Using Windows Server 2003 in a Managed Environment: Controlling Communication with the Internet

Microsoft Corporation

Published: May 2003

Table of Contents

Introduction

Products in the Microsoft® Windows Server™ 2003 family include a variety of technologies that communicate with the Internet to provide increased ease of use. Browser and e-mail technologies are obvious examples, but there are also technologies such as Automatic Updates that help you obtain the latest software and product information, including bug fixes and security patches. These technologies provide many benefits, but they also involve communication with Internet sites, which administrators might want to control.

Control of this communication can be achieved through a variety of options built into individual components, into the operating system as a whole, and into server components designed for managing configurations across your organization. For example, as an administrator you can use Group Policy to control the way some components communicate, or for some components, you can direct all communication to the organization's own internal Web site instead of to an external site on the Internet.

This white paper provides information about the communication that flows between components in Windows Server 2003 and sites on the Internet, and it describes steps to take to limit, control, or prevent that communication in an organization with many users. The white paper is designed to assist you, the administrator, in planning strategies for deploying and maintaining products in the Windows Server 2003 family in a way that helps provide an appropriate level of security and privacy for your organization's networked assets.

This white paper provides guidelines for controlling components in the following operating systems:

- Windows Server 2003, Web Edition
- Windows Server 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition

The white paper is organized around individual components found in the Windows Server 2003 family, so that you can easily find detailed information for any component you are interested in.

What This White Paper Covers and What It Does Not Cover

The subsections that follow describe:

- Types of components covered in this white paper
- Types of components not covered in this white paper
- Security basics that are beyond the scope of this white paper, with listings of some other sources of information about these security basics

Types of components covered in this white paper

This white paper provides:

- Information about components that in the normal course of operation send information to or receive information from one or more sites on the Internet. An example of this type of

component is Windows® Error Reporting; if you choose to use this component, it sends information to a site on the Internet.

- Information about components that routinely display buttons or links that make it easy for you to initiate communication with one or more sites on the Internet. An example of this type of component is Event Viewer; if you open an event in Event Viewer and click a link, you are prompted with a message box that says, "Event Viewer will send the following information across the Internet. Is this OK?" If you click OK, information about the event is sent to a Web site, which replies with any additional information that might be available about that event.
- Brief descriptions of components like Microsoft Internet Explorer and Internet Information Services (IIS) that are designed to communicate with the Internet. It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running servers that communicate across the Internet. This white paper does, however, provide basic information about how components such as Internet Information Services work, and it provides suggestions for other sources of information about balancing your organization's requirements for communication across the Internet with your organization's requirements for protection of networked assets.

Types of components not covered in this white paper

This white paper does not provide:

- Information about managing or working with applications, scripts, utilities, Web interfaces, Microsoft ActiveX® controls, extensible user interfaces, the .NET Framework, and application programming interfaces (APIs). These are either applications, or are layers that support applications, and as such provide extensions that go beyond the operating system itself.

  Windows Installer is not covered in this white paper, although Windows Installer includes some technology that (if you choose) you can use for installing drivers or other software from the Internet. Such Windows Installer packages are not described here because they are like a script or utility that is created specifically for communication across the Internet.

  Note that among the applications not covered in this white paper are Web-based and server-based applications, for example, server-based applications for databases, e-mail, or instant messaging. You must work with your application software provider to learn what you can do to mitigate any risks that are part of using particular applications (including Web-based or server-based applications), scripts, utilities, and other types of software that run on products in the Windows Server 2003 family.
- Information about components that store local logs that could potentially be sent to someone or could potentially be made available to support personnel. This information is similar to any other type of information that can be sent through e-mail or across the Internet in other ways. You must work with your support staff to provide guidelines about the handling of logs and any other similar information you might want to protect.

Security basics that are beyond the scope of this white paper

This white paper is designed to assist you, the administrator, in planning strategies for deploying and maintaining products in the Windows Server 2003 family in a way that helps provide an appropriate level of security and privacy for your organization's networked assets. The white paper does not describe security basics, that is, strategies and risk-management methods that provide a foundation for security across your organization. It is assumed you are actively evaluating and studying these security basics as a standard part of network administration.

Some of the security basics that are a standard part of network administration include:

- Monitoring. This includes using a variety of software tools, including tools to assess which ports are open on servers and clients.
- Virus-protection software.
- The principle of least privilege (for example, not logging on as an administrator if logging on as a user is just as effective).
- The principle of running only the services and software that are necessary, that is, stopping unnecessary services and keeping computers (especially servers) free of unnecessary software.
- Strong passwords, that is, requiring all users and administrators to choose passwords that are not easily deciphered.
- Risk assessment as a basic element in creating and implementing security plans.
- Software deployment and maintenance routines to help ensure that your organization's software is running with the latest security updates and patches.
- Defense-in-depth. In this context, defense-in-depth (also referred to as in-depth defense) means redundancy in security systems, for example, using firewall settings together with Group Policy to control a particular type of communication with the Internet.

Other sources of information about security basics

The following books and Web sites are a few of the many sources of information about the security basics described previously:

- Howard, Michael, et al. *Designing Secure Web-Based Applications for Microsoft Windows 2000*. Redmond, WA: Microsoft Press, 2000.
- Howard, Michael, and David LeBlanc. *Writing Secure Code*. Redmond, WA: Microsoft Press, 2002.
- Kaufman, C., R. Perlman, and M. Speciner. *Network Security: Private Communication in a Public World*. Upper Saddle River, New Jersey: Prentice-Hall Inc., 2002.
- The Prescriptive Architecture Guides on the Microsoft Technet Web site at:

  http://www.microsoft.com/technet/itsolutions/idc/pag/pag.asp

Activation and Registration for a New Installation or an Upgrade

This section provides information about:

- The purposes of activation and registration connected with a new installation or an upgrade
- How a computer running a product in the Microsoft Windows Server 2003 family communicates with sites on the Internet during activation and registration
- Choosing volume licensing so that product activation need not take place (to limit the flow of information to and from Internet sites)

Purposes of Activation and Registration for a New Installation or an Upgrade

This subsection briefly describes the differences between product activation and registration, and then describes the purpose of each.

Product registration involves the provision of personally identifiable information, such as an e-mail address, to Microsoft for the purpose of receiving information about product updates and special offers. Registration is usually done on a per-product basis and is not required. If registration is completed, all registration information is stored using a variety of security technologies and is never loaned or sold outside Microsoft.

Product activation involves the authentication with Microsoft of non-personally identifiable information, including the product identifier and a hardware hash representing the computer, for the purpose of reducing software piracy. (A hardware hash is a non-unique number generated from the computer's hardware configuration.) Activation of products in the Windows Server 2003 family is required in situations where the product is not purchased through a volume licensing program such as Microsoft Select License, Microsoft Enterprise Agreement, or Microsoft Open License. Many computer manufacturers can bypass activation on software preinstalled on a new computer by binding the software to the computer’s basic input/output system (BIOS). In this situation, no activation of that software is required. Detailed information about product activation can be found on the following Web site:

http://www.microsoft.com/piracy/basics/activation/

For more information about volume licensing, see "Choosing Volume Licensing So That Individual Product Activation Need Not Take Place," later in this section.

Activation is aimed at reducing software piracy as well as ensuring that Microsoft customers are receiving the product quality that they expect. Activation means that a specific product key becomes associated with the computer (the hardware) it is installed on. After that happens, that product key cannot be used for activation on other computers (unless you are enrolled in a special program that permits additional activations, for example, a program through the Microsoft Developer Network [MSDN]).

Overview: Activation and Registration in a Managed Environment

Product activation is an anti-piracy technology designed to verify that software products have been legitimately licensed. If you have software re-imaging rights granted under a Microsoft volume license agreement, and if you obtained a product in the Windows Server 2003 family through a retail channel or preinstalled by the computer manufacturer, you can re-image it with the product that you licensed through one of the Microsoft volume licensing programs. With volume licensing, there is no need to perform product activation.

How a Computer Communicates with Sites on the Internet During Activation and Registration

A product in the Windows Server 2003 family can be activated through the Internet or by phone. When it is activated through the Internet, the operating system communicates with Web sites as follows:

- **Specific information sent or received**: During activation, the following information is sent to the activation server at Microsoft:
  - Request information, that is, information necessary for successfully establishing communication with the activation server.
  - Product key information in the form of the product ID, plus the product key itself.
  - A hardware hash (a non-unique number generated from the computer's hardware configuration). The hardware hash does not represent any personal information or anything about the software. It is based on the MD5 message-digest hash algorithm, and consists of a combination of partial MD5 hash values of various computer components. The hardware hash cannot be used to determine the make or model of the computer, nor can it be backward-calculated to determine the raw computer information.
  - Date and time.
  - The language being used on the system (so that any error message that is sent back can be in the correct language).
  - The operating system being activated (and the version number of the activation software).

  Depending on your preference, the preceding information is either sent over the Internet to the activation system at Microsoft, or the product key information and hardware hash (combined into one number) are called in by phone.
- **Default setting and ability to disable**: Product activation can only be disabled by installing the operating system with software acquired through one of the Microsoft volume licensing programs. Product activation can be bypassed by many computer manufacturers if they bind the product to the computer’s BIOS instead. In all other cases, product activation cannot be disabled.
- **Trigger and notification for activation**: When activation is required, the operating system provides a reminder each time you log on and at common intervals until the end of the activation grace period stated in the End-User License Agreement (thirty days is the typical grace period). With software acquired through one of the Microsoft volume licensing programs, there is no need for activation, and therefore there are no reminders that appear about activation.
- **Trigger and notification for registration**: Registration is optional. You can register at the same time you activate by choosing appropriate options on the Windows Product Activation interface. As an alternative, you can type **regwiz /r** to start the Registration Wizard for Windows Server 2003. Before the wizard starts and in the first page of the wizard, brief explanations notify you that completing the wizard will cause the product to be registered.

- **Logging**: Entries that track the progress of activation and registration (for example, return codes and error codes) are logged into a text file, *systemroot*\setuplog.txt. This file can be used for troubleshooting if activation (or any part of Setup) fails. If you choose to register the product, two entries are made in the text file. One entry records the country or region that was chosen for the operating system. A second entry records whether you chose to have Microsoft (or the computer manufacturer) send information about product updates and special offers. No other registration data is logged.
- **Privacy, encryption, and storage for activation data**: Customer privacy was a paramount design goal in building the product activation technology. No personally identifiable information is collected as part of activation. The data is encrypted (HTTPS) during transmission, and it is stored on servers located in controlled facilities at Microsoft. The data is accessible to a small number of server and program support personnel who oversee and maintain the activation servers and the product activation program.

  To review the Microsoft online privacy statement on activation, see the following Web site at:

  http://www.microsoft.com/piracy/basics/activation/apolicy.asp
- **Privacy, encryption, and storage for registration data**: When you register at the same time as you activate (through the Windows Product Activation interface), registration data is encrypted (HTTPS) during transmission. When you register by using the Registration Wizard (which you start by typing **regwiz /r**), registration data is encrypted (HTTPS) during transmission unless the wizard is unable to establish an HTTPS connection through port 443 with the Microsoft registration server. In this situation, registration data will be sent unencrypted, using HTTP through port 80.

  Registration data, which contains information that you choose to send to Microsoft, is stored on servers with restricted access that are located in controlled facilities. The data can be seen by customer service representatives and marketing personnel. To review the Microsoft online privacy statement on registration, see the following Web site at:

  http://www.microsoft.com/piracy/basics/activation/prvcyms.asp
- **Transmission protocol and port**:
  - **For Windows Product Activation**: When the operating system is activated through the Internet and a modem is not used, the first transmission uses HTTP through port 80 and goes to wpa.one.microsoft.com/ to check the HTTP response code. A response code of less than 500 indicates that a product activation server is available. (With a modem, there is only a check to see whether the modem can currently be used to make a connection to the Internet.) If the product activation server can be reached (or for a modem, if a connection to the Internet can be made), any activation or registration data that is sent by Windows Product Activation uses HTTPS through port 443.
  - **For the Registration Wizard**: When you register by using the Registration Wizard (which you start by typing **regwiz /r**), HTTPS is used through port 443 unless the wizard is unable to establish an HTTPS connection through port 443 with the Microsoft registration server. In this situation, HTTP is used through port 80.

Choosing Volume Licensing So That Individual Product Activation Need Not Take Place

If you use the rights granted under a volume licensing agreement to purchase or re-image software, you cannot and need not perform activation on the individual computers that are installed under the volume license. Qualifying as a volume licensing customer is not difficult. Customers can qualify for the Microsoft Open Licensing program by purchasing as few as five licenses. For more information, see the Microsoft licensing Web site at:

http://www.microsoft.com/licensing/

Application Help

This section provides information about:

- The benefits of Application Help
- How Application Help communicates with sites on the Internet
- How to control Application Help to prevent the flow of information to and from the Internet

Benefits and Purposes of Application Help

Application Help is one of the application compatibility technologies that support the installation and operation of applications on Microsoft Windows Server 2003 family operating systems. Because some applications that work on earlier versions of Windows might not function properly on Windows Server 2003 family operating systems, the application compatibility technologies were developed to solve these potential problems and enable a better user experience.

Application Help is most commonly used to block low-level applications—such as antivirus and disk-access utilities—that were not written for or intended for use on Windows Server 2003 family operating systems. By blocking the installation of these applications, this feature serves to avert serious problems that could compromise system integrity.

Overview: Using Application Help in a Managed Environment

Despite testing applications before you deploy Windows Server 2003 family operating systems, your organization may still use some applications that can cause system instability.

Application Help is the last line of defense against users attempting to install incompatible applications, and it is invoked only in rare instances. When a user tries to run an application for which there is no compatibility fix, Application Help is invoked by default. The operating system uses information in a local database to determine if a user is about to run an incompatible application. Compatibility fixes are contained in a database file named SYSMAIN.SDB. The warning information used when an application cannot be run successfully is contained in another database file, APPHELP.SDB. The operating system uses matching information in SYSMAIN.SDB, which in turn determines what messages to draw from APPHELP.SDB to block the operation of applications with known compatibility problems and to inform users about them. The list of incompatible applications is updated through Windows Update.

Application Help generates a message that is presented to the user when a problematic process is about to initiate. A dialog box appears that contains a brief message about the problem, with the severity indicated by an icon:

- If the icon is a yellow triangle with an exclamation mark, then the application is *not blocked*, which means that the user is still able to run the application.
- If the icon is a red stop sign, then the application is *blocked*, which means that the user cannot run the application.

The way these Application Help messages lead the user to interaction with the Internet is described in the following subsection.

While Application Help provides a valuable function, administrators in a highly managed environment might want to block the installation of applications that would automatically invoke Application Help and thereby allow a user to access the Internet. You can create custom Application Help messages that redirect the user to an internal site for more information. This is described in greater detail in the subsection, "Controlling Application Help to Prevent the Flow of Information to and from the Internet."

How Application Help Communicates with Sites on the Internet

In the Application Help dialog box, the user can click the Details button, in which case additional information is displayed in Help and Support Center. The Help content comes from either Microsoft.com if the computer is online, or from a local HTML Help file.

The following list describes how interaction with the Internet takes place when Application Help is invoked:

- **Specific information sent or received**: When the Details button is selected, a specific Web page from Microsoft.com is displayed; the Web page provides information about the problem application in the language of the operating system, for example, English (United States). The page that is displayed may provide a link to a non-Microsoft Web site, depending on the application. The URL provided for non-Microsoft Web sites is unique to each application. The user is not uniquely identified.
- **Default and recommended settings**: Application Help is enabled by default. Recommended settings are presented in the following topic, "Controlling Application Help to Prevent the Flow of Information to and from the Internet."
- **Triggers**: A user tries to run an application that is not compatible with Windows Server 2003 family operating systems.
- **User notification**: When the user selects the Details button there is no indication of whether the information is coming from an internal or external site.
- **Logging**: By default events related to Application Help are not logged; however, you can enable Application Help event logging. For this procedure see “To enable event logging for Application Help,” later in this section.
- **Encryption**: The query that causes the display of an appropriate Web page (described in “Specific information sent or received,” earlier in this list) is not encrypted.
- **Access**: No information from the use of Application Help is retained at Microsoft.
- **Privacy statement**: Application Help is covered by the same privacy statement that covers Windows Update.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is HTTP 80.
- **Ability to disable**: You can prevent Application Help from sending the user to the Internet by creating custom Application Help messages.

Controlling Application Help to Prevent the Flow of Information to and from the Internet

You can block an application with known compatibility problems, such as antivirus programs. You can also create custom Application Help messages that describe the problem and redirect users to an intranet site rather than sending them to the Internet for more information.

To do this you use the Compatibility Administrator tool which is part of the Application Compatibility Toolkit.

The Application Compatibility Toolkit is a collection of tools and documents that can help you resolve application compatibility problems. For information about downloading the toolkit, see "Using the Application Compatibility Toolkit," later in this section.

How creating custom Application Help messages can affect users and applications

The user experience with Application Help does not change if you block applications with known compatibility problems and create custom Application Help messages. The only difference is that when users click the Details button they are sent to an internal site for more information instead of to the Internet. Not only can you prevent users from accessing the Internet in this way, but you can also avoid having users try to install incompatible applications.

Procedures for Configuring Application Help

This section presents three procedures. The first two procedures help you get started with the Application Compatibility Toolkit. The last procedure explains how to enable event logging.

Using the Application Compatibility Toolkit

You need to first download the Application Compatibility Toolkit, and then you can use the Compatibility Administrator tool to create custom Application Help messages and to block specific applications from running.

To install the Application Compatibility Toolkit

1. Install the toolkit from the following Web site:

   http://www.microsoft.com/windows/appexperience/

2. Follow the installation instructions. Once you have installed the toolkit you can view the Windows Application Compatibility 3.0 Reference and you can run the Compatibility Administrator tool to make the changes you need.

To create custom Application Help messages

1. Make sure that the Application Compatibility Toolkit is installed by using the previous procedure.
2. Click **Start**, point to **Programs** or **All Programs**, point to **Microsoft Windows Application Compatibility Toolkit**, and then click **Compatibility Administrator Tool 3.0**.
3. In the console tree, click **Custom Databases**, and then click **New Database**.
4. On the toolbar, click **AppHelp**. The **Create a custom AppHelp message** dialog box appears.
5. Enter information as prompted in the dialog box.
6. Save the new database file.

Note When you have completed your entries and saved the file, you can deploy your changes to multiple computers running Windows Server 2003 and Windows XP. See "Deploying Compatibility Fixes," in Compatibility Administrator Help.

Application Help event logging

Events related to Application Help are not logged by default. You can enable event logging in the Application log (Control Panel\Administrative Tools\Event Viewer) by using Group Policy.

To enable event logging for Application Help

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Application Compatibility**.
3. In the details pane, double-click **Turn On Application Help Log Events**, and then select **Enabled**.

Related Links

For complete information about application compatibility resources, see “Windows Application and Customer Experience,” at:

http://www.microsoft.com/windows/appexperience/

Certificate Support and the Update Root Certificates Component

The following subsections provide information about:

- The benefits of the certificate functionality built into operating systems in the Microsoft Windows Server 2003 family, including the benefits of Update Root Certificates
- How Update Root Certificates communicates with sites on the Internet
- How to control Update Root Certificates to limit the flow of information to and from the Internet

Benefits and Purposes of Certificate Functionality

Certificates, and the public key infrastructure of which they are a part, support authentication and encrypted exchange of information on open networks, such as the Internet, extranets, and intranets. A certificate securely binds a public key to the entity that holds the corresponding private key. With certificates, host computers on the Internet no longer have to maintain a set of passwords for individual subjects who need to be authenticated as a prerequisite to access. Instead, the host merely establishes trust in a certification authority that certifies individuals and resources that hold private keys. The host can establish this trust through a certificate hierarchy that is ultimately based on a root certificate, that is, a certificate from an authority that is trusted without assurances from any other certification authority.

Examples of times that a certificate is used are when you:

- Use a browser to engage in a Secure Sockets Layer (SSL) session
- Accept a certificate as part of installing software
- Accept a certificate when receiving an encrypted or digitally signed e-mail message

When learning about public key infrastructure, it is important to learn not only about how certificates are issued, but how certificates are revoked, and how information about those revocations is made available to clients. This is because certificate revocation information is crucial for an application that is seeking to verify that a particular certificate is currently (not just formerly) considered trustworthy. Certificate revocation information is often stored in the form of a certificate revocation list, although this is not the only form it can take. Applications that have been presented with a certificate might contact a site on an intranet or the Internet for information not only about certification authorities, but also for certificate revocation information.

In an organization where servers run products in the Microsoft Windows Server 2003 family, you have a variety of options in the way certificates and certification revocation lists (or other forms of certificate revocation information) are handled. For more information about these options, see the references listed in the next subsection, "Overview: Using Certificate Components in a Managed Environment."

The Update Root Certificates component in the Windows Server 2003 family is designed to automatically check the list of trusted authorities on the Microsoft Windows Update Web site when this check is needed by an application. Specifically, if the application is presented with a certificate issued by a certification authority that is not directly trusted, the Update Root Certificates component (if present) will contact the Microsoft Windows Update Web site to see if Microsoft has added the certification authority to its list of trusted authorities. If the certification authority has been added to the Microsoft list of trusted authorities, its certificate will automatically be added to the trusted certificate store on the computer. Note that the

Update Root Certificates component is optional, that is, it can be removed or excluded from installation on a computer running a product in the Windows Server 2003 family.

Overview: Using Certificate Components in a Managed Environment

In an organization where servers run products in the Windows Server 2003 family, you have a variety of options in the way certificates are handled. For example, you can establish a trusted root authority, also known as a root certification authority, inside your organization. The first step in establishing a trusted root authority is to install the Certificate Services component. Another step that might be appropriate is to configure the publication of certificate revocation information to the Active Directory® directory service. When implementing public key infrastructure, we recommend that you also learn about Group Policy as it applies to certificates. Procedures for these steps are provided in the resources listed at the end of this subsection.

When you configure a certification authority inside your organization, the certificates it issues can specify a location of your choosing for retrieval of additional evidence for validation. That location can be a Web server or a directory within your organization. Because it is beyond the scope of this white paper to provide full details about working with certification authorities, root certificates, certificate revocation, and other aspects of public key infrastructure, this section provides a list of conceptual information and a list of resources to help you learn about certificates.

Some of the concepts to study when learning about certificates include:

- Certificates and the X.509 V3 standard (the most widely used standard for defining digital certificates)
- Standard protocols that relate to certificates, for example, Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Secure Multipurpose Internet Mail Extensions (S/MIME)
- Encryption keys and how they are generated
- Certification authorities, including the concept of a certification authority hierarchy and the concept of an offline root certification authority
- Certificate revocation
- Ways that Active Directory and Group Policy can work with certificates

The following list of resources can help you as you plan or modify your implementation of certificates and public key infrastructure:

- Help for products in the Windows Server 2003 family.

  You can view Help for products in the Windows Server 2003 family on the Web at:

  http://www.microsoft.com/windowsserver2003/proddoc/

- The *Microsoft Windows Server 2003 Deployment Kit*.

  You can view links on the Windows Deployment and Resource Kits Web site at:

  http://www.microsoft.com/reskit/

- "Troubleshooting Certificate Status and Revocation," a white paper on the Microsoft Technet Web site at:

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp

- Links to information about public key infrastructure on the Technet Web site at:

  http://www.microsoft.com/technet/security/prodtech/pubkey/default.asp

How Update Root Certificates Communicates with Sites on the Internet

This subsection focuses on how the Update Root Certificates component communicates with sites on the Internet. The previous subsection, "Overview: Using Certificate Components in a Managed Environment," provides references for the configuration choices that control the way other certificate components communicate with sites on the Internet.

If the Update Root Certificates component is installed on a server, and an application is presented with a certificate issued by a root authority that is not directly trusted, the Update Root Certificates component communicates across the Internet as follows:

- **Specific information sent or received**: Update Root Certificates sends a request to the Windows Update Web site, asking for the current list of root certification authorities in the Microsoft Root Certificate Program. If the untrusted certificate is named in the list, Update Root Certificates obtains that certificate from Windows Update and places it in the trusted certificate store on the server. No user authentication or unique user identification is used in this exchange.

  The Windows Update Web site is located at:

  http://windowsupdate.microsoft.com/

- **Default setting and ability to disable**: Update Root Certificates is installed by default with products in the Windows Server 2003 family. You can remove or exclude this component from installation on a server.
- **Trigger and user notification**: Update Root Certificates is triggered when the server is presented with a certificate issued by a root authority that is not directly trusted. There is no user notification.
- **Logging**: Events containing information such as the following will be logged:
  - Event ID: 7

    Description: Successful auto update retrieval of third-party root list sequence number from: *URL_for_Windows_Update_Web_Site*

  - Event ID: 8

    Description: Failed auto update retrieval of third-party root list sequence number from: *URL_for_Windows_Update_Web_Site* with error: *hexadecimal_error_value*

- **Encryption, privacy, and storage**: When requests or certificates are sent to or from Update Root Certificates, no encryption is used. Information about Update Root Certificates activity is not stored on any server at Microsoft.
- **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.

Controlling the Update Root Certificates Component to Prevent the Flow of Information to and from the Internet

If you want to prevent the Update Root Certificates component in the Windows Server 2003 family from communicating automatically with the Windows Update Web site, you can remove or exclude this component from installation on servers. You can do this during deployment by using standard methods for unattended installation or remote installation, as described in

Appendix A, "Resources for Learning About Automated Installation and Deployment." If you are using an answer file, the entry is as follows:

```
[Components]
Rootautoupdate = Off
```

How removing or excluding Update Root Certificates from servers can affect applications

If a server is presented with a certificate issued by a root authority that is not directly trusted, and the Update Root Certificates component is not installed on that server, you (or your application) will be prevented from completing the action that required authentication. For example, you might be prevented from installing software, viewing an encrypted or digitally signed e-mail message, or using a browser to engage in an SSL session.

If you choose to remove or exclude Update Root Certificates from servers, consider providing instructions that tell administrators what to do if they receive untrusted certificates.

Procedures for Excluding or Removing the Update Root Certificates Component from an Individual Computer

The following procedures describe:

- How to use Control Panel to remove the Update Root Certificates component from an individual computer running a product in the Windows Server 2003 family.
- How to exclude the Update Root Certificates component during unattended installation of a product in the Windows Server 2003 family by using an answer file.

To remove the Update Root Certificates component from an individual computer running a product in the Windows Server 2003 family

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add or Remove Windows Components** (on the left).
4. Scroll down the list of components to Update Root Certificates, and make sure the check box for that component is cleared.
5. Follow the instructions to complete the Windows Components Wizard.

To exclude the Update Root Certificates component during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, include the following entry:

   Rootautoupdate = Off

Device Manager

This section provides information about:

- The benefits of Device Manager
- How Device Manager communicates with sites on the Internet
- How to control Device Manager to limit the flow of information to and from the Internet

Device Manager interacts with the Internet through the hardware wizards by contacting Windows Update when you install or update hardware. For procedures related to disabling Windows Update, see "Windows Update and Automatic Updates," in this white paper.

Benefits and Purposes of Device Manager

Device Manager provides users and administrators with information about how the hardware on their computers is installed and configured, and how the hardware interacts with the computer's applications. With Device Manager, administrators can update the drivers (or software) for hardware devices, modify hardware settings, and troubleshoot problems.

> **Note** Only administrators or users with administrative credentials can install or update device drivers.

Overview: Using Device Manager in a Managed Environment

In the Microsoft Windows Server 2003 family, you access Device Manager through Administrative Tools\Computer Management. Administrators or users with administrative credentials will typically use Device Manager to check the status of hardware and to update device drivers. Administrators who have a thorough understanding of computer hardware might also use Device Manager's diagnostic features to resolve device conflicts and change resource settings.

Device Manager works in conjunction with Windows Update to deliver updated drivers for installed hardware. When you are upgrading a driver or installing new hardware, and your computer has access to the Internet, your computer will automatically check Windows Update for an appropriate device driver. As an IT administrator in a highly managed environment you might want to block certain administrators from downloading drivers through Device Manager. You can do this by configuring Group Policy to disable Windows Update. If you disable Windows Update then Device Manager cannot communicate with the Internet. The following subsection provides details about how Device Manager interacts with the Internet.

How Device Manager Communicates with Sites on the Internet

Device Manager communicates with the Internet when an administrator uses it to update a driver. After you open Device Manager you select a hardware device and click **Update Driver** on the **Action** menu (or right-click a hardware device). This activates the Hardware Update Wizard. The way Device Manager communicates with the Internet is based on its interaction with Windows Update through the Hardware Update Wizard; therefore much of the

information in this subsection is the same as for Windows Update. Additional details are described as follows:

- **Specific information sent or received**: See the section “Windows Update and Automatic Updates,” in this white paper.
- **Default and recommended settings**: Device Manager is enabled by default. See the subsection “Controlling Device Manager to Limit the Flow of Information to and from the Internet,” for recommended settings.
- **Triggers**: Through Device Manager an administrator starts the Hardware Update Wizard, or adds new hardware to a computer.
- **User notification**: See “Windows Update and Automatic Updates.”
- **Logging**: Errors that result from problems installing hardware devices without drivers are logged to the event log.
- **Encryption, access, privacy statement, transmission protocol, and port**: See “Windows Update and Automatic Updates.”
- **Ability to disable**: You cannot disable Device Manager directly. You can, however, prevent interaction with the Internet through Device Manager by disabling Windows Update.

Controlling Device Manager to Limit the Flow of Information to and from the Internet

You can prevent the Internet from being accessed through Device Manager by disabling Windows Update or by configuring where computers search for drivers. You use Group Policy settings to perform both of these procedures.

If you disable automatic access to Windows Update, you can have selected administrators update drivers by manually downloading updates from the Windows Update Catalog, or from an intranet server, whereby they can be distributed on your managed network as needed.

For more information about the Windows Update Catalog, see the Windows Update Web site at:

http://windowsupdate.microsoft.com/

Procedure for Controlling How Drivers Are Updated Through Device Manager

Group Policy settings for Windows Update and the automatic updating function are in Computer Configuration\Administrative Templates\Windows Components and User Configuration\Administrative Templates\Windows Components. For the procedure to disable Windows Update or configure automatic updating, see the section “Windows Update and Automatic Updates,” in this white paper. The procedure to eliminate Windows Update as a driver search location using Group Policy is included here.

To disable Windows Update as a driver search location

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.

2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
3. In the details pane, double-click **Configure Driver Search Locations**, and then click **Enabled**.
4. Select **Don't Search Windows Update**.

Driver Protection

This section provides information about:

- The benefits of Driver Protection
- How Driver Protection communicates with sites on the Internet
- How to control Driver Protection to limit the flow of information to and from the Internet

Benefits and Purposes of Driver Protection

The Driver Protection feature in the Microsoft Windows Server 2003 family prevents the operating system from loading drivers that are known to cause stability problems (for example, preventing the operating system from booting). These drivers are listed in a Driver Protection List database included with the operating system. Driver Protection checks this database during operating system upgrades and at run time. These checks are performed to determine whether to load a driver under one of the operating systems in the Windows Server 2003 family.

Driver Protection also displays up-to-date content about these driver problems in Help and Support Center, including links to sites where users can find a solution. Driver Protection relies on Windows Update and Dynamic Update to update the database files so that users are presented with the most current information available on protected drivers. Users cannot directly disable Driver Protection.

Drivers are added to the Driver Protection List based on feedback from end users about problems that can be reproduced and confirmed at Microsoft. The main reasons a driver is added to this list are:

- A Windows Server 2003 family operating system cannot boot with this driver loaded.
- Setup cannot be completed with this driver loaded.
- End users experience data corruption when this driver is loaded.

Decisions to add drivers to this list are made in consultation with the vendors who produce and distribute these drivers. Microsoft engages and informs these vendors before adding a driver to the Driver Protection List.

A listing of the content in the Driver Protection List for the Windows Server 2003 family is available as part of a white paper that provides additional information about Driver Protection on the Windows Platform Development Web site at:

http://www.microsoft.com/hwdev/driver/drv_protect.asp

This section of the white paper explains how to control Driver Protection in a managed environment.

Overview: Using Driver Protection in a Managed Environment

Users have no direct control over whether to download files required by Driver Protection for updating the Driver Protection List. In a managed environment it is unlikely that users will be allowed to send and receive driver information freely; this function would normally be

controlled in some fashion by the IT department. You can indirectly block Driver Protection from downloading files by disabling Windows Update or by avoiding the use of Dynamic Update. Details on the methods and procedures for controlling Driver Protection are described in the following subsections.

How Driver Protection Communicates with Sites on the Internet

This subsection summarizes the communication process:

- **Specific information sent or received**: No information is sent to the Internet about the user's system. Driver Protection downloads updated versions of the following files:
  - drvmain.sdb, apphelp.chm, apphelp.sdb, and apphelp.dll.
- **Default and recommended settings**: Driver Protection is enabled by default. Recommended settings are described in the next subsection, "Controlling Driver Protection to Limit the Flow of Information to and from the Internet."
- **Triggers**: Driver Protection is triggered if the device driver is on the Driver Protection List when the operating system starts, when a new application or device is installed, or during the installation or upgrade of the operating system.
- **User notification**: The notification that the user receives when Driver Protection is triggered differs according to when the driver load request occurs:
  - If a driver on the Driver Protection List is matched when the operating system starts, the operating system displays a pop-up Help balloon titled "Devices or Applications disabled," in the taskbar notification area when the user logs on. If the user clicks that Help balloon, additional driver information and links to solutions for that problem are displayed in Help and Support Center.
  - If a driver on the Driver Protection List is matched during the setup of a Windows Server 2003 family operating system (for an upgrade from Windows NT® 4.0 or Windows 2000), a message will appear in the Report System Compatibility window before the operating system upgrade is completed.

    Users have two options at this point:
    - They can cancel Setup and find an alternate driver solution before installing the new operating system. If the driver that users install solves the problem, Setup will continue normally.
    - They can continue the upgrade process without first installing a driver that solves the problem. In this case, Setup may disable the driver in order to be completed. When users later log on, the operating system displays the pop-up Help balloon described in the previous case.

    If a driver on the Driver Protection List is matched during installation of a new application or device, and that driver uses system installation services (SetupAPI), the operating system displays a notification during installation and blocks the installation of that driver.

    If a driver is not installed using system installation services, the operating system cannot block the installation of that driver. It can, however, block the driver from loading. If the driver is blocked, a notification will appear every time the operating system attempts to load that driver under an operating system in the Windows Server 2003 family. For example, if a CD writing program that does not use system installation services installs a driver that is included on the Driver Protection List, the Windows Server 2003 family operating systems will display the pop-up Help balloon mentioned previously after the setup for that program is completed.

- **Logging**: If Driver Protection finds a match for a driver in the Driver Protection List, operating systems in the Windows Server 2003 family log an event in the event log.
- **Encryption**: The data packages downloaded to the user's system by Microsoft are digitally signed.
- **Access**: No data is uploaded from the user's computer.
- **Privacy statement**: Driver Protection is covered by the same privacy statement that covers Windows Update.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You cannot disable Driver Protection directly. Disabling Windows Update or avoiding the use of Dynamic Update will, however, block Driver Protection from updating the database files for the Driver Protection List on the server. (Of course you can also block the updating of Driver Protection database files by preventing access to the Internet, or by blocking HTTP over port 80.)

Controlling Driver Protection to Limit the Flow of Information to and from the Internet

You cannot disable Driver Protection directly. To block the downloading of updates for the Driver Protection database files, you can disable the settings for Windows Update and (during setup) avoid the use of Dynamic Update. (Of course you can also block downloading by preventing access to the Internet, or by blocking HTTP over port 80.)

