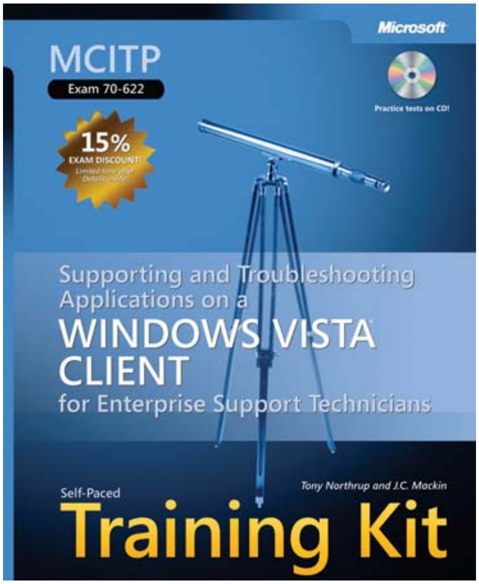


MCITP Self-Paced Training Kit (Exam 70-622): Installing, Maintaining, Supporting, and Troubleshooting Applications on a Windows Vista™ Client for Enterprise Support Technicians

Tony Northrup and
J.C. Mackin

To learn more about this book, visit Microsoft Learning at
http://www.microsoft.com/MSPress/books/10931.aspx

9780735624085

Table of Contents

Chapter 5

Protecting Internet Explorer and Other Applications

In recent years more and more security compromises are initiated when users visit a website. For example, websites might trick the user into providing confidential information, or they might exploit a vulnerability in the browser to run code without the user's explicit permission. In Windows Vista, Microsoft Internet Explorer 7.0 includes several features to reduce this risk.

Although Windows Vista is designed to minimize security risks out of the box, attackers are constantly developing new security vulnerabilities. To adapt to changing security risks, you must deploy updates to your client computers. Additionally, Windows Defender (a tool that helps give users control over the software installed on their computers) requires Windows Vista to regularly install updated definitions.

This chapter describes how to manage Internet Explorer, how to best deploy updates to Windows Vista client computers, and how to troubleshoot problems with Windows Defender.

Exam objectives in this chapter:

- Configure and troubleshoot security for Windows Internet Explorer 7+.
- Troubleshoot Windows Defender issues.
- Apply security patches and updates.
- Apply and troubleshoot updates.
- Support deployed applications.
- Maintain desktop applications.

Lessons in this chapter:

Before You Begin

To complete the lessons in this chapter, you should be familiar with Windows Vista and be comfortable with the following tasks:

- Installing Windows Vista and joining a domain
- Configuring Group Policy settings
- Performing basic configuration tasks of Microsoft Windows Server 2003 domain controllers

To complete the practice exercises in this chapter, you should have

- A lab environment with one Windows Server 2003 domain controller, one Windows Vista client computer that is a member of that domain, and, optionally, a second Windows Vista client computer that is not a member of a domain.

Lesson 1: Configuring and Troubleshooting Internet Explorer Security

Internet Explorer is one of the most important components of the Windows Vista operating system because it provides access to Web applications on both the public Internet and on internal intranets. However, because it might be used to access untrusted websites, security is a serious concern. In the past, attackers have used websites to trick users into disclosing private information, to gain elevated privileges on client computers, and to distribute malware.

How Internet Explorer Works in 64-bit Versions of Windows Vista

Because it provides a wider data bus, allowing many times greater scalability, 64-bit computing is the future. Right now, however, most users run 32-bit versions of Windows.

Unfortunately, although 64-bit versions of Windows are fundamentally superior, in the real world they do have some compatibility problems. In particular, 64-bit versions of Internet Explorer can't use 32-bit components (such as ActiveX controls, which might provide critical functionality for many websites). Although 64-bit components are becoming more common, some critical components still aren't available for 64-bit.

For that reason, the 32-bit version of Internet Explorer is the default even in 64-bit versions of Windows. If a user instead chooses to use the 64-bit version of Internet Explorer (there's also a shortcut for it on the Start menu), test any problematic webpages in the 32-bit version of Internet Explorer before doing any troubleshooting.

MORE INFO Deploying Internet Explorer

To deploy preconfigured versions of Internet Explorer, you can use the Internet Explorer Administration Kit. For more information, visit *http://technet.microsoft.com/en-us/ie/bb219556.aspx*.

After this lesson, you will be able to:

- Configure add-ons in Internet Explorer (including ActiveX controls) and troubleshoot problems related to add-ons.
- Describe and configure Protected Mode.
- Resolve problems related to Secure Sockets Layer (SSL) certificates.

Estimated lesson time: 40 minutes

Internet Explorer Add-Ons

Add-ons extend Internet Explorer capabilities to enable websites to provide much richer, more interactive content. For example, the following are commonly used add-ons:

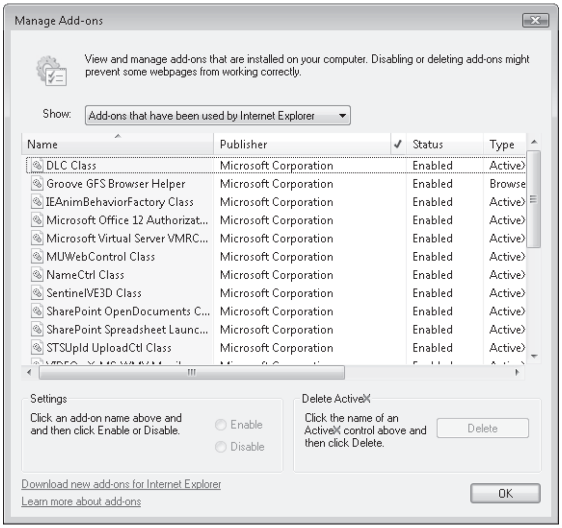
- **Shockwave Flash** An add-on that enables complex animations, games, and other interactive capabilities
- **Windows Media Player** An add-on that enables webpages to integrate audio and video
- **Microsoft Virtual Server VMRC Control** An add-on that enables users to remotely control a remote virtual machine from within Internet Explorer

The sections that follow describe how to configure add-ons and troubleshoot problems related to add-ons.

How to Enable and Disable Add-Ons

After starting Internet Explorer, you can disable or delete add-ons by following these steps:

1. Click the Tools button on the toolbar, click Manage Add-Ons, and then click Enable Or Disable Add-Ons.
2. The Manage Add-Ons dialog box appears, as shown in Figure 5-1.



View and manage add-ons that are installed on your computer. Disabling or deleting add-ons might prevent some webpages from working correctly.

Show: Add-ons that have been used by Internet Explorer

Name	Publisher	Status	Type
DLC Class	Microsoft Corporation	Enabled	Active
Groove GFS Browser Helper	Microsoft Corporation	Enabled	Browse
IEAnimBehaviorFactory Class	Microsoft Corporation	Enabled	Active
Microsoft Office 12 Authorizat...	Microsoft Corporation	Enabled	Active
Microsoft Virtual Server VMRC...	Microsoft Corporation	Enabled	Active
MUWebControl Class	Microsoft Corporation	Enabled	Active
NameCtrl Class	Microsoft Corporation	Enabled	Active
SentinelVE3D Class	Microsoft Corporation	Enabled	Active
SharePoint OpenDocuments C...	Microsoft Corporation	Enabled	Active
SharePoint Spreadsheet Launc...	Microsoft Corporation	Enabled	Active
STSUpld UploadCtl Class	Microsoft Corporation	Enabled	Active

Settings
Click an add-on name above and and then click Enable or Disable.
○ Enable
○ Disable

Delete ActiveX
Click the name of an ActiveX control above and then click Delete.

Figure 5-1 The Manage Add-Ons dialog box

3. In the Manage Add-Ons dialog box, select an add-on, and then select Disable to prevent the add-on from automatically loading. If the add-on is an ActiveX control, you can click Delete to permanently remove it.

   If an add-on is causing serious enough problems that you can't start Internet Explorer, you can disable the add-on without opening Internet Explorer by following these steps:

4. Click Start, and then click Control Panel.
5. Click the Network And Internet link.
6. Under Internet Options, click the Manage Browser Add-Ons link.
7. The Internet Properties dialog box appears.
8. Click the Manage Add-Ons button.
9. At the Manage Add-Ons dialog box, select an add-on. Then, select Disable and click OK to prevent the add-on from automatically loading.

How to Start Internet Explorer Without Add-Ons

A buggy or malicious add-on can cause problems with starting Internet Explorer. To work around this problem and launch Internet Explorer without add-ons, follow these steps:

1. Click Start. Then, click All Programs, Accessories, and System Tools.
2. Click Internet Explorer (No Add-Ons).

   Internet Explorer starts with all add-ons disabled. If a webpage opens a new window when you click on a link, that new window will also have add-ons disabled. Add-ons will automatically be enabled the next time you start Internet Explorer using the standard shortcut.

Alternatively, you can manually launch Internet Explorer using the –extoff parameter by clicking Start, typing **iexplore –extoff**, and pressing Enter.

You cannot manage add-ons when you start Internet Explorer in No Add-Ons mode. If you need to disable an add-on without opening Internet Explorer, follow the steps to use Control Panel, as described in the previous section.

How to Configure Add-Ons in Active Directory Domain Environments

As with earlier versions of Internet Explorer, you can use the Group Policy settings in User Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Add-on Management to enable or disable specific add-ons throughout your organization. Typically, you need to use two settings in this group to block all unapproved add-ons in your organization:

- **Add-On List** Enable this setting, and then specify the approved add-ons in your organization. To specify an add-on, provide the class identifier (CLSID) for the add-on you need to add as the Value Name in the Add-On List. The CLSID should be in brackets, such as "{BDB57FF2-79B9-4205-9447-F5FE85F37312}." You can find the CLSID for an add-on by reading the <object> tag from the Hypertext Markup Language (HTML) of a webpage that references the add-on. To specify that the add-on should be denied, specify a Value of 0. To allow an add-on, specify a Value of 1. To both allow an add-on and permit users to manage the add-on, specify a Value of 2.

- **Deny All Add-Ons Unless Specifically Allowed In The Add-On List** After specifying the add-ons you want to allow in the Add-On List setting, enable this policy to automatically block all other add-ons. You can use the combination of these two settings to block all unapproved add-ons.

Two other Group Policy settings related to add-on management are located within both User Configuration and Computer Configuration at Administrative Templates\Windows Components\Internet Explorer. The settings that relate to managing add-ons are:

- **Turn Off Crash Detection** By default, Internet Explorer will detect an add-on that crashes and disable it the next time you start Internet Explorer. If you have a problematic add-on that is required for a critical Web application, you can enable this policy to ensure that even a failing add-on continues to run.
- **Do Not Allow Users To Enable Or Disable Add-Ons** By default, users can open the Manage Add-Ons dialog box and enable or disable add-ons. If you enable this policy, they won't be able to configure add-ons.

How to Configure ActiveX Add-Ons

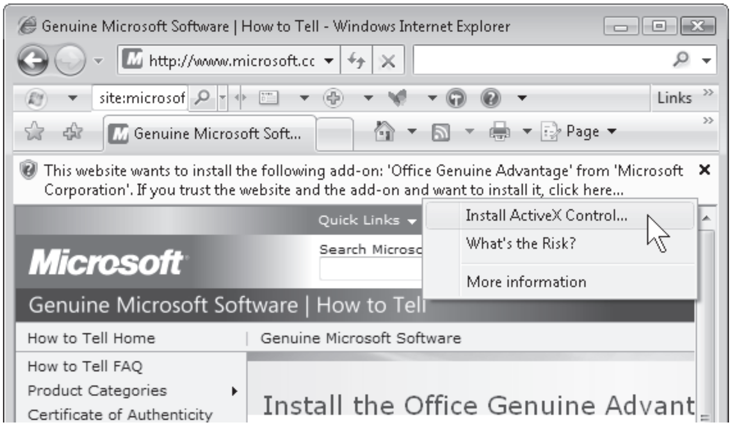
ActiveX is a technology that enables powerful applications with rich user interfaces to run within a Web browser. For that reason, many organizations have developed ActiveX components as part of a Web application. For the same reason, many attackers have created ActiveX components to abuse the platform's capabilities. Some examples of ActiveX controls include:

- A component that enables you to manage virtual computers from a Microsoft Virtual Server webpage.
- A Microsoft Update component that scans your computer for missing updates.
- Shockwave Flash, which many websites use to publish complex animations and games.

Earlier versions of Internet Explorer installed ActiveX controls without prompting the users. This provided an excellent experience for websites that used ActiveX controls because the user was able to enjoy the control's features without manually choosing to install it. However, malware developers soon abused this capability by creating malicious ActiveX controls that installed software on the user's computer or changed other settings, such as the user's home page.

To enable you to use critical ActiveX controls while blocking potentially dangerous ActiveX controls, Microsoft built strong ActiveX management capabilities into Internet Explorer. The sections that follow describe how to configure ActiveX on a single computer and within an enterprise.

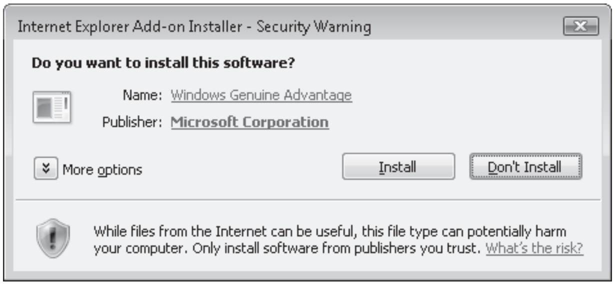
How to Configure ActiveX Opt-in In Internet Explorer 7, ActiveX controls are not installed by default. Instead, when users visit a webpage that includes an ActiveX control, they will see an information bar that informs them that an ActiveX control is required. Users will then have to click the information bar and click Install ActiveX Control. If the users do nothing, Internet Explorer does not install the ActiveX control. Figure 5-2 shows the Genuine Microsoft Software webpage, which requires users to install an ActiveX control before their copy of Windows can be validated as genuine.


Genuine Microsoft Software | How to Tell - Windows Internet Explorer
http://www.microsoft.cc
site:microsof
Links
Genuine Microsoft Soft...
Page
Install ActiveX Control...
What's the Risk?
More information
Quick Links
Search Microsc
Microsoft
Genuine Microsoft Software | How to Tell
How to Tell Home
Genuine Microsoft Software
How to Tell FAQ
Product Categories
Certificate of Authenticity
Install the Office Genuine Advant

This website wants to install the following add-on: 'Office Genuine Advantage' from 'Microsoft Corporation'. If you trust the website and the add-on and want to install it, click here...

Figure 5-2 The Genuine Microsoft Software page

After the user clicks Install ActiveX Control, the user needs to respond to a User Account Control (UAC) prompt for administrative credentials. Then the user receives a second security warning from Internet Explorer, as shown in Figure 5-3. If the user confirms this security warning, Internet Explorer installs and runs the ActiveX control.



Do you want to install this software?

