Lesson 7: Maintaining, Updating, and Protecting Windows 10

# Learning Objectives

Students will learn to:

* Explore built-in maintenance tools
* Configure and manage updates
* Defend your system from malicious software

# Objective Domain Skills

* Understanding maintenance tools 6.2
* Understanding storage 5.2
* Configuring desktop settings 1.2
* Configuring updates 6.3
* Configuring antivirus settings 3.3

# Lesson Summary — Lecture Notes

Lesson 7 helps students understand how to use a variety of tools to maintain, update, and protect Windows 10.

Begin the lecture by explaining that Windows 10 comes with many built-in maintenance tools that help to keep computers running at top performance. These tools include Disk Defragmenter, Disk Cleanup, Task Scheduler, and the Action Center Maintenance feature.

Disk Defragmenter can speed up your computer’s performance by defragmenting data on your hard disk. In Windows 10, the utility is set to automatically run once a week.

Disk Cleanup helps you remove unnecessary files from your computer, such as downloaded program files, temporary internet files, files that are left after running software, and much more.

Task Scheduler enables you to schedule and automate a variety of actions, such as starting programs, displaying messages, and even sending emails. You create a scheduled task by specifying a trigger, which is an event that causes a task to run, and an action, which is the action taken when the task runs.

Next, discuss Windows 10 Action Center, which is an improvement upon Security Center in previous versions of Windows. Within Action Center, you can view notifications for security features (firewall, antivirus software, and so on) and maintenance (backups, updates, and so on). Action Center provides a single interface in which you can view the status of security and maintenance features. Action Center alerts you to problems you need to correct and usually provides a way to fix it.

System Information displays a wealth of information about your computer’s hardware, drivers, and system software. If you’re having any type of system-related issues, you should check System Information for possible clues as to the source of the problem.

Next, you'll cover the Windows registry, which is a database of configuration settings for your computer. It’s often referred to as the “brains” of a Windows operating system. The registry is self-sufficient and rarely requires maintenance, but you can use a reputable registry cleaner occasionally to remove settings that are no longer used.

Intruders and some viruses, worms, rootkits, spyware, and adware gain access to a system by exploiting security holes in Windows, Internet Explorer, Microsoft Office, or other software applications. Therefore, the first step you should take to protect yourself against malware is to keep your system up to date with the latest service packs, security patches, and other critical fixes. Microsoft routinely releases security updates on the second Tuesday of each month, commonly known as Patch Tuesday. Although most updates are released on Patch Tuesday, there might be occasional patches (known as out-of-band patches) released at other times when the patches are deemed critical or time-sensitive.

In the next section, you'll explain that 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.

The next section explains how to view your update history by clicking the Update history option. On the Update history page, each update, includes the KB article number and the date installed. If you click Successfully installed on <date> for a specific update, it provides a short description of the update.

In the past, the Windows Insider program (which was previously accessible to developers only) allowed users to sign up for early builds of the Windows operating system. Today, the Windows Insider program has been expanded to include enterprise testers and advanced users. This enables Microsoft to get feedback before a new feature or update is released to the general public and is a way to test upcoming Windows features before they are released to the general public.

Enterprise companies are usually not willing to upgrade to the newest version of Windows, and most responsible corporations would deploy the monthly updates that Microsoft publishes every month. However, these corporations are not usually willing to deploy new or updated features because they can cause a wide range of problems. So rather than force the new and updated features to corporations, Microsoft has developed Windows 10 servicing options, which allow you to configure devices into one of three tiers based on how often you want these features deployed.

Next, students will learn that one of the most challenging problems for computer users and administrators is to prevent viruses, worms, and other types of malicious software — sometimes called malware, it is software designed to infiltrate or affect a computer system without the owner’s informed consent — from infecting your computer. To protect against malicious software, make sure your system is updated, you are using a firewall to limit exposure to malware, and you are using an up-to-date anti-malware software package.

Windows Firewall comes with Windows 10 and other Windows versions to protect your computer from traffic entering through communications ports. A firewall is a software program or device that monitors traffic entering and leaving a computer. This term comes from the building trades where it refers to a special barrier designed to delay the advance of fire from one area to another. In the computer world, threats and attacks from malicious insiders are the “fire” advancing on computers connected to the internet.

Lastly, you'll cover Windows Defender, which is designed to protect your computer against viruses, spyware, and other types of malware. It protects against these threats by providing real-time protection in which it notifies you if malware attempts to install itself on your computer or when an application tries to change critical settings.

TAKE NOTE: In the OneNote portion of this course, we include a blank space between the backward slashes that indicate the beginning of a network path (\\) and a server address (such as server\share\folder), to prevent them from becoming live links. In actual usage, there would be no space after the slashes.

# Key Terms

**action –** In Task Scheduler,the action taken when the task runs.

**Action Center** – A Windows feature that provides a single interface in which users can view the status of security and maintenance features. Action Center alerts users to problems they need to correct and usually provides a way to fix it.

**critical update** – A broadly released fix for a specific problem addressing a critical, non-security-related bug.

**cumulative patch** – Multiple hotfixes combined into a single package.

**Current Branch (CB) servicing** – A Windows servicing option in which upgrades are received immediately after Microsoft makes them publicly available.