How controlling Driver Protection can affect users and applications

Driver Protection blocks known problem drivers from loading, but it does not block any associated applications that depend on those drivers. Therefore, the behavior of applications that depend on drivers that are blocked varies depending on the implementation of the application. Some applications, such as antivirus programs, install drivers in order to provide their core functionality. For these applications, Driver Protection may cause the application not to work at all. Other applications, such as CD-burning programs, use drivers for portions of their feature set. For these applications, only those features that do not depend on the driver may work.

If you decide to disable Driver Protection from pulling down updated versions of the Driver Protection List database, drivers that affect system stability will continue to be blocked. The operating system, however, will use the version of the Driver Protection List database that comes with the operating system to identify the drivers to block, instead of a more accurate, up-to-date version of the list.

Alternate Methods for Controlling Driver Protection

A more drastic measure to take would be to disable the Upload Manager service (uploadmgr) that manages synchronous and asynchronous file transfers between clients and servers on the network. Disabling this service will block the upload of the anonymous hardware profile data (although users will still be able to complete the Hardware Wizard). The operating system will, however, use the version of the Driver Protection List database that comes with the operating system to identify the drivers to block, instead of a more accurate, up-to-date version of the list. The following subsection gives the procedure for this method.

Procedure for Disabling How Driver Protection Communicates over the Internet

You cannot disable Driver Protection directly but can do so indirectly by controlling its ability to connect to the Internet by disabling Windows Update or avoiding the use of Dynamic Update. See the sections in this white paper titled "Windows Update and Automatic Updates" and "Dynamic Update," for more information about these methods.

As mentioned in the previous subsection, a more drastic method for disabling Driver Protection is to disable the Upload Manager service.

To disable how Driver Protection communicates over the Internet by disabling the Upload Manager service

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. In the details pane, right-click **Upload Manager**, and then click **Properties**.
4. Click the **Log On** tab, then click the hardware profile that you want to configure, and then click **Disable**.

Important If this service is disabled, any services that explicitly depend on it will fail to start.

Dynamic Update

This section provides information about:

- The benefits of Dynamic Update
- How Dynamic Update communicates with sites on the Internet
- How to control Dynamic Update to limit the flow of information to and from the Internet

Benefits and Purposes of Dynamic Update

With Dynamic Update, Setup for the Microsoft Windows Server 2003 family can check the Windows Update Web site for new Setup files, including drivers and other files, while the server operating system is being installed. In an interactive installation (in contrast to an unattended installation), the person installing a product in the Windows Server 2003 family chooses whether to allow Dynamic Update.

In a managed environment, if you are using Setup (Winnt32.exe) for unattended installation, you can create a shared folder on a server and deliver Dynamic Update files to destination computers from that shared folder (instead of downloading the files directly from the Windows Update Web site to the computer being installed). For additional information about how to do this, see "How Dynamic Update Communicates with Sites on the Internet," and "Controlling Dynamic Update to Limit the Flow of Information to and from the Internet," later in this section.

Whenever an important update is made to any crucial Setup file, that update is made available through Dynamic Update functionality built into the Windows Update Web site. Some of the updated files will be replacements (for example, an updated Setup file) and some will be additions (for example, a driver not available at the time that the Setup CD was created). All files on the Dynamic Update section of the Windows Update Web site are carefully tested, and only files that are important in ensuring that Setup runs well are made available.

Using Dynamic Update reduces the need to apply patches to recently installed systems, and makes it easier to run Setup with hardware that requires a driver that was recently added or updated on Windows Update. For example, if a new video adapter requires a driver that was recently added to Windows Update, with Dynamic Update, the video adapter is recognized and supported during Setup.

Dynamic Update downloads only the files that are required for a particular computer, which means that the Dynamic Update software briefly examines the computer hardware. No personal information is collected, and no information is saved. The only purpose for examining the hardware is to select appropriate drivers for it. This keeps the download time as short as possible and ensures that only necessary drivers are downloaded to the hard disk.

Overview: Using Dynamic Update in a Managed Environment

If you do not want Dynamic Update to connect to the Windows Update Web site during the installation of a product in the Windows Server 2003 family, you have two options:

- **Creating a shared folder and delivering Dynamic Update files to destination computers from that shared folder**: You can ensure that when Setup (Winnt32.exe) for

the Windows Server 2003 family is run in your organization, Dynamic Update does not connect to the Internet but instead uses the files you place on a server. To do this, you create a shared folder on a server in your organization, download Dynamic Update files to that server, and run unattended installations using Winnt32.exe with appropriate options.

- **Avoiding Dynamic Update**: You can avoid using Dynamic Update, which means Setup will use only the files and drivers provided on the CD for products in the Windows Server 2003 family. For more information, see "Avoiding Dynamic Update," later in this section.

The subsections that follow provide more information about these options.

For additional sources of information about performing unattended installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."

How Dynamic Update Communicates with Sites on the Internet

This subsection focuses on the communication that occurs between Dynamic Update and the Windows Update Web site during an interactive installation (or a preinstallation compatibility check) when the computer has access to the Internet. This subsection also provides some description of the default behavior of Dynamic Update with unattended Setup.

For information about how you can control the behavior of Dynamic Update during unattended installation, see "Controlling Dynamic Update to Limit the Flow of Information to and from the Internet," later in this section.

- **Specific information sent or received**: When Dynamic Update contacts the Windows Update Web site, it sends only the information necessary for appropriate drivers to be selected. In other words, it collects only necessary information about the hardware (devices) on that particular computer. No personal information is collected.

  The Setup files and drivers downloaded by Dynamic Update consist only of files that are important in ensuring that Setup runs successfully. Files with minor updates that will not significantly affect Setup are not made available through the Dynamic Update section of the Windows Update Web site. Some of the updated files will be replacements (for example, an updated Setup file) and some will be additions (for example, a driver not available at the time that the Setup CD was created).

- **Default behavior and triggers**: Dynamic Update may connect to the Internet, depending on how Setup is run. The following table provides details.

Choices for running Setup and effects on Dynamic Update

Choice	Steps to take and effect on Dynamic Update	Does Dynamic Update connect to the Internet?
Running a preinstallation compatibility check	Insert the Setup CD and choose the appropriate options for checking system compatibility. You are offered the choice of running or skipping Dynamic Update.	Yes, if you choose to run Dynamic Update.
Interactive installation	Start Setup from the CD or a network and run it interactively. You are offered the choice of running or skipping Dynamic Update.	Yes, if you choose to run Dynamic Update.
Unattended Setup without an answer file and without the use of any options that affect Dynamic Update	Run the Winnt32.exe command with the **/unattend** option, but do not provide the name of an answer file and do not specify **/dudisable** or any other options that affect Dynamic Update. Dynamic Update is triggered under these conditions for both unattended installation and unattended upgrade.	Yes.

Unattended Setup with the **/dudisable** option	Run the Winnt32.exe command with the **/unattend** option and also with the **/dudisable** option. If the **/dudisable** option is used, Dynamic Update is not triggered, regardless of whether an answer file is used.	No.
Unattended Setup with an answer file that specifies that Dynamic Update should not be disabled	Create an answer file that includes an **[Unattended]** section with an entry that specifies **dudisable = No**. Run the Winnt32.exe command with the **/unattend:***answer_file* option. Dynamic Update is triggered (although see the previous entry in this table).	Yes.
Unattended Setup with an answer file that does not specify any options that affect Dynamic Update	Run the Winnt32.exe command with the **/unattend:***answer_file* option. By default, if the answer file does not specify any options that affect Dynamic Update, Dynamic Update is disabled.	No.
Unattended Setup without an answer file and with the **/dushare** option	Prepare a shared folder as outlined in "Creating a shared folder and delivering Dynamic Update files to destination computers from that shared folder," later in this section. When you run Winnt32.exe, run it with the /**dushare =** *path_to_downloaded_files* option. Dynamic Update uses the folder specified in the **/dushare** option and does not connect to the Internet.	No. Dynamic Update uses the files in the shared folder that you created.
Unattended Setup with an answer file that contains the DUShare entry	Prepare a shared folder as outlined in "Creating a shared folder and delivering Dynamic Update files to destination computers from that shared folder," later in this section. Create an answer file that includes an **[Unattended]** section with an entry that specifies **dushare =** *path_to_downloaded_files*. Run the Winnt32.exe command with the **/unattend:***answer_file* option. Dynamic Update uses the folder specified in the DUShare entry and does not connect to the Internet.	No. Dynamic Update uses the files in the shared folder that you created.

- **User notification**: During an interactive installation, the user is notified when the choice of whether to run Dynamic Update is offered. During an unattended installation, there is no notification (unattended installation by definition means that no user interaction is required).
- **Logging**: By default, the progress of Setup is logged in *systemroot*\Winnt32.log. By using command options for the Winnt32.exe command, you can control the name of the log and the level of detail it contains.
- **Encryption**: The data is transferred from Microsoft using HTTPS.
- **Access**: No information about the hardware (devices) on a particular computer is saved or stored, so no one can access this information. The information is used only to select appropriate drivers.
- **Privacy statement**: Dynamic Update is covered by the same privacy statement that covers Windows Update. To view the privacy statement for Windows Update, go the Web site and click **Read our privacy statement**:

  http://windowsupdate.microsoft.com/
- **Transmission protocol and port**: The transmission protocol is HTTPS and the port is 443.
- **Ability to disable**: You can control the behavior of Dynamic Update by running Setup in specific ways, as shown in the previous table. (You can of course disable Dynamic Update by preventing access to the Internet, or by blocking HTTPS over port 443.)

  If you do not want to disable Dynamic Update but only want to prevent it from communicating with an Internet site, as noted earlier, you can create a shared folder on a server and deliver Dynamic Update files to destination computers from that shared folder.

Controlling Dynamic Update to Limit the Flow of Information to and from the Internet

As summarized in "Overview: Using Dynamic Update in a Managed Environment," earlier in this section, if you do not want Dynamic Update to connect to the Windows Update Web site during the installation of a product in the Windows Server 2003 family, you have two options. With the appropriate methods for unattended installation, you can create a shared folder on a server and deliver Dynamic Update files to destination computers from that shared folder. Another alternative is to completely avoid using Dynamic Update.

Creating a shared folder and delivering Dynamic Update files to destination computers from that shared folder

This subsection briefly describes the steps for creating a shared folder on a server and delivering Dynamic Update files to destination computers from that shared folder. The subsection also provides links to more detailed information. The steps can be summarized as follows:

- Step 1: Determine what packages you need to download from the Windows Update Web site.
- Step 2: Download the packages and prepare them and the folder they are in for use with Dynamic Update. This step includes extracting files and placing them in folders, as well as running the **/duprepare** option with Winnt32.exe, which creates subfolders and copies appropriate files to those subfolders. This step also requires other actions, such as sharing the folder and setting permissions.
- Step 3: Configure the answer file and Winnt32.exe settings for Dynamic Update (and for any other configuration options you want).
- Step 4: Run the unattended installations.

For more detailed information about performing the preceding steps, see the *Microsoft Windows Server 2003 Deployment Kit*, specifically the book titled *Automating and Customizing Installations*. To view the *Microsoft Windows Server 2003 Deployment Kit*, see the Microsoft Web site at:

http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx

Similar information is available in the Dynamic Update article on the Microsoft Web site at:

http://www.download.windowsupdate.com/msdownload/update/v3/static/DUProcedure/Dynamic Update.htm

For additional sources of information about performing unattended installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."

Avoiding Dynamic Update

You can avoid using Dynamic Update, which means Setup will use only the files and drivers provided on the CD for products in the Windows Server 2003 family. The method by which you avoid using Dynamic Update depends on how you are performing the installation:

- **Interactive installation**: During interactive installation (not unattended installation), you can select No when offered the option to use Dynamic Update. As an alternative, you can ensure that the computer does not have Internet access.

- **Unattended Setup**: Dynamic Update is disabled when you run Setup in specific ways, as shown in the table in "How Dynamic Update Communicates with Sites on the Internet," earlier in this section. As the table shows, the simplest way to ensure that Dynamic Update does not run during unattended Setup is to use the **/dudisable** option in the command line. This ensures that Dynamic Update will not occur during the installation.

How avoiding Dynamic Update or directing Dynamic Update to a server on your network can affect users and applications

Regardless of whether you use Dynamic Update, you can obtain updated system and driver files after installations are complete (for example, through Windows Update or a service pack). Allowing Dynamic Update to run during Setup, however, helps ensure Setup success.

If you create a shared folder on a server and deliver Dynamic Update files to destination computers from that shared folder (instead of downloading the files directly from Windows Update to the computers), you can control the exact set of updated files to be installed. By contrast, when you download the current set of Dynamic Update files directly from the Windows Update Web site to users' computers, you might introduce inconsistencies among your destination computers because the Windows Web Site is periodically updated, and you cannot control when these updates occur.

Procedures for Controlling Dynamic Update

For detailed descriptions of Dynamic Update and procedures for controlling it, see the *Microsoft Windows Server 2003 Deployment Kit*, specifically the book titled *Automating and Customizing Installations*. To view the *Microsoft Windows Server 2003 Deployment Kit*, see the Microsoft Web site at:

http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx

Similar information is available in the Dynamic Update article on the Microsoft Web site at:

http://www.download.windowsupdate.com/msdownload/update/v3/static/DUProcedure/Dynamic Update.htm

Event Viewer

This section provides information about:

- The benefits of Event Viewer
- How Event Viewer communicates with sites on the Internet
- How to control Event Viewer to prevent the flow of information to and from the Internet

Benefits and Purposes of Event Viewer

Using Event Viewer, administrators can view and set logging options for event logs in order to gather information about hardware, software, and system problems. By default, a computer running an operating system in the Microsoft Windows Server 2003 family records events in three kinds of logs:

- **Application log**: The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. Application developers decide which events to log.
- **Security log**: The security log records events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. For example, if logon auditing is enabled, attempts to log on to the system are recorded in the security log.
- **System log**: The system log contains events logged by Windows system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by the server.

A computer running a Windows Server 2003 family operating system which is configured as a domain controller records events in two additional logs:

- **Directory service log**: The directory service log contains events logged by the Windows Active Directory directory service. For example, connection problems between the server and the global catalog are recorded in the directory service log.
- **File Replication service log**: The File Replication service log contains events logged by the Windows File Replication service. For example, file replication failures and events that occur while domain controllers are being updated with information about system volume changes are recorded in the file replication log.

A computer running a Windows Server 2003 operating system configured as a Domain Name System (DNS) server records events in an additional log. The DNS server log contains Windows DNS service events.

Other types of events and event logs might be available on a computer, depending on what services are installed.

Overview: Using Event Viewer in a Managed Environment

The Event Log service starts automatically when you start the operating system. Administrators access event logs for a server through Control Panel\Administrative Tools\Event Viewer. They can obtain detailed information about a particular event by either double-clicking the event, or by selecting the event and clicking **Properties** on the **Action**

menu. The dialog box gives a description of the event, which can contain one or more links to Help.

Links can either be to servers at Microsoft, or to servers managed by the software vendor for the component that generated the event. On products in the Windows Server 2003 family, most events that originate from Microsoft products will have standard text containing a URL at the end of the description ("For more information, see Help and Support Center at go.microsoft.com/fwlink/events.asp").

When you click the link, you are asked to confirm that the information presented can be sent over the Internet. If you click Yes, the information listed will be sent to the Web site named in the link. The parameters in the original URL will be replaced by a standard list of parameters whose contents are detailed in the confirmation dialog box. This list is provided in the next subsection under "Specific information sent or received."

In a highly managed environment, IT administrators might want to prevent users and administrators from sending this information over the Internet through this link and accessing a Web site. In the Windows Server 2003 family, this information flow is governed by a registry key. Administrators can edit this registry key to prevent users and administrators from accessing the Internet through Event Viewer.

How Event Viewer Communicates with Sites on the Internet

In order to access the relevant Help information provided by the link in the Event Properties dialog box, you must send the information listed about the event. The collected data is confined to what is needed to retrieve more information about the event from the Microsoft Knowledge Base. User names and e-mail addresses, names of files unrelated to the logged event, computer addresses, and any other forms of personally identifiable information are not collected.

The exchange of information that takes place over the Internet is described as follows:

- **Specific information sent or received**: Information about the event sent over the Internet includes the following:
  - Company name (software vendor)
  - Date and time
  - Event ID (for example, 1704)
  - File name and version (for example, userenv.dll, 5.1.2600.1106)
  - Product name and version (for example, Microsoft Windows Operating System, 5.1.2600.1106)
  - Registry source (for example, userenv)
  - Type of event message (for example, Error)

  The information the user receives is from the Web site named in the link.
- **Default settings**: Access to Event Viewer is enabled by default.
- **Triggers**: The user chooses to send information about the event over the Internet in order to view Help.
- **User notification**: When a user clicks the link, a dialog box listing the information that will be sent is provided.
- **Logging**: This is a feature of Event Viewer.

- **Encryption**: The information may or may not be encrypted, depending on whether it is an HTTP or HTTPS link.
- **Access**: No information is stored.
- **Privacy statement**: See the Windows Server 2003 family Help for a privacy statement. (In Help and Support, type **Linking to Microsoft for Help and Support**.)
- **Transmission protocol and port**: Communication occurs over the standard port for the protocol in the URL, either HTTP or HTTPS.
- **Ability to disable**: The ability to send information over the Internet or to be linked to a Web site can be prevented by editing the registry.

Controlling Event Viewer to Prevent the Flow of Information to and from the Internet

You can prevent users and administrators from sending information across the Internet and accessing Internet sites through Event Viewer by editing the registry. When you edit the registry as described in the following subsection, clicking Yes as previously described will still start Help, but it will not access the Internet for information specific to the event.

The Windows Server 2003 family computer registry values listed in this subsection are located in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Event Viewer

The following list describes how this registry key controls the flow of information to and from the Internet.

- **MicrosoftRedirectionProgram**

  Default value: %SystemRoot%\PCHealth\HelpCtr\Binaries\HelpCtr.exe

  Usage: This program is started with command-line parameters from MicrosoftRedirectionProgramCommandLineParameters

- **MicrosoftRedirectionProgramCommandLineParameters**

  Default value: -url hcp://services/centers/support?topic=%s

  Usage: "%s" is replaced with the URL in the link

- **MicrosoftRedirectionURL**

  Default value: http://go.microsoft.com/fwlink/events.asp

  Usage: Governs the text of the standard link for Microsoft events

Note If any of these registry values is missing or empty, the link will be started directly using ShellExecute; deleting these values is not a method for preventing information from reaching the Internet.

Procedures for Preventing the Flow of Information to and from the Internet Through Event Viewer

To prevent the flow of information to and from the Internet through Event Viewer you need to edit the registry. You can then apply the registry change to computers in a domain using Group Policy.

Editing the registry

Edit HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Event Viewer as follows:

To prevent the user from accessing the Internet when they click the link, delete the final "%s" from the value of MicrosoftRedirectionProgramCommandLineParameters (see the list in the previous subsection). With this change, clicking the link and clicking Yes will still start Help, but it will not access the Internet for information specific to this event.

For more information about the registry, see the *Registry Reference for Windows Server 2003* on the *Microsoft Windows Server 2003 Deployment Kit* companion CD, or on the Windows Deployment and Resource Kits Web site at:

http://www.microsoft.com/reskit/

> **Caution** Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

Distributing the registry change using Group Policy

You can distribute this registry change to computers in a domain by configuring a Group Policy object (GPO). You first need to create a template using the Event Viewer snap-in as described in the following procedure.

To enable the Event Viewer Group Policy snap-in

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **User Configuration**, click **Administrative Templates**, and then click **Windows Components**.
3. Click **Microsoft Management Console** and then click **Restricted/Permitted snap-ins**.
4. In the details pane under Setting, double-click **Event Viewer**.
5. In the Event Viewer Properties dialog box, select **Enabled**.

File Association Web Service

This section provides information about:

- The benefits of the file association Web service
- How the file association Web service communicates with sites on the Internet
- How to control the file association Web service to limit the flow of information to and from the Internet

Benefits and Purposes of the File Association Web Service

In products in the Microsoft Windows Server 2003 family, the file association Web service extends the scope of information stored locally by the operating system about file name extensions, file types, and the applications or components to use when opening a particular file type. Both the locally stored information and the file association Web service are intended to provide you with the ability to open (double-click) a file without having to specify which application or component to open it with. The operating system associates the file name extension (for example, .txt or .jpg) with a file type, and it opens each file type with the application or component specified for that file type. For example, file name extensions .htm and .html are both "HTML Document" file types.

The operating system first checks for the file association information locally. If no local information is available about the file name extension and its associated file type, the operating system offers you the option of looking for more information on a Microsoft Web site. For details about the URL for this Web site, see "How the File Association Web Service Communicates with Sites on the Internet," later in this section.

Overview: Using the File Association Web Service in a Managed Environment

To limit the flow of information from the file association Web service to the Internet, you have several options. You can use firewall settings, you can disable the file association Web service by setting a registry key, and you can configure automatic server-based software installation through Group Policy. You can also use scripts to limit the file types that can be stored, viewed, or used on computers in your organization, which will limit the likelihood that anyone will need to obtain information about those file types.

How the File Association Web Service Communicates with Sites on the Internet

The file association Web service communicates with sites on the Internet as follows:

- **Specific information sent or received**: If the operating system does not find local information about a file name extension, it offers you the option of sending a query to look for more information on a Microsoft Web site. The site is language-specific; the file name extension that you double-click is appended to the query. The query takes the following form:

  http://shell.windows.com/fileassoc/*nnnn***/xml/redir.asp?Ext=***AAA***

where *nnnn* is a hexadecimal value used in the Windows Server 2003 family to map to a language identifier (that is, to an RFC1766 identifier), and *AAA* is the file name extension for which information is needed. An example of a hexadecimal value and its corresponding language identifier is 0409 for en-us, English (United States).

Notes
For more information about these hexadecimal values, see the information about the multiple language (MLang) registry settings on the Microsoft Developer Network Web site at:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wceielng/htm/cooriMLangRegistrySettings.asp

To search for information about MLang registry settings or the Microsoft Internet Explorer Multiple Language application programming interface (MLang API), use the Search tool on the Microsoft Developer Network Web site at:

http://msdn.microsoft.com/

- **Default setting and ability to disable**: The service is enabled by default. It can be disabled by setting a registry key, as described in "Disabling the file association Web service," later in this section.

  There are ways of reducing the likelihood that a person will trigger the file association Web service. One basic way is to configure automatic, server-based software installation based on Group Policy settings. For more information, see "Finding information about the Software Installation extension of Group Policy," later in this section.

- **Trigger and notification**: When you try to open a file (for example, by double-clicking the file), and there is no local information about the correct application or component to use when opening the file, the operating system offers the option either to "Use the Web service to find the appropriate program" or to "Select the program from a list."

- **Logging**: No events are logged by the file association Web service.

- **Encryption, storage, access, and privacy**: The file name extension sent in a query to the Internet is not encrypted. Nothing in the query identifies the person who triggered the query. If the local computer's browser is configured to store information about recently visited Internet sites, the browser will store the query containing the file name extension. Otherwise, the query containing the file name extension is not stored anywhere.

- **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.

Controlling the File Association Web Service to Limit the Flow of Information to and from the Internet

If you want to limit the flow of information from the file association Web service to the Internet, you can use one or more of the following methods:

- Use your firewall to block access to any Web site that contains the following string: http://shell.windows.com/fileassoc/

- Disable the file association Web service by setting a registry key, as described in "Disabling the file association Web service," later in this section.

- Configure automatic, server-based software installation. To do this, configure one or more servers with the Software Installation extension of Group Policy. When you do this, if someone tries to open a file for which the corresponding application is not installed locally, a copy of the application (stored on another server) is installed automatically. In this situation, the file association Web service will not be triggered. To learn more about

the Software Installation extension, see "Finding information about the Software Installation extension of Group Policy," later in this section.

- Familiarize yourself and other administrators (if you are not already aware) with using Control Panel, Folder Options, and the File Types tab in Folder Options to associate a file name extension with a file type, and a file type with an application. Also, if a message box appears offering the two options, "Use the Web service to find the appropriate program" or "Select the program from a list," always click "Select the program from a list."
- Use scripts to scan your organization's computers for file types that you do not want stored, viewed, or used on your organization's computers. Take actions to ensure that these files do not remain on individual computers' hard disks. Reducing the number of file types on hard disks reduces the likelihood that the file association Web service will be triggered.

Procedures that Limit Internet Communication Generated by the File Association Web Service

This subsection contains the following information:

- A procedure for disabling the file association Web service by setting a registry key.
- A link to information about configuring automatic, server-based software installation through the Software Installation extension of Group Policy.
- Procedures for using the File Types tab in Folder Options to associate a file name extension with a file type, and a file type with an application.

Disabling the file association Web service

The following procedure explains how to disable the file association Web service by setting a registry key.

To disable the file association Web service by setting a registry key

1. Open Registry Editor by clicking **Start**, clicking **Run**, and then typing **regedit**.

   Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

2. Navigate to the following registry key:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

3. Click the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type the following name:
   NoInternetOpenWith
5. Click the new entry (**NoInternetOpenWith**), and then select **Modify** in the **Edit** menu.
6. Ensure that **Hexadecimal** is selected, and then for **Value data**, type:
   1
7. Close Registry Editor.

Finding information about the Software Installation extension of Group Policy

If you are not already familiar with using the Software Installation extension of Group Policy, use one of the following procedures to learn more. For additional information about Group Policy, see Appendix B, "Resources for Learning About Group Policy."

To find information about the Software Installation extension with the Group Policy Management Console

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then click **Group Policy Management**.
3. Expand items in the Group Policy Management Console until the object to which you want to apply Group Policy is displayed. For more information, see the resources listed in Appendix B, “Resources for Learning About Group Policy.”
4. Right-click the appropriate Group Policy object and then click **Edit**.
5. In the Group Policy Object Editor, in the **Help** menu, click **Help Topics**.
6. Click the **Contents** tab, click **Group Policy Management**, click **Concepts**, click **Group Policy Object Editor Extensions**, and then click **Software installation**.

To find information about the Software Installation extension without the Group Policy Management Console

1. On a computer running a product in the Windows Server 2003 family, click **Start** and then click **Help and Support**.
2. Under Help Contents, click **Common Administrative Tasks**, and then click **Deploying and upgrading software**.

Note You can also view Help on the Web at:

http://www.microsoft.com/windowsserver2003/proddoc/

Specifying associations between file name extensions, file types, and applications or components

When you associate a file name extension with a file type and an application or component, the result is that the file association Web service cannot be triggered by that file name extension on that computer.

To associate a file name extension with a file type

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Folder Options**, and then click the **File Types** tab.
3. Click **New**.
4. Type a new or existing file name extension, and then click **Advanced**.
5. In **Associated File Type**, do one of the following:

- Type or select **New** to create a file type to associate with the file name extension.
- Type or select a different file type to associate with the extension.

Note When you type a file name extension in the Create New Extension dialog box, the Associated File Type list displays the file type that is associated with that extension. To select New, scroll to the top of the list.

To associate a file name extension with an application

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Folder Options**, and then click the **File Types** tab.
3. Under **Registered file types**, click a file type.
4. Click **Change**, and then choose the application you want to use to open this file.

Help and Support Center: The Headlines and Online Search Features

This section provides information about:

- The benefits of the Headlines and Online Search features in Help and Support Center
- How the Headlines and Online Search features communicate with sites on the Internet
- How to control the Headlines and Online Search features to limit the flow of information to and from the Internet

Benefits and Purposes of Headlines and Online Search

Help and Support Center is a self-help portal that was first included in Microsoft Windows Millennium Edition. It is also included in all versions of the Windows Server 2003 family. You can access Help and Support Center in a number of ways, including:

- Selecting Help and Support from the Start menu.
- Selecting Help and Support from the Help menus for Control Panel, Windows Explorer, My Network Places, My Pictures, My Computer, or My Documents.

Headlines

A useful feature of Help and Support Center is the Headlines area. This area is typically titled "Top Issues" and is usually located in the lower-right corner of the main window, unless the window has been customized by the OEM or modified for certain languages. A page in Help and Support Center with more Headlines is exposed when you click a "View more Headlines" hyperlink at the bottom of the "Top Issues" area. Headlines provides a dynamic source of content that you can visit to find help and support on current issues as well as those that were known at the time the operating system was released. For example, it may display links to topics about new security bulletins, software updates, or new Help content.

Online Search

Online Search, another useful feature of Help and Support Center, enables you to query online Web sites automatically when performing a search. By default, the Microsoft Knowledge Base is designated as one of the Web sites for online searches. OEMs often customize the Online Search feature by, for example, adding a check box to the search window to enable the search engine to query their OEM-specific Web sites for results. To produce the most informative results when querying the Microsoft Knowledge Base, certain information such as the version of the product installed is collected from the computer and uploaded to the servers hosting the Microsoft Knowledge Base.

Overview: Using Headlines and Online Search in a Managed Environment

By creating a system registry key, or by performing unattended installation with an appropriate entry in your answer file, or using other tools available in the operating system user interface, you can control the extent to which the Headlines and Online Search features

access the Internet. More details on the methods and procedures for controlling these features are described in the following subsections.

How Headlines and Online Search Communicate with Sites on the Internet

Headlines

The Headlines area is updated only when there is Internet connectivity. You are not required or prompted to connect to the Internet. Help and Support Center uses information contained in the NewsSet.xml file (stored in the *systemroot*\pchealth\helpctr\Config folder) to determine:

- Whether or not to update the Headlines area
- How frequently to update the Headlines area
- Where on the Internet to obtain the Headlines updates

This subsection summarizes the communication process:

- **Specific information sent or received**: If there is Internet connectivity, when you start Help and Support Center the Help and Support service (helpsvc) compares the current date to the date specified by the TIMESTAMP attribute in the NewsSet.xml file and calculates the total number of days that have elapsed since the last time Headlines was successfully updated.

  Then, if the number of elapsed days is greater than the number of days specified by the FREQUENCY attribute in NewsSet.xml, the Help and Support service connects to the Web site specified by the URL attribute and downloads an updated version of the file NewsVer.xml to the *systemroot*\pchealth\helpctr\Config\News folder. The administrator (or other person at the server) is not uniquely identified.

  Note For Headlines supplied by Microsoft, the URL attribute is:

  http://go.microsoft.com/fwlink/?LinkID=11

  The downloaded NewsVer.xml file contains links to the news content files (known as news blocks) for Windows Server 2003 operating systems and the installed language. These news blocks contain the information used to update the Headlines area, that is, links to and descriptions of the latest information from Help and Support Center, Windows, or support-related articles posted on Microsoft Web sites.

  Note If the OEM has customized the Headlines feature, then the OEM-supplied Headlines may have links to the OEM's Web site.

  If there is no Internet connectivity, Help and Support Center displays an offline message in the Headlines area similar to the following:

  > When you are connected to the Internet, this area will display links to timely help and support information. If you want to connect to the Internet now, start the New Connection Wizard and see how to establish a Web connection through an Internet service provider.

- **Default and recommended settings**: The Headlines feature is enabled by default. Recommended settings are described in the next subsection, "Controlling Headlines and Online Search to Limit the Flow of Information to and from the Internet."
- **Triggers**: The Headlines feature is automatically triggered if there is Internet connectivity when you start Help and Support Center.

- **User notification**: You are not given the choice to select whether to update the Headlines area before an update is performed. An "Updating …" status indicator is displayed in the Headlines area, however, to indicate when an update is being performed. Once Help and Support Center has completed checking for new headlines, the Headlines area is labeled "Updated: *date*," where *date* is the current date.
- **Logging**: There is no information related to Headlines entered into the event log.
- **Encryption**: The data transferred to Microsoft is not encrypted.
- **Access**: The only data generated on servers at Microsoft from the process of updates to the Headlines area is a single number telling how many times a connection has been made, by any computer, to the link that supports Headlines updates. No computer is identified in the process of a Headlines update. The data can be viewed by the Microsoft group that provides support for the link through which Headlines is updated.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You can disable Headlines by setting a registry key or during unattended installation. For more information, see "Procedures for Disabling Headlines and Online Search," later in this section.

Online Search

Online Search can only query online Web sites like the Microsoft Knowledge Base when there is Internet connectivity; you are neither required nor prompted to connect to the Internet. When you perform a search in Help and Support Center, if you have set the search options to search the Microsoft Knowledge Base or an OEM-designated Web site, the search engine automatically searches the specified site.

This subsection summarizes the communication process:

- **Specific information sent or received**: To produce relevant results when querying the Microsoft Knowledge Base, certain information is collected from the computer and uploaded to a server at Microsoft that hosts the Microsoft Knowledge Base. The administrator (or other person at the server) is not uniquely identified. Following is a list of the information collected:
  - The search text string that was entered
  - The language code of the operating system
  - The product Knowledge Base to be searched (for example, the Windows Server 2003 family or Outlook)
  - The version of the operating system installed (for example, Standard Edition, Enterprise Edition, Datacenter Edition, or Web Edition)
  - The number of results specified for the result set
  - Titles field status (indicates whether or not to search the article title only)
  - Type field status (indicates whether to search using "all" or "any" of the search string)
- **Default and recommended settings**: Online Search is enabled by default. Recommended settings are described in the next subsection, "Controlling Headlines and Online Search to Limit the Flow of Information to and from the Internet."
- **Triggers**: Online Search is automatically triggered if you use the default search options or if you have set the search options to encompass searches on the Internet. (Online Search is also dependent on having Internet connectivity when the search is performed.)

- **User notification**: You are not notified before Help and Support Center performs Online Search. A permanent headline is provided in the Headlines area that tells how to set Online Search options, including how to turn the feature off.
- **Logging**: There is no information related to Online Search entered into the event log.
- **Encryption**: The data transferred to Microsoft is not encrypted.
- **Access**: The data uploaded to the server is aggregated and clustered. Information about the most common queries is later made available to the Windows Product Support Services and Windows User Assistance teams to help in developing new content or in revising existing content.
- **Privacy statement**: Microsoft does not retrieve any personally identifiable information from the computer during an online search. A permanent headline is provided in the Headlines area that tells how to set Online Search options, including how to turn the feature off.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You can disable Online Search through the Help and Support Center user interface.

Controlling Headlines and Online Search to Limit the Flow of Information to and from the Internet

Using the appropriate system registry key, or performing unattended installation with an appropriate entry in your answer file, you can disable the Headlines feature and eliminate the entire "Top Issues" area in the Help and Support Center user interface. If you perform unattended installation, the answer file entry is as follows:

```
[PCHealth]
Headlines = 0
```

The following table describes this and other configuration options for both Headlines and Online Search. For more information, see "Procedures for Disabling Headlines and Online Search," later in this section.

Configuration settings for Headlines and Online Search

Headlines: Configuration tool	**Setting**	**Result**
Unattended Installation	Include Headlines = 0 under the [PCHealth] section.	Replaces text in the Headlines area with white space.
Registry	Set HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\ PCHealth\HelpSvc\Headlines equal to 0.	Replaces text in the Headlines area with white space.
Online Search: Configuration tool	**Setting**	**Result**
Help and Support Center user interface (Set Search Options pane)	Clear any check boxes for querying the Microsoft Knowledge Base or OEM Web sites for results.	Disables online searches. The search results window neither displays an area for the online Web sites (such as the Microsoft Knowledge Base) nor returns any search results from online Web

		sites.
Headlines and Online Search: Configuration tool	**Setting**	**Result**
Firewall	Block HTTP port 80.	Displays offline message text in the Headlines area. The search results window displays an area for the online Web sites (such as the Microsoft Knowledge Base), but it does not return any search results from online Web sites.