Name: Windows Genuine Advantage
Publisher: Microsoft Corporation

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

Figure 5-3 A second security warning

ActiveX Opt-in is enabled by default for the Internet and Restricted Sites zones but disabled by default for the Local Intranet and Trusted Sites zones. Therefore, any websites on your local intranet should be able to install ActiveX controls without prompting the user. To change the setting default for a zone, follow these steps:

1. Open Internet Explorer. Click the Tools button on the toolbar, and then click Internet Options.

2. In the Internet Options dialog box, click the Security tab. Select the zone you want to edit, and then click the Custom Level button.
3. Scroll down in the Settings list. Under ActiveX Controls And Plug-Ins, change the setting for the first option, which is Allow Previously Unused ActiveX Controls To Run Without Prompt. If this is disabled, ActiveX Opt-in is enabled.

Exam Tip

The name "ActiveX Opt-in" can be confusing. Enabling ActiveX Opt-in causes Internet Explorer to *not* install ActiveX controls by default, instead requiring the user to explicitly choose to configure the add-on.

---

4. Click OK twice.

ActiveX Opt-in applies to most ActiveX controls. However, it does not apply for ActiveX controls on the preapproved list. The preapproved list is maintained in the registry at HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\PreApproved. Within this key there are several subkeys, each with a Class ID (CLSID) of a preapproved ActiveX control. You can identify an ActiveX control's CLSID by viewing the source of a webpage and searching for the <object> tag. For best results, try searching the source of a webpage for the phrase "<object."

How to Configure ActiveX on a Single Computer The previous section described how to configure ActiveX Opt-in on a single computer. In addition to that setting, you can configure several other per-zone settings related to ActiveX from the Security Settings dialog box:

- **Automatic Prompting For ActiveX Controls** This setting is disabled by default for all zones. If you choose to enable this setting, it bypasses the information bar and instead actively prompts the user to install the ActiveX control.
- **Download Signed ActiveX Controls** The developer can sign ActiveX controls. Typically, signed ActiveX controls are more trustworthy than unsigned controls, but you shouldn't trust all signed ActiveX controls. By default, this setting is set to prompt the user. You can reduce the number of prompts the user receives by changing this to Enable.
- **Download Unsigned ActiveX Controls** By default, unsigned ActiveX controls are disabled. If you must distribute an unsigned ActiveX control, add the site that requires the control to your Trusted Sites list and change this setting for the Trusted Sites zone to Prompt.
- **Initialize And Script ActiveX Controls Not Marked As Safe For Scripting** This setting is disabled by default for all zones. You should enable it only if you experience a problem with a specific ActiveX control, and the developer informs you that this setting is required. In that case you should add the site to the Trusted Sites list and enable this control only for that zone.

- **Run ActiveX Controls And Plug-Ins** This setting controls whether ActiveX controls will run, regardless of how other settings are defined. In other words, if this setting is disabled, users will not be able to run ActiveX controls, even using ActiveX Opt-in. This setting is enabled for all zones except for the Restricted Sites zone.
- **Script ActiveX Controls Marked Safe For Scripting** Some ActiveX controls are marked safe for scripting by the developer. This setting is enabled for all zones except for the Restricted Sites zone. Typically, you should leave this at the default setting. Because the developer chooses whether the control is marked safe for scripting, this marking does not indicate that the ActiveX control is more trustworthy than any other control.

How to Manage ActiveX Add-Ons on a Single Computer To configure ActiveX on a single computer, follow these steps:

1. Open Internet Explorer.
2. Click the Tools button on the toolbar, click Manage Add-Ons, and then click Enable Or Disable Add-Ons.

   The Manage Add-Ons dialog box appears.
3. Click the Show list, and then click Downloaded ActiveX Controls.
4. Select the ActiveX control you want to manage. Then select:
   - ❑ Disable to disable the ActiveX control.
   - ❑ Delete to remove the ActiveX control.
5. Click OK.

How to Configure ActiveX Installer Service Some critical Web applications might require ActiveX controls to run. This can be a challenge if your users lack administrative credentials because UAC requires administrative credentials to install ActiveX controls (although any user can access an ActiveX control after it is installed).

Fortunately, you can use the ActiveX Installer Service to enable standard users to install specific ActiveX controls. The ActiveX Installer Service is a Windows component but is not installed by default. To enable the ActiveX Installer Service on a computer, follow these steps:

1. Click Start, and then click Control Panel.
2. Click the Programs link.
3. Click the Turn Windows Features On Or Off link and reply to the UAC prompt that appears.
4. In the Windows Features dialog box, select the ActiveX Installer Service check box. Click OK.
5. Restart the computer if prompted.
6. Use the Services console (Services.msc) to start the ActiveX Installer (AxInstSV) service and configure it to start automatically. It is set to start manually by default.

After enabling the ActiveX Installer Service on a computer, configure the list of sites approved to install ActiveX controls by following these steps:

1. Open the Group Policy Object (GPO) in the Group Policy Object Editor.
2. Browse to Computer Configuration\Administrative Templates\Windows Components \ActiveX Installer Service.
3. Double-click the Approved Installation Sites For ActiveX Controls setting. Enable it.
4. Click the Show button to specify host Uniform Resource Locators (URLs) that are allowed to distribute ActiveX controls. In the Show Contents dialog box, click Add and configure the host URLs:
    - ☐ Configure each item name as the hostname of the website from which clients will download the updated ActiveX controls, such as *http://activex.microsoft.com*.
    - ☐ Configure each value name using four numbers separated by commas (such as "2,1,0,0"). These values are described later in this section.
5. Click OK to save the setting for the new policy.

When you configure the list of approved installation sites for ActiveX Controls, you configure a name and value pair for each site. The name will always be the URL of the site hosting the ActiveX control, such as *http://activex.microsoft.com*. The value consists of four numbers:

- **Trusted ActiveX Controls** Define the first number as 0 to block trusted ActiveX controls from being installed, as 1 to prompt the user to install trusted ActiveX controls, or as 2 to automatically install ActiveX controls without prompting the user.
- **Signed ActiveX Controls** Define the second number as 0 to block signed ActiveX controls from being installed, as 1 to prompt the user to install signed ActiveX controls, or as 2 to automatically install signed ActiveX controls without prompting the user.
- **Unsigned ActiveX Controls** Define the third number as 0 to block unsigned ActiveX controls from being installed or define this number as 1 to prompt the user to install unsigned ActiveX controls. You cannot configure unsigned ActiveX controls to be automatically installed.
- **Server Certificate Policy** Set this value to zero to cause the ActiveX Installer Service to abort installation if there are any certificate errors. Alternatively, you can set it to 256 to ignore an unknown CA, 512 to ignore invalid certificate usage, 4096 to ignore an unknown common name in the certificate, or 8192 to ignore an expired certificate. Add these numbers together to ignore multiple types of certificate errors.

For example, the numbers 2,1,0,0 would cause the ActiveX Installer Service to silently install trusted ActiveX controls, prompt the user for signed controls, never install unsigned controls, and abort installation if any Hypertext Transfer Protocol Secure (HTTPS) certificate error occurs.

When a user attempts to install an ActiveX control that has not been approved, the ActiveX Installer Service creates an event in the Application Log with an Event ID of 4097 and a source of AxInstallService. To be automatically notified when users need ActiveX controls that haven't been approved, configure a trigger for these events. For more information, read Chapter 6, "Monitoring Client Computers."

Protected Mode

Before Windows Vista, many computers were compromised when websites containing malicious code succeeded in abusing the Web browsers of visitors to run code on the client computer. Because any new process spawned by an existing process inherits the privileges of the parent process and the Web browser ran with the user's full privileges, maliciously spawned processes received the same privilege as the user. With the user's elevated privileges, the malicious process could install software and transfer confidential documents.

In Windows Vista, Internet Explorer hopes to reduce this type of risk using a feature called Protected Mode. With Protected Mode, Internet Explorer 7 runs with very limited privileges on the local computer—even fewer privileges than those that the standard user has in Windows Vista. Therefore, even if malicious code on a website were to successfully abuse Internet Explorer to spawn a process, that malicious process would have privileges only to access the Temporary Internet Files folder and a few other locations—it would not be able to install software, reconfigure the computer, or read the user's documents.

For example, most users log on to Windows XP computers with administrative privileges. If a website exploits a vulnerability in Windows Vista that hasn't been fixed with an update and successfully launches a process to install spyware, the spyware installation process would have full administrator privileges to the local computer. On a Windows Vista computer the spyware install process would have minimal privileges—even less than those of a standard user—regardless of whether the user was logged on as an administrator.

Protected Mode is a form of defense-in-depth. Protected Mode is a factor only if malicious code successfully compromises the Web browser and runs. In these cases, Protected Mode limits the damage the process can do without the user's permission. Protected Mode is not available when Internet Explorer 7 is installed on Windows XP because it requires several security features unique to Windows Vista.

The sections that follow provide more information about Protected Mode.

How Protected Mode Works

One of the Windows Vista features that enables Protected Mode is Mandatory Integrity Control (MIC). MIC labels processes, folders, files, and registry keys using one of four integrity access levels (ILs), as shown in Table 5-1. Internet Explorer runs with a low IL, which means it can access only other low IL resources without the user's permission.

Table 5-1 Mandatory Integrity Control Levels

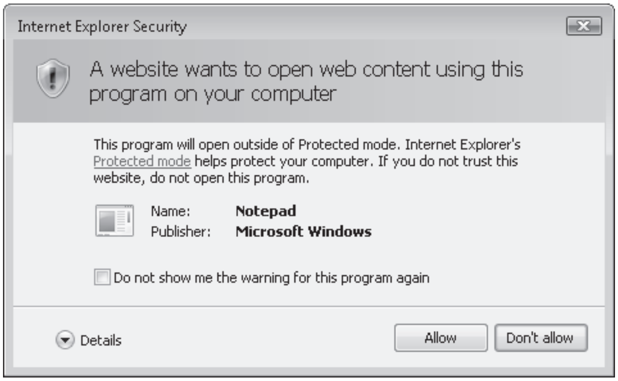
IL	System Privileges
System	System. Processes have unlimited access to the computer.
High	Administrative. Processes can install files to the Program Files folder and write to sensitive registry areas like HKEY_LOCAL_MACHINE.
Medium	User. Processes can create and modify files in the user's Documents folder and write to user-specific areas of the registry, such as HKEY_CURRENT_USER. Most files and folders on a computer have a medium integrity level because any object without a mandatory label has an implied default integrity level of Medium.
Low	Untrusted. Processes can only write to low integrity locations, such as the Temporary Internet Files\Low folder or the HKEY_CURRENT_USER\Software\LowRegistry key.

Low IL resources that Internet Explorer in Protected Mode can access include:

- The History folder.
- The Cookies folder.
- The Favorites folder.
- The %userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low \ folder.
- The Windows temporary files folders.
- The HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry key.

Using a feature called User Interface Privilege Isolation (UIPI), low IL also prevents Internet Explorer (or a malicious process launched by Internet Explorer) from sending window messages to other applications. This reduces the risk of shatter attacks, in which a process attempts to elevate privileges by directly attacking another process with higher privileges.

Unfortunately, it's not only malicious software that needs to elevate privileges. Often, legitimate websites and user tasks require more privileges than Protected Mode provides by default. Some user tasks, such as viewing the source code of a page, also require elevated privileges. In these circumstances, Internet Explorer prompts the user to grant additional privileges. Figure 5-4 shows the dialog box that appears if the user clicks the View menu and then clicks Source; Internet Explorer needs permission because it has to launch Notepad, an external application, to show the source code. Low IL processes cannot launch external applications.


Internet Explorer Security
A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: **Notepad**
Publisher: **Microsoft Windows**

☐ Do not show me the warning for this program again

Details
Allow
Don't allow

Figure 5-4 Internet Explorer prompts the user before granting elevated privileges

The warning dialog box shown in Figure 5-4 shows a yellow banner, indicating that the privileges requested require a medium IL (standard user privileges). A red banner can also appear, indicating that the privileges require a high IL (administrative privileges). Protected Mode protects Internet Explorer extensions, too, limiting the damage that could be done if an extension is malicious or contains a security vulnerability.

How the Protected Mode Compatibility Layer Works

To minimize both the number of privilege elevation requests and the number of compatibility problems, Protected Mode provides a compatibility layer. The compatibility layer redirects requests for protected resources to safer locations. For example, any requests for the My Documents folder (known as the Documents folder in Windows Vista) are automatically redirected to \%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Virtualized. The first time an add-on attempts to write to a protected object, the compatibility layer copies the object to a safe location and accesses the copy. All future requests for the same protected file will access the copy.

The compatibility layer applies only to Internet Explorer add-ons written for earlier versions of Windows because anything written for Windows Vista would natively access files in the preferred locations.

How to Enable Compatibility Logging

Some Web applications and Internet Explorer add-ons developed for earlier versions of Internet Explorer will have compatibility problems when you run them with Internet Explorer 7 and Windows Vista. One way to identify the exact compatibility problem is to enable compatibility logging using Group Policy. To enable compatibility logging on your local computer, follow these steps:

1. Click Start, type **gpedit.msc**, and then press Enter. Provide administrative credentials when prompted.
2. In the Group Policy Object Editor, browse to User Configuration\Administrative Templates\Windows Components\Internet Explorer\. If you need to enable compatibility logging for all users on the computer, browse to Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\.
3. Double-click the Turn On Compatibility Logging setting. Select Enabled, and then click OK.
4. Restart Internet Explorer if it is currently open.

With compatibility logging enabled, you should reproduce the problem you are experiencing. You can then view events in the Event Viewer snap-in under Applications And Service Logs\Internet Explorer. Some events, such as Event ID 1037, will not have a description unless you also install the Application Compatibility Toolkit.

MORE INFO Compatibility logging

For more information about compatibility logging, read "Finding Security Compatibility Issues in Internet Explorer 7" at *http://msdn.microsoft.com/library/en-us/IETechCol/cols/dnexpie/ie7_compat_log.asp*.

How to Disable Protected Mode

If you are concerned that Internet Explorer Protected Mode is causing problems with a Web application, you can temporarily disable it to test the application. Protected Mode is enabled on a zone-by-zone basis and is disabled by default for trusted sites.

To disable Protected Mode, follow these steps:

1. Open Internet Explorer.
2. Click the Tools button on the toolbar, and then click Internet Options.
3. Click the Security tab.
4. Select the zone for which you want to disable Protected Mode. Then, clear the Enable Protected Mode check box.
5. Click OK.

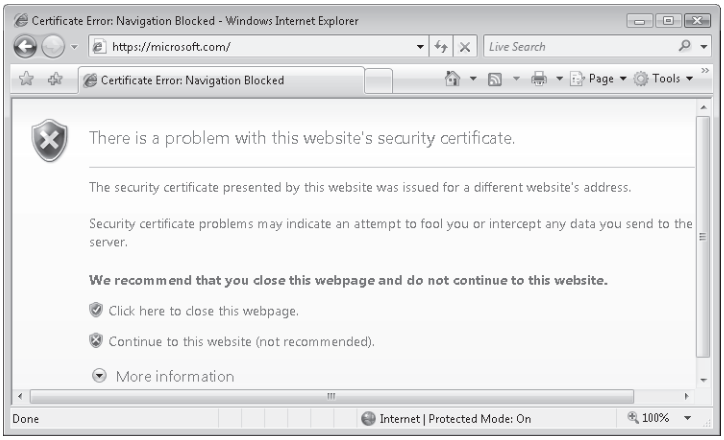
If the application works when Protected Mode is disabled, the problem is probably related to Protected Mode. In that case, you should reenable Protected Mode and work with the application developer to solve the problems in the Web application. Alternatively, you could add the site to the Trusted Sites zone, thus permanently disabling Protected Mode for that site.

