LESSON 3.1

98-349 Windows Operating System Fundamentals

Understand Application Installations

LESSON 3.1

98-349 Windows Operating System Fundamentals

Lesson Overview

Understand application installations

In this lesson, you will:

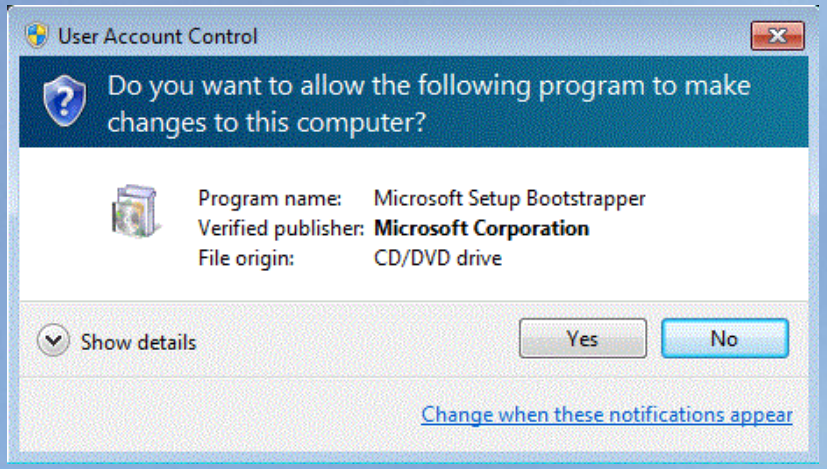
- Identify various application installation options.
- Install applications locally.
- Explore Group Policy to install applications.
- Remove installed applications.

Application Installation Methods

- Local installation—Software is installed using a downloaded executable or media such as CD, USB, or DVD. Software can be installed through a provided software setup program.
- Network installation—Software is installed using a network software distribution point or scripting technologies.
- Group Policy—Software is installed to the system using a Group Policy object (GPO).

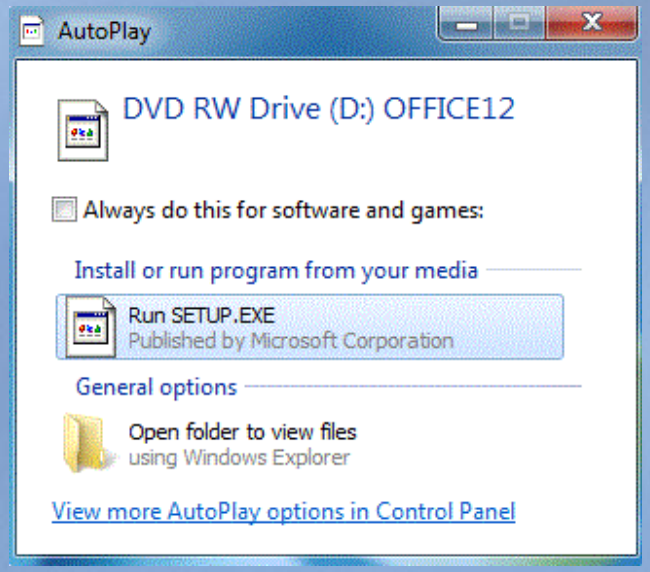
Installing Applications Locally

- Installation of software applications requires elevated privileges.
- The standard user will be prompted by User Account Control (UAC).
- UAC is a feature in Windows that can help the user stay in control of the computer by issuing notices when a program makes a change that requires administrator-level permission.
- Insert the software media and follow the instructions on the screen.



Installing Applications Locally (continued)

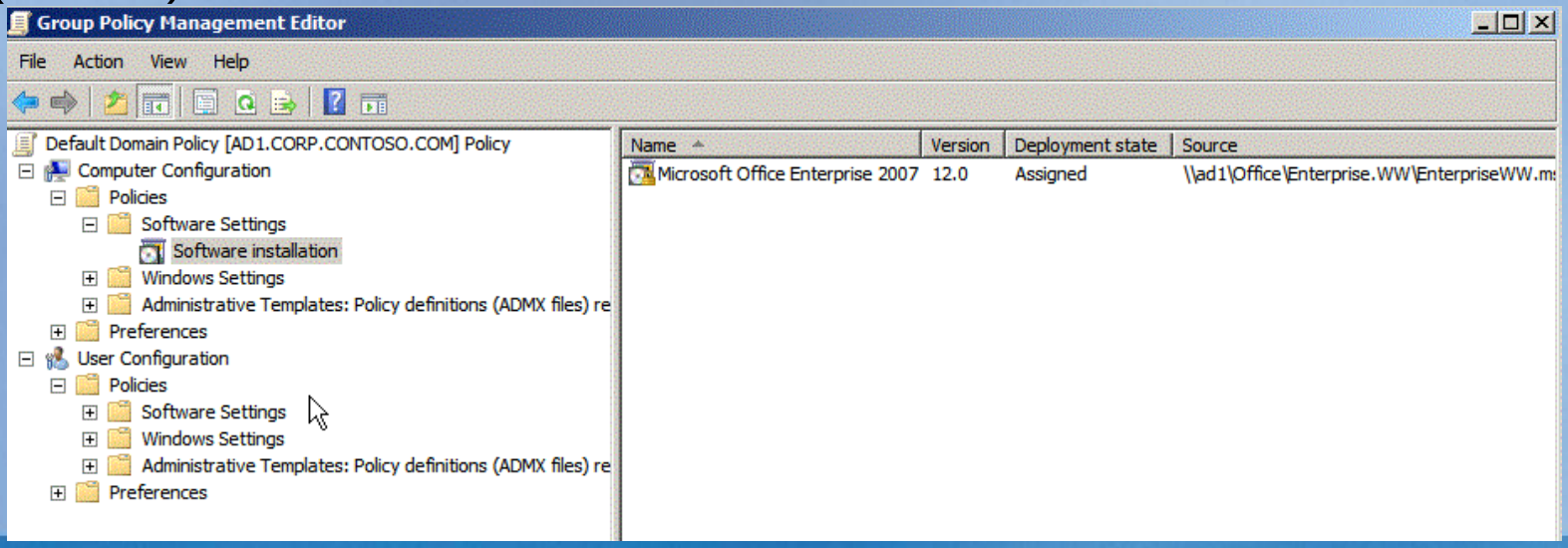
- Most software applications are packaged with an AutoPlay feature that will start the installation after the media is loaded.



- If the software does not load automatically, check the program documentation. Most software contains a setup file that is named either Setup.exe or Install.exe.

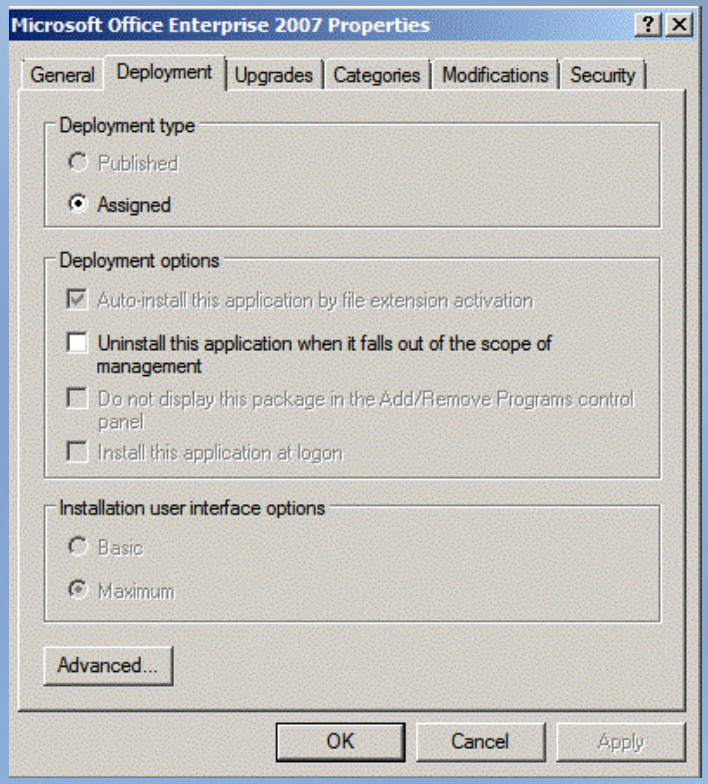
Using Group Policy

- Companies use various methods to deploy software applications rapidly across the network, including Group Policy Software Installation.
- Group Policy Software Installation enables software management throughout its life cycle. Group Policy Software Installation works in conjunction with Group Policy and Active Directory Domain Services (AD DS).