**Disk Cleanup** – A Windows utility that removes many different kinds of unnecessary files from a computer, such as downloaded program files, Temporary Internet files, offline web pages, files in the Recycle Bin, setup log files, and temporary files left by programs.

**Disk Defragmenter** – A Windows utility that helps improve a computer’s performance by moving sectors of data on the hard disk, so that files are stored sequentially. This minimizes the movement a hard disk’s arm must make to read all of the sectors that make up a file or program.

**firewall** – A software program or device that monitors traffic entering and leaving a computer.

**fragmented –** The state of a disk in which portions of files are spread across sectors on different parts of the disk.

**hotfix –** 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.

**Long-Term Servicing Branch (LTSB) servicing** – Intended for scenarios during which changes to software running on devices is limited to only essential updates (vulnerabilities and other important issues). Only Windows 10 Enterprise LTSB supports LTSB.

**malicious software** – Viruses, worms, and other forms of malware that may attack a computer connected to the internet.

**Microsoft Windows Malicious Software Removal Tool** – Scans your computer for dangerous malware and attempts to remove it immediately.

**out-of-band patch** – An occasional patch released at a time when the patch is deemed critical or time-sensitive.

**Patch Tuesday** – The second Tuesday of each month, when Microsoft routinely releases security updates.

**security update** – A broadly released fix for a product-specific, security-related vulnerability.

**service pack** – 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.

**signature** – A sequence of text or code that’s programmed into a virus and uniquely identifies it. Antivirus software uses an anti-malware engine to find viruses and other malware on a computer.

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

**Task Scheduler** – A Windows feature that enables users to schedule and automate a variety of actions, such starting programs, displaying messages, and sending e-mails.

**trigger** – In Task Scheduler, an event that causes a task to run.

**Trojan horse** – 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. Since 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 your computer to become unusable or it can bypass your system’s security, allowing your private information (including passwords, credit card numbers, and social security numbers) to be read. Also, a Trojan horse may execute adware.

**virus** – A program that can copy itself and infect a computer without the user’s consent or knowledge.

**Windows 10 Anniversary Update** – Released in August of 2016, it introduced a number of new features and enhancements over the previous November Update release, including new extension support for Microsoft Edge, biometric authentication support with Windows Hello, improvements to Cortana, and Windows Inking.

**Windows 10 Enterprise Long-Term Servicing Branch (LTSB)** – Similar to Windows 10 Enterprise, but a stripped-down version. It does include Internet Explorer 11 and is compatible with the Windows 32-bit version of Microsoft Office. It does not include Microsoft Edge, Windows Store Client, Cortana, Outlook Mail, Outlook Calendar, OneNote, Weather, News, Sports, Money, Photos, Camera, Music, and Clock.

**Windows Defender –** A free antispyware program provided by Microsoft.

**Windows Firewall** – A software program or device that monitors traffic entering and leaving a computer. Windows Firewall comes with Windows 10 and other Windows versions to protect a computer from traffic entering through communications ports.

**Windows Insider program** – Previously accessible to developers only, allowing users to sign up for early builds of the Windows operating system. Today, the Windows Insider program has been expanded to include enterprise testers and advanced users. This enables Microsoft to receive feedback before a new feature or update is released to the general public and is a way to test upcoming Windows features before they are released to the general public.

**Windows registry** – A database in Windows that stores user preferences, file locations, program configuration settings, startup information, hardware settings, and more. In addition, the registry stores the associations between file types and the applications that use them.

**Windows Update** – A service that keeps a Windows system patched and updated is vitally important to maintaining proper security.

**worm** – A self-replicating program that replicates itself to other computers over the network without any user intervention.

# Knowledge Assessment

## Multiple Choice

**Select the correct answer for each of the following questions.**

1. Which of the following Windows built-in utilities helps delete unnecessary files from a computer?

a. Disk Defragmenter

b. Disk Cleanup

c. Task Scheduler

d. Registry Editor

2. Which of the following Windows built-in utilities helps improve a computer’s performance by moving sectors of data on the hard disk?

a. Disk Defragmenter

b. Disk Cleanup

c. Task Scheduler

d. Registry Editor

3. In Task Scheduler, which of the following commands creates a task using a wizard?

a. Create Task

b. Create Scheduled Task

c. Create Task Automatically

d. Create Basic Task

4. In Windows Defender, which of the following scans is not an available option?

a. Quick

b. Full

c. Partial

d. Custom

5. Which of the following is not part of the Maintenance section in Action Center?

a. Check for solutions to problem reports

b. Virus protection

c. Backup

d. Check for updates

6. If Action Center detects a maintenance or security issue that needs attention, which of the following indicate errors that require immediate attention?

a. A red circle with white X

b. A yellow triangle with a black exclamation point

c. An orange flashing triangle

d. A green box

7. By default, the Windows 10 Disk Defragmenter utility is set to run how often?

a. Every day

b. Once a week

c. Biweekly

d. Once a month

8. Which of the following programs are always updated on Patch Tuesday?

a. Windows Defender

b. The Microsoft website

c. The Malicious Software Removal Tool

d. The Windows Firewall

9. Which of the following tools should be used to remove malware such as Mydoom from an infected computer?

a. Malicious Software Removal Tool

b. Windows Firewall

c. Windows Defender

d. Task Scheduler

10. Which of the following Windows 10 Servicing options receives updates immediately after Microsoft makes them publicly available?