How to Troubleshoot Certificate Problems

Certificates are used for several security-related tasks in Internet Explorer:

- **Encrypting traffic** The most common use for certificates in Internet Explorer. Many websites, especially e-commerce websites that accept credit card numbers, have a Secure Sockets Layer (SSL) certificate installed. This SSL certificate enables HTTPS communications, which behave similar to HTTP, but with encryption and authentication. With standard, unencrypted HTTP, if an attacker has access to the network, the attacker can read all data transferred to and from the server. With encrypted HTTPS, an attacker can capture the traffic, but it will be encrypted and cannot be decrypted without the server's private certificate.
- **Authenticating the server** SSL certificates authenticate the server by allowing the client to verify that the certificate was issued by a trusted certification authority (CA) and that the name in the certificate matches the hostname used to access the site. This helps to prevent man-in-the-middle attacks, whereby an attacker tricks a client computer into visiting a malicious server that impersonates the legitimate server. Websites on the public Internet typically have SSL certificates issued by a third-party CA that is trusted by default in Internet Explorer. Intranet websites can use certificates issued by an internal CA as long as client computers are configured to trust the internal CA.
- **Authenticating the client** Intranet websites can issue certificates to clients on their network and use the client certificates to authenticate internal websites. When using Active Directory Group Policy, it is very easy to distribute client certificates throughout your enterprise.

If Internet Explorer detects a problem with a certificate, it displays the message, "There is a problem with this website's security certificate," as shown in Figure 5-5.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://microsoft.com/
Live Search
Certificate Error: Navigation Blocked
Page
Tools
Done
Internet | Protected Mode: On
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Figure 5-5 How Internet Explorer detects mismatched SSL certificates

The following list describes common problems that can occur when using certificates in Internet Explorer and how to troubleshoot them:

- **The security certificate presented by this website was issued for a different website's address** In this case, there are several possible causes:
    - ❑ The hostname you are using to access the website is not the website's primary address. For example, you might be attempting to access the website by IP address. Alternatively, you might be accessing an alternative hostname, such as "constoso.com" instead of "www.contoso.com."
    - ❑ The server is impersonating a server with a different hostname. For example, an attacker might have set up a website to impersonate www.fabrikam.com. However, the attacker is using a different SSL certificate on the website. Earlier versions of Internet Explorer show a less intimidating error message, so many users might have bypassed the error and continued to the malicious site.
    - ❑ The server administrator made a mistake. For example, the administrator might have mistyped the server's hostname when requesting the certificate, or the administrator might have installed the wrong certificate on the server.
- **The certificate has expired** Certificates have a limited lifespan—usually one to five years. If the certificate has expired, the server administrator should request an updated certificate and apply it to the server.
- **Internet Explorer is not configured to trust the certificate authority** Anyone, including attackers, can create their own CA and issue certificates. Therefore, Internet Explorer does not trust all CAs by default. Instead, Internet Explorer trusts only a handful of public CAs. If the certificate was issued by an untrusted CA and the website is on the public Internet, the server administrator should acquire a certificate from a trusted CA. If the website is on your intranet, a client administrator should configure Internet Explorer to trust the issuing CA. In Active Directory directory service domains, member computers automatically trust enterprise CAs. For more information, complete the practices at the end of this lesson.

Practice: Troubleshoot Certificate Problems

In this practice, you first configure the ActiveX Installer Service to trust ActiveX controls from MSN. Then, you will practice troubleshooting certificate-related problems by generating an untrusted certificate, viewing how Internet Explorer responds to that certificate, and then configuring Internet Explorer to trust the certificate.

▶ Practice 1: Automate the Installation of an ActiveX Control

In this practice, you configure the ActiveX Installer Service to automatically install an ActiveX control used by MSN.com.

1. Log on as a standard user and open Internet Explorer. Visit *http://music.msn.com/client/install.aspx*. Click Install.
2. Click the Information Bar, and then click Install ActiveX Control. The UAC prompt appears, indicating that a standard user would be unable to install the add-on. Click Cancel.
3. Follow these steps to install the ActiveX Installer Service:
   a. Click Start, and then click Control Panel.
   b. Click the Programs link.
   c. Click the Turn Windows Features On Or Off link and reply to the UAC prompt that appears.
   d. In the Windows Features dialog box, select ActiveX Installer Service check box. Click OK.
   e. If prompted, do not restart the computer.
4. Follow these steps to configure Microsoft.com as a trusted installer:
   a. Use administrative privileges to open the local GPO in the Group Policy Object Editor.
   b. Browse to Computer Configuration\Administrative Templates\Windows Components\ActiveX Installer Service.
   c. Double-click the Approved Installation Sites For ActiveX Controls setting. Select Enable.
   d. Click the Show button.
   e. Click Add. Specify a value name of **http://entimg.msn.com/** and a value of **2,2,1,0**.

   NOTE Source URL and CLSID of an ActiveX control

   You can determine the source URL and CLSID of the ActiveX control by viewing the source of the webpage that installs the ActiveX control. Then, within the source, search for the phrase "<object".

   f. Click OK three times to save the setting for the new policy.
5. Restart your computer to complete the installation of the ActiveX Installer Service and to apply the updated Group Policy settings.

6. Log back on as a standard user. Open Internet Explorer and visit *http://music.msn.com/client/install.aspx* again. Click Install. Then, click the Information Bar, and click Install ActiveX Control. Notice that this time, although Internet Explorer prompts you to confirm the installation, no UAC prompt appears. After the ActiveX control is installed, click the information bar again to activate the control.
7. In Internet Explorer, click the Tools button on the toolbar, click Manage Add-Ons, and then click Enable Or Disable Add-Ons.
8. In the Manage Add-Ons dialog box, click the Show list, and then click Downloaded ActiveX Controls. Notice that the newly installed ActiveX control appears on the list.

▶ Practice 2: Simulate an Invalid Certificate

In this practice, you open a webpage using a hostname other than the common name specified in the SSL certificate and view how Internet Explorer handles it.

1. Open Internet Explorer. In the Address bar, type **https://www.microsoft.com**. Press Enter.

   When prompted to display nonsecure items, click No.
2. Internet Explorer opens the *www.microsoft.com* home page using encrypted HTTPS. Note the gold lock in the Address bar, as shown in Figure 5-6.

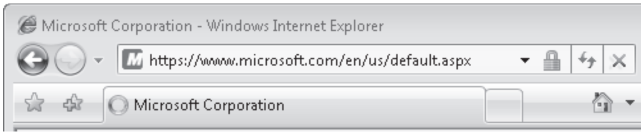

Microsoft Corporation - Windows Internet Explorer
https://www.microsoft.com/en/us/default.aspx
Microsoft Corporation

Figure 5-6 The gold lock in the address bar, which signifies that communications with the site are encrypted and the certificate is valid

3. Click the gold lock in the address bar to display the website identification. Notice that the identification page displays "www.microsoft.com," which exactly matches the hostname you typed in the address bar.
4. In the Address bar, type **https://microsoft.com**. Notice that this time the hostname does not begin with "www." Press Enter.

   Internet Explorer displays the There Is A Problem With This Website's Security Certificate webpage. This happens because the hostname in the certificate, www.microsoft.com, does not exactly match the hostname you typed in the address bar, microsoft.com. Users would see this same error message if they attempted to visit a site that was impersonating another site.

▶ Practice 3: Issue an Untrusted Certificate

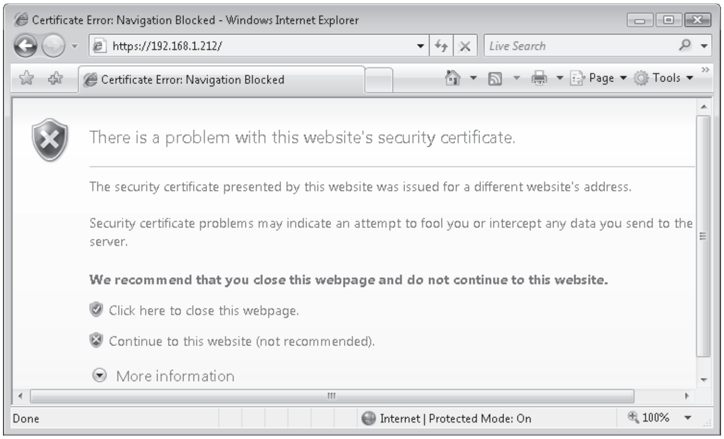
In this practice, you must issue an internal certificate to a Web server and determine how Windows Vista handles it both as a member of the domain and from outside the domain.

1. Connect to a Windows Server 2003 Active Directory domain controller in a test environment and log on as an administrator.
2. Certificate Services requires Internet Information Services (IIS). Therefore, you need to install the Application Server role if it is not already installed. Click Start, click Administrative Tools, and then click Manage Your Server. If the Application Server role is already installed, skip to step Otherwise, click Add Or Remove A Role to start the Configure Your Server Wizard.
3. On the Preliminary Steps page, click Next.
4. On the Server Role page, select Application Server (IIS, ASP.NET), and then click Next. Follow the prompts that appear to install IIS with ASP.NET enabled. Finally, click Finish.
5. After you have installed IIS, click Start, click Control Panel, and then click Add Or Remove Programs. Click Add/Remove Windows Components.
6. If the Certificate Services check box is already selected, skip to step Otherwise, select the Certificate Services check box, click Yes to close the Microsoft Certificate Services message box, and then click Next.
7. On the CA Type page, leave Enterprise Root CA selected, and then click Next.
8. On the CA Identifying Information page, type the hostname for your CA (such as DCSRV1.nwtraders.msft), and then click Next to accept the default settings. If prompted to stop IIS, click Yes.
9. On the Certificate Database Settings page, click Next. Respond to any prompts that appear to complete the installation of Certificate Services. Finally, click Finish.
10. Click Start, click All Programs, click Administrative Tools, and then click IIS Manager.
11. In the IIS Manager, expand your computer and expand Web Sites. Then, right-click Default Web Site and click Properties.
12. In the Default Web Site Properties dialog box, click the Directory Security tab. Then, click the Server Certificate button.
13. The Web Server Certificate Wizard appears. On the Welcome To The Web Server Certificate Wizard page, click Next.
14. On the Server Certificate page, select Create A New Certificate, and then click Next.

15. On the Delayed Or Immediate Request page, select Send The Request Immediately To An Online Certification Authority. Then, click Next.
16. On the Name And Security Settings page, accept the default settings by clicking Next.
17. On the Organization Information page, type **Northwind Traders** in the Organization box and type **IT** in the Organizational Unit box. Then, click Next.
18. On the Your Site's Common Name page, note that the default setting matches the site's computer name. This setting is extremely important because it must exactly match the name that users type to access your website. Computer names work well on intranet sites, but for public Internet sites the common name should resemble "www.nwtraders.com." Click Next to accept the default setting because this site will be accessed like an intranet site.
19. On the Geographical Information page, enter your geographic information. Then, click Next.
20. On the SSL Port page, accept the default standard setting of 44. Then, click Next.
21. On the Choose A Certification Authority page, verify that the CA listed matches the domain controller. Click Next.
22. On the Certificate Request Submission page, click Next.
23. On the Completing The Web Server Certificate Wizard page, click Finish.
24. In the Default Web Site Properties dialog box, click OK.
25. Now you have configured your domain controller as a Web server with an SSL certificate. On your Windows Vista client computer, open Internet Explorer. In the address bar, enter https://*common_name*, where *common_name* is the name you entered in step 19 (such as https://dcsrv1). Press Enter.

    Internet Explorer opens the page. Notice that the gold lock icon appears in the address bar, signifying that the SSL certificate is valid.
26. On a second Windows Vista computer that is not a member of your domain, open Internet Explorer. Alternatively, if you do not have a second computer, you can temporarily remove your Windows Vista computer from the domain. In Internet Explorer, enter https://*common_name* and press Enter.

    Internet Explorer displays a warning message indicating that the certificate was not issued by a trusted certificate authority, as shown in Figure 5-7.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.1.212/
Live Search
Certificate Error: Navigation Blocked
Page
Tools
Done
Internet | Protected Mode: On
100%

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website's address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Figure 5-7 The warning message given by Internet Explorer if it doesn't trust the certificate authority

Now, continue working with Practice 4 to resolve this problem.

▶ Practice 4: Trust a Certificate Authority

In this practice, you must export your CA's root certificate and trust that certificate on your nondomain Windows Vista computer so that you can open the SSL-encrypted website without a warning. To complete this practice, you must have completed Practice 2.

1. On your domain controller, in the Certification Authority console, right-click your server, and then click Properties.
2. Click the General tab. Click Certificate #0, and then click the View Certificate button.
3. In the Certificate dialog box, click the Details tab. Then, click Copy To File.
4. The Certificate Export Wizard appears. Click Next.
5. On the Export File Format page, accept the default export format, and then click Next.
6. On the File To Export tab, type **C:\root.cer**, and then click Next.
7. Click Finish. Then, click OK twice.
8. On your Windows Vista client computer that is not a member of your test domain, open Internet Explorer. In Internet Explorer, click the Tools button on the toolbar, and then click Internet Options.

9. In the Internet Options dialog box, click the Content tab, and then click Certificates.
10. In the Certificates dialog box, click the Trusted Root Certification Authorities tab. Then, click the Import button.
11. The Certificate Import Wizard appears. On the Welcome To The Certificate Import Wizard page, click Next.
12. On the File To Import page, click the Browse button. In the Open dialog box, type **\\*server_name*\c$\root.cer**. Then, click Open. Click Next.
13. On the Certificate Store page, notice that the Certificate Import Wizard will import the certificate into the Trusted Root Certification Authorities store by default. This is the correct place. Click Next.
14. On the Completing The Certificate Import Wizard page, click Finish.
15. A Security Warning dialog box appears. Click Yes to install the certificate. Then, click OK.
16. Click Close, and then click OK.
17. In Internet Explorer, enter https://*common_name*, and press Enter.

    Internet Explorer opens the page. Notice that the gold lock icon appears in the address bar, signifying that the SSL certificate is valid. Because this computer is not a member of the Active Directory domain, you had to manually trust the root certificate. Then, all certificates issued by that CA will be trusted. If the computer had been a member of the Active Directory domain, Group Policy would have caused the computer to automatically trust the enterprise CA.