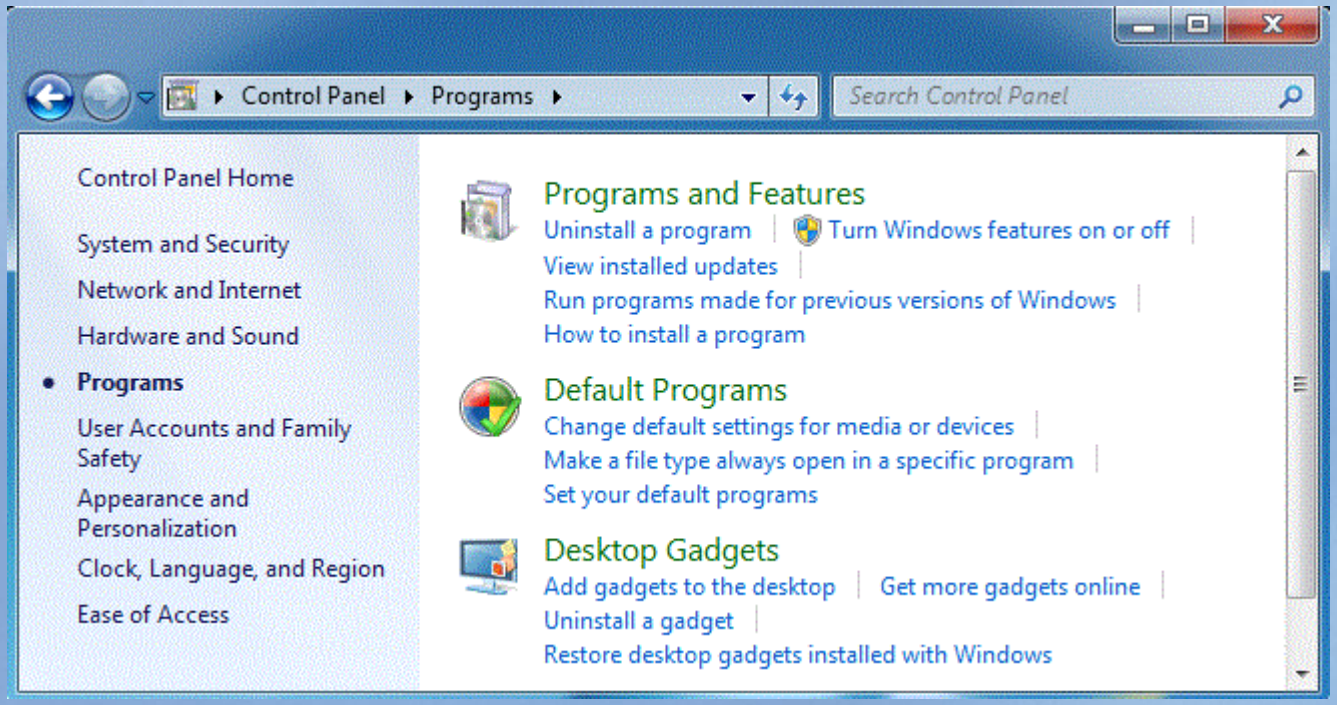
Using Group Policy (continued)

- Group Policy enables centralized management of software deployment, including uninstalling, upgrading, or modifying software packages.



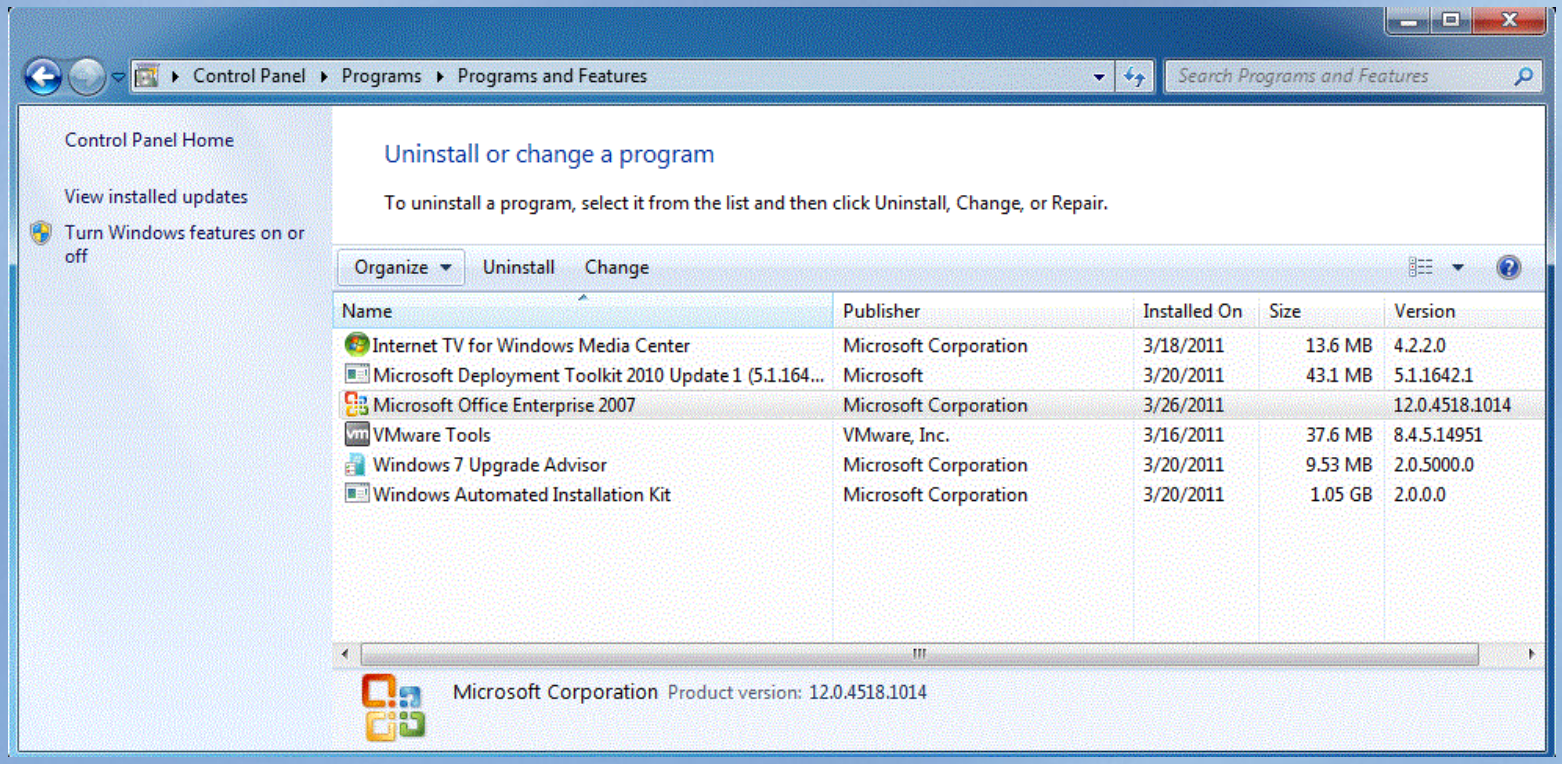
Removing Installed Applications

- Software can be removed through the Programs category in Control Panel.



