b. Windows Defender
    c. Security baseline
    d. Windows Store

19. Which of the following is a free tool that allows administrators to quickly configure and manage desktops and users using Group Policy?
    a. STRIDE
    b. DREAD
    c. Trusted Platform Module
    d. Security Compliance Manager

Fill in the Blank

Complete the following sentences by writing the correct word or words in the blanks provided.

1. _____ is software that is designed to infiltrate or infect a computer usually with ill intent.
2. A(n) _____ is a self-replicating program that copies itself to other computers while consuming network resources.
3. Microsoft's built-in antivirus and antispyware program is _____.
4. For antivirus software to be effective, it must be _____.
5. An example of a(n) _____ is a message that states you should delete the win.com file, because it is a virus.
6. To control which updates get pushed to clients within an organization, an administrator would use _____ or _____.

7. When a user is notified of an attempt by programs to make changes to their computer, the desktop will be dimmed. This dimming indicates the computer is in _____ mode, because other programs can't run until the changes are approved or disapproved.
8. _____ are copies of network files that are stored on a computer so that a user can access them when they are not connected to the network.
9. _____ is another name for junk email.
10. _____ is an email validation system that is designed to verify if an email is coming from the proper email server.

■ Business Case Scenarios

Scenario 5-1: Enforcing Physical Security

You were just hired as an IT administrator for the Contoso Corporation. Across from your desk, there is a table with seven physical servers. You ask your supervisor why the servers aren't locked up. He replies that they can be easily monitored and watched. Describe a more effective way to enforce security of these servers.

Scenario 5-2: Programming Backdoors

You are hired as a security consultant for the Contoso Corporation and are working with the CIO on a new comprehensive security policy for the company. Because the CIO is not a programmer, he asks how he can prevent a programmer from creating a backdoor on programs they write. Describe your recommended solution.

Scenario 5-3: Configuring a Windows Defender Quarantine

After working on a Windows 10 computer running Windows Defender, the computer maintains quarantined files from the past several months. Is it possible to configure the computer to remove quarantined files on a weekly basis? If so, explain the steps involved.

Scenario 5-4: Protecting Your Resources

Recently, your organization has detected several instances of malware that accessed confidential information and opened backdoors to your network. You need to defend against these malware attacks, detecting and stopping the malware as soon as it is detected. Describe your recommended course of action.

Scenario 5-5: Scanning with Microsoft Baseline Security Analyzer

As an administrator for the Contoso Corporation, you need to install the newest Microsoft Baseline Security Analyzer on a Windows server and scan the computer for missing security updates and less-optimal security settings on the Windows computer. Describe the steps necessary for completing these tasks.

Scenario 5-6: Reviewing Windows Updates

As an administrator for the Contoso Corporation, you need to review Windows Updates on a Windows 10 computer by launching Internet Explorer, and going to https://blogs.technet.microsoft.com/msrc/. Read the most recent advance notification or most recent security bulletin summary and review the executive summary. Determine how many security bulletins apply to the most recent month. Describe how to run Windows Update to update your Windows system with the newest patches in Windows.

Workplace Ready

Keeping Up with Security

Maintaining security for an organization is often a full-time job that usually requires more than one person to maintain. For example, one person may be responsible for the routers and firewalls, another person may be responsible for the servers, and yet another person may be responsible for the client computers. There might also be a security manager who oversees all items related to security, including physical security. Of course, the people who are ultimately responsible for security would be the CEO, CIOs, and other executives of a company.

However, for security to be effective, remember that it requires everyone to participate. This includes the executives, who need to support the IT department and help enforce and support security-related decisions, and the IT staff to establish and monitor the security. Also, because the weakest link could well be the end users, ensuring that they receive training in best practices and are constantly reminded to use them, is key.