Lesson Summary

- Web application developers often use Internet Explorer add-ons to extend the Web browser's capabilities. However, some add-ons can cause reliability problems, and others might compromise your organization's security. Fortunately, Internet Explorer provides tools to disable add-ons and delete ActiveX controls. If an add-on is preventing Internet Explorer from starting, you can start Internet Explorer with all add-ons disabled.
- Protected Mode is one of Internet Explorer 7.0's most significant security improvements, and it's available only when using Windows Vista. By default, Protected Mode causes Internet Explorer to run with low privileges, which prevents Internet Explorer (or any process launched by Internet Explorer) from accessing most resources on the computer. The user must confirm permissions if Internet Explorer or an add-on require elevated privileges.

- Many websites use certificates to authenticate the Web server and to provide encrypted communications. Certificates are extremely important for websites that provide access to confidential information or that collect private information from users (such as credit card numbers). The most common certificate problem is a nonmatching server hostname, which can typically be resolved by providing the hostname listed in the certificate. For servers on your intranet, users might experience certificate problems if the computer hasn't been correctly configured to trust the CA.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 1, "Configuring and Troubleshooting Internet Explorer Security." The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is right or wrong are located in the "Answers" section at the end of the book.

---

1. A user is attempting to visit one of the many internal websites run by your IT department. The user's shortcut is set up to use SSL by default. Today, when the user attempted to open the page, Internet Explorer showed the user the following message:

```
There is a problem with this websiteÕs security certificate.
The security certificate presented by this website was issued
for a different websiteÕs address.
```

   Which of the following might cause this message? (Choose all that apply.)

   A. The certificate is expired.

   B. An attacker is redirecting traffic to a malicious Web server.

   C. Internet Explorer no longer trusts the CA that issued the certificate.

   D. The website certificate was issued for a different hostname than that stored in the user's shortcut.

2. Which of the following would Internet Explorer block by default (until confirmed by a user)? (Choose all that apply.)

   A. Animated GIFs

   B. Background music in a webpage

   C. Video embedded in a webpage

   D. Viewing the source code of a webpage

3. Which of the following types of requests would the Internet Explorer compatibility layer redirect to a virtualized location?
    - **A.** Storing a cookie
    - **B.** Storing a file in the Documents folder
    - **C.** Prompting the user to choose a file to upload to a website
    - **D.** Storing a file in the Temporary Internet Files folder
4. You receive a support call from a user attempting to access an internal webpage. The user recently upgraded to Windows Vista; previously, the user had been using Windows XP and Internet Explorer 6.0. The webpage contains an ActiveX control, but it isn't appearing on the webpage for the user. Which of the following are valid ways for the user to resolve the problem? (Choose two. Each correct answer is a complete solution.)
    - **A.** Right-click the page, and then click Run ActiveX Control.
    - **B.** Click the Information Bar, and then click Run ActiveX Control.
    - **C.** Add the site to the Trusted Sites list.
    - **D.** Clear the Enable Protected Mode check box in the Internet Security dialog box.

Lesson 2: Updating Software

Because security threats are constantly evolving, Microsoft must regularly release updates to Windows Vista. Deploying and managing these updates are some of the most important security tasks an IT department can perform. To simplify this task, Windows Vista includes several improved update capabilities compared to Windows XP:

- Windows Update is a stand-alone tool instead of a webpage.
- Windows Update will immediately connect to an update server the first time Windows Vista connects to a network.
- Windows Update automatically installs drivers for devices that are using generic drivers or that do not have any driver installed.
- Administrators can configure Windows Update to automatically install recommended updates as well as critical updates.
- Now non-administrators can approve update installations without providing administrative credentials.
- Windows Update can wake a computer from sleep to install updates, so users no longer need to leave their computers running to enable updates to be installed overnight.

This lesson describes the different techniques for deploying updates to Windows Vista computers and explains how to install and manage updates and how to troubleshoot update problems.

After this lesson, you will be able to:

- Choose a deployment technique for distributing updates within your organization.
- Install updates automatically, manually, and to new computers.
- Troubleshoot problems installing updates.
- Uninstall updates.

Estimated lesson time: 30 minutes

Methods for Deploying Updates

Microsoft provides several techniques for applying updates:

- **Directly from Microsoft** For home users and small businesses, Windows Vista is configured to automatically retrieve updates directly from Microsoft. This method is suitable only for smaller networks with fewer than 50 computers.

- **Windows Server Update Services (WSUS)** WSUS enables administrators to approve updates before distributing them to computers on an intranet. Optionally, updates can be stored and retrieved from a central location on the local network, reducing Internet usage when downloading updates. This approach requires at least one infrastructure server.
- **Microsoft Systems Management Server (SMS)** The preferred method for distributing software and updates in large, enterprise networks, SMS provides highly customizable, centralized control over update deployment, with the ability to audit and inventory client systems. SMS typically requires several infrastructure services.

The sections that follow describe each of these deployment methods in more detail.

Windows Update Client

Whether you download updates from Microsoft or use WSUS, the Windows Update client is responsible for downloading and installing updates on Windows Vista computers. The Windows Update client replaces the Automatic Updates client available in earlier versions of Windows. Both Windows Update in Windows Vista and Automatic Updates in previous versions of Windows operate the same way: they download and install updates from Microsoft or an internal WSUS server. Both clients install updates at a scheduled time and automatically restart the computer if necessary. If the computer is turned off at that time, the updates can be installed as soon as the computer is turned on. Alternatively, Windows Update can wake a computer from sleep and install the updates at the specified time if the computer hardware supports it.

The Windows Update client provides for a great deal of control over its behavior. You can configure individual computers by using the Control Panel\Security\Windows Update\Change Settings page, as described in “How to Configure Windows Update Using Graphical Tools” later in this section. Networks that use Active Directory can specify the configuration of each Windows Update client by using Group Policy, as described in “How to Configure Windows Update Using Group Policy Settings.”

After the Windows Update client downloads updates, the client checks the digital signature and the Secure Hash Algorithm (SHA1) hash on the updates to verify that they have not been modified.

Windows Server Update Services

Windows Server Update Services (WSUS) is a version of the Microsoft Update service that you can host on your private network. WSUS connects to the Windows Update site, downloads information about available updates, and adds them to a list of updates that require administrative approval.

After an administrator approves and prioritizes these updates, WSUS automatically makes them available to any computer running Windows Update (or the Automatic Updates client on earlier versions of Windows). Windows Update (when properly configured) then checks the WSUS server and automatically downloads and installs updates as configured by the administrators. As shown in Figure 5-8, you can distribute WSUS across multiple servers and locations to scale to enterprise needs. WSUS meets the needs of medium-sized organizations and many enterprises.

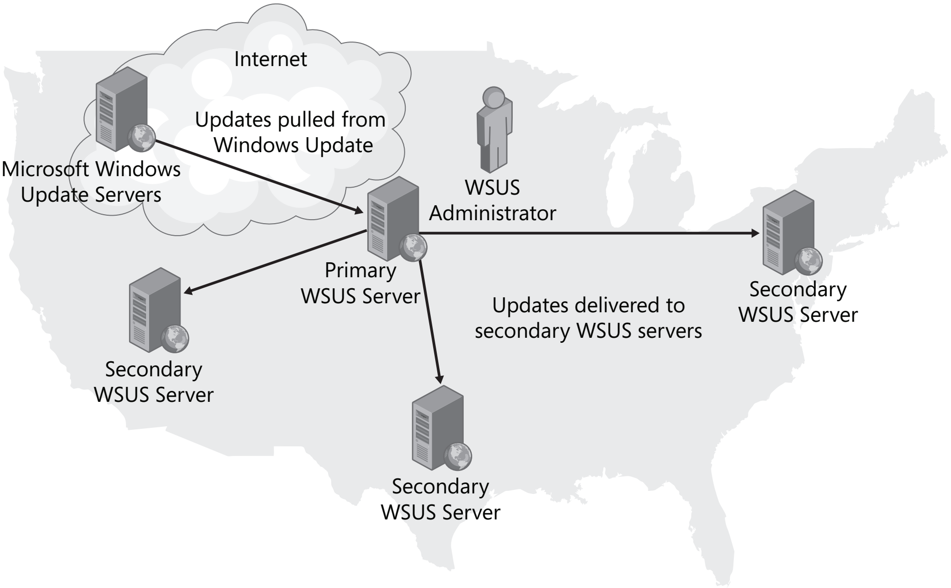


Figure 5-8 WSUS can scale to support thousands of computers

You must install WSUS on at least one infrastructure server, and you manage it by using a Web browser. To deploy updates to Windows Vista computers, you must have WSUS Service Pack 1 or later installed on your server.

MORE INFO Windows Server Update Services (WSUS)

For more information about update management with WSUS and to download WSUS, visit *http://www.microsoft.com/wsus/*.

Systems Management Server

Microsoft Systems Management Server (SMS) 2003 is a tool for efficiently managing, distributing, and inventorying software in enterprise environments. Although WSUS is sufficient to meet the needs of medium-sized organizations, SMS can supplement WSUS in enterprise organizations that manage hundreds or thousands of computers.

MORE INFO Systems Management Server (SMS)

For more information about SMS, visit the SMS website at *http://www.microsoft.com/smserver*.

MORE INFO Using SMS for update management

For information about using SMS for update management, refer to the article "Patch Management Using Systems Management Server 2003" at *http://www.microsoft.com/technet/itsolutions/cits/mo/swdist/pmsms/2003/pmsms031.mspx*.

How to Install Updates

Ideally, you would install all current updates immediately when you deploy new computers. After deployment, you can manually install updates, but you'll be much more efficient if you choose an automatic deployment technique. For situations that require complete control over update installation but still must be automated, you can script update installations.

How to Apply Updates to New Computers

When you deploy new computers, you should deploy them with as many recent updates as possible. Even though Windows Vista immediately checks for updates the first time it starts (rather than waiting for the scheduled automatic update time), this provides improved security for the computer the first time it starts, rather than waiting for it to retrieve updates after startup.

You can use the following techniques, in order of most secure to least secure, to apply updates to new computers:

- **Integrate updates into Windows Vista setup files** If you use an automatic deployment technology such as the Microsoft Solution Accelerator for Business Desktop Deployment 2007 (BDD), you can ensure that updates are present during setup by installing Windows Vista and all updates on a lab computer and then using Windows PE and the XImage tool to create an operating system image (a .wim file) that you can deploy to new computers.

  MORE INFO Solution Accelerator for Business Desktop Deployment 2007 (BDD)

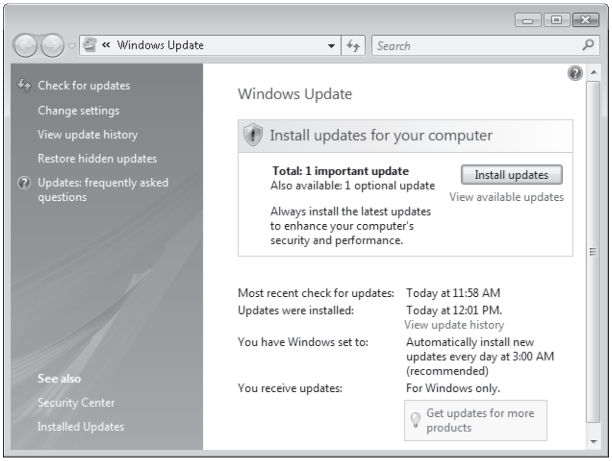
  For more information about BDD, visit *http://www.microsoft.com/technet/desktopdeployment/bdd/2007/*.

- **Install updates automatically during setup** Using scripting, you can install updates automatically during setup. Ideally, you would distribute the update files with your Windows Vista installation media or on the distribution server. You can use BDD to configure updates for installation during setup, or you can manually configure updates using one of the following techniques:
    - ❑ Use the Windows System Image Manager to add a RunSynchronous command to an Unattend.xml answer file in your Windows Vista image. RunSynchronous commands are available in the Microsoft-Windows-Setup and the Microsoft-Windows-Deployment components.
    - ❑ Edit the %windir%\Setup\Scripts\SetupComplete.cmd file in your Windows Vista image. Windows Vista runs any commands in this file after Windows Setup completes. Commands in the SetupComplete.cmd file are executed with local system privilege. You cannot reboot the system and resume running SetupComplete.cmd; therefore, you must install all updates in a single pass.
- **Manually install updates using removable media** One of the best ways to minimize the risk of a new computer being attacked before it installs updates is to deploy computers while disconnected from the network, using removable media. If you choose this approach, you should also use removable media to install updates before connecting the computer to the public Internet.
- **Use WSUS to apply updates to new computers** After Windows Vista starts the first time, it immediately attempts to download updates (rather than waiting for the scheduled Windows Update time). Therefore, even with the default settings, the time new computers spend without updates is minimized. To further minimize this, ask your WSUS administrators to configure the most critical updates with a deadline. The deadline forces new computers downloading the updates to install the critical updates and then immediately restart to apply them.

How to Manually Apply Updates

In previous versions of Windows, you could apply updates by visiting the *http://windowsupdate.com* website. In Windows Vista, you must follow these steps:

1. Click Start, click All Programs, and then click Windows Update.
2. The Windows Update window appears. Click the Check For Updates link.
3. If any updates are available, click Install Updates, as shown in Figure 5-9. To install optional updates, click View Available Updates.



Windows Update

Install updates for your computer

Total: 1 important update
Also available: 1 optional update

Always install the latest updates to enhance your computer's security and performance.

Most recent check for updates: Today at 11:58 AM
Updates were installed: Today at 12:01 PM.
You have Windows set to: Automatically install new updates every day at 3:00 AM (recommended)
You receive updates: For Windows only.

Figure 5-9 Using the Windows Update tool to check for updates

---

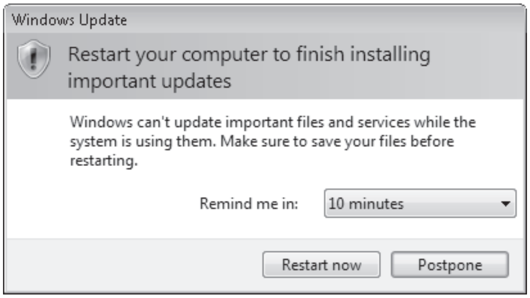
NOTE If an update is not listed

If an update does not appear on the list, it might have been hidden. To fix this, click the Restore Hidden Updates link in the Windows Update window.

---

4. Windows Updates downloads and installs the available updates.
5. If required, restart the computer by clicking Restart Now.

   If you choose not to immediately restart the computer, Windows Update will regularly prompt the user to restart, as shown in Figure 5-10. The user can postpone the update prompt for up to four hours. Administrative credentials are not required to install updates.



Restart your computer to finish installing important updates

Windows can't update important files and services while the system is using them. Make sure to save your files before restarting.

Remind me in: 10 minutes

Figure 5-10 The reminder from Windows Update that updates are waiting for the computer to be restarted

How to Automatically Apply Updates

You can configure automatic updates by using either graphical, interactive tools or by using Group Policy. The sections that follow describe each of these techniques.

How to Configure Windows Update Using Graphical Tools During an interactive setup, Windows Vista prompts users to choose update settings. Setup recommends enabling automatic updates. To manually configure automatic updates on a computer, follow these steps (which require administrative privileges):

1. Click Start, and then click Control Panel.
2. Click the Security link.
3. Under Windows Update, click the Turn Automatic Updating On Or Off link.
4. Adjust the settings, including whether updates are installed automatically and the time they are installed, and then click OK.