Removing Installed Applications (continued)

- Highlight the software that you want to uninstall and click Uninstall.
- The uninstall process may differ from one software package to another.



Complete Student Activity 3.1

LESSON 3.2

98-349 Windows Operating System Fundamentals

Understand User Account Control (UAC)

LESSON 3.2

98-349 Windows Operating System Fundamentals

Lesson Overview

Understand how to manage user account control (UAC)

In this lesson, you will:

- Differentiate standard users and administrative users
- Define UAC
- Identify UAC Group Policy settings
- Configure UAC

Differentiating Between Standard and Administrative Users

- A standard user account enables users to do the following:
  - Use most of the capabilities of the computer
  - Use most programs that are installed on the computer
  - Change settings that affect that user account
- A standard user account prevents the user from doing the following:
  - Installing or uninstalling some software and hardware
  - Deleting files that are required for the computer to work
  - Changing settings that affect other users or the security of the computer

Differentiating Between Standard and Administrative Users (continued)

- An administrator account enables users to do the following:
  - Make changes that will affect other users
  - Configure security settings
  - Install software and hardware
  - Gain access to all files on the computer
  - Make changes to other user accounts
- An administrator account doesn't have any restrictions on the computer.

User Account Control (UAC)

- User Account Control (UAC) is a feature in Windows that helps the user stay in control of the computer by issuing notices when a program makes a change that requires administrator-level permission. UAC works by adjusting the permission level of your user account.
- When changes are going to be made to the computer that require administrator-level permission, UAC notifies the user.
  - If logged on as an administrator, you can click Yes to continue.
  - If logged on as a standard user, someone with an administrator account must enter his or her password.
  - If permission is granted, rights are temporarily granted to complete the task, and then permissions return to those of a standard user.

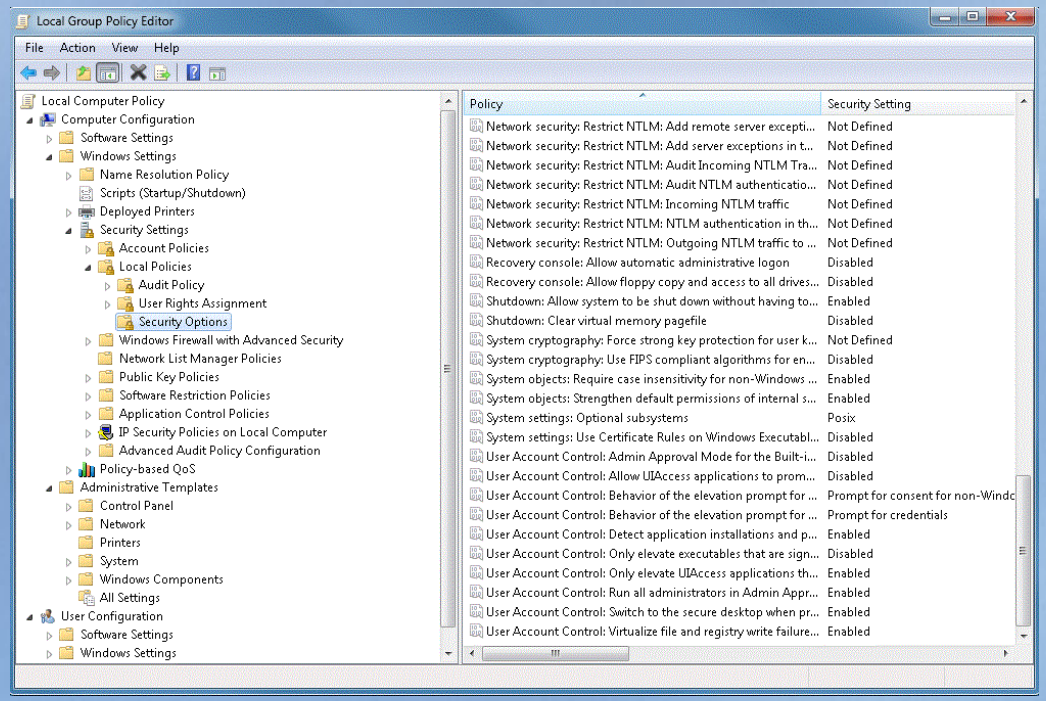
UAC (continued)

- UAC notifications:

Icon	Type	Description
	A setting or feature that is part of Windows needs permission	Microsoft is the publisher of this item
	A program that is not part of Windows needs your permission to start.	Program has a valid digital signature
	A program with an unknown publisher needs your permission	Program doesn't have a digital signature
	You have been blocked by your system administrator	Program is unknown or untrusted

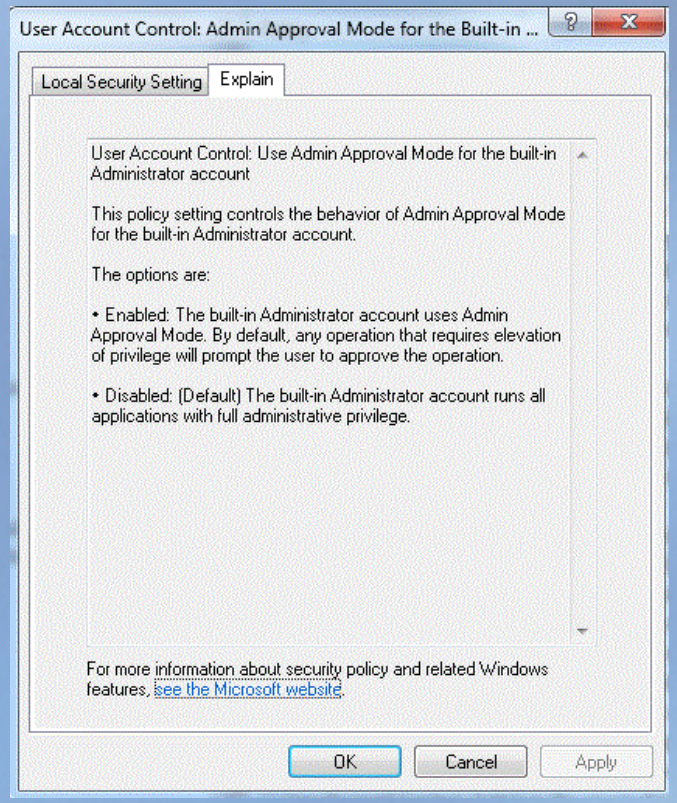
UAC Group Policy Settings

- UAC can be controlled by configuring Group Policy settings.
- Click Start and in the Search programs and files field, type **gpedit.msc**. Press ENTER.



UAC Group Policy Settings (continued)

- Explanations of each policy setting can be found by double-clicking the policy setting and clicking the Explain tab.



Configure UAC

- UAC can be configured at the application level or the system level.
- To run an application in elevated mode, perform these steps:
  1. Right-click an application icon or name that is not an administrative application.
  2. Select Properties.
  3. Select the Compatibility tab.
  4. Locate Privilege Level and select Run This Program As An Administrator.
  5. Click OK.

Configure UAC (continued)

- UAC can be turned on or off at the system level. You must be logged in as an Administrator to modify UAC settings.
- Turning off UAC reduces computer security and may expose it to increased risk from malicious software.
- To modify UAC, perform these steps:
  1. Click Start and Control Panel.
  2. Click User Accounts And Family Safety.
  3. Click User Accounts.
  4. Click Change User Account Control Settings.
  5. Click and drag the slide button to the desired setting. Dragging the button to Never Notify turns off UAC.

Complete Student Activity 3.2

LESSON 3.3

98-349 Windows Operating System Fundamentals

Remove Malicious Software

LESSON 3.3

98-349 Windows Operating System Fundamentals

Lesson Overview

How can malicious software be removed from a computer?