Alternate Methods for Controlling Headlines and Online Search

You can configure your firewall to restrict access to the Internet through HTTP port 80. You can also use the firewall to block updates to the Headlines area and to block online searches. In this scenario, for the Headlines feature, Help and Support Center displays the offline message text described in "How Headlines and Online Search Communicate with Sites on the Internet." When traffic through HTTP port 80 is blocked in this way, Help and Support Center searches will only query local Help content. The search results window will display an area for the online Web sites, such as the Microsoft Knowledge Base, but it will not contain any results.

Procedures for Disabling Headlines and Online Search

The following procedures explain how to:

- Disable the Headlines feature on individual computers by modifying the system registry.
- Disable the Headlines feature during workstation deployment by using standard methods for unattended installation or remote installation.
- Disable online searches in the Help and Support Center user interface.

To disable the Headlines feature on individual computers by modifying the system registry

1. Open Registry Editor by clicking **Start**, clicking **Run**, and then typing **regedit**.

   Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

2. In the registry tree (on the left), navigate to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\HelpSvc\.
3. On the **Edit** menu, point to **New**, and then click **DWORD value**.
4. Type **Headlines** as the name for the new value (type REG_DWORD), and then press ENTER.

   Note Setting the data value to 0 (or leaving the default for a new REG_DWORD) disables Headlines. If the Headlines REG_DWORD has another value or doesn't exist, then Headlines is enabled.

To disable the Headlines feature during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [PCHealth] section of the answer file, include the following entry:
3. **Headlines = 0**

Note Headlines = 0 specifies that no information is displayed in the Headlines ("Top Issues") area on the Help and Support Center home page. Headlines = 1 specifies that Headlines is displayed.

To disable the Online Search feature in the Help and Support Center user interface

1. Click **Start**, and then click **Help and Support**.
2. Below the Search box, click **Set search options**.
3. Clear the **Microsoft Knowledge Base** check box and any other check boxes below it. (For example, the manufacturer of your computer may have added a check box to enable your search to query their Web site for results.)
4. Close Help and Support Center.

HyperTerminal

This section provides information about:

- The benefits of HyperTerminal
- How HyperTerminal communicates with sites on the Internet
- How to control HyperTerminal to prevent the flow of information to and from the Internet

Benefits and Purposes of HyperTerminal

HyperTerminal is a program that you can use to connect to other computers, Telnet sites, bulletin board systems (BBSs), online services, and host computers. HyperTerminal connections are made using a modem, a null modem cable (used to emulate modern communication), or an Ethernet connection.

HyperTerminal has capabilities beyond making connections to other computers. It can, for example, transfer large files from a computer onto your portable computer using a serial port rather than requiring you to set up your portable computer on a network. It can help debug source code from a remote terminal. It can also communicate with many older, character-based computers.

HyperTerminal records the messages passed to and from the computer or service on the other end of your connection. It can therefore serve as a valuable troubleshooting tool when setting up and using your modem. To make sure that your modem is connected properly or to view your modem's settings, you can send commands through HyperTerminal and check the results. HyperTerminal also has scroll functionality that enables you to view received text that has scrolled off the screen.

> **Note** HyperTerminal is designed to be an easy-to-use tool yet it is not meant to replace other full-featured tools. You can use HyperTerminal as described in this subsection, but you should not attempt to use HyperTerminal for more complex communication. For more information about what HyperTerminal does and does not support, see the list of frequently asked questions on the Hilgraeve Web site at:
>
> http://www.hilgraeve.com/support/faq/index.html
>
> (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Overview: Using HyperTerminal in a Managed Environment

In a managed environment, providing access to local and remote connection points through the use of HyperTerminal may pose security risks. You can prevent HyperTerminal from being installed on products in the Microsoft Windows Server 2003 family as described later in this section. Following are a few security issues to consider when deciding how to configure HyperTerminal for your organization:

- **Viruses**: Incoming files might contain viruses or malicious programs that could compromise or destroy data on your computer. To reduce this risk, use virus-scanning software and ensure that incoming files are from a reliable and trusted source.

- **ID and password**: HyperTerminal cannot automatically provide your login ID and password when you make a connection. If you provide a password when using HyperTerminal for a Telnet session, be aware that this password will be sent to the remote computer using plaintext (as with all Telnet connections).
- **Automatic download**: The automatic download feature of the Zmodem protocol can pose a security risk by allowing remote users to send files to your computer without your explicit permission. To avoid this risk, you should select a protocol other than Zmodem in the Receive File dialog box or you should clear the **Allow remote host-initiated file transfers** check box on the Settings tab of Connection Properties.

Complete information about concepts and procedures associated with using or configuring HyperTerminal is beyond the scope of this white paper. For more information, access the HyperTerminal Help documentation in Help and Support Center on any computer running a product in the Windows Server 2003 family.

How HyperTerminal Communicates with Sites on the Internet

The exchange of information that takes place during the HyperTerminal connection is described as follows:

- **Specific information sent or received**: When using HyperTerminal for Telnet connectivity, the user ID and password are sent in plaintext format (as with all Telnet connections). If files are being transmitted, only the protocol, terminal emulation data, and file-specific binaries are sent. The computer running HyperTerminal is identified by its IP address when the connection type is TCP/IP. The computer is not uniquely identified when the connection type is not TCP/IP.
- **Default settings**: HyperTerminal is not installed by default when a product in the Windows Server 2003 family is installed manually. HyperTerminal is installed by default, however, if the Windows Server 2003 product is installed using an answer file during automated installation. To remove or uninstall HyperTerminal, see "Controlling HyperTerminal to Prevent the Flow of Information to and from the Internet," later in this section.
- **Triggers**: When HyperTerminal is set to automatically answer incoming connections, a file transfer can be initiated if the Zmodem transfer protocol is used. Otherwise, communication through HyperTerminal is only triggered when the user deliberately initiates it.
- **User notification**: After a user starts a HyperTerminal connection session, the status of the connection that is currently open within HyperTerminal is displayed in the HyperTerminal title bar. The status of the file and text transfer is displayed in the HyperTerminal window during the transfer process. HyperTerminal does not display connection or transfer status information when the automatic download feature of the Zmodem protocol is used. For more information about the HyperTerminal automatic download feature, see "Overview: Using HyperTerminal in a Managed Environment," earlier in this section.
- **Encryption:** Information sent or received by HyperTerminal is not encrypted.
- **Privacy statement and access**: No information is uploaded from the server to Microsoft.
- **Transmission protocol and port**: The protocols used are Kermit, Xmodem, 1K Xmodem, Ymodem, Ymodem-G, and Zmodem transmissions protocols on port 23.
- **Ability to disable**: You can remove HyperTerminal if it is already installed, or if you are using unattended installation for your operating system deployment, you can configure the answer file not to install HyperTerminal. To remove HyperTerminal, see "Controlling

HyperTerminal to Prevent the Flow of Information to and from the Internet," later in this section.

Controlling HyperTerminal to Prevent the Flow of Information to and from the Internet

You can prevent the use of HyperTerminal by disabling it through unattended installation during operating system deployment, or by removing HyperTerminal after installing a product in the Windows Server 2003 family.

The following procedures describe:

- How to specify the HyperTerminal installation options in an answer file that will prevent HyperTerminal from being installed during an unattended installation of a product in the Windows Server 2003 family.
- How to use the Add or Remove Programs utility in Control Panel to remove HyperTerminal after the deployment of a product in the Windows Server 2003 family.

To prevent HyperTerminal from being installed during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, include the following entry:

   hyperterm = Off

To remove HyperTerminal on an individual computer running a product in the Windows Server 2003 family

1. Click **Start**, and then either point to **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Double-click **Accessories and Utilities,** and then double-click **Communications**.
5. Make sure the check box for the HyperTerminal component is cleared.
6. Follow the instructions to complete the Windows Components Wizard.

Note You must have administrative credentials to complete this procedure.

Related Links

- For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
- For more information about what HyperTerminal does and does not support, see the HyperTerminal list of frequently asked questions on the Hilgraeve Web site at:

  http://www.hilgraeve.com/support/faq/index.html

- The Help documentation for the Windows Server 2003 family of products included on the CD and on the Web includes information about HyperTerminal. You can find the documentation on the Web at:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/hyperterminal_top_node.asp

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Using online resources. The Microsoft Web site also contains support information, including the latest downloads and Knowledge Base articles written by support professionals at Microsoft:

- You can search frequently asked questions (FAQs) by product, browse the product support newsgroups, and contact Microsoft Support at the following Web site. You can also search the Microsoft Knowledge Base of technical support information and self-help tools for Microsoft products at this site:

  http://support.microsoft.com/

- You can search for troubleshooting information, service packs, patches, and downloads for your system on the TechNet Web site at:

  http://www.microsoft.com/technet/

Internet Explorer 6.0

This section provides information about:

- The benefits of Microsoft Internet Explorer 6.0 in products in the Windows Server 2003 family.
- A description of Internet Explorer Enhanced Security Configuration, which is enabled by default when you install a product in the Windows Server 2003 family.
- Examples of security-related configuration features offered in Internet Explorer 6.0 in products in the Windows Server 2003 family (as compared to Internet Explorer 5).
- Procedures for working with security-related settings in Internet Explorer.
- Resources for learning about topics related to security in Internet Explorer 6.0.

Notes
This section of the white paper describes Internet Explorer 6.0 in general, but it does not describe Outlook Express (the e-mail component in Internet Explorer 6.0), the New Connection Wizard, or the error reporting tool in Internet Explorer. For information about these components, see the respective sections of this white paper (the error reporting tool in Internet Explorer is described in the "Windows Error Reporting" section of this white paper).

Also note that the New Connection Wizard replaces the Network Connection Wizard and the Internet Connection Wizard in Windows 2000.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization where you use browsers on servers to connect to Web sites, run software from the Internet, download items from the Internet, and perform similar actions. This section, however, provides overview information as well as suggestions for other sources of information.

Benefits and Purposes of Internet Explorer 6.0

Internet Explorer 6.0 is designed to make it easy to browse and interact with sites on an intranet or on the Internet. It differs from many of the other components described in this white paper in that its main function is to communicate with sites on the Internet or an intranet (which contrasts with components that communicate with the Internet in the process of supporting some other activity).

Internet Explorer 6.0 is also designed to be highly configurable, with security and privacy settings that can protect your organization's networked assets while at the same time providing access to useful information and tools. In addition, Internet Explorer Enhanced Security Configuration, which is enabled by default when you install a product in the Windows Server 2003 family, helps make your computer more secure by limiting its exposure to malicious Web sites.

With this enhanced level of security, however, you might find that some Web sites are not displayed correctly in Internet Explorer when you are browsing from a server. Also, you might be prompted to enter your credentials when accessing network resources, such as files in shared folders with Universal Naming Convention (UNC) names. You can easily change the enhanced security settings.

If you want to establish a specific configuration on servers (instead of using Internet Explorer Enhanced Security Configuration), Internet Explorer 6.0 offers more security-related

configuration options and settings than were available in Internet Explorer 5. The subsections that follow provide more information about Internet Explorer Enhanced Security Configuration and about the security-related configuration options and settings in Internet Explorer 6.0.

Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration is enabled by default when you install a product in the Windows Server 2003 family. With this configuration, each zone uses a higher security setting than was used by default in Windows 2000. You can easily change the enhanced security settings.

The following table outlines some of the differences that Internet Explorer Enhanced Security Configuration makes in security settings on a server. (For a description of zones, see "Examples of Security-Related Features Offered in Internet Explorer 6.0," later in this section.)

Security settings with and without Internet Explorer Enhanced Security Configuration

Zone	With Internet Explorer Enhanced Security Configuration	Without Internet Explorer Enhanced Security Configuration (the same security levels as Windows 2000)
Internet zone	High security settings	Medium security settings
Trusted sites zone	Medium security settings	Low security settings
Local intranet zone	Medium-low security settings (intranet sites are not automatically detected)	Medium-low security settings (intranet sites are automatically detected)

Also, with Internet Explorer Enhanced Security Configuration, several sites are added automatically to specific zones:

- The Windows Update Web site is added to the Trusted sites zone. This allows you to continue to get important updates for your operating system. For more information about Windows Update, see the "Windows Update and Automatic Updates" section of this white paper.
- The Windows Error Reporting site is added to the Trusted sites zone. This allows you to report problems you encounter with your operating system and search for fixes. For more information about Windows Error Reporting, see the "Windows Error Reporting" section of this white paper.
- Several local computer sites (for example, http://localhost, https://localhost, hcp://system) are added to the Local intranet zone. This allows applications and code to work locally so that you can complete common administrative tasks.

You can enable or disable the Internet Explorer Enhanced Security Configuration for administrators, all other user groups, or both. For more information, see "To remove Internet Explorer Enhanced Security Configuration and restore the default Internet Explorer 6.0 security settings," later in this section.

For more information about Internet Explorer Enhanced Security Configuration, see the resources listed in "Learning about Internet Explorer Enhanced Security Configuration," later in this section.

Examples of Security-Related Features Offered in Internet Explorer 6.0

This subsection describes enhancements in some of the security-related features in Internet Explorer 6.0, as compared to Internet Explorer 5. These features include:

- A Privacy tab that provides greater flexibility in specifying whether cookies will be blocked from specific sites or types of sites. An example of a type of site that could be blocked is one that does not have a compact policy, that is, a condensed computer-readable privacy statement. (The Privacy tab was not available in Internet Explorer 5.)
- Security settings that specify how Internet Explorer 6.0 handles such higher-risk items as ActiveX controls, downloads, and scripts. You can accept the settings in Internet Explorer Enhanced Security Configuration, you can customize these settings as needed, or you can set them to the predefined levels of high, medium, medium-low, or low. You can specify different settings for a number of zones, the most basic being the four preconfigured zones:
  - Local intranet zone: Normally contains only addresses inside your proxy server. (Note that when Internet Explorer Enhanced Security Configuration is enabled, intranet sites are not automatically detected.)
  - Trusted sites: Includes sites you designate as "trusted."
  - Restricted sites: Includes sites you designate as "restricted."
  - Internet zone: Includes everything that is not in another zone and is not on the local computer.

  You can also specify different settings for customized zones that you add programmatically using the URL security zones application programming interface (API). For more information about this API, see the Microsoft Developer Network Web site at:

  http://msdn.microsoft.com/
- Support for content-restricted IFrames (inline floating frames). This type of support enables developers to implement these frames in a way that makes it more difficult for malicious authors to start e-mail or content-based attacks.
- Improvements that increase the overall security and reliability of Internet Explorer 6.0.

For more information about features available in Internet Explorer, see “Resources for Learning About Topics Related to Security in Internet Explorer 6.0,” later in this section, as well as the Internet Explorer page on the Microsoft Web site at:

http://www.microsoft.com/windows/ie/

Procedures for Working with Security-Related Settings in Internet Explorer

This subsection describes how to carry out the following:

- View security settings for zones in Internet Explorer
- Locate Group Policy objects (GPOs) that affect Internet Explorer, and view related Help
- Determine whether Internet Explorer Enhanced Security Configuration is enabled on a specific server
- Remove Internet Explorer Enhanced Security Configuration and restore the default Internet Explorer 6.0 security settings

To view security settings for zones in Internet Explorer

1. On the server on which you want to view settings, start Internet Explorer by your preferred method, for example, by clicking the Internet Explorer icon on the taskbar.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Security** tab.
4. Select the zone for which you want to view security settings:
   - Internet
   - Local intranet
   - Trusted sites
   - Restricted sites

To locate Group Policy objects (GPOs) that affect Internet Explorer

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Internet Explorer**.
3. View the available settings.
4. Click **User Configuration**, click **Windows Settings**, and then click **Internet Explorer Maintenance**.
5. View the available settings.
6. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Internet Explorer**.
7. View the available settings.

To determine whether Internet Explorer Enhanced Security Configuration is enabled on a specific server

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Scroll down to **Internet Explorer Enhanced Security Configuration**. If the check box is selected, it is enabled. If the check box is cleared, it is not enabled.
5. If you want to see whether Internet Explorer Enhanced Security Configuration is enabled for administrator groups, all other user groups, or both, select **Internet Explorer Enhanced Security Configuration**, and then click **Details**.

To remove Internet Explorer Enhanced Security Configuration and restore the default Internet Explorer 6.0 security settings

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.

3. Click **Add/Remove Windows Components** (on the left).
4. Click **Internet Explorer Enhanced Security Configuration**, and then do one of the following:
   - To remove Internet Explorer Enhanced Security Configuration for both administrators and all other users, clear the **Internet Explorer Enhanced Security Configuration** check box, and then click **Next**.
   - To remove Internet Explorer Enhanced Security Configuration for administrators only or for users who are not in an administrator group, click **Details**, clear either the **For administrator groups** check box or the **For all other user groups** check box, and then click **Next**.
5. Follow the instructions to complete the Windows Components Wizard.

Resources for Learning About Topics Related to Security in Internet Explorer 6.0

This subsection lists resources that can help you learn about the following topics related to security in Internet Explorer 6.0:

- Internet Explorer Enhanced Security Configuration
- Security and privacy settings available in Internet Explorer 6.0
- Methods for mitigating the risks inherent in Web-based programs and scripts
- Ways to use Group Policy objects that control configuration settings for Internet Explorer 6.0
- The Internet Explorer Administration Kit

In addition, for information about unattended installation, see the resources listed in Appendix A, "Resources for Learning About Automated Installation and Deployment."

Note For information about Internet Explorer on clients, that is, for information similar to what is provided in this white paper but focused on clients instead of servers, see one of the following two white papers on the TechNet Web site:

”Using Windows 2000 with Service Pack 3 in a Managed Environment: Controlling Communication with the Internet,” at:

http://www.microsoft.com/technet/prodtechnol/windows2000pro/maintain/w2kmngd/00_abstr.asp

”Using Windows XP Professional with Service Pack 1 in a Managed Environment: Controlling Communication with the Internet,” at:

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

Learning about Internet Explorer Enhanced Security Configuration

For more information about Internet Explorer Enhanced Security Configuration, see one of the following:

- The informational pages displayed in Internet Explorer after you install a product in the Windows Server 2003 family. To view these pages, start Internet Explorer after completing the installation.

- Help topics in Internet Explorer. To view these topics, start Internet Explorer, click **Help**, and then click **Enhanced Security Configuration**.
- Help topics in Help and Support Center. To view these topics, start Internet Explorer, click **Start**, click **Help and Support**, and search for “enhanced security configuration.”

For information about adding sites to the Internet Explorer Enhanced Security Configuration zones either programmatically or by modifying the registry, see the white paper on the Web site for Windows Server 2003 at:

http://www.microsoft.com/windowsserver2003/docs/IESecConfig.doc

Learning about security and privacy settings in Internet Explorer 6.0

An important source of detailed information about security and privacy settings in Internet Explorer 6.0 is the *Microsoft Internet Explorer 6 Resource Kit*. To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

http://www.microsoft.com/reskit/

The *Microsoft Internet Explorer 6 Resource Kit* consists of a number of parts that include these titles:

- "Privacy and Security Features"
- "Preparation for Deployment"
- "Customization and Installation"
- "Maintenance and Support," including information about keeping programs updated
- Appendices, including an appendix titled "Setting System Policies and Restrictions"

You can also use the following sources for information about security and privacy settings in Internet Explorer 6.0:

- Help for Internet Explorer (with Internet Explorer open, click the **Help** menu and select an appropriate option).
- The Internet Explorer page on the Microsoft Web site at:

  http://www.microsoft.com/windows/ie/

Learning about mitigating the risks inherent in Web-based programs and scripts

In a network-based and Internet-based environment, programs can take a variety of forms including scripts within documents, scripts within e-mail, or programs or other code objects running within Web pages. These programs can move across the Internet and are sometimes referred to as "mobile code." Configuration settings provide ways for you to control the way Internet Explorer 6.0 responds when someone tries to run a particular code object on a server running a product in the Windows Server 2003 family. Two examples of the ways you can customize the Internet Explorer configuration are as follows:

- You can control the code (ActiveX controls, scripts, and so on) that administrators or operators can run. You can do this by customizing Authenticode® settings, which can, for example, prevent administrators or operators from running any unsigned code or enable them to only run code signed by specific authors.

- If you want to permit the use of ActiveX controls, but you do not want administrators or operators to download code directly from the Internet, you can specify that when Internet Explorer 6.0 looks for a requested executable, it goes to your own internal Web site instead of the Internet. For more information, see the white paper titled "Managing Mobile Code with Microsoft Technologies," at the end of this list, and search for "CodeBaseSearchPath."

You can use the following sources to learn more about mitigating the risks inherent in Web-based programs and scripts:

- To understand more about how a particular Microsoft programming or scripting language works, see the Microsoft Developer Network Web site at:

  http://msdn.microsoft.com/

- To learn about approaches to mitigating the risks presented by mobile code, see "Managing Mobile Code with Microsoft Technologies," a white paper on the Technet Web site at:

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/mblcode.asp

Learning about Group Policy objects that control configuration settings for Internet Explorer 6.0

You can control configuration settings for Internet Explorer 6.0 by using Group Policy objects (GPOs). (You can also control the configuration of Internet Explorer by using the Internet Explorer Administration Kit; for more information, see "Learning about the Internet Explorer Administration Kit," later in this section.) For sources of information about Group Policy, see Appendix B, "Resources for Learning About Group Policy."

Learning about the Internet Explorer Administration Kit

With the deployment technologies available in the Internet Explorer Administration Kit (IEAK), you can efficiently deploy Internet Explorer and control the configuration of Internet Explorer across your organization. (You can also control the configuration of Internet Explorer by using Group Policy; for more information, see "Learning about Group Policy objects that control configuration settings for Internet Explorer 6.0," earlier in this section.)

A few of the features and resources in the IEAK include:

- **Internet Explorer Customization Wizard**. Step-by-step screens guide you through the process of creating customized browser packages that can be installed on client desktops.
- **IEAK Profile Manager**. After you deploy Internet Explorer, you can use the IEAK Profile Manager to change browser settings and restrictions automatically.
- **IEAK Toolkit**. The IEAK Toolkit contains a variety of helpful tools, programs, and sample files.
- **IEAK Help**. IEAK Help includes many conceptual and procedural topics that you can view by using the Index, Contents, and Search tabs. You can also print topics from IEAK Help.

For more information about the IEAK, see the IEAK Web site at:

http://www.microsoft.com/windows/ieak/

Internet Information Services

This section provides information about:

- The benefits of Internet Information Services (IIS) in products in the Microsoft Windows Server 2003 family
- For servers from which you want to offer content on an intranet or the Internet, descriptions of some of the security-related features offered in IIS 6.0, and suggestions for other sources of information about security and IIS 6.0

  Note For servers from which you do not want to offer content on an intranet or the Internet, you do not need to remove IIS, since by default it is not installed with most products in the Windows Server 2003 family. The exception is Windows Server 2003, Web Edition, on which IIS is installed by default.

  If you use a server as a Web server and then deploy it for some other purpose, remove IIS from that server.

- Controlling Internet printing
- Subcomponents that are part of IIS, with instructions for finding out which subcomponents are installed on a given server
- Viewing Help for IIS
- Other sources of information about IIS

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running servers that communicate across the Internet. This section, however, provides overview information as well as suggestions for other sources of information about balancing your organization's requirements for communication across the Internet with your organization's requirements for protection of networked assets.

Benefits and Purposes of IIS

IIS 6.0 is one of the optional components in products in the Windows Server 2003 family. IIS is a component that provides an easy way to publish information on the Internet or an intranet. In a managed environment, IIS is usually installed on selected servers only. IIS includes innovative security features and a broad range of administrative features for managing Web sites. By using programmatic features like ASP.NET, which is an enhancement to Active Server Pages (ASP), you can more easily create and deploy scalable, flexible Web applications.

IIS is not installed by default with products in the Windows Server 2003 family other than Windows Server 2003, Web Edition. IIS and related components can be added by using either **Add or Remove Programs** in Control Panel or Manage Your Server. After IIS 6.0 is installed, it is configured by default in a "locked down" state. The locked down state means that IIS 6.0 accepts requests for static files only, until it is configured to serve dynamic content. It also means that all time-outs and settings are set to restrictive defaults. You can enable or disable IIS 6.0 functionality based on the needs of your organization by using IIS Manager. You can also enable IIS 6.0 functionality through programmatic and command-line interfaces.

For more information about IIS features, see the following Web sites:

- The product information page for IIS 6.0 at:

http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/iis.mspx

- The technical overview document for IIS 6.0 at:

  http://www.microsoft.com/windowsserver2003/techinfo/overview/iis.mspx

If you have a Web site on which you want to use Microsoft .NET Passport for authentication and you also want to use Passport Manager Administration, a component in the Windows Server 2003 family, see Appendix E, "Passport Manager Administration."

Examples of Security-Related Improvements in IIS 6.0

IIS 6.0 includes a variety of settings and features related to security, some of which are listed in the following table.

Examples of security-related settings and features in IIS 6.0

Setting or feature	Description
Disabling through Group Policy	With the Windows Server 2003 family, domain administrators can prevent users from installing IIS 6.0 on their computers.
Running as an account with limited privileges	IIS 6.0 worker processes run in a user context with limited privileges by default. This drastically reduces the attack surface of the Web server.
Secure ASP	All functions built into ASP pages always run as an account with limited privileges (anonymous user).
Recognized file extensions	IIS 6.0 serves requests only to files that have recognized file extensions and rejects requests to file extensions it doesn't recognize.
Command-line tools not accessible to Web users	Attackers often take advantage of command-line tools that are executable through the Web server. In IIS 6.0, the command-line tools cannot be executed by the default Web server identity.
Write protection for content	Once attackers get access to a server, they try to deface Web sites. By preventing anonymous Web users from overwriting Web content, these attacks can be mitigated.
Time-outs and limits	Product settings are set to aggressive and secure defaults.
Upload data limitations	Administrators can limit the size of data that can be uploaded to a server.
Buffer overflow protection	The Windows Administration Service in IIS will detect if a worker process had a buffer overflow and will exit that process.
File verification	The core server verifies that the requested content exists before it gives the request to a request handler (Internet Server Application Programming Interface [ISAPI] extension).

For more information about creating Web sites with IIS 6.0 and maintaining appropriate levels of awareness and control over the communication to and from those sites, see the IIS Help. For information about viewing the Help, see "To view Help after installing IIS," later in this section.

Another source of information about maintaining appropriate levels of awareness and control over the communication to and from your Web sites is the Internet Information Services page on the TechNet Web site at:

http://www.microsoft.com/technet/prodtechnol/iis/default.asp

Controlling Internet Printing

Internet printing makes it possible for clients to use printers located anywhere in the world by sending print jobs using Hypertext Transfer Protocol (HTTP). Additionally, a computer running a product in the Windows Server 2003 family can use IIS to create a Web page that provides information about printers and provides the transport for printing over the Internet.

For Internet printing, it is important to consider both the server and the client:

- **Server**: Internet printing is an optional component (not installed by default) of IIS 6.0. A server running a product in the Windows Server 2003 family can be configured to act as a print server allowing Internet printing. In a managed environment, you might want to ensure that the Internet printing subcomponent of IIS is not installed. For information about how to do this, see "Procedures for Checking or Controlling the Installation of IIS Subcomponents," later in this section.
- **Client**: Clients running Windows XP can install an Internet printer using a Web browser, the Add Printer Wizard, or the Run dialog box. To control whether clients running Windows XP can support Internet printing, see the section about Internet printing in the white paper titled "Using Windows XP Professional with Service Pack 1 in a Managed Environment: Controlling Communication with the Internet." You can view this white paper on the TechNet Web site at:

  http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

  Note The white paper available from the preceding link also includes a procedure for using Group Policy to disable Internet printing on a computer running IIS. That procedure is not applicable for computers running products in the Windows Server 2003 family because the Group Policy object referred to in the procedure is not available in the Windows Server 2003 family. For such servers, use the procedures in "Procedures for Checking or Controlling the Installation of IIS Subcomponents," later in this section.

Answer File Entries and Registry Keys for IIS Subcomponents

For reference purposes, the following table shows the syntax for answer file entries associated with IIS in the Windows Server 2003 family as well as the corresponding registry keys. Do not change the registry keys. They are shown for use in a script that could check whether a particular component is installed on a particular server. A registry key value of 0x00000000 means the component is not installed, and a value of 0x00000001 means the component is installed.

Note For more details about answer file entries related to IIS components, follow the steps in "To view Help after installing IIS," later in this section, and then search for the topic called "Installing IIS." In that topic, look for a table showing the answer file entries.

Answer file entries and registry keys associated with IIS subcomponents for the Windows Server 2003 family

IIS subcomponent	Syntax for answer file entry (in the [Components] section)	Registry key (for use in a script that checks whether a component is installed): 0x00000000 means it is not installed; 0x00000001 means it is installed
IIS common files	iis_common = On | Off	HKEY_LOCAL_MACHINE\Software\

		Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\iis_common
Active Server Pages (ASP) for IIS	iis_asp = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\iis_asp
File Transfer Protocol (FTP) service	iis_ftp = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\iis_ftp
IIS Manager (Microsoft Management Console [MMC] snap-in)	iis_inetmgr = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\iis_inetmgr
Internet Data Connector	iis_internetdataconnector = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\ iis_internetdataconnector
Network News Transfer Protocol (NNTP) service	iis_nntp = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\iis_nntp
Server-Side Includes	iis_serversideincludes = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\ iis_serversideincludes
Simple Mail Transfer Protocol (SMTP) service	iis_smtp = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\iis_smtp
Web Distributed Authoring and Versioning (WebDAV) publishing	iis_webdav = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\iis_webdav
World Wide Web (WWW) service	iis_www = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\iis_www
Remote administration (HTML)	sakit_web = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\sakit_web
Internet Server Application Programming Interface (ISAPI) for Background Intelligent Transfer Service (BITS) server extensions	BitsServerExtensionsISAPI = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\ bitsserverextensionsisapi
Background Intelligent Transfer Service (BITS) server extensions snap-in	BitsServerExtensionsManager = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\ bitsserverextensionsmanager
FrontPage server extensions	fp_extensions = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\fp_extensions
Internet printing	inetprint = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\inetprint
ActiveX control and sample pages for hosting Terminal Services client connections over the Web	TSWebClient = On | Off	HKEY_LOCAL_MACHINE\Software\ Microsoft\Windows\CurrentVersion\Setup\ OC Manager\Subcomponents\TSWebClient

Note For several of the subcomponents in the previous table, the software for the subcomponent is installed regardless of the answer-file entry, but the subcomponent cannot be used unless the answer-file entry is set to On (or the procedure is followed for installing the subcomponent through **Add or Remove Programs** in Control Panel). These subcomponents are Internet Data Connector, Server-Side Includes, and WebDAV publishing.

Procedures for Checking or Controlling the Installation of IIS Subcomponents

The following procedures explain how to:

- View the registry keys listed in the table in the previous subsection
- View or change the IIS components currently installed on a computer running a product in the Windows Server 2003 family
- Specify answer file entries that control whether IIS subcomponents are included during unattended installation

To view registry keys related to IIS subcomponents

1. Open Registry Editor by clicking **Start**, clicking **Run**, and then typing **regedit**.

   Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

2. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Setup\OC Manager\Subcomponents\.
3. View the registry keys listed in the table in the previous subsection, and find the value associated with each key. A value of 0x00000000 means the component is not installed. A value of 0x00000001 means the component is installed.
4. Close **Registry Editor**.

To view or change the IIS components currently installed on a computer running a product in the Windows Server 2003 family

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Select **Application Server** and then click **Details**.
5. Find **Internet Information Services (IIS)** in the list, and perform one of the following steps:
   - If IIS is installed and you want to remove it, clear the check box for IIS and complete the wizard.
   - If IIS is not installed and you want to add the default set of IIS subcomponents, select the check box for IIS and complete the wizard.

- If you want to view or select from the list of IIS subcomponents, after selecting IIS, click **Details**.

Note The Internet Printing component is in the list of components that appears when you click **Details**.

6. Follow the instructions to complete the Windows Components Wizard.

To specify answer file entries that control whether IIS subcomponents are included during unattended installation

1. Using the methods you prefer for unattended installation or remote installation, create an answer file.
2. In the [Components] section of the answer file, add the appropriate entries listed in the table in "Answer File Entries and Registry Keys for IIS Subcomponents," earlier in this section. Ensure that the entries specify **Off** for components you do not want to install and **On** for components you want to install.

   If no IIS subcomponents are listed in an answer file for unattended installation of a product in the Windows Server 2003 family, these subcomponents are *not* installed by default.

Note For more details about answer file entries related to IIS components, follow the steps in the next procedure, “To view Help after installing IIS,” and then search for the Help topic called “Installing IIS.” In that topic, look for a table showing the answer file entries.

To view Help after installing IIS

1. After installing IIS (including the IIS Manager subcomponent, which is included in default installations of IIS), click **Start**.
2. Either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
3. Double-click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
4. Click the **Help** menu and then click **Help Topics**.

Related Links

For more information about IIS, see the following Web sites:

- The product information page for IIS 6.0 at:

  http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/iis.mspx
- The technical overview document for IIS 6.0 at:

  http://www.microsoft.com/windowsserver2003/techinfo/overview/iis.mspx
- The Internet Information Services page on TechNet at:

  http://www.microsoft.com/technet/prodtechnol/iis/default.asp
- For clients running Windows XP, the section about Internet printing in the white paper titled “Using Windows XP Professional with Service Pack 1 in a Managed Environment: Controlling Communication with the Internet.” You can view this white paper on the TechNet Web site at:

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

Internet Protocol Version 6 (IPv6)

This section provides information about:

- An introduction to the IPv6 protocol
- The benefits of the IPv6 protocol
- How the IPv6 protocol communicates with sites on the Internet
- How to control the IPv6 protocol to limit the flow of information to and from the Internet
- How to monitor and troubleshoot the IPv6 protocol after configuration is complete

An Introduction to the IPv6 Protocol

The current version of the Internet Protocol (known as IP version 4 or IPv4) has not been substantially changed since 1981, when the Internet Engineering Task Force (IETF) published the definitive specification of IP (RFC 791). IPv4 has proven to be robust, easily implemented, and interoperable. It has stood the test of scaling an internetwork to a global utility the size of today's Internet, which is a tribute to its initial design.

The initial design, however, did not anticipate the exponential growth of the Internet and the exhaustion of the IPv4 address space, or the effort required to maintain routing information. Because of the way in which IPv4 network IDs are allocated, there are routinely over 70,000 routes in the routing tables of Internet backbone routers. Most current IPv4 implementations are configured either manually or through a stateful address configuration protocol such as the Dynamic Host Configuration Protocol (DHCP). With more computers and devices using IP, there is a need for a simpler and more automatic configuration of addresses and other configuration settings that do not rely on the administration of a DHCP infrastructure.

Another factor driving the development of IPv6 is the need for improved encryption. Private communication over a public medium like the Internet requires encryption services that protect the data sent from being viewed or modified in transit. There is a standard for providing security for IPv4 packets (known as Internet Protocol security or IPSec). In IPv4, however, this standard is optional and proprietary solutions are prevalent.

While standards for quality of service (QoS) exist for IPv4, real-time traffic support relies on the IPv4 Type of Service (TOS) field and the identification of the payload, typically using a User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port. Unfortunately, the IPv4 TOS field has limited functionality and has different interpretations. In addition, payload identification using a TCP or UDP port is not possible when the IPv4 packet payload is encrypted.

To address these concerns, the IETF has developed a suite of protocols and standards known as IP version 6 (IPv6). This new version, previously named IP-The Next Generation (IPng), incorporates the concepts of many proposed methods for updating the IPv4 protocol. IPv6 is intentionally designed for minimal impact on upper and lower layer protocols by avoiding the arbitrary addition of new features.