How to Configure Windows Update Using Group Policy Settings You can configure Windows Update client settings using local or domain Group Policy settings. This is useful for the following tasks:

- Configuring computers to use a local WSUS server
- Configuring automatic installation of updates at a specific time of day
- Configuring how often to check for updates
- Configuring update notifications, including whether non-administrators receive update notifications
- Configure client computers as part of a WSUS target group, which you can use to deploy different updates to different groups of computers

Windows Update settings are located at Computer Configuration\Administrative Templates\Windows Components\Windows Update. The Windows Update Group Policy settings are:

- **Configure Automatic Updates** Specifies whether client computers will receive security updates and other important downloads through the Windows Update service. You also use this setting to configure whether the updates are installed automatically and what time of day the installation occurs.
- **Specify Intranet Microsoft Update Service Location** Specifies the location of your WSUS server.
- **Automatic Updates Detection Frequency** Specifies how frequently the Windows Update client checks for new updates. By default, this is a random time between 17 and 22 hours.
- **Allow Non-Administrators To Receive Update Notifications** Determines whether all users or only administrators will receive update notifications. Non-administrators can install updates using the Windows Update client.

- **Allow Automatic Updates Immediate Installation** Specifies whether Windows Update will immediately install updates that don't require the computer to be restarted.
- **Turn On Recommended Updates Via Automatic Updates** Determines whether client computers install both critical and recommended updates, which might include updated drivers.
- **No Auto-Restart For Scheduled Automatic Updates** Specifies that to complete a scheduled installation, Windows Update will wait for the computer to be restarted by any user who is logged on instead of causing the computer to restart automatically.
- **Re-Prompt For Restart With Scheduled Installations** Specifies how often the Windows Update client prompts the user to restart. Depending on other configuration settings, users might have the option of delaying a scheduled restart. However, the Windows Update client will automatically remind them to restart based on the frequency configured in this setting.
- **Delay Restart For Scheduled Installations** Specifies how long the Windows Update client waits before automatically restarting.
- **Reschedule Automatic Updates Scheduled Installations** Specifies the amount of time for Windows Update to wait, following system startup, before continuing with a scheduled installation that was missed previously. If you don't specify this amount of time, a missed scheduled installation will occur one minute after the computer is next started.
- **Enable Client-Side Targeting** Specifies which group the computer is a member of. This option is useful only if you are using WUS; you cannot use this option with SUS.
- **Enabling Windows Update Power Management To Automatically Wake Up The System To Install Scheduled Updates** If people in your organization tend to shut down their computers when they leave the office, enable this setting to configure computers with supported hardware to automatically start up and install an update at the scheduled time. Computers will not wake up unless there is an update to be installed. If the computer is on battery power, the computer will automatically return to Sleep after two minutes.

Additionally, the following two settings are available at the same location under User Configuration (which you can use to specify per-user settings) in addition to Computer Configuration:

- **Do Not Display 'Install Updates And Shut Down' Option In Shut Down Windows Dialog Box** Specifies whether Windows XP with Service Pack 2 or later shows the Install Updates And Shut Down option.
- **Do Not Adjust Default Option To 'Install Updates And Shut Down' In Shut Down Windows Dialog Box** Specifies whether Windows XP with Service Pack 2 or later automatically changes the default shutdown option to Install Updates And Shut Down when Windows Update is waiting to install an update.

Finally, the last user setting is available only at User Configuration\Administrative Templates\Windows Components\Windows Update:

- **Remove Access To Use All Windows Update Features** When enabled, prevents user from accessing the Windows Update interface.

How to Script Updates

Windows Vista opens MSU files with the Windows Update Standalone Installer (Wusa.exe). To install an update from a script, run the script with administrative privileges, call Wusa and provide the path to the MSU file. For example, you can install an update named Windows6.0-KB929761-x86.msu in the current directory by running the following command:

```
wusa Windows6.0-KB929761-x86.msu
```

Additionally, Wusa supports the following standard command-line options:

- **/?, /h, or /help** Displays the command-line options.
- **/quiet** Quiet mode. This is the same as unattended mode, but no status or error messages are displayed. Use quiet mode when installing an update as part of a script.
- **/norestart** Does not restart when installation has completed. Use this parameter when installing multiple updates simultaneously. All but the last update installed should have the /norestart parameter.

Scripting is not usually the best way to install updates on an ongoing basis. Instead, you should use Windows Update, WSUS, or SMS. However, you might create a script to install updates on new computers or to install updates on computers that cannot participate in your standard update distribution method.

How to Troubleshoot Problems Installing Updates

Occasionally, you might experience a problem installing an update. Fortunately, Windows Vista provides detailed information about update installations. The sections that follow describe how to troubleshoot problems with Windows Update and Restart Manager.

How to Troubleshoot Windows Update

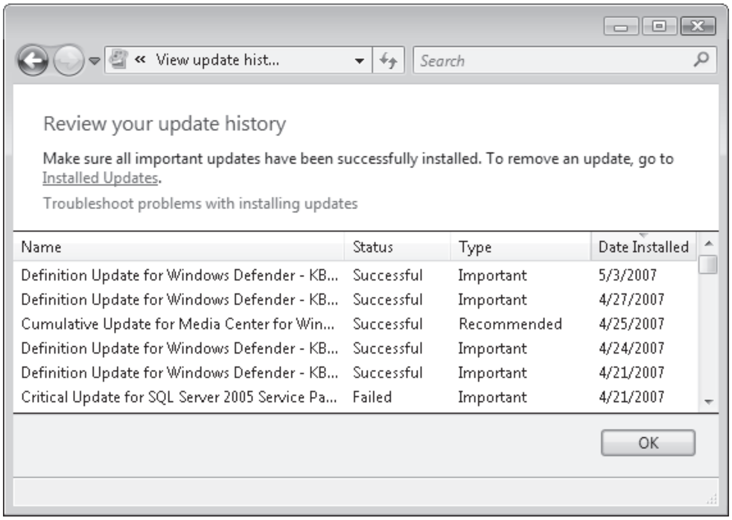
Occasionally, you might discover a client that isn't automatically installing updates correctly. You can identify missing updates using an automated tool such as the Microsoft Baseline Security Analyzer (MBSA).

MORE INFO Microsoft Baseline Security Analyzer (MBSA)

For more information about MBSA and to download the free tool, visit *http://www.microsoft.com/mbsa/*.

Alternatively, you can manually identify problems installing updates by viewing the update history. To view the update history, follow these steps:

1. Click Start, click All Programs, and then click Windows Update.
2. The Windows Update window appears. Click the View Update History link.
3. The View Update History window appears, as shown in Figure 5-11. To view the details of an update, double-click it.



Review your update history

Make sure all important updates have been successfully installed. To remove an update, go to Installed Updates.

Troubleshoot problems with installing updates

Name	Status	Type	Date Installed
Definition Update for Windows Defender - KB...	Successful	Important	5/3/2007
Definition Update for Windows Defender - KB...	Successful	Important	4/27/2007
Cumulative Update for Media Center for Win...	Successful	Recommended	4/25/2007
Definition Update for Windows Defender - KB...	Successful	Important	4/24/2007
Definition Update for Windows Defender - KB...	Successful	Important	4/21/2007
Critical Update for SQL Server 2005 Service Pa...	Failed	Important	4/21/2007

Figure 5-11 Reviewing an update history with the Windows Update tool

To identify the source of the problem causing an update to fail, follow these steps:

1. Examine the %windir%\WindowsUpdate.log file to verify that the client is contacting the correct update server and to identify any error messages. For detailed information about how to read the WindowsUpdate.log file, refer to Microsoft Knowledge Base article 902093 at *http://support.microsoft.com/kb/902093/*.
2. If your organization uses WSUS, verify that the client can connect to the WSUS server by opening a Web browser and visiting http://<*WSUSServerName*>/iuident.cab. If you are prompted to download the file, this means that the client can reach the WSUS server, and it is not a connectivity issue. Otherwise, you could have a name resolution or connectivity issue, or WSUS is not configured correctly.

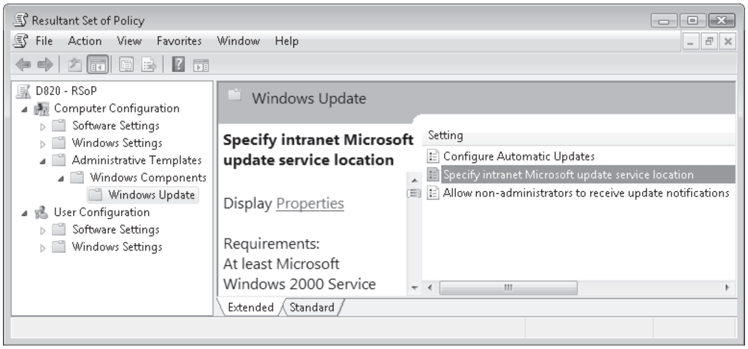
MORE INFO Troubleshooting WSUS

For more information about troubleshooting WSUS, visit *http://technet2.microsoft.com/WindowsServer/en/library/b23562a8-1a97-45c0-833e-084cd463d0371033.mspx?mfr*.

---

3. If you use Group Policy to configure the Windows Update client, use the Resultant Set of Policy (RSOP) tool (Rsop.msc) to verify the configuration. Within RSOP, browse to the Computer Configuration\Administrative Templates\Windows Compo-

nents\Windows Update node and verify the configuration settings. Figure 5-12 shows the RSOP snap-in.



Specify intranet Microsoft update service location

Display Properties

Requirements:
At least Microsoft Windows 2000 Service

Configure Automatic Updates
Specify intranet Microsoft update service location
Allow non-administrators to receive update notifications

Figure 5-12 The RSOP snap-in

If you have identified a problem and made a configuration change that you hope will resolve it, restart the Windows Update service on the client computer to make the change take effect and begin another update cycle. You can do this using the Services console or by running the following two commands:

```
net stop wuauserv
net start wuauserv
```

Within 6 to 10 minutes, Windows Update will attempt to contact your update server.

How to Troubleshoot Restart Manager

Windows Vista includes Windows Installer 4.0, a new version of the application installation infrastructure that is not available for earlier versions of Windows. One of the most significant improvements in Windows Installer 4.0 is Restart Manager. Installation routines can communicate with Restart Manager to indicate which files need to be updated. Restart Manager then coordinates updating the files while minimizing the impact on the user.

The need to update a file that is already in use is one of the most common reasons a user is required to restart a computer. Restart Manager strives to reduce this requirement by closing and restarting programs and services that have files in use. Although some installations will always require the computer to be restarted (especially if they need to upgrade system files that are in use), Restart Manager should minimize this requirement. In Windows Vista all installers must take advantage of the Restart Manager for the program to receive Certified for Windows Vista status.

To diagnose a problem with Restart Manager, open Event Viewer and view the following event logs:

- Windows Logs\Application

- Applications and Services Logs\Microsoft\Windows\RestartManager\Operational

Search for Warning or Error events with a source of RestartManager. The following is an example of a Warning event with Event ID 10010:

```
Application 'C:\Program Files\Microsoft Office\OFFICE11\OUTLOOK.EXE'
(pid 5592) cannot be restarted - Application SID does not match
Conductor SID.
```

You can also view general Windows Update events in the Application log. Search for events with a source of MsiInstaller.

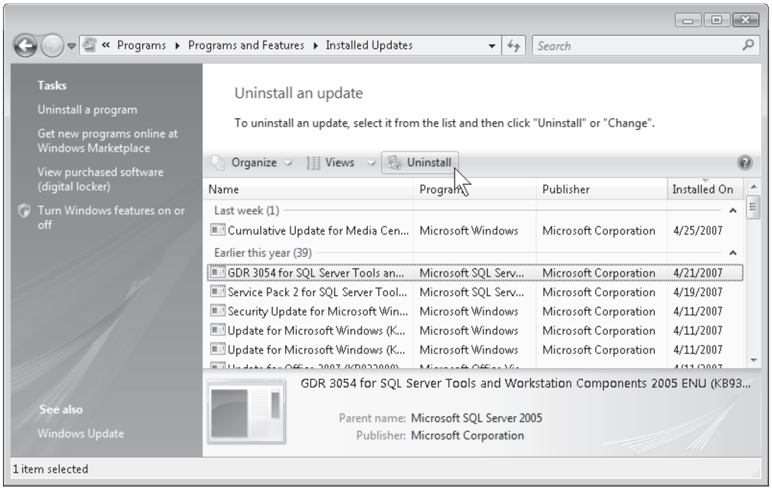
How to Remove Updates

Occasionally, an update might cause compatibility problems. If you experience problems with an application or Windows feature after installing updates and one of the updates was directly related to the problem you are experiencing, you can uninstall the update to determine whether it is related to the problem.

How to Manually Remove an Update

To remove an update, follow these steps:

1. Use Windows Update to view the update history, as described in "How to Troubleshoot Windows Update" earlier in this chapter. View the details of each update to identify the update that might be causing a problem. Make note of the Knowledge Base (KB) number for the update.
2. Click Start, and then click Control Panel.
3. Under Programs, click the Uninstall A Program link.
4. Under Tasks (in the upper-left corner of the window), click the View Installed Updates link.
5. Select the update you want to remove by using the KB number you noted in step 1. Then, click Uninstall, as shown in Figure 5-13.


« Programs ▸ Programs and Features ▸ Installed Updates
Search
Tasks
Uninstall a program
Get new programs online at Windows Marketplace
View purchased software (digital locker)
Turn Windows features on or off
See also
Windows Update
Organize
Views
Uninstall

Uninstall an update

To uninstall an update, select it from the list and then click "Uninstall" or "Change".

Name	Program	Publisher	Installed On
Last week (1)			
Cumulative Update for Media Cen...	Microsoft Windows	Microsoft Corporation	4/25/2007
Earlier this year (39)			
GDR 3054 for SQL Server Tools an...	Microsoft SQL Serv...	Microsoft Corporation	4/21/2007
Service Pack 2 for SQL Server Tool...	Microsoft SQL Serv...	Microsoft Corporation	4/19/2007
Security Update for Microsoft Win...	Microsoft Windows	Microsoft Corporation	4/11/2007
Update for Microsoft Windows (K...	Microsoft Windows	Microsoft Corporation	4/11/2007
Update for Microsoft Windows (K...	Microsoft Windows	Microsoft Corporation	4/11/2007

GDR 3054 for SQL Server Tools and Workstation Components 2005 ENU (KB93...

Parent name: Microsoft SQL Server 2005
Publisher: Microsoft Corporation

1 item selected

Figure 5-13 Uninstalling an update to determine whether it is the source of a problem

6. Follow the prompts that appear and restart the computer if required.

If removing the update does not resolve the problem, you should reapply the update. If removing the update does solve the problem, contact the application developer (in the case of a program incompatibility) or your Microsoft support representative to inform them of the incompatibility. The update probably fixes a different problem, and therefore you should make every effort to fix the compatibility problem and install the update.