In this lesson, you will:

- Identify computer security threats
- Identify security tools
- Explore the Windows Action Center

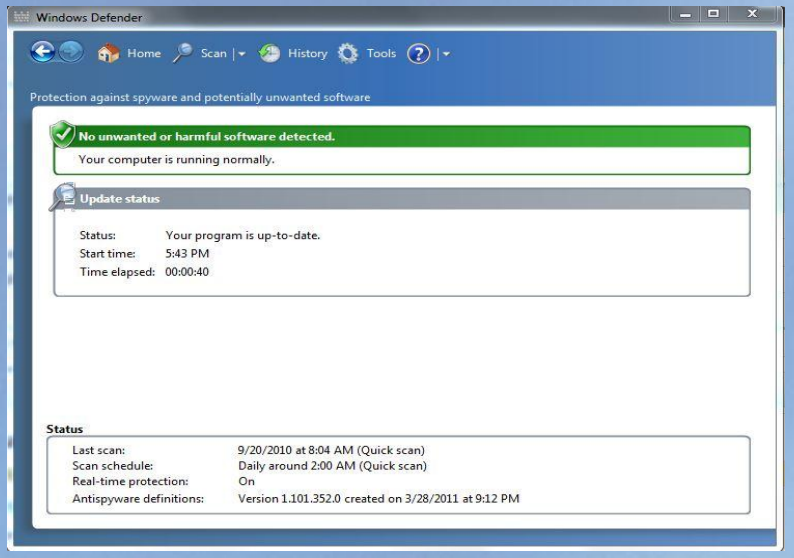
Computer Security Threats

- **Trojan horse**—a malicious application that is unable to spread of its own accord. Historically, the term has been used to refer to applications that appear legitimate and useful but perform malicious and illicit activity on an affected computer.
- **Malware**—malicious software or potentially unwanted software installed without user consent.
- **Spyware**—describes a program that collects information such as the websites a user visits without user consent. Installation may be without prominent notice or without the user's knowledge.
- **Bot**—a malicious program installed on a computer that is part of a bot network. Bots are generally back-door Trojans that allow unauthorized access and control of an affected computer.

Security Tools

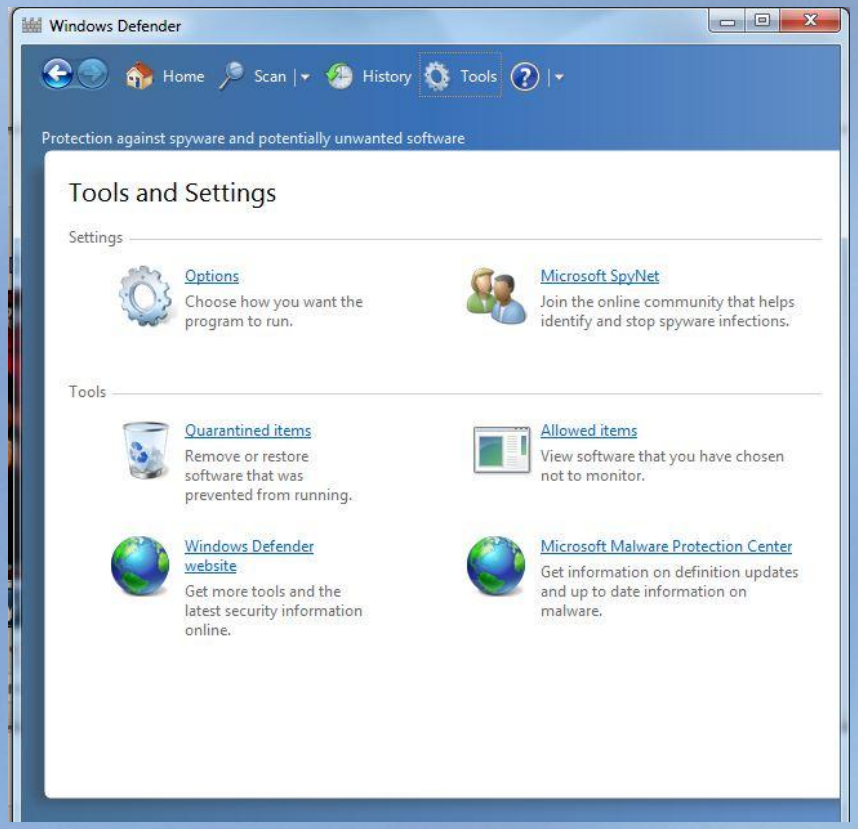
Windows Defender

- Helps protect your computer against pop-ups, slow performance, and security threats.
- Comes bundled with Windows 7.
- Detects and removes known spyware from your computer.



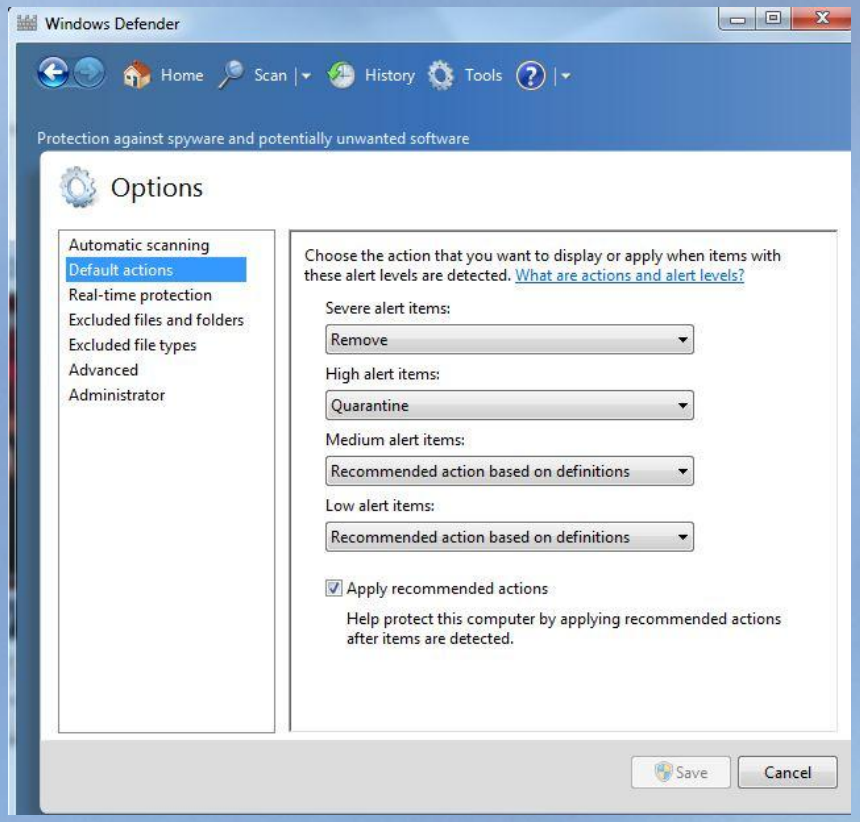
Security Tools (continued)

- The Tools And Settings window in Windows Defender allows you to change options or view Quarantined items.



Security Tools (continued)

- Windows Defender can be configured to treat alert items differently based on their severity.