For the latest set of RFCs and Internet drafts describing IPv6 and IPv4 coexistence and migration technologies, see the Next Generation Transition (ngtrans) Working Group Web site at:

http://www.ietf.org/html.charters/ngtrans-charter.html

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Benefits and Purposes of the IPv6 Protocol

The IPv6 header has a new format that is designed to minimize header validation and processing. An IPv6 address is four times larger than an IPv4 address. The global addresses used on the IPv6 portion of the Internet are designed to create an efficient, hierarchical, and summarized routing infrastructure that addresses the common occurrence of multiple levels of Internet service providers. On the IPv6 Internet, the backbone routers have an efficient and hierarchical addressing and routing infrastructure that uses smaller routing tables.

IPv6 supports both stateful address configuration, such as address configuration in the presence of a DHCP server, and stateless address configuration, or address configuration in the absence of a DHCP server. The support for IPSec is an IPv6 protocol suite requirement. This requirement provides a standards-based solution for network security needs and promotes interoperability between different IPv6 implementations. The new fields in the IPv6 header define how traffic is handled and identified.

Traffic identification, by using a Flow Label field in the IPv6 header, allows routers to identify and provide special handling for packets that belong to a flow. (A flow is a series of packets between a source and destination.) Because the traffic is identified in the IPv6 header, support for quality of service (QoS) can be easily achieved even when the packet payload is encrypted with IPSec.

The new Neighbor Discovery protocol for neighboring node interaction in IPv6 is a series of messages from the Internet Control Message Protocol for IPv6 (ICMPv6) that manage the interaction of neighboring nodes. Neighbor Discovery replaces Address Resolution Protocol (ARP), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast messages.

IPv6 can be extended for new features by adding extension headers after the IPv6 header. Unlike the IPv4 header, which can only support 40 bytes of options, the size of IPv6 extension headers is only constrained by the size of the IPv6 packet.

The following table compares the key features of the IPv4 and IPv6 protocols.

Comparison of features in IPv4 and IPv6

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPsec support is optional.	IPsec support is required.
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	All optional data is moved to IPv6 extension headers.
The Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbor Solicitation messages.

The Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
Links must support a 576-byte packet size (possibly fragmented).	Links must support a 1280-byte packet size (without fragmentation).

For more information about IP version 6, see the Microsoft Web site at:

http://www.microsoft.com/windowsserver2003/technologies/ipv6/

Overview: Using the IPv6 Protocol in a Non-Native IPv6 Environment

On networks that do not have native support for IPv6 traffic, the IPv6 traffic is transmitted on the network by encapsulating the IPv6 packets within IPv4 packet headers. One such method of transmission is referred to as 6to4 tunneling.

For more information about the 6to4 tunneling technique, see "Connection of IPv6 Domains via IPv4 Clouds," in RFC 3056 on the Internet Engineering Task Force (IETF) Web site at:

http://www.ietf.org/rfc/rfc3056.txt?number=3056/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

How the IPv6 Protocol Communicates with Sites on the Internet

Although there are differences between the two protocol versions IPv4 and IPv6, their differences do not prevent them from coexisting or communicating on the IPv4 network.

If native IPv6 connectivity does not exist, a computer makes a Domain Name System (DNS) query for network relay routers that provide IPv6 service as part of the startup process. By default, this DNS query is presently set to "6to4.ipv6.microsoft.com" and the response contains a well-known IPv4 anycast address. (An anycast address is one that identifies multiple nodes and interfaces.) As more IPv6 relay routers are added in the future, this address will be assigned to more computers that are owned by various Internet service providers (ISPs).

If the DNS query provides multiple addresses, the host selects an appropriate relay router by sending an IPv6 packet to each one and choosing the one that responds first.

> **Note** 6to4 tunneling is enabled when IPv6 services are not native to your network and there is a public IPv4 Internet address present on the network access point.

The use of IPv6 in the Microsoft Windows Server 2003 family is currently supported only when IPv4 is also installed.

Security information for IPv6

TCP/IP networks are susceptible to a variety of possible attacks, from passive attacks (such as eavesdropping) to active attacks (such as denial-of-service attacks). For more information about general security issues with IP, especially in a large organization, see "Best Practices for Enterprise Security," on the Microsoft Web site at:

http://www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp

Controlling the IPv6 Protocol to Limit the Flow of Information to and from the Internet

You can stop the ingress or egress of IPv6 traffic on your network by configuring your network firewall to block all IPv6-specific packets. When the 6to4 tunneling technique is used, you can configure your firewall to block all IPv4 packets that include the IPv6 protocol designation of 41 in the protocol field of the IPv4 packet header.

The default settings for a member of the computer users group do not permit those users to install networking protocols. You should limit who is allowed to install the IPv6 stack on network computers by carefully limiting the number of users that have administrative logon credentials.

You can use the Active Directory directory service and Group Policy to filter and control the user's ability to add new networking protocols, or to modify existing networking configurations. For more information about these configuration methods, see "Group Policy," in the Help and Support Center index. For information about installing and uninstalling IPv6, see the list of procedures in the next subsection.

Procedures for Configuration of the IPv6 Protocol

Installing and uninstalling the IPv6 protocol stack can be done by using the Network Connections folder or the command prompt.

The following two procedures describe installing and uninstalling the IPv6 protocol stack by using the Network Connections folder.

To install IPv6 using the Network Connections folder

1. Click **Start**.
2. Either point to **Control Panel** and then double-click **Network Connections**, or point to **Settings**, click **Control Panel**, and then double-click **Network Connections**.
3. Right-click any local area connection, and then click **Properties**.
4. Click **Install**.

5. In the **Select Network Component Type** dialog box, click **Protocol**, and then click **Add**.
6. In the **Select Network Protocol** dialog box, click **Microsoft TCP/IP version 6**.

To uninstall IPv6 using the Network Connections folder

1. Click **Start**.
2. Either point to **Control Panel** and then double-click **Network Connections**, or point to **Settings**, click **Control Panel**, and then double-click **Network Connections**.
3. Right-click any local area connection, and then click **Properties**.
4. Click **Microsoft TCP/IP version 6** in the list of installed components, and then click **Uninstall**.

The following two procedures describe installing and uninstalling the IPv6 protocol stack by using the command prompt.

To install IPv6 on a computer using the command prompt

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **netsh interface ipv6 install**, and then press ENTER.

To uninstall IPv6 from a computer using the command prompt

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **netsh interface ipv6 uninstall**, and then press ENTER.

Note The IPv6 configuration options require that you have administrative credentials on the computer.

Monitoring and Troubleshooting the IPv6 Protocol

The following procedures describe ways to view TCP/IP configurations.

To display the complete list of TCP/IP interface configurations for a computer using the command prompt

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **ipconfig /all**, and then press ENTER.

To display the TCP/IP routing table using the command prompt

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **route print**, and then press ENTER.

Note For more information about TCP/IP configurations, see "TCP/IP utilities," in the Help and Support Center index.

Troubleshooting a command-line installation error

The installation of the IPv6 protocol stack requires that you have administrative credentials. The command-line prompt will yield the "Access is denied" error (0x800700005) if you attempt to install the IPv6 protocol from the command-line prompt without having the required account credentials.

Accessing Help documentation for Internet Protocol version 6 (IPv6) for the Windows Server 2003 family

Products in the Windows Server 2003 family have Help documentation describing Internet Protocol version 6 (IPv6). You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any server running a product in the Windows Server 2003 family. The following procedure provides the details.

To access Help documentation for a server running a product in the Windows Server 2003 family

1. Open Help for a product in the Windows Server 2003 family by doing one of the following:
   - On any computer running a product in the Windows Server 2003 family, click **Start**, and then click **Help and Support**.
   - View Help on the Web at:

     http://www.microsoft.com/windowsserver2003/proddoc/

     As appropriate, navigate from this Web site to the documentation for the server product you are using.
2. To view information about IPv6, navigate to Network Services\Managing Core Network Services\IP Version 6.

Related Links

Online resources

- For information about using IP version 6, see Help for products in the Windows Server 2003 family (click **Start** and then click **Help and Support**).

  You can view Help for products in the Windows Server 2003 family on the Web at:

  http://www.microsoft.com/windowsserver2003/proddoc/
- For more information about the 6to4 tunneling technique, see "Connection of IPv6 Domains via IPv4 Clouds," in RFC 3056 on the IETF Web site at:

  http://www.ietf.org/rfc/rfc3056.txt?number=3056/
- For more information about IP version 6, see the Microsoft Web site at:

  http://www.microsoft.com/windowsserver2003/technologies/ipv6/
- For more information about enterprise security, see "Best Practices for Enterprise Security," on the Microsoft Web site at:

  http://www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp
- For more information about IPv6 addressing, see "IP Version 6 Addressing Architecture," in RFC 2373 on the IETF Web site at:

  http://www.ietf.org/rfc/rfc2373.txt?number=2373/

- For the latest set of RFCs and Internet drafts describing IPv6 and IPv4 coexistence and migration technologies, see the Next Generation Transition (ngtrans) Working Group Web site at:

  http://www.ietf.org/html.charters/ngtrans-charter.html

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Printed references

For more information about the IPv6 protocol suite, you can consult the following references:

- Davies, J. *Understanding IPv6.* Redmond, WA: Microsoft Press, 2002.
- Huitema, C. *IPv6: The New Internet Protocol.* Second edition. Upper Saddle River, NJ: Prentice Hall, 1998.
- Miller, M. *Implementing IPv6*: *Supporting the Next Generation of Protocols*. Second edition. Foster City, CA: M&T Books, 2000.

NetMeeting

This section provides information about:

- The benefits of NetMeeting
- Using NetMeeting in a managed environment
- How NetMeeting communicates with sites on the Internet
- How to control NetMeeting to limit the flow of information to and from the Internet

> **Note** A variety of technologies and protocols are built into the Microsoft Windows Server 2003 family to support applications that enable real-time communications (RTC). For information about these technologies, including information about the RTC Client application programming interface (API), see the Real-Time Communications Web page on the Microsoft Web site at:
>
> http://www.microsoft.com/rtc/

Benefits and Purposes of NetMeeting

NetMeeting® conferencing software, which is included in the Microsoft Windows Server 2003 family, enables real-time communication and collaboration over the Internet or an intranet. From a computer running the Windows 95, Windows 98, Windows NT 4.0, Windows 2000, or Windows XP operating system, users can communicate over a network with real-time voice and video technology. Users can work together on virtually any Windows-based application, exchange or mark up graphics on an electronic whiteboard, transfer files, or use the text-based chat program.

NetMeeting helps small and large organizations take full advantage of their corporate intranet for real-time communication and collaboration. On the Internet, connecting to other NetMeeting users is made easy with Internet Locator Service (ILS), enabling participants to call each other from a dynamic directory within NetMeeting or from a Web page. Features include remote desktop sharing, virtual conferencing using Microsoft Outlook, security features, and the ability to embed the NetMeeting user interface in an organization's intranet Web pages.

> **Note** NetMeeting is not available on the 64-bit versions of the Windows Server 2003 family.

To learn more about the NetMeeting features, see the article on the Microsoft TechNet Web site at:

http://www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp

Overview: Using NetMeeting in a Managed Environment

NetMeeting supports communication standards for audio, video, and data conferencing. NetMeeting users can communicate and collaborate with users of other standards-based, compatible products. They can connect by modem, Integrated Services Digital Network (ISDN), or local area network (LAN) using Transmission Control Protocol/Internet Protocol (TCP/IP). In addition, support for Group Policy in NetMeeting makes it easy for administrators to centrally control and manage the NetMeeting work environment.

You can use Active Directory directory service and Group Policy to configure NetMeeting to help meet your security requirements. You can also control the configuration of NetMeeting by using the NetMeeting Resource Kit. For more information about the NetMeeting Resource Kit, see "Alternate Methods for Controlling NetMeeting," later in this section.

NetMeeting components and features require that several ports be open from the firewall. For more information, see "NetMeeting and firewalls," later in this section.

How NetMeeting Communicates with Sites on the Internet

NetMeeting provides an infrastructure for communication between network applications and services. In this infrastructure, NetMeeting is both an application and a platform for other applications or services. The components and services in NetMeeting provide real-time communication and collaboration over the Internet or an organization's intranet.

NetMeeting audio and video conferencing features are based on the H.323 infrastructure, which enables NetMeeting to interoperate with other H.323 standards-based products. (H.323 is a standard approved by the International Telecommunication Union [ITU] that defines how audiovisual conferencing data is transmitted across networks.) NetMeeting data conferencing features are based on the T.120 infrastructure, enabling NetMeeting to interoperate with other T.120 standards-based products. (The T.120 standard is a suite of communication and application protocols developed for real-time, multipoint data connections and conferencing.)

Detailed information about the H.323 and T.120 standards is beyond the scope of this white paper. Further information can be found on the following sites:

- For more information about the H.323 standard and NetMeeting, see Part 3, Chapter 11, "Understanding the H.323 Standard," in the *Microsoft NetMeeting 3 Resource Kit* at:

  http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part3/chaptr11.asp

- For more information about the H.323 specification, see the following Web sites at:

  http://www.itu.int/home/index.html

  http://www.imtc.org/h323.htm

- To learn more about the T.120 standard and NetMeeting, see Part 3, Chapter 10, "Understanding the T.120 Standard," in the *Microsoft NetMeeting 3 Resource Kit* at:

  http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part3/chaptr10.asp

- For more information about the T.120 architecture, see the International Multimedia Teleconferencing Consortium (IMTC) Web site at:

  http://www.imtc.org/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

NetMeeting port assignments

When you use NetMeeting to call other users over the Internet, several IP ports are required to establish the outbound connection. The following table describes the port numbers, their functions, and the resulting connection.

Port assignments for NetMeeting

Port	Function	Outbound connection

389	Internet Locator Service (ILS)	TCP
522	User Location Service (ULS)	TCP
1503	T.120	TCP
1720	H.323 call setup	TCP
1731	Audio call control	TCP
1024 through 65535 (dynamic)	H.323 call control	TCP
1024 through 65535 (dynamic)	H.323 streaming	Real-Time Transfer Protocol (RTP) over User Datagram Protocol (UDP)

For more information about NetMeeting communication ports and firewall configuration topics, see Part 2, Chapter 4, "Firewall Configuration," in the *Microsoft NetMeeting 3 Resource Kit* at:

http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

Controlling NetMeeting to Limit the Flow of Information to and from the Internet

You can configure NetMeeting by using Group Policy objects (GPOs) on servers running products in the Windows Server 2003 family. (You can also control the configuration of NetMeeting by using the NetMeeting Resource Kit; for more information, see "Alternate Methods for Controlling NetMeeting," later in this section.)

This subsection includes information about the following topics:

- NetMeeting and Group Policy
- NetMeeting security
- NetMeeting and firewalls
- Establishing a NetMeeting connection with a firewall
- Firewall limitations for NetMeeting

NetMeeting and Group Policy

Group Policy can be used to define the default NetMeeting configuration settings that will be automatically applied to users and computers. These settings determine which NetMeeting features and capabilities are available to a particular group of users. The Group Policy configuration settings that are specific to NetMeeting are grouped into two different categories. These category groupings enable you to independently manage NetMeeting configuration settings for computers and users within your organization. Through the use of Group Policy you can enable, disable, or set configuration options for NetMeeting features or capabilities.

For additional information about Group Policy, see Appendix B, "Resources for Learning About Group Policy."

You can use Group Policy to manage the following NetMeeting configuration options for users in your organization:

- NetMeeting Group Policy settings for computers

- NetMeeting Group Policy settings for users

Configuring NetMeeting settings for computers through Group Policy

You can use Group Policy to determine the NetMeeting features and capabilities that are available to all users of the computers that are affected by the application of the NetMeeting Group Policy settings.

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for Configuration of NetMeeting," later in this section. The NetMeeting Group Policy configuration setting that is specific to computers is as follows:

- **Disable remote Desktop Sharing**: You can use Group Policy to set remote desktop sharing choices in NetMeeting for all the users who are affected by the application of this Group Policy setting.

For more information about how to use Group Policy to manage the NetMeeting computer settings, see "To disable the NetMeeting remote desktop sharing feature through Group Policy," later in this section.

> **Note** Computer-related Group Policy settings are applied when the operating system starts and during the periodic refresh cycle.

Configuring NetMeeting settings through Group Policy

You can use Group Policy to determine the NetMeeting features and capabilities that are available for a user or a group of users that are affected by the application of the NetMeeting Group Policy settings.

These Group Policy configuration options include the policy settings for NetMeeting, application sharing, audio and video, and the options page.

For more information about how to use Group Policy to manage the NetMeeting user settings, see "Procedures for Configuration of NetMeeting," later in this section.

The NetMeeting Group Policy configuration settings that are specific to users are as follows:

Configuring NetMeeting settings for users through Group Policy

For details about locating the Group Policy objects for NetMeeting, see "Procedures for Configuration of NetMeeting," later in this section. You can use Group Policy to set configuration settings for the following NetMeeting features:

- **Enable Automatic Configuration**: Configures NetMeeting to download settings for users each time it starts.
- **Disable Directory services**: Disables the directory feature—users will not log on to a directory server when NetMeeting starts. Users will not be able to view or make calls using the NetMeeting directory.
- **Prevent adding Directory servers**: Prevents the user from adding directory servers to the list of available directory servers they can use for placing calls.
- **Prevent viewing Web directory**: Prevents the user from viewing directories as Web pages in a browser.

- **Set the intranet support Web page**: Sets the Web address that NetMeeting will display when users choose the Online Support command from the NetMeeting Help menu.
- **Set Call Security options**: Sets the level of security for outgoing and incoming NetMeeting calls.
- **Prevent changing Call placement method**: Prevents the user from changing the way calls are placed, either directly or by means of a gatekeeper server.
- **Prevent automatic acceptance of Calls**: Prevents the user from turning on automatic acceptance of incoming calls.
- **Allow persisting automatic acceptance of Calls**: Sets automatic acceptance of incoming calls to be persistent.
- **Prevent sending files**: Prevents users from sending files to others in a conference.
- **Prevent receiving files**: Prevents users from receiving files from others in a conference.
- **Limit the size of sent files**: Sets the maximum file size that can be sent to others in a conference.
- **Disable Chat**: Disables the chat feature of NetMeeting.
- **Disable NetMeeting 2.x Whiteboard**: Disables the NetMeeting 2.x Whiteboard feature. (The 2.x feature provides compatibility with earlier versions of NetMeeting only.)
- **Disable Whiteboard**: Disables the whiteboard feature of NetMeeting.

Configuring NetMeeting application sharing settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for Configuration of NetMeeting," later in this section. You can use Group Policy to set configuration settings for the following elements of the NetMeeting Application Sharing feature:

- **Disable application Sharing**: Disables the NetMeeting application sharing feature completely. Users will not be able to host or view shared applications.
- **Prevent Sharing**: Prevents users from sharing anything themselves. They will still be able to view shared applications or desktops from others.
- **Prevent Desktop Sharing**: Prevents users from sharing their Windows desktop. They will still be able to share individual applications.
- **Prevent Sharing Command Prompts**: Prevents the user from sharing command prompts. Enabling this prevents the user from inadvertently sharing applications, since command prompts can be used to start other applications.
- **Prevent Sharing Explorer windows**: Prevents the user from sharing Windows Explorer windows. Enabling this prevents the user from inadvertently sharing applications, since Windows Explorer windows can be used to start other applications.
- **Prevent Control**: Prevents users from allowing others in a conference to control what they have shared. Enabling this enforces a read-only mode whereby the other participants cannot change the data in the shared application.
- **Prevent Application Sharing in true color**: Prevents users from sharing applications in true color, which uses more bandwidth.

Configuring NetMeeting audio and video settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for Configuration of NetMeeting," later in this section. You can use Group Policy to set configuration settings for the following audio and video elements in NetMeeting:

- **Limit the bandwidth of Audio and Video**: Configures the maximum bandwidth, specified in kilobytes per second, to be used for audio and video.
- **Disable Audio**: Disables the audio feature of NetMeeting; users will not be able to send or receive audio.
- **Disable full duplex Audio**: Disables the full duplex audio mode. Users will not be able to listen to incoming audio while speaking into the microphone. Older audio hardware may not perform well when full duplex audio is enabled.
- **Prevent changing DirectSound Audio setting**: Prevents the user from changing the DirectSound audio setting. DirectSound has a better audio quality, although earlier audio hardware may not support it.
- **Prevent sending Video**: Prevents the user from sending video. Setting this option does not prevent the user from receiving video.
- **Prevent receiving Video**: Prevents the user from receiving video. Setting this option does not prevent the user from sending video.

Configuring NetMeeting options settings through Group Policy

For details about locating the Group Policy objects (GPOs) for NetMeeting, see "Procedures for Configuration of NetMeeting," later in this section. You can use Group Policy to set configuration settings for the following elements of the NetMeeting Options page:

- **Hide the General page**: Removes the General tab on the NetMeeting Options page.
- **Disable the Advanced Calling button**: Disables the Advanced Calling button from the General page.
- **Hide the Security page**: Removes the Security tab on the NetMeeting Options page.
- **Hide the Audio page**: Removes the Audio tab on the NetMeeting Options page.
- **Hide the Video page**: Removes the Video tab on the NetMeeting Options page.

Note User-related Group Policy settings are applied when a user logs on to the computer and during the periodic refresh cycle.

NetMeeting security

The NetMeeting security architecture for data conferencing takes advantage of the existing, standards-compliant security features of the Windows Server 2003 family and Microsoft Internet Explorer. The NetMeeting security architecture utilizes a 40-bit encryption technology and has the following security features:

- **Password protection**: This feature enables the user to create or participate in a meeting that requires a password to join. Password protection helps to ensure that only authorized users participate in a password-protected meeting. A password is also required to use the remote desktop sharing feature.
- **User authentication**: This feature provides a way to verify the identity of a caller or meeting participant using a certificate.
- **Data encryption**: This feature helps to protect data exchanged during a meeting so that it is not easily read by any unauthorized parties that may intercept the data. The 40-bit data

encryption applies to the whiteboard and chat features, shared applications, and transferred files. Audio and video communications are not encrypted.

If you need stronger encryption than the 40-bit encryption supported in NetMeeting, you can use applications based on the RTC protocols and technologies built into products in the Windows Server 2003 family. For more information about these protocols and technologies, see the Real-Time Communications Web page on the Microsoft Web site at:

http://www.microsoft.com/rtc/

NetMeeting security features integrate with security in the Windows Server 2003 family and Internet Explorer in a variety of ways, including the following:

- NetMeeting uses the NetMeeting private certificate store to provide personal certificates for user authentication and data encryption.
- NetMeeting uses the Windows certificate store to maintain NetMeeting certificates.
- NetMeeting uses Security Support Provider Interface (SSPI) functions to generate and process security tokens.

These security features can be implemented by an administrator or a NetMeeting user. Using the NetMeeting Resource Kit Wizard or Group Policy in NetMeeting, the administrator can enforce security settings that apply to all users. If allowed by the administrator, NetMeeting users can also select their own security settings in the NetMeeting user interface (UI) and change security settings for individual calls.

You can use the following sources to learn more about NetMeeting configuration and security topics:

- For more information about the NetMeeting Resource Kit Wizard, see Part 2, Chapter 2, "Firewall Configuration," in the *Microsoft NetMeeting 3 Resource Kit* at:

  http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter2.asp
- For more information about the security features available in NetMeeting, see Part 2, Chapter 5, “NetMeeting Security,” in the *Microsoft NetMeeting 3 Resource Kit* at:

  http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter5.asp

NetMeeting and firewalls

You can configure firewall components in a variety of ways, depending on your organization's specific security policies and overall operations. While most firewalls are capable of allowing primary (initial) and secondary (subsequent) Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections, it is possible that they are configured to support only specific connections based on security considerations. For example, some firewalls support only primary TCP connections, which some professionals view as the most reliable.

For NetMeeting multipoint data conferencing—program sharing, whiteboard, chat, file transfer, and directory access—your firewall only needs to pass through primary TCP connections on assigned ports. NetMeeting audio and video features require secondary TCP and UDP connections on dynamically assigned ports.

Note NetMeeting audio and video features require secondary TCP and UDP connections. Therefore, when you establish connections through firewalls that accept only primary TCP connections, you are not able to use the audio or video features of NetMeeting.

Detailed firewall configuration procedures for NetMeeting are beyond the scope of this white paper. For more information about NetMeeting firewall connections, see Part 2, Chapter 4,

"Firewall Configuration," of the *Microsoft NetMeeting 3 Resource Kit,* particularly the section titled, "Establishing a NetMeeting Connection with a Firewall," at:

http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

Microsoft NetMeeting can be configured to work with an organization's existing firewall security. Because of limitations in most firewall technology, however, few products are available that enable you to securely transport inbound and outbound NetMeeting calls containing audio, video, and data across a firewall. You should consider carefully the relative security risks of enabling different parts of a NetMeeting call in your firewall product. You must especially consider the security risks involved when modifying your firewall configuration to enable any component of an inbound NetMeeting call.

Some organizations have security or policy concerns that require them to limit how fully they support NetMeeting in their firewall configuration. These concerns are based on network capacity planning or weaknesses in the firewall technology being used. For example, security concerns might prohibit an organization from accepting any inbound or outbound flow of UDP data through the firewall. Because these UDP connections are required for NetMeeting audio and video features, disabling this function excludes audio and video features in NetMeeting for calls through the firewall. The organization can still use NetMeeting data conferencing features such as program sharing, file transfer, whiteboard, and chat for calls through the firewall by allowing only TCP connections on ports 522 and 1503.

For more information about NetMeeting firewall security, see the section titled "Security and Policy Concerns," in the chapter of the NetMeeting Resource Kit from the previous link (scroll through the chapter until you find the section).

Establishing a NetMeeting connection with a firewall

When you use NetMeeting to call other users over the Internet, several IP ports are required to establish the outbound connection.

If you use a firewall to connect to the Internet, it must be configured so that the following IP ports are not blocked:

- TCP ports 389, 522, 1503, 1720, and 1731
- TCP and UDP ports (1024 through 65535)

To establish outbound NetMeeting connections through a firewall, the firewall must be configured to do the following:

- Pass through primary TCP connections on ports 389, 522, 1503, 1720, and 1731
- Pass through secondary TCP and UDP connections on dynamically assigned ports (1024 through 65535)

The H.323 call setup protocol dynamically negotiates a TCP port for use by the H.323 call control protocol. Also, both the audio call control protocol and the H.323 call setup protocol dynamically negotiate UDP ports for use by the H.323 streaming protocol, called the Real-Time Transfer Protocol (RTP). In NetMeeting, two UDP ports are designated on each side of the firewall for audio and video streaming, for a total of four ports for inbound and outbound audio and video. These dynamically negotiated ports are selected arbitrarily from all ports that can be assigned dynamically.

NetMeeting directory services require either port 389 or port 522, depending on the type of server you are using. The Microsoft Internet Locator Service (ILS), which supports LDAP for NetMeeting, requires port 389. The Microsoft User Location Service (ULS), developed for NetMeeting 1.0, requires port 522.

Firewall limitations for NetMeeting

Some firewalls cannot support an arbitrary number of virtual internal IP addresses, or cannot do so dynamically. With these firewalls, you can establish outbound NetMeeting connections from computers inside the firewall to computers outside the firewall, and you can use the audio and video features of NetMeeting. Users outside the organization cannot, however, establish inbound connections from outside the firewall to computers inside the firewall. Typically, this restriction is due to limitations in the network implementation of the firewall.

> **Note** Some firewalls are capable of accepting only certain protocols and cannot handle TCP connections. For example, if your firewall is a Web proxy server with no generic connection-handling mechanism, you will not be able to use NetMeeting through the firewall.

You can use the following sources to learn more about NetMeeting configuration and firewall topics:

For more information about NetMeeting firewall connections, see Part 2, Chapter 4, "Firewall Configuration," of the *Microsoft NetMeeting 3 Resource Kit*, particularly the section titled, "Establishing a NetMeeting Connection with a Firewall," at:

http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/part2/chapter4.asp

For more information about using NetMeeting and your firewall, see article 158623, "How to Establish NetMeeting Connections through a Firewall," in the Microsoft Knowledge Base at:

http://support.microsoft.com/default.aspx?scid=KB;en-us;158623

Alternate Methods for Controlling NetMeeting

You can create customized installation options for specific users or groups within your organization by using the NetMeeting Resource Kit Wizard. Additionally, you can use the NetMeeting Resource Kit Wizard to control user and computer access rights by creating custom configurations of client settings and specific features that you have selected to restrict or allow. For example, you can control audio and video access, set data throughput limits and network speeds, and choose to display online support. The Resource Kit Wizard can also help you set up various configurations of NetMeeting for different types of users and different levels of security. It can help you save network bandwidth by restricting specific features. You can also use the Resource Kit Wizard to both change registry settings for all NetMeeting users, and to implement such changes globally.

> **Note** By selecting certain options in the Resource Kit Wizard, be aware that you may be changing the NetMeeting user interface. For example, if you click **Restrict the Use of Video**, the Video tab doesn't appear in the NetMeeting user's Options dialog box.

The Resource Kit for NetMeeting has a section that provides detailed information about responding to NetMeeting problems, including problem descriptions, causes, and resolutions. For more information about the *Microsoft NetMeeting 3 Resource Kit*, see the Microsoft Web site at:

http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/nm3dldoc.asp

Procedures for Configuration of NetMeeting

NetMeeting is designed to enhance the enterprise environment and enable users to communicate internally and externally with other NetMeeting users. You can use Group Policy to develop a NetMeeting feature management policy to support the specific business rules or communication policies that exist within your organization. For example, your organization may not want users to be able to access or use the NetMeeting chat feature from their computers. By using Active Directory and Group Policy, you can disable the chat feature from any or all computers that are affected by the application of the Group Policy configuration settings.

For lists of Group Policy settings that you can use to manage NetMeeting configuration options, see "NetMeeting and Group Policy," earlier in this section.

Procedures for managing NetMeeting features through Group Policy

This subsection provides procedures for the following configuration methods:

- Locating the Group Policy objects (GPOs) for NetMeeting configuration settings. These are the settings listed in "NetMeeting and Group Policy," earlier in this section.
- Disabling the NetMeeting remote desktop sharing feature. This prevents users from using this feature.

To locate the Group Policy objects (GPOs) for NetMeeting user configuration settings

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. View the Group Policy objects that are available. For more information about these objects, see "NetMeeting and Group Policy," earlier in this section.

For more information about the GPOs for NetMeeting user configuration settings, see “Configuring NetMeeting settings for users through Group Policy,” earlier in this section.

To disable the NetMeeting remote desktop sharing feature through Group Policy

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **NetMeeting**.
3. In the details pane, double-click **Disable remote Desktop Sharing**.
4. Select **Enabled**.

Note Computer-related Group Policy settings are applied when the operating system starts and during the periodic refresh cycle.

Related Links

You can learn more about NetMeeting from the following online resources:

- For information about technologies and protocols that are built into the Windows Server 2003 family to support applications that enable real-time communications (RTC), see the Real-Time Communications Web page on the Microsoft Web site at:

  http://www.microsoft.com/rtc/

- To view Help for NetMeeting, start NetMeeting by clicking **Start**, clicking **Run**, and typing **conf**. In NetMeeting, on the **Help** menu, click **Help Topics**.

- For more information about using NetMeeting and your firewall, see article 158623, "How to Establish NetMeeting Connections through a Firewall," in the Microsoft Knowledge Base at:

  http://support.microsoft.com/default.aspx?scid=KB;en-us;158623

- For more information about NetMeeting, see Windows NetMeeting on the Microsoft Web site at:

  http://www.microsoft.com/windows/NetMeeting/

- For more information about configuring NetMeeting, see the *Microsoft NetMeeting 3 Resource Kit* on the Microsoft Web site at:

  http://www.microsoft.com/windows/NetMeeting/Corp/ResKit/

- To learn more about NetMeeting features, see the Microsoft Web site at:

  http://www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp

- To view articles that explain how to use some of the features in NetMeeting, see the Microsoft Web site at:

  http://support.microsoft.com/default.aspx?scid=/support/netmeeting/howto/default.asp

- For more information about the H.323 specification, search for “H.323” on the ITU-T Web site at:

  http://www.itu.int/home/index.html

- For more information about the T.120 architecture, see the International Multimedia Teleconferencing Consortium (IMTC) Web site at:

  http://www.imtc.org/

(Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

Printed references

For more information about firewall design, policy, and security considerations for firewall design in general, you can consult the following reference:

- Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly & Associates, Inc., 1995.

Online Device Help

This section provides information about:

- The benefits of Online Device Help
- How Online Device Help communicates with sites on the Internet
- How to control Online Device Help to limit the flow of information to and from the Internet

Benefits and Purposes of Online Device Help

Online Device Help (also known as the "Get help for my hardware device" wizard) delivers targeted content on problems with hardware and peripheral devices installed on the system. This mitigates the need for users to call support professionals to resolve hardware issues. Users interact with Online Device Help in products in the Microsoft Windows Server 2003 family when installing new hardware (through the Found New Hardware Wizard).

At the conclusion of the Found New Hardware Wizard, when the user's system uses a device driver that is not found on the operating system installation CD or is not available through Windows Update, Online Device Help collects anonymous data on the problem device (including a unique hardware identifier for that device) and sends that information over the Internet to a server at Microsoft. If a match for the device is found, content on that device is then downloaded to the user's system and is displayed in the Help and Support Center user interface. This content may include:

- Information from the independent hardware vendor (IHV) about upcoming and planned device support.
- Links to the product compatibility area in Help and Support Center to enable users to search or browse the Windows Catalog Web site for compatible devices. The Windows Catalog Web site is located at:

  http://www.microsoft.com/windows/catalog/server/
- A link to the Web site of the IHV for that device.

The data provided by Online Device Help enables Microsoft to identify the number and system locale of users experiencing hardware problems due to missing drivers and to identify the most common problem devices. Microsoft works with these hardware vendors to provide targeted troubleshooting content on the most common problem hardware devices.

This section of the white paper explains how to control Online Device Help in a managed environment.

Overview: Using Online Device Help in a Managed Environment

Users have control over whether to upload the data required by Online Device Help. In a managed environment, however, it is unlikely that users can choose to install any device; this function would normally be controlled in some fashion by the IT department. You can block Online Device Help at the firewall or through the Services snap-in. The configuration options and procedures for controlling Online Device Help are described later in this section.

How Online Device Help Communicates with Sites on the Internet

If no information for a particular hardware device is found on either the installation CD for the operating system or through Windows Update, users are prompted to release anonymous information about their hardware profile through Online Device Help. This subsection summarizes the communication process:

- **Specific information sent or received**: The following information is collected from the user's computer and uploaded to a server at Microsoft. The user is not uniquely identified.
  - The hardware ID, also known as the PnPID (code that indicates the device manufacturer, device name, and version)
  - The time and date that the data was sent
  - Language code of the operating system, and platform and build information
- **Default and recommended settings**: Online Device Help is enabled by default. Recommended settings are described in the next subsection, "Controlling Online Device Help to Limit the Flow of Information to and from the Internet."
- **Triggers**: Online Device Help is triggered if no information for a particular hardware device is found after the user has completed the Found New Hardware Wizard.
- **User notification**: Users are prompted to send anonymous hardware profile data to a server at Microsoft. If users opt to send this information, the privacy statement is displayed. Users can view the contents of the hardware.xml file being uploaded by clicking a link on the privacy statement page.
- **Logging**: Errors that result from problems installing hardware devices without drivers are logged to the event log.
- **Encryption**: The data transferred to Microsoft is not encrypted.
- **Access**: The raw data uploaded to the server is accessible to operations engineers at Microsoft.com and is used in the Windows Hardware Quality Labs (WHQL) to improve Windows-compatible hardware and drivers.
- **Privacy statement**: Online Device Help is covered by its own privacy statement. The privacy statement (located in a file on the user's computer at *systemroot*\pchealth\helpctr\system\dfs\privacy.htm) is displayed when users opt to send the anonymous hardware profile data to Microsoft.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: You cannot disable Online Device Help directly. Disabling Internet access or HTTP port 80 will, however, block Online Device Help.