a. CB

b. CBB

c. LTSB

d. CTSB

## Fill in the Blank

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

1. A hard disk that is fragmented has file data spread across many different sectors.

2. Disk Cleanup is a utility that removes many kinds of unnecessary files from a computer.

3. In Task Scheduler, a trigger is an event that causes a task to run.

4. The Windows registry is a database in Windows that stores user preferences, file locations, program configuration settings, startup information, hardware settings, and more.

5. Microsoft provides regularly scheduled updates to the Windows operating system via the Windows Update feature.

6. Windows Update delivers updates for Microsoft software in addition to the Windows operating system.

7. Malware describes a wide variety of malicious software, such as viruses and worms that attack computers.

8. A service pack is a collection of updates issued from Microsoft after the last version of Windows or another Microsoft product was released.

9. Windows Defender is Microsoft's free antimalware program.

10. System Information is used to view the computer’s hardware, drivers, and system software.

## True / False

**Circle T if the statement is true or F if the statement is false.**

**T F** 1. Microsoft includes Windows built-in maintenance tools in the Maintenance Tools folder in Accessories.

**T F** 2. Disk Cleanup can be run on demand, but the utility does not have its own scheduling feature.

**T F** 3. Windows Update provides hotfixes and service packs for Windows computers.

**T F** 4. Windows Defender protects only against spyware.

**T F** 5.Windows Firewall is enabled automatically in new installations of Windows 10.

# Business Case Scenarios

## Scenario 7-1: Automating Computer Maintenance and Program Launching

Maria is a busy freelance writer who uses her computer several hours a day to research and write articles for several national magazines and newspapers. Her computer, which runs Windows 10 Professional, must be running at peak performance with little downtime. Maria has little time to devote to computer maintenance tasks. She also uses Internet Explorer 11 and Microsoft Word 2016 every day and would like them to start automatically when Windows starts. Maria asks you for insight on how to maintain her computer with relatively little effort, and how to configure her computer to start programs automatically. Describe your recommended solution.

Advise Maria to ensure that Disk Defragmenter is scheduled to run at least once a month, that Windows Firewall is enabled and operating correctly, that she has real-time protection installed such as an antivirus program or internet security suite, and that Windows Update is enabled to check for updates automatically. She should configure Task Scheduler to run Disk Cleanup weekly and set Internet Explorer 11 and Microsoft Word 2016 to start when Windows starts.

To schedule Disk Cleanup to run weekly and the other programs to start when Windows starts, she should select the Create Basic Task in Task Scheduler. The wizard will guide her through the prompts. For the trigger, she should select Weekly. In the Weekly screen, she should select a start date, time, and the day of the week Disk Cleanup will run. In the Start a Program screen of the wizard, she should click Browse, click Disk Cleanup, navigate to the Disk Cleanup program, select it, and then click Open. (Disk Cleanup is located in the Accessories/System Tools folder.) When she completes the wizard, Disk Cleanup will be added to her scheduled tasks list.

The same general steps apply to Internet Explorer 11 and Word 2016, but for each program, she will select When the computer starts as the trigger. She will need to browse to locate the Internet Explorer 11 executable file and the Word 2016 executable file.

## Scenario 7-2: Removing Viruses Safely

You are a support person for a computer consulting company. Rajeem is an independent tax consultant who calls you to report that he believes he infected his computer with a virus after downloading and installing a tax-related utility from the web. Describe your recommended solution.

Tell Rajeem to download and run the Microsoft Windows Malicious Software Removal Tool. Have him perform a full scan of his computer and remove any infections the tool detects. When his system is clean, ensure that he has a reputable, current antivirus software program installed on his computer, such as Windows Defender.

## Scenario 7-3: Gathering System Information

In an effort to troubleshoot an issue on a client computer, you posted a message on an online PC support forum. The forum moderator posts a message asking you to list all of the programs that launch at startup on the affected computer. Describe the easiest way to provide this information.

On the affected computer, open System Information. Expand the Software Environment category, click the Startup Programs category, click File > Export and then save the file to the desktop or another location that’s easy to access. Open the .txt file, highlight all information, copy the information, and then paste the information in a reply to the support forum moderator, along with a short message.

## Scenario 7-4: Distributing Windows Updates Across a Network

You support a brokerage firm that employs 20 brokers. Each broker has his own client computer, and the firm has a server running Windows Server. All the client computers are configured identically.

Over the past six months, some Windows updates have caused the computers to stop responding, leaving the brokers without computers to conduct business. Describe how to ensure that the Windows updates that install on client computers will not cause usability issues.

Implement WSUS on the brokerage firm’s server and set up a test client computer that’s configured exactly as the broker’s computers. When new updates and hotfixes are available through Windows Update, test them on the test computer. Install only approved updates and hotfixes over the network to client computers.