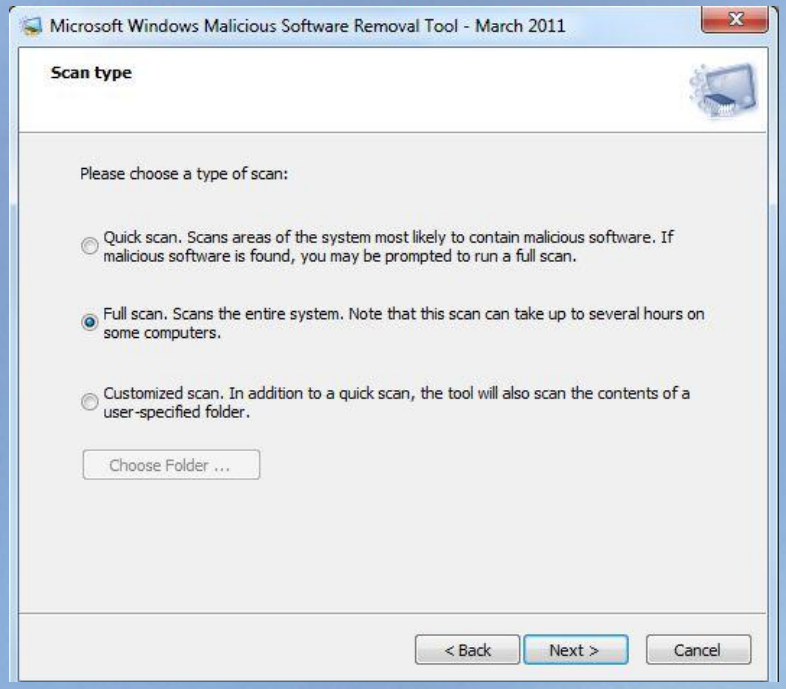


Malicious Software Removal Tool

- Checks computers running Windows 7, Windows Vista, Windows XP, Microsoft Windows 2000, Windows Server 2003, and Windows Server 2008 R2.
- Checks for infections by specific, prevalent malicious software, including Blaster, Sasser, and Mydoom, and helps remove any infection it finds.
- 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.
- Downloaded from Microsoft at the following link:
  - ***http://www.microsoft.com/security/pc-security/malware-removal.aspx***

Malicious Software Removal Tool (continued)

- After the download, browse to the file location and double-click the file.
- Follow the wizard instructions and scan for any malicious software.



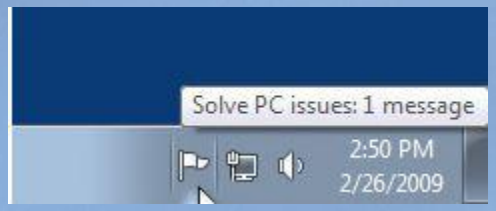
More Security Tools

Antivirus software can prevent threats from infecting your systems.

- Microsoft Security Essentials
  - Free download for personal use and small business.
  - http://www.microsoft.com/en-us/security_essentials/default.aspx
- Microsoft Forefront Endpoint Protection
  - An enterprise-based solution.
  - http://www.microsoft.com/forefront/endpoint-protection/en/us/default.aspx

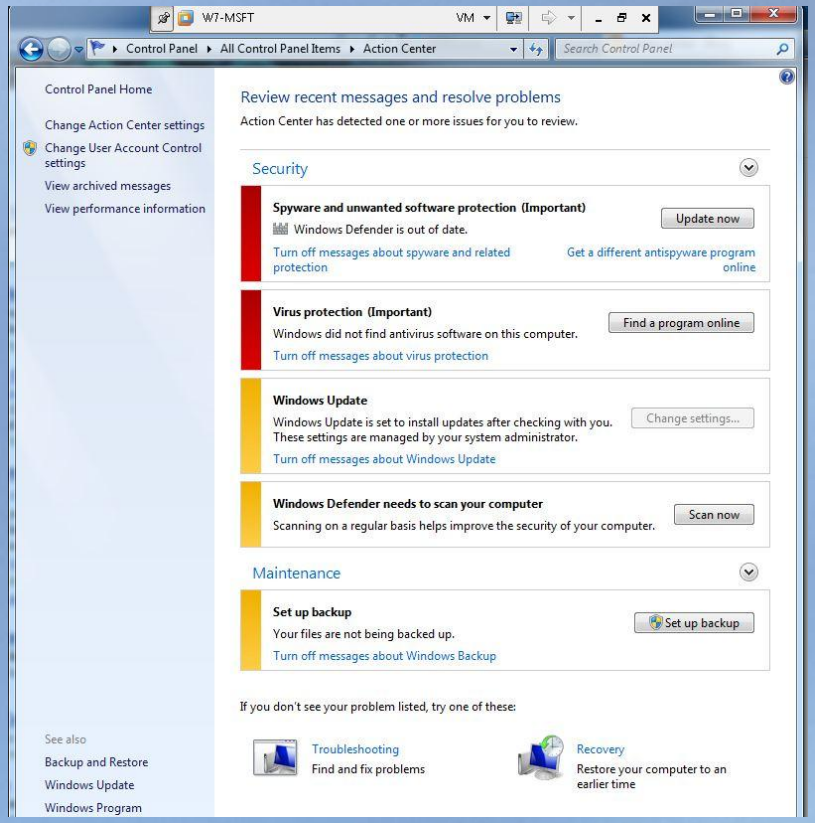
Action Center

- Windows Action Center is a central place to view alerts and take actions that can help keep Windows running smoothly.
- Lists important messages about security and maintenance settings that need your attention.
  - Red items in Action Center are labeled Important, and indicate significant issues that should be addressed soon.
  - Yellow items are suggested tasks that you should consider addressing, like recommended maintenance tasks.
- Action Center messages can be viewed quickly by placing your mouse over the icon in the notification area.



Action Center (continued)

- Action Center can be found by clicking Start, Control Panel, and typing **Action Center** in the search field.



Complete Student Activity 3.3

LESSON 3.4

98-349 Windows Operating System Fundamentals

Understand Services

LESSON 3.4

98-349 Windows Operating System Fundamentals

Lesson Overview

Understanding services

In this lesson, you will:

- Explore Windows services.
- Learn to manage Windows services.