Controlling Online Device Help to Limit the Flow of Information to and from the Internet

Users have control over whether to upload anonymous hardware profile information about their system. You cannot, however, disable Online Device Help directly. To block Online Device Help, you can restrict Internet access. You can also use a firewall or configure the Services snap-in. The following table describes the result of each option.

Configuration settings for Online Device Help

Configuration tool	Setting	Result
Firewall	Block HTTP port 80.	Blocks Online Device Help.
Services snap-in	Disable the Upload Manager service (uploadmgr).	Blocks Online Device Help. Any other services that depend on uploadmgr will also fail to start.

How controlling Online Device Help can affect users and applications

If you decide to disable Online Device Help, users will not be prompted to upload anonymous hardware profile information and they will not receive up-to-date, targeted self-help content on hardware issues relating to missing or problem drivers.

Note If you restrict Internet access to block Online Device Help, the feature will queue the data and periodically retry to upload the hardware profile information for some period of time. If an Internet connection becomes available during that period, Online Device Help will upload the queued data. If an Internet connection does not become available, no data will be uploaded. Users will not be impacted in either case.

Alternate Methods for Controlling Online Device Help

You can also control Online Device Help by disabling the Upload Manager service (uploadmgr) that manages synchronous and asynchronous file transfers between clients and servers on the network. Disabling this service will block the upload of the anonymous hardware profile data (although users will still be able to complete the Found New Hardware Wizard). The following subsection gives the procedure for this method.

Procedure for Controlling Online Device Help

You cannot disable Online Device Help directly but can do so indirectly by disabling the Upload Manager service in products in the Windows Server 2003 family.

To disable Online Device Help by disabling the Upload Manager service

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. In the details pane, right-click **Upload Manager**, and then click **Properties**.
4. Click the **Log On** tab, then click the hardware profile that you want to configure, and then click **Disable**.

Important If the Upload Manager service is disabled, any services that explicitly depend on it will fail to start.

Outlook Express 6.0 (Included in Internet Explorer 6.0)

The subsections that follow provide:

- A description of Microsoft Outlook® Express 6.0, which is included in Microsoft Internet Explorer 6.0, and a comparison of Outlook and Outlook Express.
- Descriptions of new security-related features in Outlook Express 6.0 (as compared to Outlook Express 5), with information about how they are configured at the desktop.
- Information about controlling Outlook Express 6.0 through Group Policy to limit the risk associated with e-mail attachments. The Group Policy setting you use for this is **Block attachments that could contain a virus**.

Notes
This section of the white paper describes Outlook Express 6.0, but it does not describe Internet Explorer 6.0 (of which Outlook Express is part), the New Connection Wizard, or the tool that can report errors that occur in Outlook Express. For information about these components, see the respective sections of this white paper (the error reporting tool is described in "Windows Error Reporting").

Also note that the New Connection Wizard replaces the Network Connection Wizard and the Internet Connection Wizard in Windows 2000.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization where users send e-mail, receive e-mail, open attachments in e-mail, and perform similar actions. This section, however, provides information about features and configuration methods in Outlook Express 6.0 that can reduce the inherent risks associated with sending and receiving e-mail.

For more information about Outlook Express, see the following resources:

- Help for Outlook Express (which can be accessed in Outlook Express by clicking the **Help** menu and then selecting an appropriate option).
- The section about Internet Explorer 6.0 in this white paper, which describes security zones in Internet Explorer 6.0. These security zones are also used in Outlook Express 6.0.
- The Internet Explorer page on the Microsoft Web site at:

  http://www.microsoft.com/windows/ie/
- The Resource Kit for Internet Explorer (specifically, the chapter describing what's new in Internet Explorer 6.0). To learn about this and other Resource Kits, see the Windows Deployment and Resource Kits Web site at:

  http://www.microsoft.com/reskit/

Benefits and Purposes of Outlook Express 6.0

Outlook Express 6.0 is designed to make it easy to send or receive e-mail and to browse or participate in newsgroups. It differs from most of the other components described in this white paper in that its main function is to communicate through the Internet or an intranet (in contrast to components that communicate with the Internet in the process of supporting some other activity).

Outlook Express is part of Internet Explorer, in contrast to Microsoft Outlook, which is an application included in Microsoft Office. Outlook provides comprehensive e-mail capabilities, including information management and collaboration capabilities, useful to a wide spectrum of users from home to small business to large enterprise. Outlook Express, included as part of Internet Explorer, offers standard Internet e-mail and news access, useful to many home and small-business users. Outlook Express supports Post Office Protocol 3 (POP3) or Internet Message Access Protocol (IMAP).

Outlook Express 6.0 offers more security-related options and settings than were available in Outlook Express 5, as described in the subsections that follow.

New Security-Related Features in Outlook Express 6.0

Outlook Express 6.0 is the e-mail component in Internet Explorer 6.0. This version of Outlook Express includes the following new security-related features. The table that follows this list shows how each option is configured in Outlook Express.

- **Warning about harmful e-mail**. To prevent e-mail messages from being sent without your knowledge, Outlook Express warns you when other programs, such as viruses or harmful attachments, attempt to send messages from your computer. This warning appears only if Outlook Express is configured as the default simple MAPI client, and another program attempts to use simple MAPI to programmatically send e-mail messages without presenting a visible user interface on the computer.
- **Blocking of potentially harmful attachments**. If this option is enabled, Outlook Express 6.0 blocks the opening or saving of specific e-mail attachments that are considered "unsafe." To determine whether an attachment is unsafe, Outlook Express 6.0 uses the Internet Explorer 6.0 unsafe file list, plus some additional file types, plus file types you configure with the **Confirm open after download** setting in Folder Options (on the Files Types tab). Any e-mail attachment with a file type reported as "unsafe" is blocked. This option can be enabled or disabled through Group Policy as well as at the local computer. For more information about using this setting, see the table that follows and "To locate the Group Policy object (GPO) for blocking e-mail attachments in Outlook Express 6.0," later in this section.

  For information about the unsafe file list in Internet Explorer 6.0, you can search the Microsoft Knowledge Base. To do this, follow the instructions for searching on the Web site, and search for the phrase "unsafe file list":

  http://support.microsoft.com/
- **Software Restriction Policies technology**. When running with an operating system in the Microsoft Windows Server 2003 family, Outlook Express 6.0 takes advantage of Software Restriction Policies technology to run potentially harmful attachments in a sandbox, which is an area in memory outside of which the program cannot make calls. When you attempt to run or save attachments, Software Restriction Policies technology determines whether the file formats are blocked. If so, Outlook Express displays a warning, and the program running the attachment has only limited access to the computer's hard disk and registry.
- **Plain text format option for reading of e-mail**. Starting with Outlook Express 6.0, Outlook Express can be configured to read all e-mail messages in plain text format. Some HTML e-mail messages may not appear correctly in plain text, but no active content in the e-mail message is run when this setting is enabled.

The following table shows how each option is configured in Outlook Express 6.0 .

Options for configuring Outlook Express 6.0

Option to configure in Outlook Express 6.0	Menu to click	Menu item to click	Tab to click
Warning about harmful e-mail	Tools	Options	Security
Blocking of potentially harmful attachments (also configurable through Group Policy)	Tools	Options	Security
Software Restriction Policies technology	Tools	Options	Security
Plain text format option for reading of e-mail	Tools	Options	Read (in Outlook Express 6.0 only)

Overview: Using Outlook Express 6.0 in a Managed Environment

Although there are inherent risks associated with sending and receiving e-mail (and e-mail attachments), you can use several different features and configuration methods in Outlook Express 6.0 to reduce the risks:

- You can use the graphical user interface to configure the security-related features in Outlook Express 6.0. For more information, see "New Security-Related Features in Outlook Express 6.0," earlier in this section and "To start Outlook Express 6.0 and view or configure security settings," later in this section.
- You can use a Group Policy setting, **Block attachments that could contain a virus**, to limit the risk associated with e-mail attachments in Outlook Express 6.0. For more information, see "To locate the Group Policy object (GPO) for blocking e-mail attachments in Outlook Express 6.0," later in this section.

Procedures for Working with Outlook Express 6.0

This subsection provides procedures for the following:

- Opening the dialog box from which you can configure security settings for Outlook Express 6.0.
- Locating the Group Policy setting, **Block attachments that could contain a virus**.

  You can use this Group Policy setting in situations where you want Outlook Express 6.0 to be available but where you want to limit the risk associated with e-mail attachments. For more information about this policy setting, see "New Security-Related Features in Outlook Express 6.0," earlier in this section.

To start Outlook Express 6.0 and view or configure security settings

1. Click **Start**, point to **All Programs** or **Programs**, and then click **Outlook Express**.
2. On the **Tools** menu, click **Options**.
3. Click the **Security** tab and view or configure the settings, including the check boxes for the following two options:
   - **Warn me when other applications try to send mail as me**.
   - **Do not allow attachments to be saved or opened that could potentially be a virus**.

You can also view or configure the security zones setting. Outlook Express 6.0 uses two of the same security zones that you configure in Internet Explorer 6.0. For more information about security zones, see the section about Internet Explorer 6.0 in this white paper.

4. Click the **Read** tab, and view or configure the settings, including the check box for **Read all messages in plain text**.

To locate the Group Policy object (GPO) for blocking e-mail attachments in Outlook Express 6.0

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Internet Explorer**.
3. In the details pane, double-click **Configure Outlook Express**.
4. Select or clear the check box for **Block attachments that could contain a virus**.

Plug and Play

This section provides information about:

- The benefits of Plug and Play
- How Plug and Play communicates with sites on the Internet
- How to control Plug and Play to prevent the flow of information to and from the Internet

Benefits and Purposes of Plug and Play

Windows Plug and Play provides ease of support for installing devices on computers in your network. You can simply plug in a Plug and Play device and the operating system does the rest by installing any necessary drivers, updating the system, and allocating resources. After you install a Plug and Play device, the driver is configured and loaded dynamically, typically without requiring user input.

Plug and Play in the Microsoft Windows Server 2003 family provides the following services:

- Detects a Plug and Play device and determines its hardware resource requirements and device identification number (Plug and Play ID).
- Locates an appropriate device driver for newly installed devices.
- Allocates hardware resources.
- Dynamically loads, initializes, and unloads drivers.
- Notifies other drivers and applications when a new device is available.
- In conjunction with power management, handles stop and start processes for devices during hibernation, standby, and startup and shutdown operations.
- Supports a wide range of device types.

Overview: Using Plug and Play in a Managed Environment

When you install a Plug and Play device, and you are connected to the Internet, the operating system automatically accesses Windows Update to search for a device driver.

> **Note** Some buses, such as Peripheral Component Interconnect (PCI) and universal serial bus (USB), take full advantage of Plug and Play. Older buses, such as Industry Standard Architecture (ISA), do not take full advantage of Plug and Play and require more user interaction to ensure that devices are correctly installed.

In order to install devices using the hardware wizards, you must be logged on as an administrator or a member of the Administrators group. You then use the hardware wizards, such as the Hardware Update Wizard, to search the Windows Update site for device drivers. All drivers obtained through Windows Update are signed by Windows Hardware Quality Labs (WHQL). The WHQL provides compatibility testing services to test hardware and drivers for Windows operating systems.

As an IT administrator in a highly managed network environment, you want to control the ability of administrators to install new hardware and to thereby access the Internet automatically when the operating system searches for device drivers. For a more secure

environment you can control how administrators update and install hardware devices by using Group Policy.

There are also policy settings you can use to disable any access to Windows Update. If you do prevent certain administrators from automatically accessing Windows Update, there is the option for manually downloading the updates from the Windows Update Catalog, whereby they can be distributed on your organization's network as needed.

Using Group Policy to disable automatic updating and access to Windows Update, and to configure driver search locations, is described in the subsection, "Controlling Automatic Device Updating to Prevent the Flow of Information to and from the Internet."

How Plug and Play Communicates with Sites on the Internet

There are two instances when a computer running a product in the Windows Server 2003 family operating system will access the Internet as part of Plug and Play:

- When Plug and Play searches for a driver for newly installed hardware
- When an administrator updates the driver for existing hardware

When you connect a new hardware device and there is no driver available on the computer, the operating system will use the Windows Update service to search for available drivers on the Windows Update site. If an appropriate driver is found on the Windows Update site, the operating system copies it and installs it on your computer. If your computer is not connected to the Internet, a message prompts you to connect to the Internet.

As part of Plug and Play, when the operating system searches for a device driver, interaction with the Internet takes place as follows:

- **Specific information sent or received**: The Code Download Manager (CDM) calls Windows Update to find and download device drivers. The CDM also calls Help and Support Center, which logs Plug and Play IDs for devices that Microsoft does not have drivers for. Neither of these communications is under the direct control of Plug and Play. The CDM handles all of the communication between the computer and Windows Update. None of the communication between the computer and the Internet uniquely identifies the user.
- **Default and recommended settings**: Plug and Play is enabled by default. Recommended settings are presented in the following subsection, "Controlling Automatic Device Updating to Prevent the Flow of Information to and from the Internet."
- **Triggers**: When an administrator adds hardware or updates a driver on a computer, and the computer is connected to the Internet, Windows Update is automatically contacted for driver updates.
- **User notification**: When searching for a device driver Windows Update sends a list of available drivers to the user's computer.
- **Logging**: If you use a Plug and Play driver with a non-Plug and Play device, any associated issues or problems are recorded in the event log.
- **Encryption**: Data transfer is based on interaction with Windows Update. The data is transferred using HTTPS.
- **Transmission protocol and ports**: The transmission protocols and ports are HTTP 80 and HTTPS 443.
- **Ability to disable**: Plug and Play cannot be disabled as system instability would result. You can disable access to Windows Update using Group Policy.

Controlling Automatic Device Updating to Prevent the Flow of Information to and from the Internet

Windows Server 2003 family operating systems will automatically update device drivers using Plug and Play, and they will even search for compatible drivers for non-Plug and Play devices. You therefore might want to exercise various levels of control over administrators' ability to install new hardware and to update hardware devices and drivers.

Using Group Policy there are several levels of control you can configure in order to prevent Plug and Play and associated hardware wizards from accessing the Internet. You can target search locations for drivers, or you can prevent users and computers from automatically accessing the Windows Update Web site in any instance. You can disable automatic updating for some servers and enable it for others, and then have client computers and servers access an intranet server for selected updates.

You can use Group Policy to:

- Control whether Windows Update is included when Plug and Play searches for a device driver.

  This procedure is presented in the next subsection.

- Eliminate automatic update calls to Windows Update.

  Policy settings related to automatic updating are located at Computer Configuration\Administrative Templates\Windows Components\Windows Update.

  If you disable **Configure Automatic Updates**, any updates that are available on the Windows Update Web site must be downloaded and installed manually.

- Remove access to Windows Update.

  The policy setting for Windows Update is located at User Configuration\Administrative Templates\Windows Components\Windows Update.

  When you enable the policy setting **Remove access to use all Windows Update features**, you block access to the Windows Update site from the Windows Update hyperlink on the Start menu and also on the Tools menu in Microsoft Internet Explorer. Automatic updating is also disabled; you will neither be notified about nor will you receive critical updates from Windows Update. This policy setting also prevents Device Manager from automatically installing driver updates from the Windows Update Web site.

  The Windows Update site is located at:

  http://windowsupdate.microsoft.com/

Procedure for Controlling Where Plug and Play Searches for Drivers

When you install new hardware, the operating system automatically searches four different locations for drivers in the following order: the hard drive, the floppy drive, the CD-ROM drive, and Windows Update. The default approach is to search all four locations successively until the correct device driver is found; however, you can configure the driver search locations to remove selected locations.

Included here is the procedure for configuring the Group Policy setting **Configure driver search locations**. For additional procedures to configure policy settings for Windows Update, see the section "Windows Update and Automatic Updates," in this white paper.

To disable Windows Update as a driver search location for Plug and Play devices

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
3. In the details pane, double-click **Configure driver search locations**, and then select **Enabled**.
4. Select **Don't Search Windows Update**.

Related Links

For more information about Windows Update, see the Windows Update Web site at:

http://windowsupdate.microsoft.com/

Program Compatibility Wizard

This section provides information about:

- The benefits of the Program Compatibility Wizard
- How the Program Compatibility Wizard communicates with sites on the Internet
- How to control the Program Compatibility Wizard to prevent the flow of information to the Internet

Benefits and Purposes of the Program Compatibility Wizard

Most programs run properly on products in the Microsoft Windows Server 2003 family. The exceptions are some older games and other programs that were written specifically for an earlier version of Windows.

To enable a better user experience, Microsoft has integrated technologies for application compatibility into the Windows Server 2003 family. Application compatibility technologies are applied whenever an application is installed on the operating system, whether in the course of a system upgrade or during regular operations. Some of these technologies work automatically to apply compatibility fixes, while others can be selected by users or administrators.

This section addresses a component that users and administrators can use, the Program Compatibility Wizard. If you have an application compatibility problem, you can use the wizard to make setting adjustments and to run the application successfully.

Overview: Using the Program Compatibility Wizard in a Managed Environment

IT administrators who want to get an application to work quickly, without addressing compatibility for the application throughout their organization, may choose to use the Program Compatibility Wizard. You can use the wizard to detect and test compatibility settings. If compatibility problems prevent you from installing a program, you can run the Program Compatibility Wizard on the Setup file for the program.

In the Windows Server 2003 family you can access the Program Compatibility Wizard by default through Programs\Accessories or All Programs\Accessories. At the completion of the wizard you are presented with “Program Compatibility Data” that states, “Microsoft has created temporary files that contain information about the settings you selected and whether the problems were fixed. Sending this information to Microsoft will help us improve program compatibility.” You can then choose to send this information to Microsoft or not. You can also choose to click a link to a Web site to view the data collection policy and you can choose to view the temporary files that will be sent. Allowing users or administrators to do this, however, may present a privacy problem for highly managed organizations.

Note As an alternative to running the Program Compatibility Wizard, you can set the compatibility properties manually through the Compatibility tab of a program’s Properties sheet. To do this you right-click the program icon, click **Properties**, click **Compatibility**, and then change the compatibility settings.

Administrators can use Group Policy to disable access to the Program Compatibility Wizard. Alternatively, if you want to allow use of the wizard you can control where data collected by the Program Compatibility Wizard is sent. You can prevent data transfer to the Internet by using Group Policy settings related to error reporting and you can have data from the wizard sent to a server on your intranet instead of to Microsoft. For more information about these procedures, see "Controlling Program Compatibility Wizard Data to Prevent the Flow of Information to the Internet," later in this section.

How the Program Compatibility Wizard Communicates with Sites on the Internet

Although you can control information sent by the Program Compatibility Wizard, it is designed to communicate over the Internet to expedite problem solving. This subsection lists details of the communication process:

- **Specific information sent or received**: The results of the Program Compatibility Wizard data, including settings and problems that were encountered with the application being installed, are sent to Microsoft. The user is not uniquely identified.
- **Default and recommended settings**: Use of the Program Compatibility Wizard is enabled by default. Recommended settings are discussed in the next subsection, "Controlling Program Compatibility Wizard Data to Prevent the Flow of Information to the Internet."
- **Trigger and notification**: In the last dialog box of the wizard, users are asked if they want to send information to Microsoft. Data is not sent automatically.
- **Logging**: There is no information related to the Program Compatibility Wizard entered into the event log.
- **Encryption**: HTTPS is used to perform the data transfer to Microsoft.
- **Access**: The Microsoft product group has access to the raw data only.
- **Privacy statement**: The privacy statement is the same as that associated with Windows Error Reporting (WER) data. A link to the privacy statement on the Web is provided in the wizard.
- **Transmission protocol and port**: The transmission protocol used is HTTPS and the port is 443.
- **Ability to disable**: You can disable the Program Compatibility Wizard by using Group Policy.

For more information about the type of information sent to Microsoft, how the data is used, encryption, and the privacy statement, see the section of this white paper titled "Windows Error Reporting."

Controlling Program Compatibility Wizard Data to Prevent the Flow of Information to the Internet

To control use of the Program Compatibility Wizard you can either disable it or control where information collected by the wizard is sent.

Disabling the wizard

If you want to prevent the use of the Program Compatibility Wizard you can disable it by using Group Policy. In Computer Configuration\Administrative Templates\Windows Components\Application Compatibility, configure **Turn Off Program Compatibility Wizard**. This policy setting does the following:

- When enabled, this policy setting disables the start page of the wizard in Help and Support Center, and in the Start menu.
- These entry points will still exist, but the first page of Help and Support Center will let the user know that this option has been disabled.

Routing the data to an intranet server

Using Group Policy you can configure the **Report Errors** policy setting to prevent data collected by the Program Compatibility Wizard from being sent to Microsoft. By using configuration options within error reporting you can have the data sent to a server on your intranet instead of to Microsoft. When you configure error reporting this way you activate Corporate Error Reporting (CER).

The **Report Errors** policy setting is located in Computer Configuration\Administrative Templates\System\Error Reporting. For more information and procedures for configuring error reporting see the section of this white paper titled “Windows Error Reporting.”

If you use this approach for reporting errors, the user experience with the Program Compatibility Wizard does not change. The dialog box that presents the option of sending data to Microsoft is the same. If the user selects Yes, the data is sent to the designated server on your intranet.

Procedure for Disabling the Program Compatibility Wizard

Use the following procedure to disable the Program Compatibility Wizard. For the procedure to configure error reporting see the section, “Windows Error Reporting.”

To disable the Program Compatibility Wizard

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Application Compatibility**.
3. In the details pane, double-click **Turn Off Program Compatibility Wizard**, and then click **Enabled**.

Remote Assistance

This section provides information about:

- The benefits of Remote Assistance
- How Remote Assistance communicates with sites on the Internet
- How to control Remote Assistance to prevent the flow of information to and from the Internet

Benefits and Purposes of Remote Assistance

With operating systems in the Microsoft Windows Server 2003 family, users and administrators in your organization can use Remote Assistance to get help from a member of your support staff. Users or administrators can also collaborate in other ways through screen sharing. Remote Assistance is a convenient way for support professionals to connect to a computer from another computer running a compatible operating system, such as Windows XP, and to show the users or administrators a solution to their problem.

Using Windows Messenger Service or an e-mail program, such as Microsoft Outlook or Outlook Express, you can provide support to users by connecting to their computer. After you are connected you can view their computer screen, communicate with them in real time about what you both see on their computer, send files, use voice communication, and use your mouse and keyboard to work on their computer.

Overview: Using Remote Assistance in a Managed Environment

Remote Assistance is disabled by default. You configure Remote Assistance through Control Panel\System\Remote tab on an individual computer, or through Group Policy for groups of users or computers. When it is enabled users and administrators can access Remote Assistance through Help and Support Center under Support Tasks\Support, or Support Tasks\Tools\Help and Support Center Tools.

While a firewall on your organization's network will likely prevent outsiders from connecting directly to a computer on your intranet, the potential for users or administrators to connect remotely to someone outside your network is available through Remote Assistance. There is also the option of a support person or IT administrator in your organization offering unsolicited assistance. An administrator in the domain or a user explicitly authorized through Group Policy settings may offer assistance to users in the same domain without being asked; however, users can decline the offer.

As an administrator in a highly managed environment you might want to prevent access for groups of users and administrators to this feature. You can do this through Group Policy. Controlling the use of unsolicited as well as solicited Remote Assistance is described further in the subsection "Controlling Remote Assistance to Prevent the Flow of Information to and from the Internet."

How Remote Assistance Communicates with Sites on the Internet

When a user (referred to as the "novice") initiates a request for assistance through either the e-mail option or the Save invitation as a file option in Remote Assistance, the operating system starts Help and Support Center. Help and Support Center then passes the information to Remote Assistance.

When the person who is being contacted (the "expert") accepts the invitation from the novice, Remote Assistance calls Help and Support Center application programming interfaces (APIs) to initiate the session. Help and Support Center relies on Terminal Services to negotiate the session. Help and Support Center passes the Remote Assistance invitation (the "ticket") file to Terminal Services. The Remote Assistance session is established using RDP (Remote Desktop Protocol) and port 3389 through Terminal Services on the novice and expert computers.

There are safeguards built into the Remote Assistance feature. All sessions are encrypted and can be password-protected. The novice (user soliciting the assistance) sets the maximum time for the duration of the ticket. Also, firewalls on your organization's network might prevent users from making a connection.

The following information presents additional details on how information transfer over the Internet takes place when a connection is made:

- **Specific information sent or received**: Information that is transmitted in a Remote Assistance ticket includes user name, IP address, and computer name. Information necessary to provide functionality for Remote Assistance (for example, screen sharing, file transfer, and voice) is sent in real time using point-to-point connections.
- **Default and recommended settings**: Anyone with access to Help and Support Center can access the Remote Assistance feature. Users can prevent someone from connecting to their computer by declining an invitation. You can also prevent someone from remotely controlling a server running one of the Windows Server 2003 family operating systems through Control Panel settings or Group Policy.
- **Triggers**: A user or administrator establishes contact with the expert by sending an invitation through e-mail, instant messaging, or by saving an invitation as a file and transferring it manually, such as on a floppy disk, to the expert. Or, an expert offers unsolicited assistance to a user.
- **User notification**: The expert is asked through e-mail or instant messaging to provide help to the novice. A connection is not made unless the expert accepts the invitation or opens the ticket. When users are offered unsolicited assistance, they as the novice have to click Yes to start a connection.
- **Logging**: Events such as a person initiating a connection or a user or administrator accepting or rejecting an invitation are recorded in the event logs.
- **Encryption**: The RDP (Remote Desktop Protocol) encryption algorithm for the main Remote Assistance communication and the RTC (Real-Time Communication) encryption algorithm for voice are used. The RDP encryption algorithm is RC4 128-bit.
- **Access**: No information is stored at Microsoft.
- **Transmission protocol and port**: The port is 3389 and the transmission protocols are RDP and RTC.
- **Ability to disable**: Yes, using Group Policy, and locally through Control Panel.
- **Firewall protection**: Any firewall that blocks port 3389 should not allow a connection to users outside the firewall. This does not prevent users from within the network protected by the firewall from connecting to each other. If you close port 3389, you will block all Remote Desktop and Terminal Services events through it as well. If you want to allow these services but want to limit Remote Assistance requests, use Group Policy. If the port is opened only for outbound traffic, a user can request Remote Assistance by using Windows Messenger.

For more information about the Remote Assistance connection process, see article 300692, "Description of the Remote Assistance Connection Process," in the Microsoft Knowledge Base at:

http://support.microsoft.com/default.aspx?scid=kb;en-us;300692

Controlling Remote Assistance to Prevent the Flow of Information to and from the Internet

Administrators can control the use of Remote Assistance in the following ways:

- Group Policy to disable users or administrators from soliciting or offering Remote Assistance
- Local controls of Remote Assistance through Control Panel

Group Policy settings are described in detail in this subsection. Procedures for disabling Remote Assistance are presented in the next subsection.

There are two Group Policy settings you can configure to control the use of Remote Assistance:

- **Solicited Remote Assistance**

  Use this policy setting to determine whether or not solicited remote assistance is allowed from a computer. In **Solicited Remote Assistance** the user of a computer explicitly requests help from another party.

- **Offer Remote Assistance**

  Use this policy setting to determine whether a support person or IT administrator (expert) can offer remote assistance to a computer without a user explicitly requesting it first, through e-mail, a file, or instant messaging.

These policy settings are located in Computer Configuration\Administrative Templates\System\Remote Assistance. Configuration options for these policy settings are described in the following table.

Group Policy settings for controlling Remote Assistance

Policy setting	Description
Solicited Remote Assistance (enabled)	When this policy setting is enabled, a user can create a Remote Assistance invitation that a person (“expert”) can use at another computer to connect to the user’s computer. If given permission, the expert can view the user’s screen, mouse, and keyboard activity in real time. Additional configuration options are available when you enable this policy setting.
Solicited Remote Assistance (disabled)	If the status is set to Disabled, users cannot request Remote Assistance and this computer cannot be controlled from another computer. If this policy setting is disabled, the **Offer Remote Assistance** policy setting is also disabled.
Solicited Remote Assistance (not configured)	If the status is set to Not Configured, all additional configuration is determined by the Control Panel settings.
Offer Remote Assistance (enabled)	When this policy setting is enabled, a remote user or administrator can offer Remote Assistance to the computer.

	When you configure this policy setting, you have two choices: you can select either "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." In addition to making this selection, when you configure this policy setting you also specify the list of users or user groups that will be allowed to offer remote assistance. Administrators can offer remote assistance by default; they do not need to be added to the list.
Offer Remote Assistance (disabled or not configured)	If you disable or do not configure this policy setting, users or groups cannot offer unsolicited remote assistance to this computer.

For additional configuration options see the Remote Assistance policy settings in Group Policy. To find more information about editing Group Policy, see Appendix B, "Resources for Learning About Group Policy."

Procedures for Disabling Remote Assistance

This subsection presents procedures administrators can use for disabling Remote Assistance through Group Policy or Control Panel.

To disable the use of Remote Assistance using Group Policy

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, and then click **Remote Assistance**.
3. In the details pane, double-click **Solicited Remote Assistance,** and then select **Disabled**.

Note When you disable this policy setting, **Offer Remote Assistance** is also disabled.

To disable the use of Remote Assistance through Control Panel

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **System**.
3. In System Properties, click the **Remote** tab.
4. Under Remote Assistance, clear the check box labeled **Turn on Remote Assistance and allow invitations to be sent from this computer**.

Search Companion

This section provides information about:

- The benefits of Search Companion
- How Search Companion communicates with sites on the Internet
- How to control Search Companion to prevent the flow of information to and from the Internet

Benefits and Purposes of Search Companion

The Microsoft Search Companion Web service enables users to search for files and folders on their desktop computer, to search for files, people, and other computers on their internal network, and to search for information on the Internet. Search Companion uses Indexing Service to maintain an index of all the files on users' computers, making searches faster.

When employing Search Companion, users can specify several search criteria. For example, they can search for files and folders by name, type, or size. They can find files based on when they were last modified, or search for files containing specific text. When searching for information on the Internet, Search Companion enables users to enter search queries in natural language (meaning informal, or conversational language). It then suggests the best way to conduct the search, and sends the query to Internet services that are most likely to yield positive results.

Overview: Using Search Companion in a Managed Environment

When the user searches the Internet using Search Companion, the following information is collected:

- The text of the Internet search query
- Grammatical information about the query
- The list of tasks (suggestions) that the Search Companion Web service recommends to refine the search
- Any tasks the user selected from the recommendation list

Search Companion does not collect:

- Personal information
- Demographic information

Microsoft does not use the information it collects to identify the user individually and does not use such information in conjunction with other data sources that may contain personal data. Microsoft does not collect information when the user searches on the local system, LAN, or intranet.

The Search Companion Web service is designed to upgrade automatically as new features become available. It therefore uses the Internet connection periodically to check for and replace necessary files.

If you want to disable the Search Companion Web service, you can do so by changing to Classic Search for the Internet. Microsoft Windows does not collect any query information when Classic Search is used. You can also disable Search Companion by modifying the registry settings. The procedures for both of these methods are described later in this section of the white paper.

How Search Companion Communicates with Sites on the Internet

Search Companion in Microsoft Windows Server 2003 family operating systems improves the search process by consolidating search tasks, optimizing searches for the most common scenarios, and offering suggestions for refining the search.

The form the user creates to collect search criteria will post information to an ASP page that displays the search results. The search pages use a combination of XML and Microsoft Visual Basic® development system, Scripting Edition (VBScript) and Microsoft JScript® development software for accessing the search objects. Because the script is run on the server, users can view the search pages from any browser.

Search Companion uses XML files to define both the user interface (UI) and some functional parameters of its tasks (for example, what list of file extensions constitutes the "Music" category of files). The first time in each Search Companion session that an XML file is referenced, Search Companion checks to see if a later version of that XML file is available from sa.windows.com. The "check" is really a file download request, conditioned on the modified date of the file. If there is a later version of the XML file, Search Companion downloads it and replaces the earlier version. The XML files are located in a language-specific subfolder of *systemroot*\srchasst\, and if the current user does not have administrative credentials, the old XML file cannot be overwritten.

This subsection describes various aspects of the data that is sent to and from the Internet through Search Companion, and how the exchange of information takes place:

- **Specific information sent or received**: When you search the Internet using Search Companion, the following information is collected regarding your use of the service: the text of your Internet search query, grammatical information about the query, the list of tasks that the Search Companion Web service recommends, and any tasks you select from the recommendation list.
- **Default and recommended settings**: Search Companion is enabled by default.
- **Triggers**: The user selects Start\Search and uses search options to search the Internet.
- **User notification**: There is no provision in Search Companion for user review or notification of data sent.
- **Uniquely identify users**: The user is not uniquely identified. Session-based cookies are used to maintain state information, but these randomly assigned GUIDs do not persist across browser sessions.
- **Logging**: No information is collected when you search your local system, LAN, or intranet. The only "storage" is the Internet Information Services (IIS) log of the file request on the server at Microsoft that provides the Search Companion Web service. Search Companion does not record your choice of Internet search engines, and it does not collect or request any personal or demographic information.
- **Encryption**: There is no encryption of data.
- **Access**: No user information is collected. The IIS logs (described in the "Logging" item, earlier in this list) are cycled annually, that is, logs are retained for twelve months, and discarded in the thirteenth month following collection.

- **Privacy statement**: The privacy statement is located on the following Web site at: http://sa.windows.com/privacy/
- **Transmission protocol and port**: The transmission protocol is HTTP and the port is 80.
- **Ability to disable**: The feature can be disabled by changing to Classic Search.

Controlling Search Companion to Prevent the Flow of Information to and from the Internet

You can disable the Search Companion Web service by changing preferences to Classic Search for the Internet. You can also disable Search Companion by changing the registry settings manually. Procedures for both of these approaches are provided in the following subsection.

Procedures for Configuration of Search Companion

Search Companion can be configured in several ways as described previously. This subsection lists the procedures to change or disable the features in accordance with your organization's security policies.

To change to Classic Search for the Internet

1. Click **Start**, and then either click **Search**, or point to **Search** and click **On the Internet**.
2. Click **Change preferences**.
3. Click **Change Internet search behavior**.
4. Click **With classic Internet search**.

To disable Search Companion through the registry key

1. Close Internet Explorer (all instances).
2. Open Registry Editor by clicking **Start**, clicking **Run**, and then typing **regedit**.

   Caution Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on the computer. You can also use the Last Known Good Configuration startup option if you encounter problems after manual changes have been applied.

3. Navigate to HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState
4. On the **Edit** menu, point to **New**, and then click **String value**.
5. Type **Use Search Asst** as the name for the new value (the type is REG_SZ), and then press ENTER.
6. Click the new entry (**Use Search Asst**), and then on the **Edit** menu, click **Modify**.
7. For **Value data**, type:

   no

   Note Type the entry and value exactly as shown, including spaces and capitalization.

Terminal Server Licensing

This section provides information about:

- The purposes of Terminal Server Licensing
- How Terminal Server Licensing communicates with sites on the Internet
- How to control Terminal Server Licensing to limit the flow of information to and from the Internet

> **Note** In operating systems in the Microsoft Windows Server 2003 family, several components that use technology related to Terminal Server have different names than they had in Windows 2000. Terminal Server was previously known as Terminal Services in Application Server mode. Remote Desktop for Administration was previously known as Terminal Services in Remote Administration mode.

Purposes of Terminal Server Licensing

Terminal Server Licensing is an administrative tool that helps manage your Terminal Server licenses. Terminal Server Licensing can be installed on Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition. If you install Terminal Server, you must also install Terminal Server Licensing (although not necessarily on the same computer). However, there is a grace period of 120 days during which you can use Terminal Server even though you have not set up license servers yet and have not installed client license key packs.