How to Remove an Update using WSUS

If you use Windows Software Update Services (WSUS) to distribute updates internally, you might be able to remove the update from the WSUS server to prevent it from being distributed. Many updates do not support being removed. To remove an update for a group of computers or all computers with WUSA, follow these steps:

1. View the WSUS Updates page.
2. Select the update, and then click Change Approval under Update Tasks.
3. Click the Approval list, and then click Remove (if available).
4. Click OK.

How to Recover a Computer that Won't Start

If an update prevents Windows Vista from starting correctly, you can use the Startup Repair tool to quickly restore the computer. To run Startup Repair, follow these steps:

1. Insert the Windows Vista DVD in your computer.

2. Restart your computer. When prompted to boot from the DVD, press any key. If you are not prompted to boot from the DVD, you might have to configure your computer's startup sequence.

   Windows Vista Setup loads.
3. When prompted, select your regional preferences and keyboard layout, and then click Next.
4. Click Repair Your Computer.

   System Recovery scans your hard disks for Windows Vista installations.
5. If the standard Windows Vista drivers do not detect a hard disk because the disk requires drivers that were not included with Windows Vista, click the Load Drivers button to load the drivers, and then select an operating system to repair. Click Next.
6. If Windows failed to start during its last attempt, Windows Vista launches the Startup Repair tool automatically. Otherwise, the Choose A Recovery Tool page appears. Click Startup Repair, and then follow the prompts that appear.
7. After the Startup Repair tool completes its diagnosis and repair, click Click Here For Diagnostic And Repair Details. At the bottom of the report, Startup Repair lists a root cause, if found, and any steps taken to repair the problem.

If Startup Repair does not repair the problem, repeat steps 1–5. Then, in the System Recovery Options dialog box, click System Restore and follow the prompts that appear. Windows Vista automatically creates a System Restore point before any update is installed, so restoring a System Restore point effectively uninstalls any updates.

Practice: Distribute Updates

In this lab, you configure a Windows Vista client to download updates from a WSUS server.

▶ Practice 1: Distribute Updates with Windows Server Update Services

In this practice, you install WSUS on a server, approve updates, and then configure a Windows Vista client to retrieve updates from that server.

1. Log on to a Windows Server 2003 computer as an administrator. If necessary, add the Application Server role (a requirement of WSUS).
2. Visit *http://www.microsoft.com/wsus/* to download and install the latest version of WSUS on your Windows Server 2003 computer.
3. Configure WSUS to install updates only after you approve them. Then, open the WSUS management webpage and approve several recent updates that need to be installed on your Windows Vista computer.
4. Log on to your Windows Vista computer. If you have installed any of the updates you approved within WSUS, uninstall them now using the Control Panel.
5. Click Start, type **Mmc**, and then press Enter.

6. An empty MMC console opens.
7. Click File, and then click Add/Remove Snap-In. From the Available Snap-Ins list, select Group Policy Object Editor. Click Add.
8. On the Welcome To The Group Policy Wizard page, click Browse. Select the Default Domain Policy, and then click OK. Click Finish.
9. In the Add Or Remove Snap-In dialog box, click OK.
10. In the Group Policy Object Editor snap-in, browse to Computer Configuration\Administrative Templates\Windows Components\Windows Update. Specify the policy settings shown in Table 5-2.

Table 5-2 Sample Policy Settings

Policy	Setting
Specify Intranet Microsoft Update Service Location	Enabled. Also, specify your WSUS server name in the Set The Intranet Update Service For Detecting Updates box.
Configure Automatic Updates	Enabled. Also, set Configure Automatic Updating to 4.
Enable Recommended Updates Via Automatic Updates	Enabled.
Enabling Windows Update Power Management To Automatically Wake Up The System To Install Scheduled Updates	Enabled.

11. Click start, type **gpupdate /force**, and press Enter. This retrieves the latest Group Policy settings from the domain controller.
12. Wait a few minutes for Windows Vista to display a notification bubble informing the user of the presence of updates. Allow them to be automatically installed and the computer to restart.

Lesson Summary

- Microsoft provides three techniques for distributing updates: the Windows Update client (built into Windows Vista), Windows Server Update Services (a free tool that can be installed on a Windows Server 2003 computer), and Systems Management Tool (an enterprise software distribution tool). These tools are designed for small, medium, and large organizations, respectively.
- You can install updates interactively using the Windows Update tool. This would be very time-consuming, however. Instead, you should configure Windows Update either using graphical tools or by using Group Policy settings. If you need to install updates immediately (for example, as soon as a user logs on), you can create scripts that install updates.

- If you have a problem installing an update, you can diagnose the problem by viewing the Windows Update history, by analyzing the %windir%\WindowsUpdate.log file, or by examining WSUS logs. You can often resolve simple problems by restarting the Windows Update service.
- If you discover a compatibility problem after deploying an update, you can manually remove it or use WSUS to uninstall it.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 2, "Updating Software." The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is right or wrong are located in the "Answers" section at the end of the book.

1. Which of the following would you recommend for distributing updates to a small business with five Windows Vista client computers?
   - **A.** Instructing employees to manually launch Windows Update when they experience problems
   - **B.** Configuring Windows Update on each computer to download updates directly from Microsoft
   - **C.** Installing WSUS and configuring Windows Update to download updates from the WSUS server
   - **D.** Deploying updates using SMS and WSUS
2. You are working for a medium-sized organization that manages about 100 client computers. The IT department insists on testing all updates before they are applied to computers. Which of the following would you recommend for distributing updates within this organization?
   - **A.** Instructing employees to manually launch Windows Update when they experience problems
   - **B.** Configuring Windows Update on each computer to download updates directly from Microsoft
   - **C.** Installing WSUS and configuring Windows Update to download updates from the WSUS server
   - **D.** Deploying updates using SMS and WSUS

3. You are creating a batch file that installs updates when a Windows Vista computer starts for the first time. How should you do this?
   - **A.** Call Update.exe and provide the path to the update file.
   - **B.** Call Msiexec.exe and provide the path to the update file.
   - **C.** Run the executable file included with the update.
   - **D.** Call Wusa.exe and provide the path to the update file.

Lesson 3: Troubleshooting Windows Defender

Windows Defender, which is also available as a free download for Windows XP, is a tool that informs users about changes programs make to their computers and gives users greater control over which programs are installed. One of Windows Defender's goals is to reduce the impact of spyware and potentially unwanted programs.

However, as with many features that improve security, Windows Defender can cause compatibility problems. This lesson describes how to diagnose and resolve problems using Windows Defender.

After this lesson, you will be able to:

- Troubleshoot problems downloading Windows Defender definitions.
- Identify changes that Windows Defender has blocked.
- Avoid Windows Defender alerts for necessary programs.

Estimated lesson time: 15 minutes

How to Troubleshoot Problems Downloading Definitions

If Windows Defender cannot download updates, the most likely cause is that a firewall is blocking access to Windows Update. Often, network administrators block Windows Update because the organization uses WSUS to approve updates, and client computers should never retrieve updates directly from Microsoft.

To identify the source of the problem, first examine the System event log for information about updates. To view the System event log, follow these steps:

1. Click Start. Right-click Computer, and then click Manage. Provide administrative credentials at the UAC prompt.
2. Under System Tools, expand Event Viewer, Windows Logs, and then select System.

Within the System event log, view events with a source of "Windows Defender." The following shows an event with an Event ID of 2000, in which Windows Defender successfully installed a definition update:

```
Windows Defender signature version has been updated.
     Current Signature Version: 1.15.2224.9
     Previous Signature Version: 1.15.2220.1
     Update Source: User
     Signature Type: AntiSpyware
     Update Type: Delta
     User: NT AUTHORITY\SYSTEM
     Current Engine Version: 1.1.2101.0
     Previous Engine Version: 1.1.2101.0
```

Windows Defender uses Event ID 2002 to log updates to the Windows Defender engine itself.

Next, examine the %windir%\WindowsUpdate.log file for error messages, and then search related Microsoft Knowledge Base articles for more information about errors in the WindowsUpdate.log file. This log file will typically have thousands of entries, but you can quickly find the Windows Defender–related entries by searching for the phrase “Windows Defender.” The following example shows a successful Windows Defender definition update (with some fields omitted for simplicity):

```
DnldMgr     *************
DnldMgr     ** START **  DnldMgr: Downloading updates [CallerId = AutomaticUpdates]
DnldMgr     *********
DnldMgr       * Call ID = {DA5A072F-A9F9-43B4-B67B-5435D3301B01}
DnldMgr       * Priority = 2, Interactive = 0, Owner is system = 1,
 Explicit proxy = 0, Proxy session id = -1, ServiceId =
{7971F918-A847-4430-9279-4A52D1EFE18D}
DnldMgr       * Updates to download = 1
Agent       *   Title = Definition Update 1.14.1921.2 for Windows Defender (KB915597)
Agent       *   UpdateId = {EAF6F766-3E8B-4F45-B50F-9F30EF004044}.100
Agent       *     Bundles 1 updates:
Agent       *       {B47FBF08-503F-428C-96BB-11509FBDF3A5}.100
DtaStor     Update service properties: service registered with AU is
 {7971F918-A847-4430-9279-4A52D1EFE18D}
DnldMgr     ***********  DnldMgr: New download job [UpdateId =
{B47FBF08-503F-428C-96BB-11509FBDF3A5}.100]  ***********
DnldMgr       * BITS job initialized, JobId = {99086C54-EAD1-4093-A226-92F021003FCF}
DnldMgr       * Downloading from http://au.download.windowsupdate.com/msdownload/update
/v3-19990518/cabpool/mpas-fe_7e35a762b4eb36bdef0bcfddafbafc1dc750dd54.exe
 to C:\Windows\SoftwareDistribution\Download
\714d679af4e2c432e404256a7e7e0782
\7e35a762b4eb36bdef0bcfddafbafc1dc750dd54 (full file).
Agent     *********
Agent     **  END  **  Agent: Downloading updates [CallerId = AutomaticUpdates]
Agent     *************
Report     REPORT EVENT: {712F6CF3-4DAC-4DBD-AA73-7AB74B5DC419}
2006-11-29 16:17:13:272-0500     1     147     101
{00000000-0000-0000-0000-000000000000}     0     0
AutomaticUpdates     Success     Software Synchronization
Windows Update Client successfully detected 2 updates.
```

As you can see from this log file excerpt, the Windows Defender update agent logs the exact source and destination location. If you experience a problem downloading definitions, you can attempt to download the specified update file (*http://au.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/mpas-fe_7e35a762b4eb36bdef0bcfddafbafc1dc750dd54.exe* in the sample log file) directly from the computer by using Internet Explorer. If you can’t download the file in Internet Explorer, the Windows Defender update agent also won’t be able to download the file.

If you can't manually reach the file by using Internet Explorer, verify the following:

- You can use a Web browser to reach the public Internet.
- If your computer is a member of a domain, it has the latest version of the domain Group Policy settings. You can refresh these settings by running **gpupdate /force** with administrative privileges. These settings might configure the Windows Update client to retrieve updates from a WSUS server instead of downloading them directly from Microsoft.
- Any firewalls allow HTTP requests to the windowsupdate.com domain and subdomains (that is, download.windowsupdate.com).
- Internet Explorer is not configured to block requests to the windowsupdate.com domain. To verify that the problem is not related to the Internet Explorer configuration, add http://*.windowsupdate.com/ to the computer's Trusted Sites list.

How to Identify Changes Blocked by Windows Defender

Windows Defender adds events to the System event log when it detects changes that require the user's confirmation. Within the System event log, view events with a source of "Windows Defender." The following shows an event with an Event ID of 3004, in which Windows Defender blocked the installation of a program that registered an icon in the system tray:

```
Windows Defender Real-Time Protection agent has detected changes.
Microsoft recommends you analyze the software that made these changes
for potential risks. You can use information about how these programs
 operate to choose whether to allow them to run or remove them from
your computer.  Allow changes only if you trust the program or the
software publisher. Windows Defender can't undo changes that you allow.
 For more information please see the following:
Not Applicable
     Scan ID: {14DC2DCC-A5C9-47CF-90EC-0B01BF0C7B58}
     User: computer\user
     Name: Unknown
     ID:
     Severity ID:
     Category ID:
     Path Found: regkey:HKLM\Software\Microsoft\Windows\CurrentVersion\Run
\\SigmatelSysTrayApp;runkey:HKLM\Software\Microsoft\Windows
\CurrentVersion\Run\\SigmatelSysTrayApp;file:C:\Windows\sttray.exe
     Alert Type: Unclassified software
     Detection Type:
```

Shortly thereafter, the System event log might show an event with an Event ID of 3005, which will show how the user chose to handle the change. The following example event demonstrates that the user approved the previous change, as evidenced by the Ignore action:

```
Windows Defender Real-Time Protection agent has taken action to protect
 this machine from spyware or other potentially unwanted software.
 For more information please see the following:
Not Applicable
```

```
Scan ID: {14DC2DCC-A5C9-47CF-90EC-0B01BF0C7B58}
User: computer\user
Name: Unknown
ID:
Severity ID:
Category ID:
Alert Type: Unclassified software
Action: Ignore
```

You can use the Scan ID to match related Windows Defender events.

How to Work Around False Alarms

It is possible for Windows Defender to warn users about a file that you consider to be trustworthy. You can selectively avoid these warnings by trusting specific files and folders or by disabling different types of real-time protection. Making these changes always requires administrator privileges.

The sections that follow describe different techniques for avoiding these false alarms. Whenever possible, ignore specific files and folders that cause problems in your organization. Only disable real-time protection or heuristics if the Windows Defender warnings are extremely problematic and frequent.

NOTE Tracking Windows Defender changes

Malware might attempt to change the Windows Defender configuration to avoid detection. So that you can track all Windows Defender configuration changes, it adds events with a source of "Windows Defender" and an Event ID of 5007 to the System event log.

How to Ignore Specific Files and Folders

To configure Windows Defender to ignore specific files or folders, follow these steps:

1. Start Windows Defender. Then, click Tools on the toolbar.
2. Click the Options link.
3. Scroll down to the Advanced Options section.
4. Under Do Not Scan These Files Or Locations, click the Add button. In the Browse For Files Or Folders dialog box, select the file or folder you want Windows Defender to ignore. Click OK.

NOTE Where to find Document folders

The Browse For Files Or Folders dialog box doesn't show users' Documents folders. However, you can find these under C:\Users by default.

---

5. Click Save.

Windows Vista will not scan the specified files or folders.

How to Ignore Specific Types of Real-Time Protection

Windows Defender monitors many aspects of the operating system. You can disable any of these aspects if they prove problematic in your organization because of a large number of false alarms.