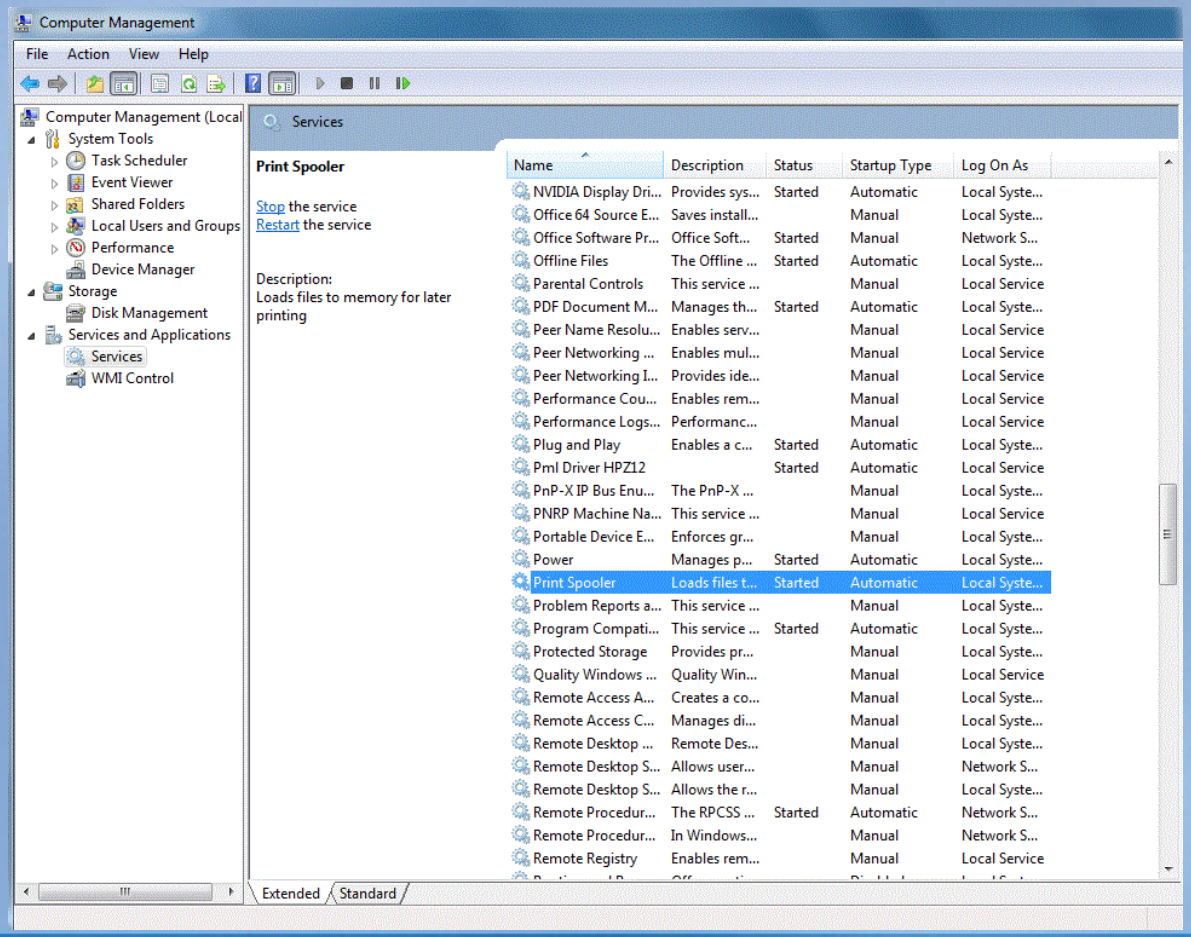
Windows Services

- Windows Services include an application type that runs in the system background without a user interface.
- Provide core operating system features, such as event logging, file serving, printing, cryptography, and error reporting.
  - Antivirus software runs as a Windows service.
- Installed and running services will vary from machine to machine based upon software or features installed.
- Access Services by clicking Start, typing **services.msc** in the Search programs and files field, and pressing ENTER.
- You also can access Services through the Computer Management application as follows:
  - Click Start, right-click Computer and select Manage, locate and expand Services And Applications, and select Services.

LESSON 3.4

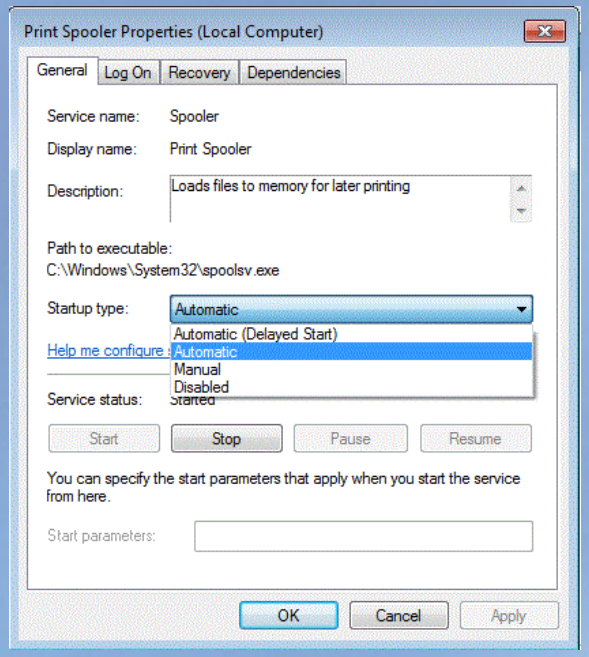
98-349 Windows Operating System Fundamentals

Windows Services (continued)



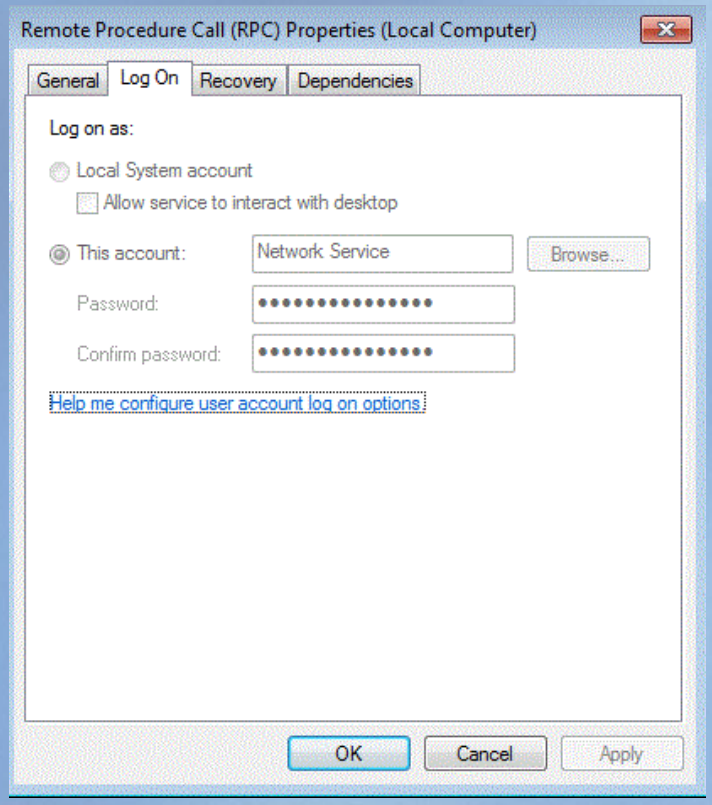
Managing Windows Services

- Four startup types:
  - Automatic (Delayed Start), Automatic, Manual, and Disabled.
- Disabling a service can help optimize the operating system if the service is not needed.



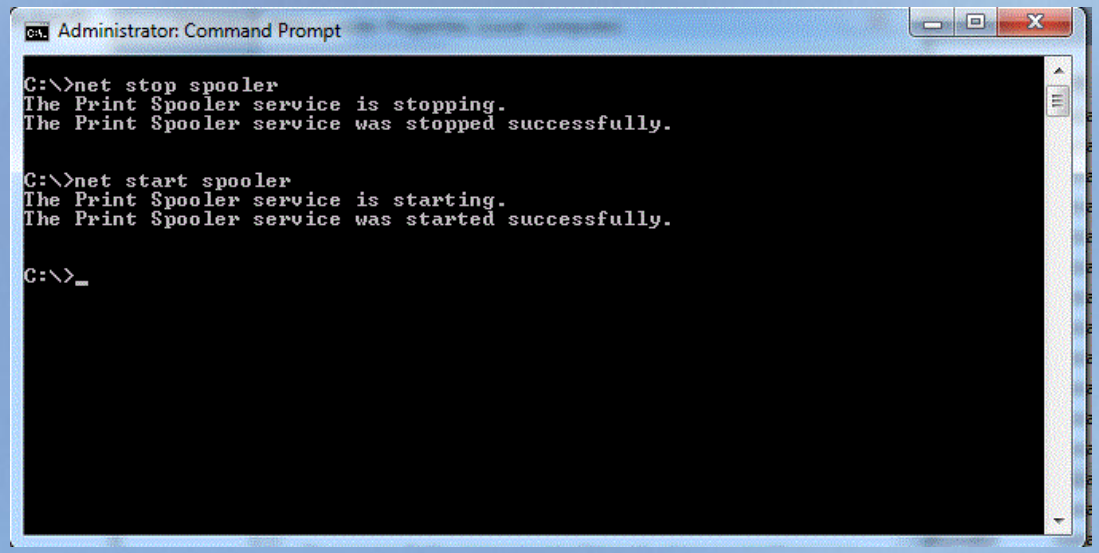
Managing Windows Services (continued)

- Windows services require authentication to run.
- Logon options:
  - Network Service
  - Local System Account
  - User Account