> **Note** Terminal Server and Terminal Server Licensing are not available in Windows Server 2003, Web Edition. Remote Desktop for Administration, however, is available in Windows Server 2003, Web Edition.

When you set up Terminal Server on a server, users can access applications running on that server, which means they can run the applications you provide even if they are working from hardware that might not otherwise support the applications.

Microsoft has introduced new licensing options to address business customer needs and to complement the technical capabilities of the Windows Server 2003 family of products. For details about these changes, see the Windows Server 2003 licensing overview at:

http://www.microsoft.com/windowsserver2003/howtobuy/licensing/overview.mspx

Overview: Using Terminal Server Licensing in a Managed Environment

You can control the communication that occurs between the Terminal Server Licensing component and sites on the Internet by choosing the server or servers on which to install the Terminal Server Licensing component, and by choosing among three methods for activation. (You also choose among the same three activation methods for obtaining client license key packs, which are digital representations of a group of client access licenses.) The three methods for activation are as follows:

- **Automatic**. This method requires the server running Terminal Server Licensing to have an Internet connection.

- **Web Browser**. This method requires an Internet connection, but the connection can be made from any computer, not just the computer that is running Terminal Server Licensing.

- **Telephone**. This method is used to contact the nearest Customer Support Center and receive an ID number to activate the Terminal Server License Server by phone.

For more details on these methods, see the subsections that follow.

How Terminal Server Licensing Communicates with Sites on the Internet

A server running the Terminal Server Licensing component communicates with the Microsoft Clearinghouse (a database for managing licensing) on the Internet only when you activate Terminal Server Licensing or when you initiate subsequent transactions with Microsoft to obtain client license key packs. The following list describes the communication that occurs when you activate or obtain client license key packs directly over the Internet or when you connect to the Microsoft Clearinghouse from a computer other than the one where Terminal Server Licensing is installed.

> **Note** The information in the following list applies only to activation or obtaining client license key packs over the Internet. It does not apply when you activate by phone.
>
> Activation by phone is done as follows: When you activate by phone, you start the licensing wizard, choose a country or region from the list that is displayed, and call the number shown.

The rest of this subsection describes various aspects of the data that is sent to and from the Internet from Terminal Server Licensing and how the exchange of information takes place.

- **Specific information sent or received**: The information sent to the Microsoft Clearinghouse includes company name, first and last name of the user, license server name, and license server ID. Client license key packs are returned to the Terminal Server License Server.

- **Default and recommended settings**: Terminal Server Licensing is not installed by default.

- **User notification and triggers**: The administrator triggers activating, obtaining client license packs, or deactivating Terminal Server Licensing by performing the steps described in the subsection “Procedures for Configuration of Terminal Server Licensing.” When the Terminal Server Licensing component starts, the administrator is notified that activating, obtaining client license packs, or deactivating will initiate communication with Microsoft.

- **Logging**: Terminal Server Licensing logs events in the system log. The events can be viewed through Event Viewer.

- **Encryption**: Terminal Server Licensing uses the HTTP protocol over SSL (Secure Sockets Layer) to communicate on the Internet and the Web.

- **Access**: The Microsoft Clearinghouse is the database Microsoft maintains to activate license servers and to issue client license key packs. Microsoft customer service representatives have access to the licensing information and are able to successfully re-create the information on your Terminal Server License Server if technical problems occur. The information you provide might also be used internally at Microsoft to perform aggregate quality testing of the Terminal Server Licensing program.

- **Privacy statement**: To see the privacy statement for Terminal Server Licensing, from the Terminal Services Licensing Web site, click **Microsoft's Terminal Server Licensing privacy policy** at:

  https://activate.microsoft.com/prpolicy.asp

- **Transmission protocol and port**: HTTPS over port 443, and remote procedure call (RPC) over port 135.

- **Ability to disable**: Terminal Server Licensing is not installed by default. Once installed, however, it can be disabled by the procedures described later in this section.

External Connector license

In place of individual Terminal Server client access licenses (TS CALs), you have the option of purchasing the Terminal Server External Connector license. This license enables external users to access a company's terminal servers without the need to purchase individual TS CALS for them or their devices. Generally speaking, an external user is a person who is not an employee or similar personnel of a company or its affiliates, and who is not a customer of hosted services (for specific information, see the External Connector license).

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running servers that communicate with the Internet. For more information about security and the Internet, see the introduction to this white paper, or see the Microsoft TechNet Web site at:

http://www.microsoft.com/technet/security/

Controlling Terminal Server Licensing to Limit the Flow of Information to and from the Internet

You can control the communication that occurs between the Terminal Server Licensing component and sites on the Internet in the following ways:

- **Install the Terminal Server Licensing component on selected servers only**. This follows the basic principle of stopping unnecessary services and keeping computers (especially servers) free of unnecessary software. For information about choosing which computer or computers on which to install Terminal Server Licensing, see the *Microsoft Windows Server 2003 Deployment Kit*, which is available on the Microsoft Web site at:

  http://www.microsoft.com/reskit/

  When searching in documentation about Terminal Server Licensing, use the phrases "domain license server" and "enterprise license server" to discover information about these two options.

- **Review the method you want to use for activating Terminal Server Licensing before starting the licensing wizard**. Automatic activation is the fastest method, but if you prefer, you can activate by the other methods mentioned previously (connecting to a Web site from a computer other than the one where Terminal Server Licensing is installed, or activating by phone).

  You are required to activate a license server before it can issue licenses to Terminal Server clients. You are required to activate a license server only once. When you activate the license server, Microsoft provides the server with a limited-use digital certificate that validates server ownership and identity. Microsoft uses the X.509 industry standard

certificate for this purpose. Using this certificate, a license server can make subsequent transactions with Microsoft and receive client license key packs.

Procedures for Configuration of Terminal Server Licensing

Terminal Server Licensing servers can be configured in several ways as described previously. This subsection provides procedures for:

- Installing and uninstalling Terminal Server Licensing
- Activating Terminal Server Licensing
- Deactivating Terminal Server Licensing
- Viewing Help for Terminal Server and Terminal Server Licensing

To install or uninstall Terminal Server Licensing

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Select **Terminal Server Licensing**, and do one of the following:
   - If Terminal Server Licensing is installed and you want to remove it, clear the check box for **Terminal Server Licensing** and complete the licensing wizard.
   - If Terminal Server Licensing is not installed and you want to add it, select the check box for **Terminal Server Licensing** and then click **Next**.
5. In Terminal Server Licensing setup, do one of the following:
   - If your network includes several domains, click **Your entire enterprise**, and then provide the database location. An enterprise license server can serve terminal servers on any Windows Server 2003 family domain.
   - If you want to maintain a separate license server for each domain, or if your network includes workgroups or Windows NT 4.0 domains, click **Your domain or workgroup**, and then provide the database location.

To activate a license server

As mentioned previously in this section, you must activate a Terminal Server License Server before it can issue licenses to Terminal Server clients. Use Terminal Server Licensing to activate a Terminal Server License Server through the Microsoft Clearinghouse.

You can find procedure checklists along with complete instructions for configuring and activating Terminal Server License Servers in Help and Support Center. For more detailed instructions, see the procedure below titled, “To view Help for Terminal Server and Terminal Server Licensing” and "To view Help topics specific to Terminal Server Licensing."

Deactivating a license server

If Terminal Server and Terminal Server Licensing are already installed and you want to deactivate the license server, use one of the following procedures. You might need to deactivate a license server when the certificate of the server has expired, when the server becomes corrupted, or when the server is being redeployed. Note that when a license server's registration has expired, you are prompted to reactive the license server (not deactivate it). When you deactivate a license server, you will not be able to license additional clients from this server until the license server is reactivated.

To deactivate a license using the automatic method

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Terminal Server Licensing**.
3. In the console tree, right-click the license server you want to deactivate, point to **Advanced**, and then click **Deactivate Server**. The licensing wizard starts.
4. In **Information Needed**, confirm that your name, phone number (optional), and e-mail address (required if you are using the Internet method) are correct, and then click **Next**.
5. Your request to deactivate the license server is sent to Microsoft where it is processed.

   Note The information sent to the Microsoft Clearinghouse during deactivation is the same information sent during activation, which includes company name, first and last name of the user, license server name, and license server ID.

6. Click **Finish**.

To deactivate a license using the telephone method

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Terminal Server Licensing**.
3. In the console tree, right-click the Terminal Server License Server you want to deactivate, point to **Advanced**, and then click **Deactivate Server**. The Terminal Server License Server Wizard starts.
4. Select **Telephone** and then click **Next**.
5. Specify your location and then click **Next**.
6. Call the telephone number displayed in the wizard, and give the customer support representative the product ID that is displayed below the telephone number.
7. Type the 35-digit confirmation code provided by the customer support representative in the boxes in the wizard, and then click **Next**.
8. Click **Finish**.

   Notes
   Deactivating a license server does not remove the component. As mentioned previously, follow the basic principle of stopping unnecessary services and keeping computers (especially servers) free from unnecessary software by removing the Terminal Server Licensing component if you no longer plan to use it as a license server.

   You cannot deactivate a license server using either the fax or Internet connection methods.

To view Help for Terminal Server and Terminal Server Licensing

1. Click **Start** and then click **Help and Support**.
2. Click **Software Deployment** and then expand **Terminal Services**.

To view Help topics specific to Terminal Server Licensing

1. Click **Start** and then click **Help and Support**.
2. Click **Software Deployment** and then expand **Terminal Services**.
3. Expand **Terminal Server** and then expand **Checklists: Setting up Terminal Server**.

   When you are finished viewing appropriate checklists, collapse the items you were viewing.
4. Expand **Terminal Server Licensing**.
5. To get information about the following procedures, expand **How To**:
   - Install Terminal Server Licensing
   - Activate Terminal Server Licensing server
   - Install client license key packs
   - Deactivate a Terminal Server Licensing server
   - Reactivate a Terminal Server Licensing server
   - Repeat the installation of a client license key pack
   - Connect to a Terminal Server Licensing server
   - Change Terminal Server Licensing server properties

Related Links

- For details about new licensing options for the Windows Server 2003 family, as well as information about the licenses necessary with Terminal Server, see the Windows Server 2003 licensing overview at:

  http://www.microsoft.com/windowsserver2003/howtobuy/licensing/overview.mspx
- For descriptions of other ways you can use Terminal Server, see the Terminal Server overviews on the Microsoft Web site at:

  http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx
- For information about controlling the issuance of Terminal Server licenses, see the topic, “To control the issuance of Terminal Server licenses,” in Help and Support Center. For details about viewing Help and Support Center topics, see “To view Help for Terminal Server and Terminal Server Licensing,” earlier in this section.

Windows Error Reporting

This section provides information about:

- The benefits of Windows Error Reporting
- How Windows Error Reporting communicates with sites on the Internet
- How to control Windows Error Reporting to prevent the flow of information to and from the Internet

Benefits and Purposes of Windows Error Reporting

The Windows Error Reporting feature in Microsoft Windows Server 2003 family operating systems provides a service which allows Microsoft to track and address errors relating to the operating system, Windows components, and applications. This service, called the Error Reporting service, gives administrators and users with administrative credentials the opportunity to send data about errors to Microsoft and to receive information about them. Moreover, developers can use the Error Reporting service as a problem-solving tool to address customer problems in a timely manner and to improve the quality of Microsoft products.

In addition to having users or administrators send information to Microsoft, in some cases Microsoft may provide information, such as a way to work around a problem or a link to a Web site for updated drivers, patches, or Microsoft Knowledge Base articles.

Overview: Using Windows Error Reporting in a Managed Environment

In Windows Server 2003 family operating systems, error reporting is enabled by default and you can report system and application errors to Microsoft if you choose to. When an error occurs, a dialog box is displayed, giving you the option to report the problem. If you choose to report the problem, technical information about it is collected and then sent to Microsoft over the Internet. No information is sent unless you confirm that the error report be sent to Microsoft.

On Windows Server 2003 family operating systems you can configure or disable error reporting through the Control Panel\System\Advanced tab. You can configure error reporting to send specified information such as system errors only, unplanned shutdowns, or errors for Windows components, such as Windows Explorer, Paint, or Microsoft Internet Explorer. You can also send information for applications, such as Microsoft Word. An operating system error causes the computer to display a Stop error screen with error values. An application or component error causes the application or component to stop working.

The default settings for the Windows Server 2003 family are:

- Enable error reporting for the operating system, unplanned computer shutdowns, and applications.

  For application errors, you can configure error reporting in one of two ways: either have the error reporting dialog box appear as soon as an error occurs for any user, or do not have the dialog box appear until the next time an administrator logs on.

  Windows treats operating system errors and unplanned shutdowns differently from the way it treats application errors. If an operating system error or unplanned shutdown

occurs, Windows writes the error information to a log file. The next time an administrator logs on, the error reporting dialog box prompts them to report the error.

- Force queue mode for application errors.

  The queued mode displays the last ten errors the next time the administrator logs on to the computer. Each error is displayed in its own window so the administrator can choose the errors to report to Microsoft. In this mode errors are displayed only to an administrator; if users logged on to the server they would not see the errors.

Since error reporting is a valuable service, we do not recommend that IT administrators disable it, but that they control what information is reported and where it is sent. For an organization where privacy is a concern, we recommend that the IT department review and filter error reports before they are sent to Microsoft. The best method to use to prevent the automatic flow of error reporting information to and from the Internet is to redirect error reports to a server on your intranet by using Group Policy and to set up Corporate Error Reporting (CER). You can configure error reporting to control various aspects of how errors are reported.

IT administrators can use the Corporate Error Reporting tool to manage error reports that have been redirected to a network server. You use the tool to review the redirected error reports and then filter the reports that are sent to Microsoft based on your policies and the data contained within the error report. The tool is also useful for determining the types of problems users are experiencing most often.

If you have not yet deployed the operating system, you can use unattended installation files to configure error reporting in the same way as in Group Policy. If it is necessary in your organization to completely disable Windows Error Reporting you can do so with the unattended installation file or with Group Policy. For more information about these methods, see "Controlling Error Reporting to Prevent the Flow of Information to and from the Internet," later in this section.

How Windows Error Reporting Communicates with Sites on the Internet

The data that Microsoft collects is used strictly for the purpose of tracking down and solving problems that users or administrators are experiencing. The information is stored in a secure database with limited access. This subsection describes various aspects of the data that is sent to and from the Internet during error reporting, and how the exchange of information takes place.

- **Specific information sent or received**: Microsoft collects various types of information related to two types of errors, user mode or application errors, and kernel mode or operating system failures. Some information that uniquely identifies the user might inadvertently be collected as part of the crash report. This information, if present, is never used to contact a user. The specific data collected is described later in this subsection. Also, Microsoft may send information about a problem, including links to Web sites.
- **Default and recommended settings**: Error reporting for application and system errors is enabled by default. For more information about recommended settings, see "Controlling Error Reporting to Prevent the Flow of Information to and from the Internet," later in this section.
- **Triggers**: The opportunity to send an error report is triggered by application or system errors.
- **User notification**: A dialog box appears notifying users that an error has occurred and asks if they want to send an error report to Microsoft. Users can review the data that will be sent.

- **Logging**: Descriptions of system and application errors are recorded in the event log.
- **Encryption**: All data that could include personally identifiable information is encrypted (HTTPS) during transmission. The "crash signature," which includes such information as the application name and version, module name and version, and offset (location) is not encrypted.
- **Access**: Microsoft employees and contingent staff who have submitted a business justification for reviewing the information are granted access to the data.
- **Privacy statement**: The privacy statement for Microsoft Error Reporting is located at the following Web site:

  http://watson.microsoft.com/dw/1033/dcp.asp

  Details related to privacy of data are presented in "Types of data collected," later in this section.
- **Transmission protocol and port**: The transmission protocol is HTTP and the ports are HTTP 80 and HTTPS 443.
- **Ability to disable**: The feature can be disabled through Group Policy or by administrators on individual servers.

Types of errors reported

There are two types of errors that are reported, user mode and kernel mode.

User mode reporting

When a user mode error occurs, such as an application error, the Error Reporting service does the following:

- Displays an alert stating that the operating system detected a problem.

  Users can choose to report the problem or not. If they do report it, they will see that the information is being sent to Microsoft.
- Sends a problem report to Microsoft.

  Users may then be queried for additional computer information and again may choose to send it or not. If they choose to do so, the Error Reporting service sends the error report to Microsoft. Users might be prompted to provide additional information to complete the error report. When the process is complete, users have the option of selecting More Information, which directs them to updated drivers, patches, or Microsoft Knowledge Base articles.

If the error report indicates that one or more non-Microsoft products were involved in causing the problem, Microsoft may send the report to the respective companies. Qualified software or hardware developers (employed by Microsoft or one of its partners) will analyze the fault data and try to identify and correct the problem.

Kernel mode reporting

When a kernel mode or system error occurs, Windows displays a Stop message and writes diagnostic information to a memory dump file. When you restart your computer using normal mode or Safe Mode (with networking) and log on to Windows, the Error Reporting service gathers information about the problem and displays a dialog box that gives you the option of sending a report to Microsoft.

Types of data collected

The Error Reporting service collects Internet Protocol (IP) addresses, which are not used to identify users. It does not intentionally collect anyone's name, address, e-mail address, computer name, or any other form of personally identifiable information. It is possible that such information may be captured in memory or in the data collected from open files, but Microsoft does not use it to identify users.

In rare cases, such as problems that are especially difficult to solve, Microsoft may request additional data, including sections of memory (which may include memory shared by any or all applications running at the time the problem occurred), some registry settings, and one or more files from the user's computer. The user's current documents may also be included. When additional data is requested, the user can review the data and choose to send the information or not.

The specific type of data that is collected when application errors or kernel failures occur is as follows.

Application errors

If you have an application error the Error Reporting service collects the following information:

- The Digital Product ID, which can be used to identify your license.
- Information regarding the condition of the computer and the application at the time the error occurred. This includes data stored in memory and stacks, information about files in the application's directory, as well as the operating system version and the computer hardware in use. This information is packaged into what is called a "minidump." The minidump contains the following:
    - Exception information: This is information regarding the problem that occurred; it tells Microsoft what kind of instruction the application received that caused it to generate an error.
    - System information: This is data about the kind of CPU (processor) you have and what operating system you are running.
    - A list of all the modules that are currently loaded and their version information.
    - A list of all the threads that are currently running. For each thread, the current context and the whole stack are collected.
    - Global data.

    The minidump data is shown as a hexadecimal representation that the user cannot read.

Note For the exact specification of the minidump format, see the Microsoft Platform SDK, which is available on the Microsoft Developers Network (MSDN) Web site.

Windows kernel failures

Windows kernel fault reports contain information about what your operating system was doing when the problem occurred. These event reports contain the minimum information that can help to identify why the operating system stopped unexpectedly. The report includes:

- The operating system name (for example, Microsoft Windows 2000).
- The operating system version (for example, 5.1.2426 0.0).

- The operating system language as represented by the locale identifier (LCID) (for example, 1033 for United States English). This is a standard international numeric abbreviation.
- The loaded and recently unloaded drivers. These identify the modules used by the kernel when the Stop error occurred, and the modules that were used recently.
- The list of drivers in the Drivers folder on your hard disk, that is, *systemroot*\System32\Drivers.
- The file size, date created, version, manufacturer, and full product name for each driver.
- The number of available processors.
- The amount of random access memory (RAM).
- The time stamp that indicates when the Stop error occurred.
- The messages and parameters that describe the Stop error.
- The processor context for the process that stopped. This includes the processor, hardware state, performance counters, multiprocessor packet information, deferred procedure call information, and interrupts (requests from software or devices for processor attention).
- The process information and kernel context for the halted process. This includes the offset (location) of the directory table and the database that maintains the information about every physical page (block of memory) in the operating system.
- The process information and kernel context for the thread that stopped. This information identifies registers (data-storage blocks of memory in the processor) and interrupt request levels, and includes pointers to data structures for operating system data.
- The kernel-mode call stack for the interrupted thread. This is a data structure that consists of a series of memory locations and includes a pointer to the initial location.

Controlling Error Reporting to Prevent the Flow of Information to and from the Internet

To prevent the automatic flow of information to and from the Internet when users and administrators report errors, you can configure error reporting in two ways: while deploying the operating system using answer files with unattended or remote installation, or after deployment using Group Policy. There may be some aspects of error reporting you want to configure using answer files, and others you may want to configure using Group Policy. Review the tables in this subsection to determine the configuration options that will work best for your organization.

Using unattended installation

You can configure error reporting by using standard methods for unattended or remote installation. You use the [PCHealth] section of an answer file to make entries for this feature. The following table describes those entries.

Entries for configuring error reporting in an answer file (for unattended installation)

Entry	Description
ER_Display_UI	Specifies whether Setup notifies the user that an error has occurred and shows details about the error. When the entry is **ER_Display_UI = 0**, Setup does not notify the user that an error has

	occurred.
ER_Enable_Applications ER_Include_EXE(*n*) and ER_Exclude_EXE(*n*)	**ER_Enable_Applications = All** Reports errors for all applications except for those listed in ER_Exclude_EXE(*n*). **ER_Enable_Applications = Listed** Reports errors only for those applications listed in ER_Include_EXE(*n*). You can automatically include Microsoft applications by using ER_Include_MSApps. **ER_Enable_Applications = None** Reports no application errors. Examples of entries that list included applications are: **ER_Include_EXE1 = iexplore.exe** **ER_Include_EXE2 = explorer.exe** Examples of entries that list excluded applications are: **ER_Exclude_EXE1 = calc.exe** **ER_Exclude_EXE2 = notepad.exe**
ER_Enable_Kernel Errors	Specifies whether Windows reports errors in the Windows kernel. When the entry is **ER_Enable_Kernel Errors = 0**, Windows does not report errors in the Windows kernel.
ER_Enable_Reporting	Specifies whether Windows automatically reports errors. When the entry is **ER_Enable_Reporting = 0**, Windows does not report errors.
ER_Enable_Windows_ Components	Specifies whether to report errors in Windows components. When the entry is **ER_Enable_Windows_Components = 0**, Windows does not report errors in Windows components. To exclude individual Windows components, use ER_Exclude_EXE(*n*), as described earlier in this table.
ER_Force_Queue_Mode	Specifies whether to send all reports in queue mode. When the entry is **ER_Force_Queue_Mode = 0**, Windows does not send reports in queue mode.
ER_Include_MSApps	Specifies whether to track and report errors in Microsoft applications. When the entry is **ER_Include_MSApps = 0**, errors in Microsoft applications are not tracked and reported.
ER_Include_Shutdown_ Errs	Specifies whether to report shutdown errors. When the entry is **ER_Include_Shutdown_Errs = 0**, shutdown errors are not reported.

For complete details about the entries for error reporting, see the resources listed in Appendix A, "Resources for Learning About Automated Installation and Deployment." Be sure to review the information in the Deploy.chm file (whose location is provided in that appendix).

Using Group Policy

To enable Corporate Error Reporting, perform these steps:

- Configure the **Error Reporting** policy settings in Group Policy so that error reports go to a server on your intranet.
- Use the Corporate Error Reporting tool to filter reports.

Enable error reporting through Group Policy so you can override actions users or administrators might take, and so you can redirect error reports to a server on your intranet instead of to the Internet. Once you have initiated Corporate Error Reporting, you can use this tool to manage error reports.

In addition to the **Error Reporting** policy settings, this subsection also includes a list of the **Advanced Error Reporting** policy settings you may want to use for additional configuration options.

Using Error Reporting policy settings

To configure servers for Corporate Error Reporting you need first to enable the **Report Errors** policy setting. Once you enable this policy setting, you can enter a file path to a server on your intranet, limit data that is exchanged on the Internet when errors are reported, control how users and administrators interact with the Error Reporting service, and take other steps to control information.

For details about locating the error reporting policy settings, see "Procedures for Configuring Error Reporting," later in this section. The following table describes the policy settings.

Group Policy settings for configuring error reporting

Policy setting	What it does	Configuration options
Report Errors (enabled)	Errors are reported to Microsoft through the Internet or to a server on your intranet. Enabling **Report Errors** will override any settings made using Control Panel for error reporting. Default values will be used for any error reporting settings that are not configured, even if settings were adjusted through Control Panel.	Can select: • Do not display links to any Microsoft provided "more information" Web sites • Do not collect additional files • Do not collect additional computer data • Force queue mode for application errors (note that this is the default configuration for servers) Can enter: • Corporate file path • Text to replace instances of the word "Microsoft"
Report Errors (disabled)	Users will not be given the option to report errors. If **Display Error Notification** is enabled, users will still get a message indicating that a problem occurred, but they will not have the option to report it. Disabling Report Errors is useful for servers that do not have interactive users.	Not applicable
Report Errors (not configured)	Users will be able to adjust the setting using Control Panel, which is set to "enable reporting" by default.	Not applicable
Display Error Notification (enabled)	This setting controls whether a user is given the choice to report an error. When enabled, the user will be notified that an error has occurred and will be given access to details about the error.	Not applicable
Display Error Notification (disabled)	The user is not given the choice of whether to report the error. If **Report Errors** is enabled, the error will be automatically reported, but the user will not be notified that an error has occurred. Disabling this setting is useful for servers that do not have interactive users. (Default setting for servers.)	Not applicable

Display Error Notification (not configured)	The user will be able to adjust the setting through Control Panel, which is set to enable notification by default.	Not applicable

Using Advanced Error Reporting policy settings

When you enable error reporting you can choose to specify the types of errors that are reported. In a highly managed environment administrators might want to do this based on the kinds of information included in the error report (see "Types of data collected," in the previous subsection).

With **Advanced Error Reporting** you can configure the following policy settings:

- **Default application reporting settings**
- **List of applications to always report errors for**
- **List of applications to never report errors for**
- **Report operating system errors**
- **Report unplanned shutdown events**

These policy settings are located in Computer Configuration\Administrative Templates\System\Error Reporting. When you configure these policy settings they will override any adjustments to error reporting administrators might make through Control Panel. You can configure these same policy settings in an answer file for unattended installation.

To find more information about editing Group Policy, see Appendix B, "Resources for Learning About Group Policy."

How controlling error reporting can affect administrators

What administrators will see on a server when an error occurs depends on how you have configured the **Error Reporting** policy settings. You can have certain administrators sending error reports to your intranet server only and others using CER to filter reports and send selected ones on to Microsoft. On some servers, for example, administrators may see only operating system or unplanned computer shutdown error reports and not application errors. Or, on some servers you might choose not to have error notification on.

Procedures for Configuring Error Reporting

This subsection presents the recommended procedure for enabling Corporate Error Reporting by configuring the **Report Errors** policy setting in Group Policy, for IT administrators who want to control the information that goes out to the Internet. This subsection also presents steps for configuring error reporting during unattended installation of the operating system by using an answer file.

Use the following procedure to configure the **Report Errors** policy setting so error reports are sent to a server on your intranet instead of to Microsoft.

To enable Corporate Error Reporting by using Group Policy

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in

Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.

2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, and then click **Error Reporting**.
3. In the details pane, double-click **Display Error Notification**, and then select **Enabled**.
4. Click **Next Setting**, and then under Report Errors, select **Enabled**.
5. In the Corporate upload file path box, enter a UNC (Universal Naming Convention) path (*servername**sharename*).

Note Administrators can then filter the error reports using the CER tool described in the previous subsection, "Controlling Error Reporting to Prevent the Flow of Information to and from the Internet."

To configure error reporting during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For information about unattended installation, and for details about the entries for error reporting, see the resources listed in Appendix A, "Resources for Learning About Automated Installation and Deployment." Be sure to review the information in the Deploy.chm file (whose location is provided in that appendix).
2. In the [PCHealth] section of the answer file, create entries according to the table in "Using unattended installation," earlier in this section. For example, to disable error reporting the entry is:

```
[PCHealth]
ER_Enable_Reporting = 0
```

Related Links

- For more information about Windows Error Reporting, see the article on the Microsoft Developer Network Web site at:

  http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/windows_error_reporting.asp

- To obtain the Corporate Error Reporting tool, see the Microsoft Web site at:

  http://oca.microsoft.com/en/cerintro.asp

- To read the Microsoft privacy statement for error reporting, see “Microsoft Error Reporting” at:

  http://watson.microsoft.com/dw/1033/dcp.asp

Windows Media Player

This section provides information about:

- The benefits of Windows Media Player
- How Windows Media Player communicates with sites on the Internet
- Procedures for configuration of Windows Media Player

Resources describing Windows Media Player configuration options

This section of the white paper describes Microsoft Windows Media Player (also called the Player) in the context of use on a server. The Player is not commonly used in a server environment, unless it is being used to test a Windows Media server, so this section of the white paper does not provide extensive information about implementing a specific configuration for the Player. For example, this section does not provide information about allowing or preventing downloads of codecs or other software for the Player. (A codec, short for compressor/decompressor, is software that compresses or decompresses audio or video data.) This section of the white paper also does not describe Windows Media Services, which is described in a separate section of the white paper.

For more information about configuring the Player, see the following resources:

- For information about implementing a specific configuration for Windows Media Player 9 Series in your organization, see the white paper titled “Using Windows 2000 with Service Pack 3 in a Managed Environment: Controlling Communication with the Internet.” This white paper includes information about allowing or preventing downloads for the Player (for example, downloads of codecs or other software for the Player), whether the Player is installed on a client or a server. This white paper can be found on the TechNet Web site at:

  http://www.microsoft.com/technet/prodtechnol/windows2000pro/maintain/w2kmngd/00_abstr.asp

- For information about implementing a specific configuration for the version of Windows Media Player included with Windows XP Professional SP1, see the white paper titled “Using Windows XP Professional with Service Pack 1 in a Managed Environment: Controlling Communication with the Internet.” This white paper can be found on the TechNet Web site at:

  http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

Benefits and Purposes of Windows Media Player

Windows Media Player 9 Series is the media player included with products in the Microsoft Windows Server 2003 family. The Player enables playing and organizing digital media files on computers and on the Internet. If you choose to use the Player on a server, you can listen to radio stations, search for and organize digital media files, and (with the right hardware) play CDs and DVDs, create custom CDs, and copy files to a portable device.

Windows Media Player 9 Series is described in this white paper because it can access media files on the Internet. In a highly managed network environment, you might want to control access to the Internet, including access gained through Windows Media Player. The rest of

this section describes how the Player communicates with the Internet, and how to control this communication.

Overview: Using Windows Media Player in a Managed Environment

Windows Media Player 9 Series in the Windows Server 2003 family is an integral component of the operating system and is installed by default. The Windows Media Player interface is accessed by navigating to Programs\Accessories\Entertainment or All Programs\Accessories\Entertainment from the Start menu. The Player is not commonly used in a server environment, unless it is being used to test a Windows Media server. If you do not want the Player accessible you can use Group Policy to block access to the Player. The procedure for this configuration method is described later in this section.

How Windows Media Player Communicates with Sites on the Internet

The Windows Media Player has a number of features that connect to sites on the Internet. When the user selects a feature such as Media Guide, Radio Tuner, Premium Services, or Skin Chooser\More Skins from the Player taskbar, Windows Media Player connects to www.WindowsMedia.com through either a local area network (LAN) or a modem connection.

WindowsMedia.com is a Web site operated by Microsoft and is tightly integrated into Windows Media Player. Media Guide and Radio Tuner are Web pages provided by WindowsMedia.com. All the CD audio data, DVD data, radio presets, and the information in the Info Center View area of the Now Playing feature also come directly from WindowsMedia.com. Other services provided by WindowsMedia.com include the Player updates and download support for codecs, skins, and visualizations. (A codec, short for compressor/decompressor, is software that compresses or decompresses audio or video data.)

To support the playback of secure content, Windows Media Player will also contact:

- Non-Microsoft digital rights management (DRM) license servers
- Microsoft DRM upgrade service

The other common Internet connections that Windows Media Player makes are to Windows Media servers run by content providers.

If you want more information about how Windows Media Player 9 Series communicates with the Internet (from the client or the server) and how to configure the Player for use, see “Related Links,” later in this section.

Procedure for Controlling Windows Media Player

Windows Media Player can be configured as described previously. This subsection provides a procedure for using Group Policy to prevent users or administrators from starting Windows Media Player.

> **Note** For information about implementing a specific configuration for Windows Media Player in your organization, see the sources listed in “Related Links,” later in this section.

To use Group Policy to prevent users and administrators from starting Windows Media Player

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **User Configuration**, click **Administrative Templates**, and then click **System**.
3. In the details pane, double-click **Don't run specified Windows applications**.
4. Select **Enabled**, click **Show**, click **Add**, and then enter the application executable name, Wmplayer.exe.

Related Links

- For more information about deploying and managing Windows Media Player in an enterprise environment, see the following pages on the Windows Media Web site at:
  - http://www.microsoft.com/windows/windowsmedia/
  - http://www.microsoft.com/Windows/WindowsMedia/howto/articles/intranet.aspx
  - http://www.microsoft.com/Windows/WindowsMedia/enterprise/TechResources/default.aspx
- For information about implementing a specific configuration for Windows Media Player 9 Series in your organization, see the white paper titled "Using Windows 2000 with Service Pack 3 in a Managed Environment: Controlling Communication with the Internet." This white paper can be found on the TechNet Web site at:

  http://www.microsoft.com/technet/prodtechnol/windows2000pro/maintain/w2kmngd/00_abstr.asp
- For information about implementing a specific configuration for the version of Windows Media Player included with Windows XP Professional SP1, see the white paper titled "Using Windows XP Professional with Service Pack 1 in a Managed Environment: Controlling Communication with the Internet." This white paper can be found on the TechNet Web site at:

  http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp
- For information about Windows Media Services, see the corresponding section of this white paper.

Windows Media Services

This section provides information about:

- The benefits of Windows Media® Services on servers running an operating system in the Microsoft Windows Server 2003 family.

  Note Windows Media Services 9 Series is included in Windows Server 2003, Standard Edition, the 32-bit version of Windows Server 2003, Enterprise Edition, and the 32-bit version of Windows Server 2003, Datacenter Edition. Windows Media Services is not included in Windows Server 2003, Web Edition, or in the 64-bit versions of the Windows Server 2003 family.

  In the 32-bit versions of Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition, Windows Media Services delivers advanced streaming functionality such as multicasting, wireless network support, Internet authentication, server plug-ins, and Cache/Proxy APIs.

- For servers from which you want to offer content that will be streamed to an intranet or the Internet, the following types of information are provided:
  - Examples of features in Windows Media Services 9 Series that help you control communication to and from a Windows Media server. Windows Media Services 9 Series is the version of Windows Media Services included with the Windows Server 2003 family.
  - References to more detailed information about Windows Media Services, including information about ports and security-related topics.
  - Information about installing the Windows Media Services and the Windows Media Services subcomponents, along with instructions for viewing the Help that comes with Windows Media Services.
- For servers from which you do not want to offer content on an intranet or the Internet, information about excluding or removing Windows Media Services.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running servers that communicate across the Internet. This section, however, provides overview information as well as suggestions for other sources of information about balancing your organization's requirements for communication across the Internet with your organization's requirements for protection of networked assets.

Note This section of the white paper describes Windows Media Services (the server component), but it does not describe Windows Media Player (the client component) or Internet Information Services (IIS), both of which are involved in carrying out communication of multimedia content across the Internet. For information about these components, see the respective sections of this white paper.

Benefits and Purposes of Windows Media Services

Windows Media Services is an optional component in products in the Windows Server 2003 family. With Windows Media Services, you can create, manage, and deliver Windows Media content over an intranet or the Internet. The clients receiving the content can render it as it is being received, that is, without downloading the content first. Streaming greatly reduces the wait time and storage requirements on the client. It also permits presentations of unlimited length, as well as live broadcasts.