1. Start Windows Defender. Then, click Tools on the toolbar.
2. Click the Options link.
3. Scroll down to the Real-Time Protection Options section. Clear the check boxes for the specific types of protection you want to disable:
    - **Auto Start** Monitors changes to the list of programs that start automatically when Windows starts or when a user logs on. This is one of the most important configuration settings to monitor; if unwanted software adds itself to the Auto Start list, it will continue to run after restarting the computer.
    - **System Configuration (Settings)** Monitors changes to the system configuration. This is important to leave enabled because many types of unwanted software attempt to change aspects of the computer's configuration.
    - **Internet Explorer Add-Ons** Monitors changes to Internet Explorer add-ons. Typically, you should leave this enabled even if you have a custom add-on that you need installed. If this is disabled, unwanted software might be able to install add-ons, which can change how webpages appear.
    - **Internet Explorer Configurations (Settings)** Monitors changes to Internet Explorer configuration. This is very important, because changes to the Web browser configuration could disable important security settings, exposing weaknesses that other unwanted software might abuse.
    - **Internet Explorer Downloads** Monitors files that users download with Internet Explorer. Many unwanted software installations are initiated when a user intentionally downloads a program because the program contains unwanted, bundled software. Disabling this type of real-time protection increases the likelihood of users accidentally installing unwanted software. You should clear this setting only if you have tightly configured Internet Explorer to prevent users from downloading unwanted software.
    - **Services And Drivers** Monitors additions and changes to services and drivers. Services and drivers can start automatically and run with system-level privileges, so it is important to keep this real-time protection enabled.
    - **Application Execution** Monitors when unknown applications run.

- ❑ **Application Registration** Monitors when an application installs itself.
- ❑ **Windows Add-Ons** Monitors new components that register themselves as add-ons.
- ❑ **Software That Has Not Yet Been Classified For Risks** Monitors software that does not yet have a Windows Defender definition. This capability allows Windows Defender to detect potentially unwanted software that Microsoft has not analyzed.
- ❑ **Changes Made To Your Computer By Software That Is Permitted To Run** This is the only form of real-time protection that is disabled by default. You can enable this for additional security; however, users can find it annoying.

4. Click Save.

Windows Vista will not perform the types of scans for which you cleared the associated check boxes. If you must disable some form of real-time protection to troubleshoot an issue, disable one form of real-time protection at a time and test the problem to verify that it is fixed. Avoid disabling real-time protection unnecessarily to reduce security risks.

How to Ignore False Alarms for Unknown Software

Windows Vista can use heuristics to alert users to unknown software running. Unknown software includes any program that Microsoft has not yet analyzed and provided a definition for. If you determine that Windows Defender frequently alerts users to problems detected using heuristics, you can disable this feature by clearing the Use Heuristics To Detect Potentially Harmful Or Unwanted Behavior By Software That Hasn't Been Analyzed For Risks check box on the Windows Defender Options page.

Practice: Distribute Updates and Analyze Windows Defender Problems

In this practice, you configure a Windows Vista client to download updates from a WSUS server. Then you simulate the installation of an application by monitoring changes to a file that Windows Defender protects.

▶ Practice 1: Analyze Windows Defender Changes

In this practice, you perform a change that Windows Defender will detect as potentially unwanted. Then you examine the System event log to identify how Windows Defender records the attempted change.

1. Log on to your Windows Vista test computer.
2. Click Start. Type **notepad %windir%\system32\drivers\etc\hosts**. Press Ctrl+Shift+Enter to run Notepad with administrative privileges. Respond to the UAC prompt.

   Notepad opens your Hosts file, which is one of the files Windows Defender monitors.

3. At the top of the file, type **# Testing Windows Defender**. Save the file and close Notepad.
4. Click Start, right-click Computer, and then click Manage. Respond to the UAC prompt.

   Windows Vista opens Computer Management.
5. Expand Event Viewer, Windows Logs, and then select System.
6. Identify the Windows Defender event that describes the change you made to the Hosts file.

In production environments you can use this technique to identify important or dangerous change attempts that Windows Defender might have blocked.

Lesson Summary

- To troubleshoot problems downloading updated Windows Defender definitions, view the System event log. For more detailed information, analyze the %windir%\Windowsupdate.log file.
- To identify changes that Windows Defender has blocked, search the System event log for events with a source of "Windows Defender."
- You should test programs before deploying them to Windows Vista clients to verify that they work properly with Windows Defender. If Windows Defender does block legitimate changes made by one of your programs, you can configure Windows Defender to ignore the change to prevent problems when you deploy the program.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 3, "Troubleshooting Windows Defender." The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is right or wrong are located in the "Answers" section at the end of the book.

---

1. A user complains that an application installed incorrectly. How can you determine whether Windows Defender blocked any aspect of the application installation? (Choose two. Each correct answer is a complete solution.)
   - A. Examine the System event log.
   - B. Examine the Application event log.
   - C. Examine the Security event log.
   - D. View the Windows Defender History.

2. Where would you look to identify whether Windows Defender was experiencing problems downloading updated definitions from Microsoft?
   - **A.** The System event log
   - **B.** The Application event log
   - **C.** The Security event log
   - **D.** The Windows Defender History
3. Which of the following types of changes might Windows Defender alert the user to? (Choose all that apply.)
   - **A.** A new service being installed
   - **B.** A program that automatically starts
   - **C.** A Microsoft Word document that contains a macro
   - **D.** An Internet Explorer Add-on being installed

Lesson 4: Supporting Applications

Windows Vista alone isn't enough for most users—they need applications as well. Although every application has unique support requirements, all applications have some things in common. This lesson describes the most common way to deploy, install, and uninstall applications and explains how to configure multiple monitors to give users more desktop space and how to configure the Windows Sidebar.

After this lesson, you will be able to:

- Deploy and install applications.
- Configure and maintain applications.
- Run the Microsoft Support Diagnostic Tool.

Estimated lesson time: 15 minutes

Deploying Applications

Before users can run most applications, they must be installed. To simplify installation, Windows Vista (as well as earlier versions of Windows) includes Windows Installer. Windows Installer allows you to install programs manually, from a script, or using Group Policy software distribution. The sections that follow provide an overview of Windows Installer and instructions for installing Windows Installer packages.

Windows Installer

Windows Installer is a Windows component that makes it easy to install, update, and uninstall programs. Windows Installer relies on a special file format with an .MSI file extension that contains all the files and settings required to install an application. Almost all applications developed in recent years include an .MSI file to allow the application to be deployed with Windows Installer.

If an application provides a Windows Installer package, you can deploy it in several ways:

- Manually, using a wizard interface. You can start the manual setup simply by double-clicking the .MSI file from the computer you want to install the program on. This technique resembles running the Setup.exe file included with most software installer's programs.
- Automatically, from a script using the MsiExec.exe tool. All Windows Installer packages can be automatically installed without prompting the user.
- Using Group Policy Software Distribution. Group Policy only supports distributing .MSI files, so many organizations often repackage an application in an .MSI file if it does not already include one.

MORE INFO **Repackaging programs**

For more information about repackaging programs, refer to the Microsoft Solution Accelerator for Business Desktop Deployment 2007 at *http://www.microsoft.com/technet/desktopdeployment/bdd/2007/*.

- Using Microsoft Systems Management Server (SMS).

MORE INFO **SMS**

For more information about SMS, visit *http://www.microsoft.com/sms*.

Using the MsiExec.exe Tool

You can use MsiExec.exe to install Windows Installer packages automatically. For example, to install a Windows Installer package named Update.MSI without prompting the user, you would run the following command:

```
Msiexec /package Update.msi /quiet
```

Similarly, to uninstall the same file, you would run the following command:

```
Msiexec /uninstall Update.msi /quiet
```

MsiExec.exe also supports the following useful parameters:

- **/norestart** Prevents Windows from restarting, even if the application requires it. Use this parameter when you will be installing several programs in sequence and you don't want Windows to restart until after all programs have been installed.
- **/promptrestart** Prompts the user to restart the computer only if a restart is necessary.
- **/forcerestart** Always restarts the computer after installation, even if it is not required. You might use this if you previously used /norestart to install another program.

If you experience a problem during an automatic installation with the /quiet parameter, MsiExec does not inform the user of the problem; it just fails quietly. By default, MsiExec adds events to the Application event log with a source of MsiInstaller after any successful installation or unsuccessful installation attempt. For example, event ID 11925 indicates that an installation failed because the package requires administrative privileges to install, and the user lacked those privileges, and it would include a description resembling the following:

```
Product: Microsoft Baseline Security Analyzer 2.1 -- Error 1925.
You do not have sufficient privileges to complete this installation
for all users of the machine.  Log on as administrator and then
retry this installation.
```

Similarly, Event ID 11730 indicates that an uninstallation failed because the user lacked sufficient privileges, and it includes a description resembling the following:

```
Product: Microsoft Baseline Security Analyzer 2.1 -- Error 1730.
You must be an Administrator to remove this application. To remove
this application, you can log on as an Administrator, or contact your technical support group
for assistance.
```

A successful installation generates a message with Event ID 11707, with a description resembling the following:

```
Product: Microsoft Baseline Security Analyzer 2.1 Ð
Installation completed successfully.
```

The Application event log provides most of the troubleshooting information you will need. However, you can use the */l <log_file_name>* parameter with MsiExec to create a detailed text log file, as the following example demonstrates. Typically, this information contains the same information as the events in the Application event log.

```
Msiexec /uninstall Update.msi /quiet /l install_log.txt
```

For complete usage information, click Start, type **Msiexec**, and then press Enter.

Using Group Policy Software Distribution

In Active Directory environments, you can use Group Policy Software Distribution to deploy Windows Installer packages to member computers. To deploy a package using Group Policy, follow these steps:

1. Open the Group Policy Object Editor for the Group Policy Object you want to use to distribute the software.
2. Expand either Computer Configuration or User Configuration, and then select Software Settings.
3. Right-click Software Installation, click New, and then click Package.
4. In the Open dialog box, type the UNC path to the .MSI package you want to deploy, and then click Open. It's important that you specify the location with a UNC path (such as \\server\share\package.msi) that all clients can also use to access the .MSI file.
5. In the Deploy Software dialog box, select one of the following options:
    - ❑ **Published** Make the application available to users from the Control Panel. Publishing is an option only when deploying the package using the User Configuration node of the Group Policy object.
    - ❑ **Assigned** Automatically install the application with the default settings the next time Group Policy is applied. If you added the package under Computer Configuration, it will be installed regardless of which user logs on. If you install the package under User Configuration, it will be installed only when that user logs on.

  - ☐ **Advanced** Configure additional options by immediately viewing the package properties. You can also configure settings by viewing the package properties later.

6. Click OK.
7. In the left pane of the Group Policy Object Editor, click Software Installation. You will see your Windows Installer package in the right pane.

To edit the settings of a package after adding it to Group Policy, click the Software Installation node in the Group Policy Object Editor. In the right pane, right-click the package, and then click Properties.

One of the most useful settings is found on the Deployment tab; by selecting the Uninstall This Application When It Falls Out Of The Scope Of Management check box, you configure Group Policy to automatically remove the program if the Group Policy object no longer applies to a user or computer. For example, you could use this to automatically uninstall accounting software if a member of the Accounting organizational unit (OU) moved to the Human Resources OU.

Configuring Applications and the Desktop Environment

Some applications and environments require special configuration, such as changing environment variables. Another common configuration request is using multiple monitors, enabling users to maximize two or more windows on different displays. Additionally, Windows Vista includes a new application platform called Windows Sidebar that you need to know how to disable or configure. The sections that follow describe each of these features.

Configuring Environment Variables

Environment variables are settings that are universal to Windows or to a user that applications reference to identify the location of system files, user documents, temporary files, and many other settings. Typically, you should leave environment variables at their default settings to provide the greatest application compatibility because some applications simply assume that the user has environment variables set to the default values.

You can view environment variables from a command prompt by running the Set command, as the following example shows:

```
C:\>Set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\user1\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=D820
ComSpec=C:\Windows\system32\cmd.exe
HOMEDRIVE=C:
HOMEPATH=\Users\user1
LOCALAPPDATA=C:\Users\user1\AppData\Local
LOGONSERVER=\\D820
```

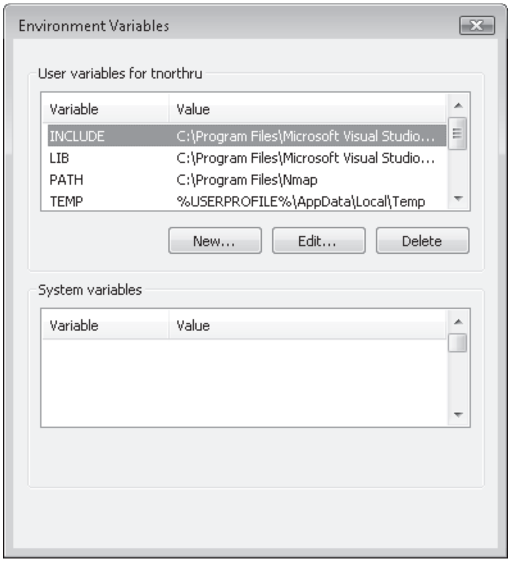
```
NUMBER_OF_PROCESSORS=2
Path=C:\Windows\system32;C:\Windows;C:\Program Files\Microsoft SQL Server\90\DTS\Binn\;
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
PUBLIC=C:\Users\Public
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\user1\AppData\Local\Temp
TMP=C:\Users\user1\AppData\Local\Temp
USERDOMAIN=D820
USERNAME=user1
USERPROFILE=C:\Users\user1
windir=C:\Windows
```

You can also use the Set command to change environment variables. For example, to change the temporary folder to C:\Temp for the current user, you could run the following command:

```
set TEMP=C:\temp
```

You can also change environment variables using the System Properties dialog box by following these steps:

1. Click Start, right-click Computer, and then click Properties.
2. Click the Advanced System Settings link, and then respond to the UAC prompt that appears.
3. Click the Advanced tab, and then click the Environment Variables button.
4. The Environment Variables dialog box appears, as shown in Figure 5-14.



Variable	Value
INCLUDE	C:\Program Files\Microsoft Visual Studio...
LIB	C:\Program Files\Microsoft Visual Studio...
PATH	C:\Program Files\Nmap
TEMP	%USERPROFILE%\AppData\Local\Temp

Variable	Value

Figure 5-14 The Environment Variables dialog box

5. Select the environment variable you want to change, and then click Edit.
6. Type the new value, and then click OK.
7. Click OK again to close the Environment Variables dialog box, and then click OK again to close the System Properties dialog box.

You can reference environment variables in scripts by surrounding the environment variable name with percent symbols. For example, running the following command at a command prompt would display the name of the current domain:

```
echo %userdomain%
```

Configuring Multiple Monitors

One of the best ways to increase the usefulness of Windows is to double the desktop space by adding a second monitor. If you do add a second monitor, you have two options for configuring it:

- **Mirrored** The same desktop shows on both monitors. This is primarily useful for putting on a presentation when a mobile computer is connected to a projector. By mirroring both screens, the presenter can face the audience and look at the built-in display while being assured that the display on the projector matches exactly. To configure an extended desktop, open the Display Properties dialog box, select the new monitor, and then clear the Extend The Desktop Onto This Monitor check box.
- **Extended desktop** Windows Vista extends the desktop across two monitors, allowing the user to move windows between the displays. For example, a user could keep e-mail open on one screen and Microsoft Word on another, or a developer could keep his or her development open on one screen and reference files on the other. To configure an extended desktop, open the Display Properties dialog box, select the new monitor, and then select the Extend The Desktop Onto This Monitor check box. Then, click the monitor that you want to have the taskbar and Start menu and select the This Is My Main Monitor check box.