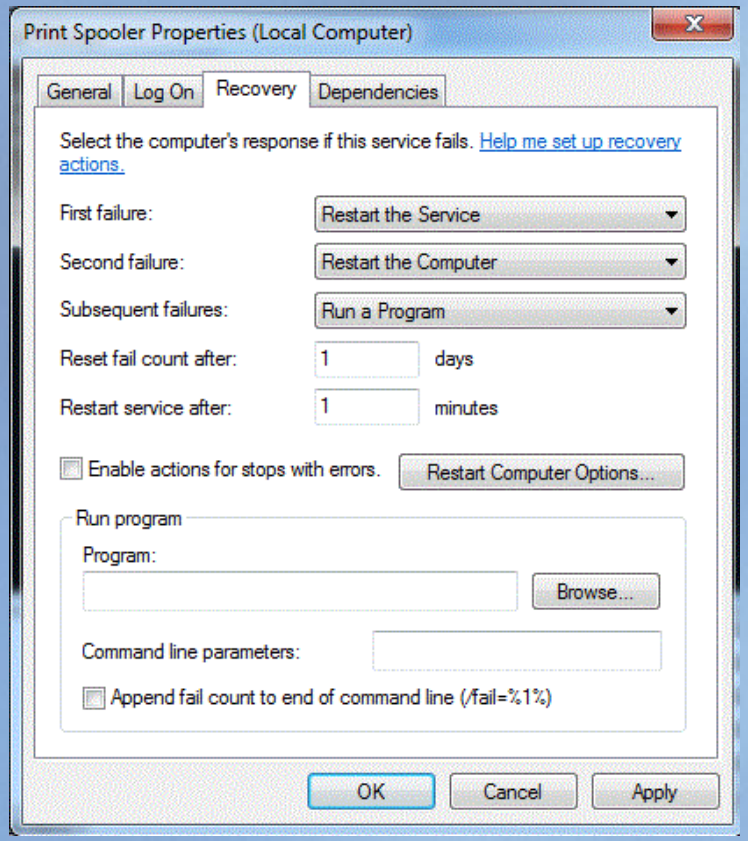
Managing Windows Services (continued)

- Services can be started, stopped, and restarted using Services.msc and the Computer Management Services snap-in.
- Services can be started and stopped through the command-line interface.



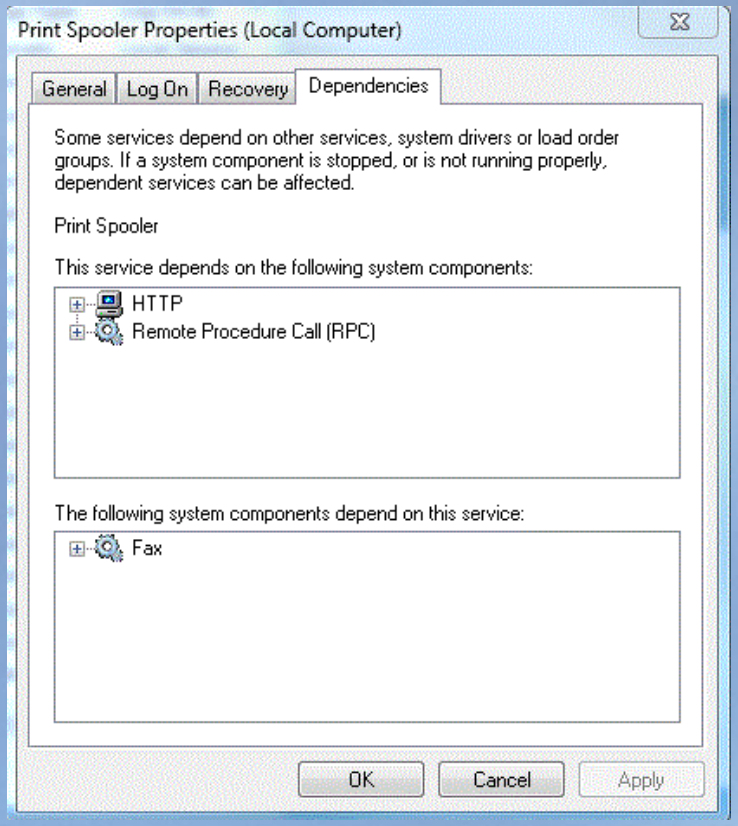
Managing Windows Services (continued)

- Services can be configured to respond to multiple failures.
  - Restart The Service
  - Restart The Computer
  - Run A program



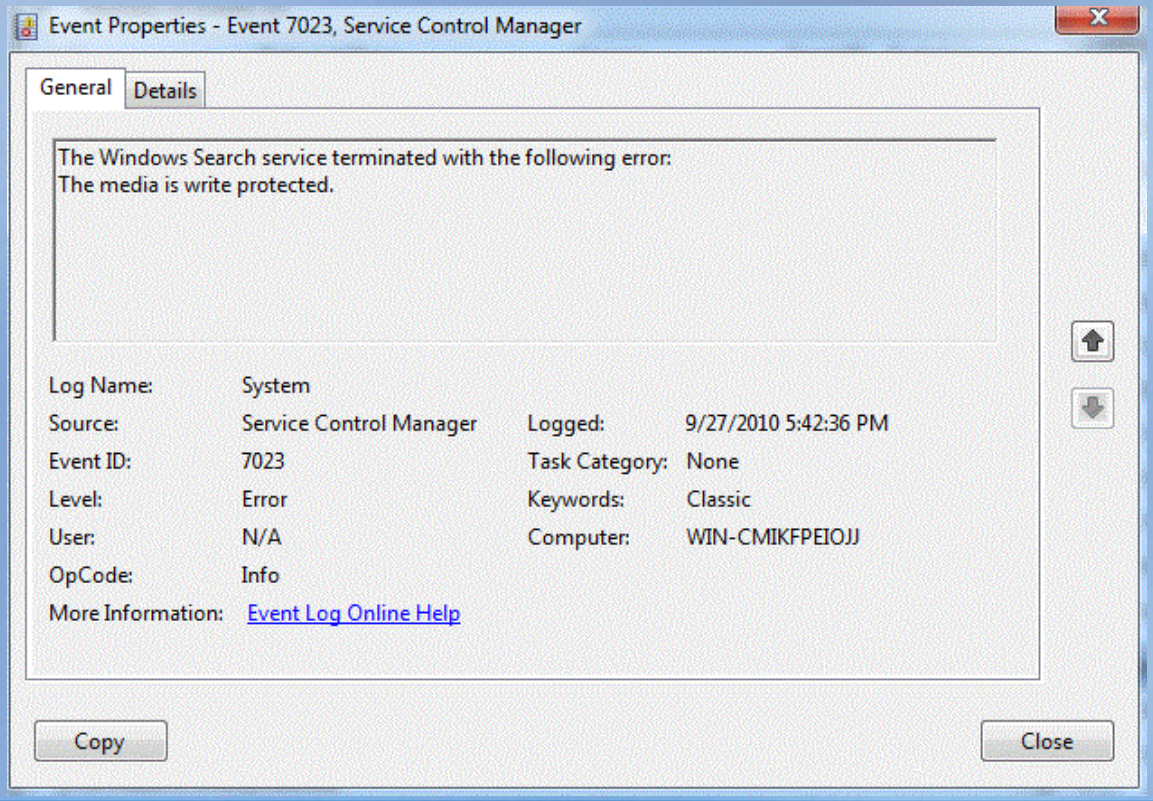
Managing Windows Services (continued)

- Services can also be dependent on other services.



Managing Windows Services (continued)

- An event is written to the System Event log when a service fails to start.



Complete Student Activity 3.4

LESSON 3.5

98-349 Windows Operating System Fundamentals

Understand Application Virtualization

LESSON 3.5

98-349 Windows Operating System Fundamentals

Lesson Overview

Understanding application virtualization

In this lesson, you will explore:

- Application virtualization
- Remote Desktop Services (RDS)
- Microsoft Enterprise Desktop Virtualization (MED-V)

Application Virtualization

- Application virtualization can take on many forms and has several definitions.
- A virtual application is an application that can run in a self-contained, virtual environment.
- The virtual environment contains the information necessary to run the application on the client without installing the application locally.

Application Virtualization (continued)

- A software technology that allows you to isolate a specific application from the operating system and other applications.
- Applications can be made available to the user's computer without having to install the application directly to the computer.
- Each application runs in its own virtual environment.
- Virtualization eliminates application conflicts.
- Virtualization allows the application to interact with the client.