For more information about features in Windows Media Services, see the sources in "Related Documentation and Links," later in this section.

Examples of Features that Help You Control Communication to and from a Windows Media Server

This subsection provides brief descriptions of some features in Windows Media Services 9 Series that help you control communication to and from a Windows Media server. These features are integrated with two aspects of basic functionality built into the Windows Server 2003 operating system:

- Authentication
- Authorization

Authentication

Authentication is a fundamental aspect of security for a server running Windows Media Services. It confirms the identity of any unicast client trying to access resources on your Windows Media server. Windows Media Services includes authentication plug-ins that you can enable in order to validate user credentials for unicast clients. Authentication plug-ins work together with authorization plug-ins: after users are authenticated, authorization plug-ins control access to unicast content.

Windows Media Services authentication plug-ins fall into the following categories:

- **Anonymous authentication**. These are plug-ins that do not exchange challenge and response information between the server and a player, such as the WMS Anonymous User Authentication plug-in.
- **Network authentication**. These are plug-ins that validate unicast clients based on user logon credentials, such as the WMS Negotiate Authentication plug-in.

When you make decisions about how authentication might affect users, consider the following points:

- For multicast streaming with Windows Media Services 9 Series, clients do not establish a connection, and therefore authentication and authorization do not apply for multicasting. (Multicast streaming is only available if you have the 32-bit version of Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition.)
- If a player is connected through HTTP, the player disconnects from the server each time the user stops, pauses, fast-forwards, or rewinds the content. If the user tries to continue receiving the content, the authentication and authorization process occurs again.

For more information about authentication and about the specific authentication plug-ins that you can enable for Windows Media Services, see the list in "Related Documentation and Links," later in this section.

Authorization

In order to control access to unicast content on your Windows Media server, unless you identify users only by IP address, you must enable one or more authentication plug-ins and also one or more authorization plug-ins. Authentication plug-ins verify the credentials of unicast clients attempting to connect to the server. Authorization plug-ins verify that the unicast client is allowed to connect to the server. Authorization occurs after authentication is successful.

You can enable authorization plug-ins to control the access to content by authenticated users. If you enable an authorization plug-in, with one exception, you must also enable an authentication plug-in for unicast clients to be able to access your publishing points. The exception is the WMS IP Address Authorization plug-in, which does not require an authentication plug-in to authenticate a unicast client.

Note that for multicast streaming with Windows Media Services 9 Series, clients do not establish a connection, and therefore authentication and authorization do not apply for multicasting. (Multicast streaming is only available if you have the 32-bit version of Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition.)

During the authorization process, the server checks the user against the set of access permissions for the resource to which the user is trying to connect.

For more information about authorization, see the list in "Related Documentation and Links," later in this section.

Firewall Information for Windows Media Services

This subsection provides information about configuring firewalls (or proxy servers or both) for use with Windows Media Services. For more information about firewalls, see the sources in "Related Documentation and Links," later in this section.

You can configure each control protocol plug-in (Microsoft Media Server [MMS] protocol, Real Time Streaming Protocol [RTSP], and HTTP) to use a specific port to make firewall configuration easier. If opening ports on your firewall is not possible, Windows Media Services can stream content by using the HTTP protocol over port 80.

Note Using HTTP to stream content is disabled by default.

Windows Media Services was formerly known as Microsoft NetShow Services; some firewalls have a preconfigured NetShow setting, which may work for Windows Media Services.

Configuring firewalls for unicast streaming

To configure a firewall for unicast streaming, you must open the ports on the firewall that are required for the connection protocols enabled on your server. If you are streaming content by using either the Microsoft Media Server (MMS) protocol or the Real Time Streaming Protocol (RTSP), you need to support both the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

To enable Windows Media Player and other clients to use the HTTP, RTSP, or MMS protocols to connect to a Windows Media server that is behind a firewall, open the ports described in the following table.

Ports to open when clients are connecting using HTTP, RTSP, or MMS protocols

Ports	Description
In: TCP on ports 80, 554, and 1755	The Windows Media server uses the TCP In ports to accept an incoming HTTP connection (port 80), RTSP connection (port 554), or MMS connection (port 1755) from Windows Media Player and other clients.
In: UDP on ports 1755 and 5005	The Windows Media server uses UDP In port 1755 to receive resend requests from clients streaming by using MMSU (MMS used with UDP), and UDP In port 5005 to receive resend requests from clients

	streaming by using RTSPU (RTSP used with UDP).
Out: UDP on ports 1024 through 5000.	The Windows Media server uses UDP Out ports 1024 through 5000 to send data to Windows Media Player and other clients.

To enable a distribution server that is behind a firewall to use the HTTP or RTSP protocols to stream content that originates from a server outside the firewall, open the ports described in the following table.

Ports to open when a distribution server is behind a firewall and uses HTTP or RTSP to stream content that originates from a server outside the firewall

Ports	Description
In: UDP on ports 1024 through 5000	The Windows Media server uses UDP In ports 1024 through 5000 to receive data from another server.
Out: TCP on ports 80 and 554	The Windows Media server uses the TCP Out ports to establish an HTTP connection (port 80) or RTSP connection (port 554) to another server or encoder.
Out: UDP on port 5005	When RTSPU distribution is used, the Windows Media server uses UDP Out port 5005 to send resend requests to another server.

Note If it is not possible to open all the UDP Out ports on a firewall, UDP packets sent by a Windows Media server may be blocked by the firewall and may not be able to reach the clients on the other side of the firewall. If this is the case, clients may still be able to receive a stream by automatically rolling over to a TCP-based protocol, such as HTTP or RTSPT (RTSP used with TCP). However, the rollover will cause a delay for the client receiving the stream.

If you know you will not be able to support UDP streaming through a firewall, you can decrease the rollover delay by clearing the UDP check box in the Unicast Data Writer plug-in Properties dialog box. For more information, see the Help for Windows Media Services. A procedure for viewing Help is included in "Procedures for Installing, Removing, or Excluding Windows Media Services and Its Subcomponents," later in this section.

Configuring firewalls for multicast streaming

If you distribute content using multicast streaming, network traffic is directed through the standard Class D IP addresses (224.0.0.0 through 239.255.255.255). For multicast streaming, you must enable multicast-forwarding on your network. The Internet Group Management Protocol (IGMP), supported by Windows Media Services, ensures that multicast traffic passes through your network only when a player requests a multicast connection, so that enabling multicasting on your routers does not flood your network.

The following firewall configuration enables multicast packets to traverse your firewall:

IP multicast address range: 224.0.0.1 through 239.255.255.255

To enable IP multicasting, you must allow packets sent to the standard IP multicast address range to come through your firewall. This IP multicast address range must be enabled on both the player and server sides, as well as on every router in between.

Enabling access to an encoder outside a firewall

Encoders use HTTP to connect to a server running Windows Media Services. By default, Windows Media Encoder uses port 8080 for HTTP connections; however, the encoder administrator can specify a different port. If a different port is used, you must specify the same port when you identify the encoder connection URL for the Windows Media server and when opening the port on your firewall.

The following example of a firewall configuration allows a computer running Windows Media Encoder outside a firewall to access a Windows Media server behind a firewall by using HTTP:
In/Out: Transmission Control Protocol (TCP) on port 8080.

(The In port is the port through which the server accepts connections. The Out port is the port through which the server sends data to clients.)

Answer File Entries and Registry Keys for Windows Media Services Subcomponents

For reference purposes, the following table shows the syntax for answer file entries associated with Windows Media Services in the Windows Server 2003 family. The table also shows the corresponding registry keys. Do not change the registry keys. They are shown for use in a script that could check whether a particular subcomponent is installed on a particular server. A registry key value of 0x00000000 means the subcomponent is not installed, and a value of 0x00000001 means the subcomponent is installed.

> **Note** For more details about answer-file entries related to Windows Media Services subcomponents, including information about dependencies between the entries, see the references listed in Appendix A, "Resources for Learning About Automated Installation and Deployment." Be sure to review the information in the Deploy.chm file (whose location is provided in that appendix).

Answer file entries and registry keys for Windows Media Services subcomponents for the Windows Server 2003 family

Windows Media Services subcomponent	Answer file entry (in the [Components] section)	Registry key (for use in a script that checks whether a subcomponent is installed): 0x00000000 means it is not installed; 0x00000001 mean it is installed
Core Windows Media server components	wms = On | Off	No key available (check for subcomponents by using other keys)
Windows Media Services Administrator for the Web	wms_admin_asp = On | Off	HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Setup\OC Manager\ Subcomponents\wms_admin_asp
Windows Media Services MMC snap-in	wms_admin_mmc = On | Off	HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Setup\OC Manager\ Subcomponents\wms_admin_mmc
Multicast and Advertisement Logging Agent components	wms_isapi = On | Off	HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Setup\OC Manager\ Subcomponents\wms_isapi
Windows Media Services server components	wms_server = On | Off	HKEY_LOCAL_MACHINE\Software\Microsoft\ Windows\CurrentVersion\Setup\OC Manager\ Subcomponents\wms_server

Procedures for Installing, Removing, or Excluding Windows Media Services and Its Subcomponents

The following procedures explain how to:

- Add or remove Windows Media Services on a computer after setup is complete for a product in the Windows Server 2003 family.
- View the Help that comes with Windows Media Services.
- Prevent the installation of Windows Media Services during unattended installation by using an answer file.
- Specify answer file entries that control whether Windows Media Services subcomponents are included during unattended installation.

Note Windows Media Services is included in Windows Server 2003, Standard Edition, the 32-bit version of Windows Server 2003, Enterprise Edition, and the 32-bit version of Windows Server 2003, Datacenter Edition. Windows Media Services is not included in Windows Server 2003, Web Edition or in the 64-bit versions of the Windows Server 2003 family.

In the 32-bit versions of Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition, Windows Media Services delivers advanced streaming functionality, such as multicasting, wireless network support, Internet authentication, server plug-ins, and Cache/Proxy APIs.

To add or remove Windows Media Services on an individual computer after setup is complete

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components** (on the left).
4. Select **Windows Media Services**.
5. Perform one of the following steps:
   - If Windows Media Services is installed and you want to remove it, clear the check box for **Windows Media Services** and complete the wizard.
   - If Windows Media Services is not installed and you want to add it, select the check box for **Windows Media Services** and complete the wizard.
   - If you want to view the list of Windows Media Services subcomponents, after selecting **Windows Media Services**, click **Details**.

To view the Help that comes with Windows Media Services

1. Make sure that Windows Media Services is installed by using the previous procedure.
2. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
3. Double-click **Administrative Tools** and then click **Windows Media Services**.
4. Click the **Help** menu and then click **Help Topics**.

To specify answer file entries that control whether Windows Media Services subcomponents are included during unattended installation

1. Using the methods you prefer for unattended installation or remote installation, create an answer file.
2. In the [Components] section of the answer file, add the appropriate entries listed in the table in "Answer File Entries and Registry Keys for Windows Media Services Subcomponents," earlier in this section. Ensure that the entries specify **Off** for components you do not want to install and **On** for components you want to install.

   If no Windows Media Services subcomponents are listed in an answer file for unattended installation of a Windows Server 2003 family operating system, these components are *not* installed by default.

   Note For more information about unattended installation, and for details about dependencies between answer-file entries related to Windows Media Services subcomponents, see the references listed in Appendix A, "Resources for Learning About Automated Installation and Deployment." Be sure to review the information in the Deploy.chm file (whose location is provided in that appendix).

To prevent the installation of Windows Media Services during unattended installation by using an answer file

1. Using the methods you prefer for unattended installation or remote installation, create an answer file. For more information about unattended and remote installation, see Appendix A, "Resources for Learning About Automated Installation and Deployment."
2. In the [Components] section of the answer file, ensure that there are no entries for the subcomponents listed in the table in "Answer File Entries and Registry Keys for Windows Media Services Subcomponents," earlier in this section. If you want to list any of these subcomponents, ensure that the entries specify **Off**.

   If no Windows Media Services subcomponents are listed in an answer file for unattended installation of a Windows Server 2003 family operating system, these subcomponents are *not* installed by default.

Related Documentation and Links

The following list of resources can help you as you plan or modify your implementation of Windows Media Services and Windows Media Player in your organization:

- For technical information about Windows Media, see “Windows Media Technical Resources for the Enterprise,” on the Microsoft Web site at:

  http://www.microsoft.com/windows/windowsmedia/enterprise/techresources/default.aspx

  A variety of technical resources are available on the preceding Web site, including:

  - The Windows Media 9 Series Deployment Guide.
  - The Enterprise Deployment Pack for Windows Media Player 9 Series, a downloadable packaging tool that simplifies the configuration, deployment, and management of Windows Media Player 9 Series.
  - Other technical articles.
- For information about deploying over an intranet, see “Deploying Windows Media 9 Series over an Intranet,” on the Microsoft Web site at:

  http://www.microsoft.com/Windows/WindowsMedia/howto/articles/intranet.aspx

- For conceptual and how-to information about using Windows Media Services, including information about authentication, authorization, ports, and firewall settings, see the Help that comes with Windows Media Services. For information about installing Windows Media Services and viewing Help, see "Procedures for Installing, Removing, or Excluding Windows Media Services and Its Subcomponents," earlier in this section.
- For general information about features, and information about ports and firewall or proxy settings, search for the latest information on the Windows Media Web site at:

  http://www.microsoft.com/windows/windowsmedia/
- For information about Windows Media Services 9 Series, for example, information about upgrading, optimizing, features, and logging, see the following page on the Windows Media Web site:

  http://www.microsoft.com/windows/windowsmedia/9series/server.aspx
- For documentation on the distribution of content, see the Windows Media Web site at:

  http://www.microsoft.com/windows/windowsmedia/distribute.aspx
- For information about using Windows Media run-time components in a custom application, see "Redistributing Windows Media 9 Series Components," on the Microsoft Developer Network Web site at:

  http://msdn.microsoft.com/library/en-us/dnwmt/html/RedisWMedC.asp
- For information about Windows Media Services Software Development Kits (SDKs), see the Microsoft Developer Network Web site at:

  http://msdn.microsoft.com/downloads/list/winmedia.asp

Printed reference

- Birney, B., Tricia Gill, and members of the Microsoft Windows Media Team. *Microsoft Windows Media Resource Kit*. Redmond, WA: Microsoft Press, 2003.

  You can read a sample chapter and view information about the *Microsoft Windows Media Resource Kit* on the MS Press Web site at:

  http://www.microsoft.com/MSPress/books/6280.asp

Windows Time Service

The following sections provide information about:

- The benefits of Windows Time Service
- How Windows Time Service communicates with sites on the Internet
- How to control Windows Time Service to limit the flow of information to and from the Internet
- How to monitor and troubleshoot Windows Time Service after configuration is complete

Benefits and Purposes of Windows Time Service

Many components of operating systems in the Microsoft Windows Server 2003 family rely on accurate and synchronized time to function correctly. For example, without clocks that are synchronized to the correct time on all computers, Windows Server 2003 family authentication might falsely interpret logon requests as intrusion attempts and consequently deny access to users.

With time synchronization, you can correlate events on different computers in an enterprise. With synchronized clocks on all of your computers, you ensure that you can correctly analyze events that happen in sequence on multiple computers. Windows Time Service automatically synchronizes a local computer’s time with other computers on a network to improve security and performance in your organization.

Overview: Using Windows Time Service in a Managed Environment

Computers keep the time on their internal clocks, which allows them to perform any function that requires the date or time. For scheduling purposes, however, the clocks must be set to the correct date and time, and they must be synchronized with the other clocks in the network. Without some other method in place, these clocks must be set manually.

With time synchronization, computers set their clocks automatically to match another computer's clock. One computer maintains very accurate time, and then all other computers set their clocks to match that computer. In this way, you can set accurate time on all computers.

Windows Time Service is installed by default on all computers running Windows 2000, Windows XP, and products in the Windows Server 2003 family. Windows Time Service uses Coordinated Universal Time (UTC), which is based on an atomic time scale and is therefore independent of time zone. Time zone information is stored in the computer's registry and is added to the system time just before it is displayed to the user.

Windows Time Service starts automatically on computers that are joined to a domain. (For computers that are not joined to a domain, you can start the time service manually.) In a domain, time synchronization takes place when Windows Time Service turns on during system startup. In the default configuration, the Net Logon service looks for a domain controller that can authenticate and synchronize time with the client. When a domain controller is found, the client sends a request for time and waits for a reply from the domain controller. This communication is an exchange of Network Time Protocol (NTP) packets intended to calculate the time offset and roundtrip delay between the two computers.

How Windows Time Service Communicates with Sites on the Internet

In the Windows Server 2003 family, Windows Time Service automatically synchronizes the local computer's time with other computers on the network. The time source for this synchronization varies, depending on whether the computer is joined to a domain in the Active Directory directory service or to a workgroup.

When a server running a product in the Windows Server 2003 family is part of a workgroup

In this scenario, the default setting for the time synchronization frequency is set to "once per week," and this default setting uses the time.windows.com site as the trusted time synchronization source. This setting will remain until you manually set it otherwise. One or more computers might be identified as a locally reliable time source by configuring Windows Time Service on those computers to use a known accurate time source, either by using special hardware or a time source available on the Internet. All other workgroup computers can be configured manually to synchronize their time with these local time sources.

When a server running a product in the Windows Server 2003 family is a member of a domain

On servers in this scenario, Windows Time Service configures itself automatically, using the Windows Time Service that is available on the domain controllers.

Windows Time Service on a domain controller can be configured as either a reliable or an unreliable time source. Windows Time Service running on a client will attempt to synchronize its time source with servers that are indicated as reliable. Windows Time Service can configure a domain controller within its domain as a reliable time source, and it synchronizes itself periodically with this source. These settings can be modified or overwritten, depending on specific needs.

When a computer running Windows 2000 or a Windows Server 2003 family operating system is not a member of a domain

Windows Time Service must be manually started for computers running Windows 2000 that are not members of a domain. For computers running a Windows Server 2003 operating system that are not members of a domain, Windows Time Service is configured by default to synchronize its time source with time.windows.com. Windows Time Service starts automatically for computers running a Windows Server 2003 operating system. These computers use the Network Time Protocol (NTP), while computers running Windows 2000 use the Simple Network Time Protocol (SNTP).

The following list describes various aspects of Windows Time Service data that is sent to and from the Internet and how the exchange of information takes place:

- **Specific information sent or received**: The service sends information in the form of a Network Time Protocol (NTP) packet. For more information about Windows Time Service and NTP packets, see the references listed in “Related Documentation and Links,” later in this section.
- **Default and recommended settings**: Computers that are members of an Active Directory domain synchronize time with domain controllers by default. Domain controllers synchronize time with their parent domain controller. By default, the root parent domain

controller will not synchronize to a time source. The root parent domain controller can be set to either synchronize to a known and trusted Internet-based time source, or a hardware time device that provides an NTP (Network Time Protocol) or SNTP interface. Its time accuracy can also be maintained manually.

- **Triggers**: Windows Time Service is started when the computer starts. Additionally, the service will continue to synchronize time with the designated network time source and adjust the computer time of the local computer when necessary.
- **User notification**: Notification is not sent to the user.
- **Logging**: Information related to the service is stored in the Windows System event log. The time and network address of the time synchronization source is contained in the Windows event log entries. Additionally, warning or error condition information related to the service is stored in the Windows System event log.
- **Encryption**: Encryption is used in the network time synchronization for domain peers.
- **Information storage**: The service does not store information, as all information that results from the time synchronization process is lost when the time synchronization service request is completed.
- **Port**: NTP and SNTP default to using User Datagram Protocol (UDP) port 123. If this port is not open to the Internet, you cannot synchronize your server to Internet SNTP servers.
- **Communication protocol**: The service on Windows 2000 implements SNTP to communicate with other computers on the network. The service on the Windows Server 2003 family implements NTP to communicate with other computers on the network.
- **Ability to disable**: Disabling the service has no direct effect on applications or other services. Applications and services that depend on time synchronization, such as Kerberos V5 authentication protocol, may fail, or they may yield undesirable results if there is a significant time discrepancy among computers. Because most computers' hardware-based clocks are imprecise, the difference between computer clocks on the network usually increases over time.

Controlling Windows Time Service to Limit the Flow of Information to and from the Internet

Group Policy can be used to control Windows Time Service for computers that are running a Windows Server 2003 family operating system to limit the flow of information to and from the Internet.

The synchronization type and NTP time server information can be managed and controlled through Group Policy. The Windows Time Service Group Policy object (GPO) contains configuration settings that specify the synchronization type. When the synchronization type is set to Nt5DS, Windows Time Service synchronizes its time resource with the network domain controller. Alternatively, setting the type attribute to NTP configures Windows Time Service to synchronize with a specified NTP time server. The NTP server is specified by either its Domain Name System (DNS) name or its IP address when you select NTP as the synchronization type.

For more information about configuring Windows Time Service during deployment of products in the Windows Server 2003 family, see *Designing and Deploying Directory and Security Services* and *Designing a Managed Environment* in the *Microsoft Windows Server 2003 Deployment Kit* at:

http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx

Clients on a managed network can be configured to synchronize computer clock settings to an NTP server on the network to minimize traffic out to the Internet and to ensure that the clients synchronize to a single reliable time source. If you choose to do so, you can disable time synchronization for both non-domain and domain computers running Windows Server 2003 family operating systems by using Group Policy. The procedures for configuring Windows Time Service are given at the end of this section of the white paper.

How Windows Time Service can affect users and applications

Windows components and services depend on time synchronization. For example, the Kerberos V5 authentication protocol on a Windows Server 2003 family domain has a default time synchronization threshold of five minutes. Computers that are more than five minutes out of synchronization on the domain will fail to authenticate using the Kerberos protocol. This time value is also configurable, allowing for smaller thresholds. Failure to authenticate using the Kerberos protocol can prevent logons, access to Web sites, file shares, printers, and other resources or services within a domain.

When the local clock offset has been determined, the following adjustments are made to the time:

- If the local clock time of the client is behind the current time received from the server, Windows Time Service will change the local clock time immediately.
- If the local clock time of the client is more than three minutes ahead of the time on the server, the service will change the local clock time immediately.
- If the local clock time of the client is less than three minutes ahead of the time on the server, the service will quarter or halve the clock frequency for long enough to synchronize the clocks.
- If the client is less than 15 seconds ahead, it will halve the frequency; otherwise, it will quarter the frequency. The amount of time the clock spends running at an unusual frequency depends on the size of the offset that is being corrected.

Configuration Settings for Windows Time Service

You can set the global configuration settings for Windows Time Service by using Group Policy. For details about locating Windows Time Service policy settings, see "Procedures for Configuring Windows Time Service," later in this section. The following table describes the policy settings.

These Group Policy settings correspond to registry entries of the same name, which are located in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time.

Group Policy settings for configuring Windows Time Service

Policy setting	Effect of policy setting	Default setting
FrequencyCorrectRate	One over the rate at which the clock is corrected. If this value is too small, the clock will be unstable and will overcorrect. If the value is too large, the clock will take a long time to synchronize.	4
HoldPeriod	The period of time for which spike detection is disabled in order to bring the local clock into synchronization quickly. A spike is a time sample indicating that time is off a number of seconds, usually received after good time samples have been returned consistently.	5

LargePhaseOffset	A time offset greater than or equal to this value is considered suspicious by the time service. This occurrence might be caused by a noise spike.	1,280,000
MaxAllowedPhaseOffset	The maximum offset (in seconds) for which Windows Time Service attempts to adjust the computer clock by using the clock rate. When the offset exceeds this rate, the service sets the computer clock directly.	300
MaxNegPhaseCorrection	The largest negative time correction in seconds that the service will make. If the service determines that a change larger than this is required, it logs an event instead.	54,000 (15 hrs)
MaxPosPhaseCorrection	The largest positive time correction in seconds that the service will make. If the service determines a change larger than this is required, it will log an event instead.	54,000 (15 hrs)
PhaseCorrectRate	One over how much of the remaining phase error in order to correct this update interval.	7
PollAdjustFactor	Controls the decision to increase or decrease the poll interval for the system. The larger the value, the smaller the amount of error that causes the poll interval to be decreased.	5
SpikeWatchPeriod	The amount of time that a suspicious offset must persist before it is accepted as correct (in seconds).	90
UpdateInterval	The number of clock ticks between phase correction adjustments.	100
AnnounceFlags	Controls whether this computer is marked as a reliable time server. A computer is not marked as reliable unless it is also marked as a time server.	6
EventLogFlags	Controls the events that the time service logs.	2
LocalClockDispersion	The dispersion (in seconds) that you must assume when the only time source is the built-in complementary metal oxide semiconductor (CMOS) clock.	10
MaxPollInterval	The largest interval, in log2 seconds, allowed for the system polling interval. Note that while a system must poll according to the scheduled interval, a provider can refuse to produce samples when requested to do so.	15
MinPollInterval	The smallest interval, in log2 seconds, allowed for the system polling interval. Note that while a system does not request samples more frequently than this, a provider can produce samples at times other than the scheduled interval.	4

You can set the Windows NTP Client configuration settings for Windows Time Service by using Group Policy. For details about locating Windows Time Service policy settings, see "Procedures for Configuring Windows Time Service," later in this section. The following table describes the policy settings.

These Group Policy settings correspond to the registry entries of the same name located in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters.

Group Policy settings for configuring the Windows Time Service NTP Client for computers running Windows Server 2003

Policy setting	Effect of setting	Default setting

NtpServer	Establishes a space-delimited list of peers from which a computer obtains time stamps, consisting of one or more DNS names or IP addresses per line. Computers connected to a domain must synchronize with a more reliable time source, such as the official U.S. time clock.	time.microsoft.com
Type	Indicates which peers to accept synchronization from: **NoSync**. The time service does not synchronize with other sources. **NTP**. The time service synchronizes from the servers specified in the NtpServer registry entry. **NT5DS**. The time service synchronizes from the domain hierarchy. **AllSync**. The time service uses all the available synchronization mechanisms.	Default options **NTP**. Use on computers that are not joined to a domain. **NT5DS**. Use on computers that are joined to a domain.
ServiceDll	Provides the directory location of the Windows Time service dynamic-link library (DLL).	C:\WINDOWS\system32\w32time.dll
ServiceMain	Service Control Manager (SCM) calls this value.	SvchostEntry_W32Time
CrossSiteSyncFlags	Determines whether the service chooses synchronization partners outside the domain of the computer. None 0 PdcOnly 1 All 2 This value is ignored if the NT5DS value is not set.	2
ResolvePeerBackoffMinutes	Specifies the initial interval to wait, in minutes, before attempting to locate a peer to synchronize with.	15
ResolvePeerBackoffMaxTimes	Specifies the maximum number of times to double the wait interval when repeated attempts to locate a peer to synchronize with fail. A value of zero means that the wait interval is always the minimum.	7
SpecialPollInterval	Specifies the special poll interval in seconds for peers that have been configured manually. When a special poll is enabled, Windows Time Service will use this poll interval instead of a dynamic one that is determined by synchronization algorithms built into Windows Time Service.	3600
EventLogFlags	Controls the events that the time service logs.	0

Note Group Policy and Active Directory are tools that are available for controlling and managing computers and services within an enterprise or organization. The full description of the rich feature set and methods for using Group Policy are beyond the intended scope of this document. For other sources of information about Group Policy, see Appendix B, "Resources for Learning About Group Policy."

Procedures for Configuring Windows Time Service

The following procedures explain how to set Windows Time Service configuration settings through Group Policy on operating systems in the Windows Server 2003 family to achieve the configurations described in the previous subsections.

To set Group Policy for Windows Time Service global configuration settings

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, and then click **Windows Time Service**.
3. In the details pane, double-click **Global Configuration Settings**, and then click **Enabled**.

To configure the Group Policy setting to prevent your computer from synchronizing its computer clock with other NTP servers

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, click **Windows Time Service**, and then click **Time Providers**.
3. In the details pane, double-click **Enable Windows NTP Client** and then select **Disabled**.

To configure the Group Policy setting to prevent your computer from synchronizing its computer clock from the domain hierarchy or a manually configured NTP server

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, click **Windows Time Service**, and then click **Time Providers**.
3. In the details pane, double-click **Configure Windows NTP Client**, and then select **Disabled**.

To configure the Group Policy setting to prevent your computer from servicing time synchronization requests from other computers on the network

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **System**, click **Windows Time Service**, and then click **Time Providers**.
3. In the details pane, double-click **Enable Windows NTP Server**, and then select **Disabled**.

Starting and stopping Windows Time Service

By default, Windows Time Service starts automatically at system startup. You can, however, start or stop the service manually by accessing services in Administrative Tools or by using the **net** command.

To manually start Windows Time Service using the graphical interface

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. Select **Windows Time** from the list of services.
4. On the **Action** menu, click **Start** to begin the service.

To manually stop Windows Time Service using the graphical interface

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Double-click **Administrative Tools**, and then double-click **Services**.
3. Select **Windows Time** from the list of services.
4. On the **Action** menu, click **Stop** to discontinue the service.

To manually start Windows Time Service using the net command

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **net start w32time**, and then press ENTER.

To manually stop Windows Time Service using the net command

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **net stop w32time**, and then press ENTER.

Synchronizing computers with time sources

Use the following procedures to synchronize the internal time server with an external time source, and to synchronize the client time with a time server.

To synchronize an internal time server with an external time source

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type the following, where *PeerList* is a comma-separated list of Domain Name System (DNS) names or Internet protocol (IP) addresses of the desired time sources:
   w32tm /config /syncfromflags:manual /manualpeerlist:*PeerList*
   and then press ENTER.
3. Type **w32tm /config /update**, and then press ENTER.

Notes
The most common use of this procedure is to synchronize the internal network's authoritative time source with precise external time source. This procedure can be run on any computer running Windows 2000, Windows XP, or an operating system in the Windows Server 2003 family.

If the computer cannot reach the servers, the procedure fails and an entry is written to the Windows System event log.

To synchronize the client time with a time server

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **w32tm /resync**, and then press ENTER.

Notes
This procedure only works on computers that are joined to a domain.

The W32tm command-line tool is used for diagnosing problems that can occur with Windows Time Service. If you are going to use the tool on a domain controller, it is necessary to stop the service. Running the tool and Windows Time Service at the same time on a domain controller generates an error because both are attempting to use the same UDP port. When you finish using W32tm command-line tool, the service must be restarted.

Monitoring and Troubleshooting Windows Time Service

In many cases problems with Windows Time Service can be attributed to network configuration. If the network is not configured correctly computers might not be able to communicate to send time samples back and forth. Viewing the contents of NTP packets can help you to identify exactly where a packet is blocked on a network. An error associated with Windows Time Service might occur when a computer is unable to synchronize with an authoritative source. You can use the W32tm command-line tool to assist you in troubleshooting this and other types of errors associated with Windows Time Service.

The W32tm command-line tool is the preferred command-line tool for configuring, monitoring, and troubleshooting Windows Time Service. All tasks that can be performed by using the **net** command can be accomplished by using this tool or Group Policy. For more information, look up "W32tm" in the Help and Support Center index.

Procedure to follow when a computer is unable to synchronize

A computer running Windows Time Service refuses to synchronize with a time source if the computer's time is more than 15 hours off. Such occurrences are rare, and are often caused by configuration setting errors. For example, if a user sets the date on the computer incorrectly, the time does not synchronize. Under these circumstances, most often the time is off by a day or more. Be sure to check the computer's calendar and ensure that the correct date has been set.

To resynchronize the client time with a time server

1. To open a command prompt, click **Start**, click **Run**, type **cmd**, and then click **OK**.
2. Type **w32tm /resync /rediscover**, and then press ENTER.

Notes
When you run the preceding command, it redetects the network configuration and rediscovers network resources, causing resynchronization. This procedure only works on computers that are joined to a domain. You can then view the event log for more information about why the time service does not synchronize. For more information, look up "Monitoring and controlling services on computers," in Help and Support Center.

The W32tm tool is used for diagnosing problems that can occur with Windows Time Service. If you are going to use the W32tm tool on a domain controller, it is necessary to stop the service. Running W32tm and Windows Time Service at the same time on

a domain controller generates an error because both are attempting to use the same UDP port. When you finish using W32tm, the service must be restarted.

Related Documentation and Links

- For more information about configuring Windows Time Service during deployment of products in the Windows Server 2003 family, see *Designing and Deploying Directory and Security Services* and *Designing a Managed Environment* in the *Microsoft Windows Server 2003 Deployment Kit* at:

  http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx

Using online resources. The Microsoft Web site contains support information, including the latest downloads and Knowledge Base articles written by support professionals at Microsoft:

- You can search frequently asked questions (FAQs) by product, browse the product support newsgroups, and contact Microsoft Support at the following Web site. You can also search the Microsoft Knowledge Base of technical support information and self-help tools for Microsoft products at this site:

  http://support.microsoft.com/

- You can search for troubleshooting information, service packs, patches, and downloads for your system on the Technet Web site at

  http://www.microsoft.com/technet/

Windows Update and Automatic Updates

This section provides information about:

- The benefits of Windows Update and Automatic Updates
- How Windows Update and Automatic Updates communicate with sites on the Internet
- How to control Windows Update and Automatic Updates to limit the flow of information to and from the Internet

Important This section describes methods for controlling the way the Automatic Updates component interacts with the Windows Update Web site. One basic way, however, of controlling whether a particular person can install software (including software updates) on a particular computer is to control the type of account that the person has. If the account does not allow the person to install software (for example, if the account is a user account) the person will not be able to use Automatic Updates to install software while logged on with that account.

Benefits and Purposes of Windows Update and Automatic Updates

Windows Update

Windows Update is an online catalog customized for computers running a product in the Microsoft Windows Server 2003 family that consists of items such as drivers, critical updates, Help files, and Internet products. Windows Update scans the user's computer and provides a tailored selection of updates that apply only to the software and hardware on that specific computer. Windows Update then enables users to choose updates for their computer's operating system and hardware. New content is added to the Windows Update Web site regularly, so users can always get the most recent and secure updates and solutions.

Windows Update contains two key components:

- **Content update**: Content updates occur when the user accesses the Windows Update Web site and selects component updates to download and install. The user is fully aware of downloads to the computer. The Windows Update Web site is located at:

  http://windowsupdate.microsoft.com/

- **Web service control update**: The Windows Update Web service includes an ActiveX Web control program that downloads and installs the content updates. The Windows Update team receives feedback from their customers on how to improve their Web service and the Windows Update service control is changed to reflect that feedback. In order to access the new content and services customers need, the Web controls are updated periodically. This service automatically downloads a new version of the Web control program when the user visits the Windows Update site or when any of the other Windows features calls on the Windows Update control. Just like downloading an ActiveX control, the user may receive a security dialog box that a Web control is attempting to be installed. Users may not receive the dialog box if they have selected to always trust Microsoft as a content provider (using their security settings in Microsoft Internet Explorer). If users do not click Yes on the security dialog box, the control will not be updated and they will not be able to access the Windows Update site.

Automatic Updates

This option for updating a computer allows for updates without interrupting the user's Web experience. Automatic Updates is not enabled by default; users are prompted to enable this option following setup. When Automatic Updates is enabled, users do not need to visit special Web pages or remember to periodically check for new updates. An icon appears in the notification area each time new updates are available. Updates can be downloaded in the background with minimal impact on the user's network connections. Once the update is downloaded, operating systems in the Windows Server 2003 family prompt the user to install it. Users can set Automatic Updates options in one of three ways to control how and when they want the operating system to update their computers. They can:

- Choose to have the operating system send a notification before downloading and installing any updates.
- Choose to have the operating system download and install updates automatically on a schedule that they specify.
- Choose to have the operating system send a notification whenever it finds updates available for their computers; the operating system will then download the updates in the background, enabling users to continue working uninterrupted. After the download is complete, an icon in the notification area will prompt users that the updates are ready to be installed.