To open the Display Properties dialog box, follow these steps:

1. Click Start, and then click Control Panel.
2. Under Appearance And Personalization, click the Adjust Screen Resolution link.
3. Make your configuration changes, and then click OK.

Configuring Windows Sidebar

Windows Sidebar provides a platform for Windows Sidebar Gadgets, as shown in Figure 5-15. Gadgets are visually small applications that reside on the Sidebar or that you can remove to float on the desktop. Windows Vista includes several gadgets, and you can download others from *http://gallery.live.com/results.aspx?l=1*.

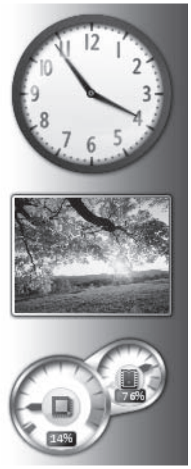


Figure 5-15 Windows Sidebar Gadgets

You can control the Sidebar by using Group Policy. Sidebar Group Policy settings are located in both Computer Configuration and User Configuration at Administrative Templates\Windows Components\Windows Sidebar. You can configure the following settings:

- **Override The More Gadgets Link** By right-clicking the Sidebar, clicking Add Gadgets, and then clicking Get More Gadgets Online, users visit a Microsoft site where they can download new gadgets. Enable this setting to provide your own link for more gadgets (for example, to allow users to download gadgets from an intranet website).
- **Turn Off Windows Sidebar** Enable this setting to prevent Windows Sidebar from running.
- **Disable Unpacking And Installation Of Gadgets That Are Not Digitally Signed** Enable this setting to prevent Windows Sidebar from running gadgets that are not digitally signed. If you leave this setting at the default (disabled), Sidebar will warn users that a gadget is not digitally signed but still allow it to be installed.
- **Turn Off User Installed Windows Sidebar Gadgets** Enable this setting to prevent users from installing their own gadgets.

The Microsoft Support Diagnostic Tool

The Microsoft Support Diagnostic Tool (MSDT) is a Windows Vista feature that Microsoft Support might instruct you to use to gather information about a problem. This can speed the troubleshooting process by decreasing the amount of information users must convey using the phone or e-mail. The tool collects some information by prompting the user and also gathers other information automatically based on computer settings and recorded events. Microsoft Support will provide a pass key and incident number for the user to enter into the tool to allow the tool to retrieve problem-specific configuration settings.

If configured by Microsoft Support, MSDT will download and run other diagnostic tools. After gathering the required information, MSDT can send the information to Microsoft across the Internet. If the computer with the problem isn't connected to the Internet, you can save the data to removable storage, such as a universal serial bus (USB) flash drive, and then send the data to Microsoft using a different computer.

You need to start MSDT only when instructed by Microsoft Support. In that case, they will direct you to the MSDT webpage, which will allow you to launch the tool. You must have administrative privileges to launch MSDT (you will receive a User Account Control prompt). To manually run MSDT, follow these steps:

1. Click Start, type **MSDT**, and then press Enter.
2. Respond to the UAC prompt that appears.

   MSDT appears.
3. On the Which Computer Has A Problem page, click This Computer or A Different Computer.
4. On the Type Your Pass Key page, type the pass key provided by Microsoft support.

   MSDT will connect to Microsoft to retrieve problem-specific information and diagnostic tools.
5. Follow the prompts that appear (the specific steps will vary depending on the nature of the problem).

Practice: Automating Software Installations

In this practice, you automate a software installation using a batch file, which you might do in a production environment to automatically install a program using a logon script.

▶ Practice 1: Automatically Installing a Windows Installer Package

In this practice, you use MsiExec to automatically install and then uninstall a Windows Installer package using a script.

1. Visit *http://www.microsoft.com/mbsa/* and download the latest version of the Microsoft Baseline Security Advisor (MBSA) from Microsoft. Save it to your Windows Vista computer without running it. Make note of the name and the path of the .MSI file.
2. Open Notepad and create a new batch file named InstallApp.bat. Save the file in your Documents folder.
3. Use Notepad to add the following line to your batch file and save the file:

   msiexec /package <*path*>\<*filename*>.msi /passive

   For example, if you saved the MBSA .MSI file as mbsasetup-en.msi in the root of your C drive, you would add the following line to your batch file:

   ```
   msiexec /package C:\mbsasetup-en.msi /passive
   ```

4. Now, double-click the InstallApp.bat file from Explorer. Wait a few moments while Windows Installer begins to install MBSA. Respond to the UAC prompt that appears. Because you used the /passive parameter, Windows Installer will display a progress bar and a UAC prompt, but it will not prompt you for any configuration information. Instead, Windows Installer will use the default settings.
5. After several minutes, verify that MBSA is installed correctly by clicking Start, All Programs, and then clicking Microsoft Baseline Security Advisor to launch the tool. Close the tool after you verify that it runs correctly.
6. Use Notepad to add the replace the current command in your batch file with the following command:

   msiexec /uninstall <*path*>\<*filename*>.msi /quiet
7. Now, right-click the InstallApp.bat file in Explorer, and then click Run As Administrator. Respond to the UAC prompt that appears. Because you are using /quiet this time, Windows Installer cannot provide a UAC prompt to gain administrative credentials, and you must run it with sufficient privileges.

   The batch file starts Windows Installer, which uninstalls MBSA without prompting you.
8. Wait several minutes, and then verify that MBSA was uninstalled correctly by looking for the shortcut on the Start menu.

Lesson Summary

- Windows Installer simplifies the installation and management of Windows applications. Applications are distributed in Windows Installer packages, which are files that use an .MSI file extension. Although you can install a Windows Installer package by simply double-clicking it, you can also automate the installation using the MsiExec command-line tool or by using Group Policy software distribution.
- Windows Vista stores some computer-wide and user-wide settings in environment variables. For example, applications can determine the current temporary directory by accessing the %TEMP% environment variable. You can change environment variables using the Set command-line utility or using the System Properties dialog box. If you need to configure a user for multiple monitors side-by-side, view the Desktop Properties dialog box, select the new monitor, and then select the Extend The Desktop Onto This Monitor check box. If a user wants to mirror the display on a projector, clear that check box.
- If you need to escalate a problem to Microsoft Support, they might request that you run the Microsoft Support Diagnostic Tool. Although the specific steps are problem-specific, you can start the tool by clicking Start, typing **MSDT**, and then pressing Enter.

Lesson Review

You can use the following questions to test your knowledge of the information in Lesson 4, “Supporting Applications.” The questions are also available on the companion CD if you prefer to review them in electronic form.

NOTE Answers

Answers to these questions and explanations of why each answer choice is right or wrong are located in the “Answers” section at the end of the book.

---

1. You are a desktop support engineer. You need to distribute a Windows Installer package to the mobile computer user’s OU in your Active Directory domain. To prevent the large download from occurring when users are connected to the internal network using a low-bandwidth connection, you want users to manually initiate the installation. Which of the following software distribution options should you choose?
   - **A.** Published under Computer Configuration
   - **B.** Published under User Configuration
   - **C.** Assigned under Computer Configuration
   - **D.** Assigned under User Configuration
2. You are a Windows Vista systems administrator. You need to create a logon script that installs a Windows Installer package without prompting the user. Which of the following tools would you use to install the package?
   - **A.** FC
   - **B.** RACAgent
   - **C.** WUAgent
   - **D.** MSIExec
3. Your chief security officer has decided that users should not be able to run any Windows Sidebar Gadgets. Which is the most effective way to implement this?
   - **A.** In the Default Domain Group Policy Object, disable the Turn Off User Installed Windows Sidebar Gadgets policy.
   - **B.** In the Default Domain Group Policy Object, enable the Turn Off User Installed Windows Sidebar Gadgets policy.
   - **C.** In the Default Domain Group Policy Object, enable the Turn Off Windows Sidebar policy.
   - **D.** Use a software restriction to block all *.gadget programs.

Chapter Review

To further practice and reinforce the skills you learned in this chapter, you can

- Review the chapter summary.
- Review the list of key terms introduced in this chapter.
- Complete the case scenarios. These scenarios set up real-world situations involving the topics of this chapter and ask you to create a solution.
- Complete the suggested practices.
- Take a practice test.

Chapter Summary

- Internet Explorer is one of the most important tools in Windows Vista because it provides users access to Web applications and the Internet. Therefore, it's vital that you know how to configure Internet Explorer and troubleshoot common problems. Historically, many users have experienced problems with add-ons, which extend Internet Explorer's capabilities but also have the potential to behave unreliably or maliciously. Fortunately, Internet Explorer gives administrators complete control over which add-ons can be installed, as well as the capability to quickly start Internet Explorer without any add-ons. To reduce security risks when using Internet Explorer, Protected Mode runs Internet Explorer with minimal privileges. If a webpage, Internet Explorer, an add-on, or any process launched from within Internet Explorer requires elevated privileges, the elevation must be approved before Internet Explorer can take action. To provide privacy and authentication, many websites use SSL certificates. Therefore, it's vital that you understand the causes of common certificate problems and how to fix these problems.
- Over time, computers can become less secure because attackers might discover new vulnerabilities. To maintain the security of your computers, you must regularly install updates. Microsoft provides several techniques for distributing updates throughout an organization. You should be familiar with these techniques, as well as the tools for troubleshooting problems deploying updates.
- To reduce the risk of potentially unwanted software, Windows Defender prompts users when some types of software attempt to make changes. Users can then choose to allow or block a change. To avoid compatibility problems, you should test applications with Windows Defender enabled and configure Windows Defender to ignore changes made by the applications your users require.

- Windows Installer makes it much simpler to install programs on Windows Vista. Most programs include a Windows Installer package in an .MSI file. With this .MSI file, you can manually install it just like a standard Setup.exe file, you can distribute it using Group Policy software distribution, or you can install it using the MsiExec.exe command-line tool. Applications use environment variables to determine computer settings such as the user's home directory, the location of system files, and where temporary files should be stored.

Key Terms

Do you know what these key terms mean? You can check your answers by looking up the terms in the glossary at the end of the book.

- ActiveX
- Mandatory Integrity Control (MIC)
- Protected Mode
- Protected Mode Compatibility Layer
- Restart Manager
- Windows Defender
- Windows Server Update Services (WSUS)

Case Scenarios

In the following case scenarios, you will apply what you've learned about how to manage Internet Explorer and Windows Update. You can find answers to these questions in the "Answers" section at the end of this book.

Case Scenario 1: Unwanted Internet Explorer Add-On

You are a systems administrator for Humongous Insurance. Recently, one of your brokers called the support desk because he was experiencing odd problems when using Internet Explorer. Specifically, his home page had changed, and the pop-up blocker no longer seemed to be working.

Your manager is concerned that this will be more than an isolated incident and asks you to interview key people and then come to his office to make recommendations about how to deal with this type of problem in the future.

Interviews

Following is a list of company personnel interviewed and their statements:

- **David Barber, Broker** “I had installed an add-on because it said it would make browsing the Web faster. I didn’t notice any improvement. After that, though, my Internet Explorer home page changed, and I began to get a lot of advertisements popping up on my screen.”
- **Julian Price, Internet Development Project Manager** “We recently converted all of our internal software to the ASP.NET Web application platform. To do some of the more complicated stuff, we install custom client-side add-ons in Internet Explorer. So, whatever you do, don’t block all add-ons. We use add-ons internally, and we update them regularly, so we really need users to be able to install the add-ons automatically.”

Questions

Answer the following questions for your manager:

1. If this comes up again, what’s the best way to remove the unwanted add-on?
2. Are there any features enabled by default in Windows Vista that protect users from unwanted add-ons? What are they?
3. What’s the best way to prevent unwanted add-ons in the future?

Case Scenario 2: Distribute Updates

You are a systems administrator working at the administrative offices of Fourth Coffee, a small shop with three Windows XP computers, three Windows Vista computers, and a Windows Server 2003 domain controller. Recently, an update caused a compatibility problem with Fourth Coffee’s internal accounting program. Currently, all computers are configured to download updates from Microsoft and automatically install them overnight.

Your manager has asked you to find a way to test updates before they’re deployed to the computers in your organization.

Questions

Answer the following questions for your manager:

1. How can you test updates before they’re deployed?
2. Would your recommended deployment technology require any infrastructure?
3. Will your recommended deployment technology work with both the Windows XP and Windows Vista computers?
4. How can you configure the client computers to use your new deployment technology?

Suggested Practices

To successfully master the objectives covered by this chapter, complete the following tasks.

Configuring and Troubleshooting Internet Explorer

For this task, you should complete at least Practices 1 through 3. If you want in-depth knowledge of how Internet Explorer handles both legitimate and malicious changes, complete Practice 4 as well.

- **Practice 1: Manage Add-ons** On your day-to-day computer, open Internet Explorer and view the Manage Add-Ons dialog box. Examine the different add-ons that are already installed.
- **Practice 2: Browsing Without Add-ons** Launch Internet Explorer with add-ons disabled. Browse to your favorite websites and notice any differences caused by the missing add-ons.
- **Practice 3: Applications that Internet Explorer Has Virtualized** On your day-to-day computer, use Explorer to browse \%userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Virtualized\ and its subfolders. Make note of the applications that the Internet Explorer compatibility layer has virtualized and the types of files that were virtualized.
- **Practice 4: Browsing Dangerous Websites** Perform a fresh installation of Windows Vista. Browse to your favorite websites and notice how the Information Bar, Protected Mode, and UAC work together to protect the user from potentially unwanted add-ons. Next, use Internet Explorer to browse to potentially dangerous websites that might try to install malicious software and view how Internet Explorer responds (hint: search for combinations of words such as “crack,” “hack,” “warez,” and “serials”).

Updating Software

For this task, you should complete all three practices to gain experience analyzing update installations.

- **Practice 1: Remove an Update** Uninstall a recent update, and then reinstall it.
- **Practice 2: View the System Event Log** Examine the System event log and identify any updates that have been recently installed.
- **Practice 3: Examine the WindowsUpdate.log File** Examine the %windir%\WindowsUpdate.log file and identify any updates that have been recently installed.

Troubleshoot Windows Defender issues

For this task, you should complete all three practices to gain experience with Windows Defender.

- **Practice 1** On a test computer with Windows Defender enabled, download and install a program that includes potentially unwanted software. For example, you might install a peer-to-peer file sharing application. Monitor Windows Defender notifications. Choose to reject any changes made by the potentially unwanted software.
- **Practice 2** Using the same potentially unwanted software, configure Windows Defender to ignore the software so that it installs correctly without alerting the user.
- **Practice 3** Examine the Windows Defender history and the System event log to analyze changes monitored by Windows Defender during the software installation.

Take a Practice Test

The practice tests on this book's companion CD offer many options. For example, you can test yourself on just the content covered in this chapter, or you can test yourself on all the 70-622 certification exam content. You can set up the test so that it closely simulates the experience of taking a certification exam, or you can set it up in study mode so that you can look at the correct answers and explanations after you answer each question.

MORE INFO **Practice tests**

For details about all the practice test options available, see "How to Use the Practice Tests" in this book's Introduction.