Microsoft Application Virtualization (App-V)

- Microsoft software technology that transforms applications into centrally managed services that are never installed and don't conflict with other applications.
- Allows administrators to configure traditional or earlier applications into centrally managed, virtual applications.
- Integrates with System Center Configuration Manager so that you can manage virtual and physical applications.
- Benefits include:
  - Reducing application conflict
  - Centralizing and simplifying patch management
  - Accelerating new application deployment

Remote Desktop Services (RDS)

- RDS is a hosted application server.
- RDS uses RemoteApp to deploy applications to client machines.
- RDS is packaged with Windows Server 2008 R2.
- RemoteApp programs are applications that are accessed through Remote Desktop and appear as if they are running on the client's local computer.
- Applications are installed on the RDS server and can be deployed through a variety of methods.
- Applications are updated only on the server.
- RDS can be used to help implement Microsoft's Virtual Desktop Infrastructure (VDI).

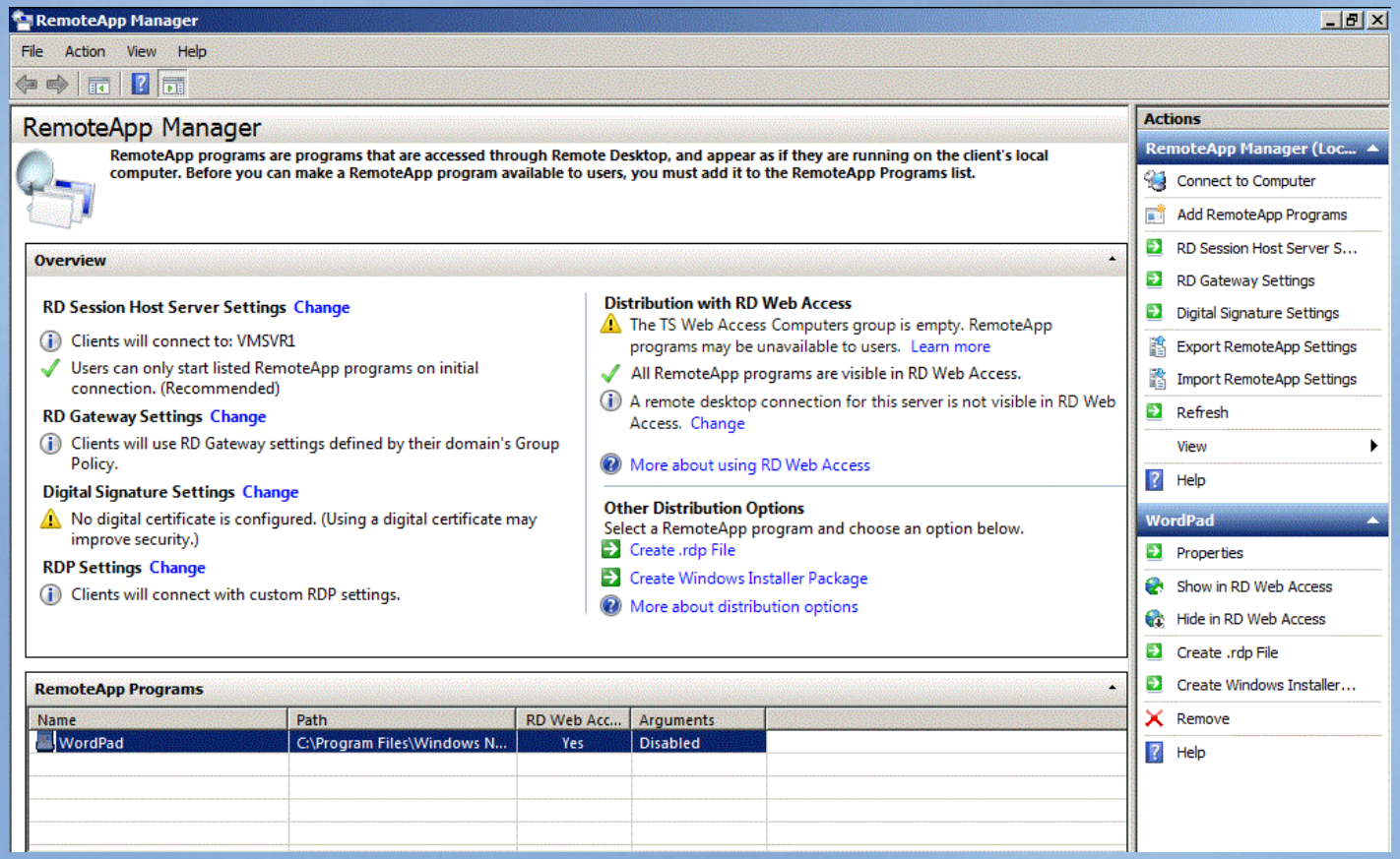
RDS (continued)

- Users can access RemoteApp programs in several ways:
  - Access a link to the program through RemoteApp and Desktop Connection by using Remote Desktop Web Access (RD Web Access).
  - Double-click a Remote Desktop Protocol (.rdp) file that has been created and distributed by their administrator.
  - Double-click a program icon on the desktop or Start menu item that has been created and distributed by the administrator with a Windows Installer (.msi) package.
  - Double-click a file where the file name extension is associated with a RemoteApp program. This can be configured by their administrator with a Windows Installer package.

LESSON 3.5

98-349 Windows Operating System Fundamentals

RDS (continued)

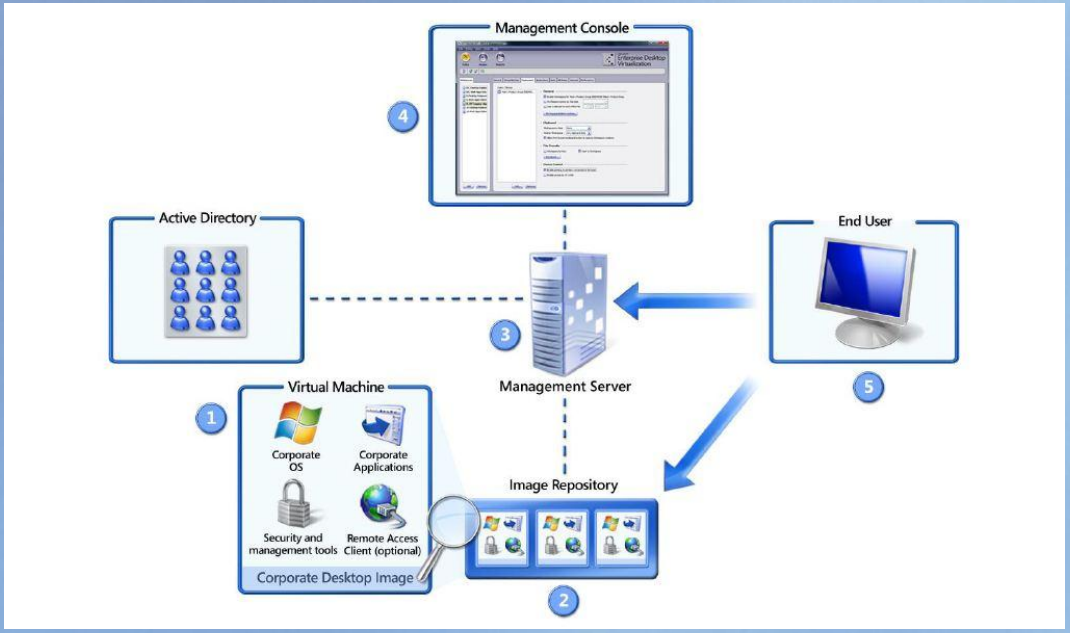


Microsoft Enterprise Desktop Virtualization (MED-V)

- MED-V is an integral component of the Microsoft Desktop Optimization Pack.
- Uses Microsoft Virtual PC to provide an enterprise solution for desktop virtualization.
- Removes the barriers to Windows upgrades by resolving application incompatibility with Windows 7 and delivering applications in a Windows XP-based application compatibility workspace.
- Allows users to start legacy applications from the Start menu in Windows.
- Applications appear and operate as if they were installed on the desktop

MED-V (continued)

- The MED-V solution has the following components:
  1. Administrator-defined virtual machine
  2. Image repository
  3. Management server
  4. Management console
  5. User client



Complete Student Activity 3.5