Users can choose not to install a specific update that has been downloaded; in that case, the operating system will delete those files from the computer. Users can download those deleted files again by opening **System** in Control Panel, clicking the **Automatic Updates** tab, and then clicking **Declined Updates**. If any of the updates users previously declined can still be applied to their computers, they will appear the next time an operating system in the Windows Server 2003 family notifies those users of available updates.

Alternatives to Windows Update and Automatic Updates

For managed environments, there are several alternatives to Windows Update:

- Windows Update Catalog Web site.
- Microsoft Software Update Services (SUS).
- Distribution software, such as Microsoft Systems Management Server, that can be used to distribute software updates. For more information, see the documentation for your distribution software, and see Appendix A, "Resources for Learning About Automated Installation and Deployment," especially the "Related Documentation and Links" subsection in that appendix.

Windows Update Catalog Web Site

You can deploy updates to Windows in a managed environment without requiring users to connect to the Windows Update Web site by using the Windows Update Catalog site. This site provides a comprehensive catalog of updates that can be distributed over a managed network. It provides a single location for Windows Update content and drivers that display the Designed for Windows logo. Administrators can search the site using keywords or predefined search criteria to select the relevant downloads and then to download the updates to a location on their internal network.

An enhancement in products in the Windows Server 2003 family enables you to select updates that you plan to deploy later, which means you can control how and when the updates are deployed. For additional information, see information about Windows Update on the Microsoft Web site at:

http://windowsupdate.microsoft.com/

Microsoft Software Update Services (SUS)

Microsoft Software Update Services (SUS) is a version of Windows Update designed for installation inside an organization's firewall. This feature is very useful for organizations that:

- Do not want their systems or users connecting to an external Web site
- Want to first test these updates before deploying them throughout their organization

Microsoft Software Update Services enables administrators to quickly and reliably deploy critical updates to their computers running Windows Server 2003 operating systems.

For more information about software update services, see the Microsoft Web site at:

http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp

Note that the preceding Web site has information about both Windows 2000 and products in the Windows Server 2003 family.

Overview: Using Windows Update and Automatic Updates in a Managed Environment

Users have control over whether to enable Automatic Updates following setup and they also have direct control over accepting downloaded files from Windows Update. In a managed environment, however, it is unlikely that users will be allowed unlimited access to install updated drivers and other updated files; this function would normally be controlled in some fashion by the IT department. You can use Group Policy to block users from accessing Windows Update in the user interface or to specify an internal server for Windows Update to use when searching for updates. You can also disable Automatic Updates using Control Panel or Group Policy. Details on the methods and procedures for controlling these features are described in the following subsections.

How Windows Update and Automatic Updates Communicate with Sites on the Internet

This subsection summarizes the communication process:

- **Specific information sent or received**: Drivers and replacement files (critical updates, Help files, and Internet products) may be downloaded to the user's computer. The computer is uniquely identified and is logged in the download and installation success report, but the user is not uniquely identified.
- **Data storage and access**: Windows Update tracks the total number of unique computers that visit the Windows Update Web site. The success or failure of downloading and installing updates is also recorded but no personally identifiable information is recorded as part of this. This information is stored on servers at Microsoft with limited access that are located in controlled facilities. No other information collected during a Windows Update session is retained past the end of the session.

  For more information, see "Privacy statement," later in this list.

  Note If you want to block the use of the Windows Update Web site, you can apply Group Policy settings to specify an internal server for updates and for storing upload

statistics. For more information see "Procedures for Disabling Windows Update and Automatic Updates."

- **Default and recommended settings**: By default, operating systems in the Windows Server 2003 family provide access to the Windows Update Web site. Recommended settings are described in the next subsection, "Controlling Windows Update and Automatic Updates to Limit the Flow of Information to and from the Internet."
- **Triggers**: The user controls whether to run Windows Update. If Automatic Updates is enabled following setup, it is triggered about once per day when there is an Internet connection.
- **User notification**:
  - **Windows Update**: Users are notified when Windows Update downloads files to their computer, and they have control over whether to install those downloads.
  - **Automatic Updates**: Administrators can specify one of two notification settings for Automatic Updates:
    - Notify users before downloading and installing any updates.
    - Download the updates automatically and notify users when they are ready to be installed.

Note Administrators can also specify that updates be automatically downloaded and installed following a set schedule without user notification. For more information about these settings, click the **Learn more about automatic updating** link on the Automatic Updates dialog box.

- **Logging**: Automatic Updates logs events to the event log.
- **Encryption**: The data is transferred using HTTPS. The data packages downloaded to the user's system by Microsoft are digitally signed.
- **Privacy statement**: To view the privacy statement for Windows Update, see the Windows Update Web site, and click **Read our privacy statement**. The Windows Update Web site is located at:

  http://windowsupdate.microsoft.com/

  Automatic Updates is covered by the same privacy statement that covers Windows Update.
- **Transmission protocols and ports**: The transmission protocols and ports used are HTTP 80 and HTTPS 443.
- **Ability to disable**: You can use Group Policy to remove user access to Windows Update in the user interface. You can use Group Policy to specify an internal server to use for Windows Update and block it from searching the Windows Update Web site. You can disable Automatic Updates using Control Panel tools or Group Policy. Procedures for these methods are given at the end of this section.

Controlling Windows Update and Automatic Updates to Limit the Flow of Information to and from the Internet

The recommended methods for controlling Windows Update and Automatic Updates or both are as follows:

- You can use Group Policy settings to control Windows Update and Automatic Updates by removing end user access to Windows Update.

- You can block Windows Update from searching the Windows Update Web site by using Group Policy settings to specify an internal server for updates.
- You can use Control Panel or Group Policy settings to selectively disable Automatic Updates.
- You can control both Windows Update and Automatic Updates by blocking HTTP port 80 or HTTPS port 443 or both at the firewall.

See the following table for more information about the configuration options.

Configuration settings for Windows Update and Automatic Updates

Automatic Updates: Configuration tool	**Setting**	**Result**
Control Panel (Automatic Updates tool)	In the Automatic Updates dialog box, clear **Keep my computer up to date**.	Disables Automatic Updates.
Group Policy	Disable the **Configure Automatic Updates** policy setting in the Wuau.adm Group Policy template. For more information, see "Procedures for Disabling Windows Update and Automatic Updates," later in this section.	Disables Automatic Updates.
Windows Update and Automatic Updates: Configuration tool	**Setting**	**Result**
Firewall	Block HTTP port 80 or HTTPS port 443 or both.	Blocks Windows Update and Automatic Updates.
Group Policy	Enable the **Remove access to use all Windows Update features** policy setting in the Wuau.adm Group Policy template. For more information, see “Procedures for Disabling Windows Update and Automatic Updates," later in this section.	Blocks the user from accessing Windows Update in operating systems in the Windows Server 2003 family user interface. Also blocks Automatic Updates.
Group Policy	Enable the **Specify intranet Microsoft update service location** policy setting in the Wuau.adm Group Policy template. For more information, see "Procedures for Disabling Windows Update and Automatic Updates," later in this section.	Blocks Windows Updates from searching for updates on the http://windowsupdate.microsoft.com Web site. Instead, Windows Update searches for updates on a specified internal server.

How controlling Windows Update and Automatic Updates can affect users and applications

When you remove user access to Windows Update, Windows will still search for and download updates to the local computer. Users will not, however, be prompted to install downloaded updates, nor will they be able to access the Windows Update Web site from any of the following locations:

- The Windows Update option on the Start menu
- The Tools menu in Microsoft Internet Explorer

- The Windows Update button in Add New Programs (Add New Programs is in Control Panel under Add or Remove Programs)

Removing user access to Windows Update also disables Automatic Updates; that is, the user for which this policy setting is enabled will neither be notified about nor will receive critical updates from Windows Update. Removing user access to Windows Update is a user-based, not system-based, policy; other users on the same computer will still receive critical updates unless this policy setting is also enabled for those users individually.

Removing end user access to Windows Update also prevents Device Manager from automatically installing driver updates from the Windows Update Web site. For more information about controlling Device Manager, see the section of this white paper titled "Device Manager."

Blocking Windows Update and Automatic Updates will not block applications from running.

The Windows Update site is located at:

http://windowsupdate.microsoft.com/

Procedures for Disabling Windows Update and Automatic Updates

This subsection provides procedures for the following configurations:

- Specifying that Windows Update search an internal server, rather than the Windows Update Web site, for updates.
- Removing user access to Windows Update by using Group Policy, which will also block Automatic Updates.
- Disabling and configuring Automatic Updates by using Group Policy.
- Disabling Automatic Updates by using Control Panel tools.

To specify an internal server for Windows Update using Group Policy

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Update**.
3. In the details pane, double-click **Specify intranet Microsoft update service location**, supply the name of the internal server to function as the update server, and supply the name of the server to store upload statistics.
4. Click **Enabled**.

Important The upgrade server and the server you specify to store upload statistics can be the same server.

To remove user access to Windows Update using Group Policy

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in

Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.

2. Click **User Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Update**.
3. In the details pane, double-click **Remove access to use all Windows Update features**, and then click **Enabled**.

Important Removing user access to Windows Update also disables Automatic Updates.

To disable Automatic Updates using Group Policy

1. Use the resources described in Appendix B, "Resources for Learning About Group Policy," to learn about the Group Policy Management Console, and to find information in Help about Group Policy. Follow the instructions in Help to apply Group Policy objects (GPOs) to an organizational unit, a domain, or a site, as appropriate for your situation.
2. Click **Computer Configuration**, click **Administrative Templates**, click **Windows Components**, and then click **Windows Update**.
3. In the details pane, double-click **Configure Automatic Updates**, and then click **Disabled**.

To disable Automatic Updates using Control Panel tools

1. Click **Start**, and then either click **Control Panel**, or point to **Settings** and then click **Control Panel**.
2. Click **System**, and then click the **Automatic Updates** tab.
3. In the **Automatic Updates** dialog box, clear the **Keep my computer up to date** check box.

Appendix A: Resources for Learning About Automated Installation and Deployment

The following appendix provides:

- An overview of automated installation and deployment
- Procedures and resources for obtaining more information about automated installation and deployment

Overview: Automated Installation and Deployment

In the enterprise environment, it is often not cost-effective to install products in the Microsoft Windows Server 2003 family using the standard interactive setup on each computer. To greatly lower the total cost of ownership (TCO) and ensure configuration uniformity, you can perform an automated installation of any product in the Windows Server 2003 family on multiple computers. By using an automated installation method, you can ensure that certain components and applications are not available on your organization's computers, or that certain components and applications are preconfigured in such a way that helps prevent unwanted communication over the Internet.

Methods for automating the setup process

There are several options for automating the setup process. Any or all of the following tools can help ensure that all of your servers and clients are configured to appropriately limit communication over the Internet:

- Unattended setup using Setup (Winnt32.exe)

  Unattended setup enables you to simplify the process of setting up the operating system on multiple computers by running Setup unattended. To do this, you can create and use an answer file, which is a customized script that answers Setup questions automatically. Then you can run Setup (Winnt32.exe) from the command line with the appropriate options for invoking unattended setup.

  Using Winnt32.exe, you can upgrade your previous version of the operating system using all user settings from the previous installation, or you can perform a fresh installation using the answer file that provides Setup with your custom specifications. The latter method is most likely the best option to limit component communication over the Internet, provided you use an appropriate answer file. Details about specific answer file entries are included in the appropriate component sections of this white paper.

- Remote Installation Services (RIS)

  You can use RIS to create installation images of operating systems or of complete computer configurations, including desktop settings and applications. You can then make these installation images available to users at client computers. You can also specify which RIS server will provide installations to a given client computer, or you can allow any RIS server to provide the installation.

- Image-based installation using the System Preparation (Sysprep) tool

  Image-based installation is also a good choice if you need to install an identical configuration on multiple computers. On a master computer, you install the operating system and any applications that you want installed on all of the target computers. Then you run Sysprep and a disk imaging utility. Sysprep prepares the hard disk on the master computer so that the disk imaging utility can transfer an image of the hard disk to the

other computers. This method decreases deployment time dramatically compared to standard or scripted installations. You can customize the images so that only the files required for a specific configuration appear on the image, such as additional Plug and Play drivers that might be needed on various systems. The image can also be copied to a CD and distributed to remote sites that have slow links.

- System management software, such as Microsoft Systems Management Server (SMS)

  This type of software assists with the many tasks that are involved when you apply automated procedures to multiple servers and client computers throughout your organization. These tasks include:

  - Selecting computers that are equipped for the operating system and that you are ready to support.
  - Distributing the operating system source files to all sites, including remote sites and sites without technical support staff.
  - Monitoring the distribution to all sites.
  - Providing the appropriate user rights to do the upgrade.
  - Automatically initiating the installation of the software package with the possibility of having the user control the timing.
  - Resolving problems related to the distributions or installations.
  - Reporting on the rate and success of deployment.

Using system management software helps to further ensure that all computers within your organization have received the standardized operating system configuration that helps prevent unwanted communication over the Internet.

Using scripts for configuring computers

In addition to the automated installation methods described here, another common method of controlling Internet connections is to use a script to configure Group Policy on each client computer. The script can be sent to each client computer using a tool such as Microsoft Systems Management Server (SMS) and can run remotely using Windows Script Host. Alternatively, Group Policy can be applied to a domain, site, or organizational unit. The policy settings would then automatically be applied to every computer in the domain, site, or organizational unit the first time the computer starts after the operating system is installed. For more information about scripts and Group Policy, see “Related Documentation and Links," at the end of this section.

You can also use scripts to monitor activity on client computers and to take appropriate action if certain restricted activities occur. For example, if a user were to start an unauthorized application, a script could be used to detect this and to immediately stop that application. Similarly, scripts can be used to monitor the setup of each computer in order to, for example, determine which applications are installed and which folders are being shared. Configuring these scripts is beyond the scope of this document; however, you can refer to "Related Documentation and Links," at the end of this section for more information.

Procedures for Accessing Additional Information About Other Automated Setup Tools

Accessing the Windows Server 2003 Help documentation

Products in the Windows Server 2003 family have Help documentation describing unattended installation, RIS, and image-based installation. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any computer running a product in the Windows Server 2003 family. The following procedure gives the details.

To access the Help documentation for a computer running a product in the Windows Server 2003 family

1. Open Help and Support by doing one of the following:
   - On any computer running a product in the Windows Server 2003 family, click **Start**, and then click **Help and Support.**
   - View Help on the Web at:

     http://www.microsoft.com/windowsserver2003/proddoc/

     On this site, click the link for the appropriate product. You can then view the Help documentation by expanding the appropriate product listed under **Product Documentation** in the Help navigation pane, on the left.
2. Locate the specific topics as follows:
   - For unattended installation: Navigate to Getting Started\Installing and upgrading the operating system\Concepts\Planning for unattended Setup
   - For RIS: Navigate to Software Deployment\Remote Installation Services
   - For Winnt32.exe: Navigate to Administration and scripting tools\Command-line reference\Command-line reference A-Z\Winnt32

Related Documentation and Links

You can also find additional information about all of the topics described earlier in this appendix in a variety of other locations:

- On the CD for any product in the Windows Server 2003 family, you can find additional information about unattended installations in Deploy.chm in Support\Tools\deploy.cab.
- For extensive information about unattended setup, including information about Systems Management Server, see the *Microsoft Windows Server 2003 Deployment Kit*, especially the book titled *Automating and Customizing Installations*. The *Microsoft Windows Server 2003 Deployment Kit* is available on the Web at:

  http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx
- For general information about Group Policy, see the resources listed in Appendix B, "Resources for Learning About Group Policy."
- The Help documentation for the Windows Server 2003 family of products included on the CD and on the Web includes information about Windows Script Host. You can find the documentation on the Web at:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/sag_WSHtopnode.asp

Appendix B: Resources for Learning About Group Policy

The following appendix provides:

- An overview of Group Policy, including information about the new Microsoft Group Policy Management Console (GPMC)
- Procedures for obtaining more information about Group Policy

Overview: Group Policy

As described in earlier sections of this white paper, you can use Group Policy to configure many Microsoft Windows Server 2003 components in a way that will prevent users from accessing these components, or alternatively, in a way that will control how these components communicate with sites on the Internet. Group Policy settings define the various aspects of the user's desktop environment that a system administrator can manage; for example, the applications that are available to users and how those applications operate.

Group Policy includes **User Configuration** policy settings, which affect users, and **Computer Configuration** policy settings, which affect computers. Using Group Policy you can, among other tasks:

- Make certain Windows components unavailable to particular users.
- Assign scripts (such as computer startup and shutdown, and logon and logoff).
- Specify security options.
- Manage registry-based policy settings through Administrative Templates. Group Policy creates a set of default files that contain registry settings that are written to the User or Local Machine portion of the registry database. In addition, you can create custom Administrative Templates further extending Group Policy settings. User settings that are specific to a user who logs on to a given workstation or server are written to the registry under HKEY_CURRENT_USER (HKCU). Computer-specific settings are written under HKEY_LOCAL_MACHINE (HKLM).

How and when Group Policy is applied

User policy settings are obtained when a user logs on. Computer policy settings are obtained when a computer boots.

Order of application

Policy settings are applied in this order:

1. The unique local Group Policy object (GPO). (A GPO is a collection of policy settings.)
2. Group Policy objects for sites, in administratively specified order.
3. Group Policy objects for domains, in administratively specified order.
4. Group Policy objects for organizational units, from the largest to the smallest organizational unit (parent to child organizational unit), and in administratively specified order at the level of each organizational unit.

By default, policy settings applied later overwrite previously applied policy settings when there is an inconsistency. If the policy settings are not inconsistent, however, earlier and later policy settings both contribute to the effective policy.

Blocking policy inheritance

Policy settings that would otherwise be inherited from higher site, domain, or organizational units can be blocked at the site, domain, or organizational unit level.

Enforcing policy from above

Policy settings that would otherwise be overwritten by policy settings in child organizational units can be set to **No Override** at the Group Policy object level. Policy settings set to **No Override** cannot be blocked.

Group Policy Management Console

Along with the release of the Windows Server 2003 family of products, Microsoft is introducing a new administrative tool that unifies the management of Group Policy. The Microsoft Group Policy Management Console (GPMC) provides a single solution for managing tasks related to Group Policy.

GPMC lets administrators manage Group Policy for multiple domains and sites within a given forest, all in a simplified user interface (UI) with drag-and-drop support. Highlights include new functionality such as backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These operations can be fully scripted, which lets administrators customize and automate management. Together these advantages make Group Policy much easier to use and help you manage your enterprise more cost-effectively. For more information about GPMC, see the Web page at:

http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx

You can use GPMC to manage both Windows 2000 domains and Windows Server 2003 domains with Active Directory directory service. In either case, the administrative computer on which the tool itself runs must be running one of the following:

- A product in the Windows Server 2003 family.
- Windows XP Professional with Service Pack 1 (SP1), plus an additional post-SP1 hotfix, and the Microsoft .NET Framework.

We recommend that you use GPMC to make the Group Policy changes detailed earlier in this white paper. For users with at least one licensed copy of a product in the Windows Server 2003 family, GPMC can be downloaded for free by clicking the appropriate links on the following site:

http://www.microsoft.com/windowsserver2003/gpmc/

Procedures for Accessing Additional Information About Group Policy

For more information about how to use GPMC to make the Group Policy changes detailed in previous sections of this white paper, refer to the GPMC. Help for GPMC is installed when you install GPMC. This subsection provides instructions for viewing Help for GPMC, and also

for using Help and Support Center to view the set of Help topics that are available before you install GPMC.

To view Help for GPMC

1. On a computer running one of the operating systems listed in the previous subsection, use links on the following Web site to install GPMC:

   http://www.microsoft.com/windowsserver2003/gpmc/

2. Use one of the following methods (depending on your Taskbar and Start menu settings) to open GPMC:

   - Click **Start**, point to **Control Panel**, point to **Administrative Tools**, and then click **Group Policy Management**.
   - Click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Group Policy Management**.

3. In GPMC, click **Help** and then click **Help Topics**.

Note Additional information about GPMC can be found at the Web site listed in Step 1.

To view Group Policy Help documentation if you have not installed GPMC

1. Open Help and Support Center on any computer running a product in the Windows Server 2003 family by clicking **Start**, and then clicking **Help and Support**.
2. Click **Software Deployment**.
3. Click **Group Policy**.

Related Links

For more information about GPMC and Group Policy, see the following references:

- Detailed information about GPMC, as well as links for downloading GPMC, at:

  http://www.microsoft.com/windowsserver2003/gpmc/

- General information about Group Policy at:
  - http://www.microsoft.com/grouppolicy/
  - http://www.microsoft.com/technet/grouppolicy
- Deployment and reference information related to Group Policy for Windows Server 2003 in the Windows Deployment and Resource Kits at:

  http://www.microsoft.com/reskit/

- If you have clients in your organization running Windows XP, see the following resources:
  - "Using Group Policy to Manage Desktops," in the *Microsoft Windows XP Professional Resource Kit* (under Part II, Chapter 5, "Managing Desktops") at:

    http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/prda_dcm_jplq.asp

  - "Windows XP Professional Resource Kit, Group Policy Object Settings," at:

    http://www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp

- For information about how to create your own administrative templates for controlling application settings, see:

  http://www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp

Note Although some of the previous links lead to documentation written for Windows 2000 and Windows XP Service Pack 1, many of the topics described are also applicable to managing Group Policy on servers running a product in the Windows Server 2003 family.

Appendix C: Message Queuing

This section provides information about:

- The purposes of Message Queuing
- How Message Queuing communicates with sites on the Internet
- Controlling Message Queuing to prevent the flow of information to and from the Internet

Purposes of Message Queuing 3.0

Message Queuing (MSMQ) is one of the optional components in the Microsoft Windows Server 2003 family operating systems. Information about Message Queuing is presented here so you as an IT administrator can be aware of the potential capabilities for use within your organization's network, if you determine that you will be installing Message Queuing.

Message Queuing 3.0, the version in products in the Microsoft Windows Server 2003 family, is a message queuing service that enables applications on different systems to communicate with each other. Message Queuing implements asynchronous communication by enabling applications to send messages to and receive messages from other applications that may be running on the same computer or on different computers connected by a network. With Message Queuing, these applications can communicate across the Internet and other heterogeneous networks, and with computers that might be temporarily offline.

Overview: Using Message Queuing in a Managed Environment

Applications can use Message Queuing to send messages and to continue running regardless of whether the receiving application is running or reachable over the network. To create a message, an application specifies the message fields or properties and supplies the field values. The application then issues an MSMQ application programming interface (API) call to send the message. The MSMQ queue manager (the designated server) transmits the message to the destination message queue. If the destination location is not connected to the network when the message is sent, the message queuing system stores the message at an interim location. The system forwards the message automatically when a connection is established.

To receive a message, an application issues an API call that reads the message from the queue. When an application receives a request message, it processes the request by reading the contents of the message and acting accordingly. If required, the receiving application can send a response message back to the original requester. While in transit between senders and receivers, MSMQ keeps messages in holding areas called queues. MSMQ queues protect messages from being lost in transit and provide a place to retrieve messages when the receivers are ready to receive them.

Message Queuing 3.0 provides support for sending messages over the Internet. This support includes referencing queues by URLs, sending and receiving XML-based messages that are formatted using Simple Object Access Protocol (SOAP), and providing security for HTTP messaging. MSMQ also provides support for Web farms and firewalls. For more information about sending messages over the Internet, refer to "Related Links," later in this section.

It is beyond the scope of this white paper to describe all aspects of maintaining appropriate levels of security in an organization running applications that communicate across the Internet. This section, however, provides overview information as well as suggestions for other sources of information about balancing your organization's requirements for running Internet applications with your organization's requirements for protection of networked assets.

Controlling Message Queuing to Prevent the Flow of Information to and from the Internet

Installing and uninstalling Message Queuing

Message Queuing is not installed by default, however, if your organization has determined that MSMQ is an essential component of the business process it can be installed as described in this subsection. Although MSMQ is highly configurable, it is beyond the scope of this white paper to describe all the configuration options available to you. If you will be using MSMQ, you can refer to the "Related Links" subsection following these procedures for more detailed information about deploying Message Queuing.

To install or uninstall Message Queuing

1. Click **Start**, point to **Control Panel**, and click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components** (on the left).
3. In Windows Components, select **Application Server**, and then click **Details.**
4. Click **Message Queuing** and do one of the following:
   - If Message Queuing is installed and you want to remove it, clear the check box for **Message Queuing** and complete the Message Queuing wizard.
   - If Message Queuing is not installed and you want to add it, select the check box for **Message Queuing**.
5. If you are installing Message Queuing, select **Details**, select one or more of the options listed, and then click **Next**.

Accessing the operating system Help documentation for Message Queuing

The operating system has Help documentation describing the use of Message Queuing. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any server running a product in the Windows Server 2003 family.

To access the Help documentation for Message Queuing

- Open Help for the Windows Server 2003 family by doing one of the following:
  - Click **Start**, and then click **Help and Support**. Click **Application and Development Support**, and then click **Using Message Queuing**.
  - View Help on the Web at:

    http://www.microsoft.com/windowsserver2003/proddoc/

Related Links

For more information about Message Queuing, see the following references:

- The Message Queuing Web site at:

  http://www.microsoft.com/msmq/

- Frequently asked questions on the Message Queuing Web site at:

  http://www.microsoft.com/msmq/faq.htm

- Message Queuing developer resources:

  http://www.microsoft.com/msmq/developer.htm

- The Message Queuing and Queued Components (MSMQ) SDK documentation, as described in the following list:

  - "Using Message Queuing"

    http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msmq/msmq_using_intro_7fmv.asp

  - “Internet Messaging”

    http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msmq/msmq_about_messages_69k7.asp

  - “HTTP Messages”

    http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msmq/msmq_about_messages_2kab.asp

  - “New Features for Windows XP and the Windows Server 2003 family”

    http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msmq/msmq_about_newfeatures_114p.asp

  - Technical articles that can be found by navigating from the top level of the Message Queuing SDK on the Microsoft Developers Network Web site at:

    http://msdn.microsoft.com/library/en-us/msmq/msmq_overview_4ilh.asp

Appendix D: Connection Manager

This section provides information about:

- The benefits of Connection Manager 1.3
- How Connection Manager communicates with sites on the Internet
- Controlling Connection Manager to limit the flow of information to and from the Internet

Benefits and Purposes of Connection Manager 1.3

Connection Manager 1.3 is a client dialer and connection software program included with products in the Microsoft Windows Server 2003 family. It provides support for local and remote connections to your network service using a network of access points, such as those available worldwide through Internet service providers (ISPs). Connection Manager 1.3 includes features that both simplify and enhance the implementation of connection support for you and your users.

Connection Manager is implemented using the Connection Manager Administration Kit (CMAK). CMAK is designed for network administrators, information officers, and other team members who are responsible for the design, development, testing, distribution, and support of connection software for users who connect to your Internet or network service.

You can customize Connection Manager so that the set of files you distribute to your users (called a service profile) can be easily installed and run. Using Connection Point Services you install Phone Book Service, which enables the distribution of phone books for a Connection Manager service profile.

In addition to the support for basic dial-up connections, you can also use the CMAK wizard to incorporate support for virtual private network (VPN) connections using tunneling protocols to tunnel through a public network (such as when dialing into an ISP to access an organization's server). Connection Manager can create a VPN connection through a preexisting dial-up session, local area network (LAN), or digital subscriber line (DSL).

For more information about Connection Manager, see the instructions in "Accessing Help documentation for Connection Manager for the Windows Server 2003 family," later in this appendix.

How Connection Manager Communicates with Sites on the Internet

Administrators control whether to enable the phonebook download feature and which server the client computer sends the request to. The client computer initiates the connection to the phone book server in order to update its data. The phone book server sends one of the following elements to the Connection Manager client while there is a connection:

- Phone book update file: The server sends a phone book update file when the version of the phone book of the connecting client is earlier than the version of the phone book server.
- Replacement phone book: This is sent when there is a difference of more than five versions between the client and the server phone book file versions.
- Standard HTTP error message

The following list describes various aspects of the Connection Manager information that is sent to and from the Internet and how the exchange of information takes place:

- **Specific information sent or received**: The information sent by Connection Manager in the phone book server query string contains the following elements:
  - **osarch**: Specifies the type of processor that the requesting computer is using.
  - **ostype**: Specifies the version of the Windows operating system of the computer making the request.
  - **cmver**: Specifies the version of Connection Manager of the computer making the request.
  - **lcid**: Specifies the locale identifier (LCID) describing the system default locale information of the computer making the request.
  - **pbver**: Specifies the current version of the phone book being used by the computer making the request.
  - **pb**: Specifies the name of the phone book being used by the computer making the request.
- **Default settings**: By default, Connection Point Services and the Connection Manager Administration Kit are not installed with products in the Windows Server 2003 family. (You can add these components by using Add or Remove Programs in Control Panel.)
- **Triggers**: Connection Manager is triggered when users start it to connect to the Internet or their organization's network.
- **Logging**: Information is logged in the Connection Manager log file but not in the operating system event log. The logging feature for Connection Manager is used for troubleshooting and can be disabled.
- **Encryption**: The information contained in the query string is sent as plaintext and is not encrypted.
- **Storage**: The information that is sent is used by the phone book server to process the request being made, although the information is not stored.
- **Transmission protocol and port**: The transmission protocol used is HTTP and the port is 80.
- **Ability to disable**: On the server, you can prevent Connection Point Services and the Connection Manager Administration Kit from being installed, which prevents Connection Manager from being used. For clients, you can disable Connection Manager by not providing the user with a Connection Manager service profile. Also for clients, the Connection Manager phone book download and synchronization feature can be disabled using a Connection Manager service profile.

For more information about the Connection Manager Administration Kit (CMAK), see "Before you start: Understanding Connection Manager and the Administration Kit," on the Microsoft Web site at:

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/cmak_ops_03.asp

You can also view the same information in Help, as described in "Accessing Help documentation for Connection Manager for the Windows Server 2003 family," later in this appendix.

Controlling Connection Manager to Limit the Flow of Information to and from the Internet

Connection Manager client software is installed by default. Administrators determine when to create and distribute a Connection Manager service profile, without which Connection Manager cannot run.

You can limit the use of Connection Manager by creating and distributing a service profile only to users and administrators who need to use the Connection Manager client to initiate local or remote network access point connections. You can use the Connection Manager Administration Kit (CMAK) wizard to create a customized service profile to configure Connection Manager not to update the client phone book information.

Procedures for Installing the Connection Manager Administration Kit and for Viewing Help

This subsection lists procedures for the following tasks:

- Installing the Connection Manager Administration Kit on your server
- Accessing Help documentation for Connection Manager for the Windows Server 2003 family

Installing Connection Manager Administration Kit on your server

The Connection Manager Administration Kit (CMAK) and Connection Point Services (used to install Phone Book Service) are not installed by default on products in the Windows Server 2003 family. Use the following procedure to add these components.

To add the Connection Manager Administration Kit and Connection Point Services after server installation

1. Click **Start**, point to **Control Panel**, and click **Add or Remove Programs**.
2. Click **Add/Remove Windows Components** (on the left).
3. In the Windows Components Wizard scroll down and double-click **Management and Monitoring Tools**.
4. Select **Connection Manager Administration Kit** and **Connection Point Services** and any other subcomponents you want to install.
5. Follow the instructions to complete the Windows Components Wizard.

Accessing Help documentation for Connection Manager for the Windows Server 2003 family

Products in the Windows Server 2003 family have Help documentation describing the Connection Manager Administration Kit. You can view this documentation from any computer that has Internet access (regardless of the operating system running on that computer), or from any server running a product in the Windows Server 2003 family. The following procedure provides the details.

To access Help documentation for a server running a product in the Windows Server 2003 family

1. Open Help for a product in the Windows Server 2003 family by doing one of the following:
   - On any computer running a product in the Windows Server 2003 family, click **Start**, and then click **Help and Support**.
   - View Help on the Web at:

     http://www.microsoft.com/windowsserver2003/proddoc/

     As appropriate, navigate from this Web site to the documentation for the server product you are using.
2. To view information about Connection Manager Administration Kit, navigate to Network Services\Managing Remote Connections\Connection Manager Administration Kit.

Related Links

For information about the Connection Manager Administration Kit (CMAK), see the following Web site:

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/cmak_ops_03.asp

Appendix E: Passport Manager Administration

The following appendix provides information about:

- The benefits and purposes of Passport Manager Administration
- Using Passport Manager Administration in a managed environment
- Resources for learning about Passport Manager Administration

Benefits and Purposes of Passport Manager Administration

Passport Manager Administration is a utility designed for use on Web sites on which you want to use Microsoft .NET Passport for authentication. In Microsoft Server 2003 family operating systems, Passport Manager Administration provides a graphical-interface alternative to editing the registry to change Passport Manager object settings. The most common use of the Passport Manager Administration utility is to change the default object settings that Passport Manager methods use if certain optional parameters are omitted when the methods are called.

Although some parameters of Microsoft .NET Passport methods are listed as optional, these methods still generate URLs or results that reflect inherent default values when called. These default parameter values can be used to provide consistent values for your Web site, such as the required time window within which all users must be authenticated.

Primary default object settings that affect Passport Manager implementation include: Time Window, Force Login, and Language ID.

Using Passport Manager Administration in a Managed Environment

By configuring options in Passport Manager Administration to work with software on your Web site, you can control how Web browsers are authenticated to your Web site. With Passport Manager Administration, you can configure the settings for cookies, such as choosing to disable the use of cookies. You can also choose to have cookies deleted once users sign out of your Web site. (Cookies are a form of data passed both ways between Web browsers and servers. Cookies sent to a user's browser have some implications for privacy.)

To ensure that cookies are deleted when users sign out of a Web site, make sure the following conditions are met:

- The Site ID value in Passport Manager Administration should be the value given to you when you received your Passport encryption key.
- The path and file name of the page to which cookies are written (specified in Passport Manager Administration) should match the ExpireCookieURL provided when you registered your site. Also, if cookies are written to a page in a subdomain of your own domain, you should precede the domain path with a dot (“.”).
- The path to the page where cookies are written should be the root directory of the Web site. This ensures that cookies written to all possible paths are deleted. If this is not done, not all the cookies may be deleted.

- If your site uses multiple servers with Passport Manager installed on them, you should verify that all of the servers are writing the cookies to the same domain and path.

Related Links

You can find additional information about Passport Manager Administration at these sites:

- The Help file for Passport Manager Administration utility provides detailed information about configuring settings for this utility. You can find this Help file at:

  http://msdn.microsoft.com/library/default.asp?url=/library/en-us/passport25/NET_Passport_VBScript_Documentation/NET_Passport_Fundamentals/Passport_Manager_Administration_Utility.asp

- For more information about .NET Passport and how to download it, see the SDK documentation on the MSDN Web site at:

  http://msdn.microsoft.com/library/default.asp?url=/downloads/list/websrvpass.asp

Appendix F: Internet Connection Sharing and Related Networking Features

Internet Connection Sharing, Internet Connection Firewall, and Network Bridge are features designed for home and small office networks. These features are offered in some of the Microsoft Windows Server 2003 family operating systems. Information about these features is presented here so you as an IT administrator can be aware of these potential capabilities within your organization's network.

These home and small office features are included only with Windows Server 2003, Standard Edition, and Windows Server 2003, Enterprise Edition. These features are not included with Windows Server 2003, Web Edition; Windows Server 2003, Datacenter Edition; or the 64-bit versions of the Windows Server 2003 family.

This appendix includes the following information:

- An overview of Internet Connection Sharing and related networking features.
- How Internet Connection Sharing and related features can be used in a large organization's network.
- How to control or prevent the use of Internet Connection Sharing and related features.

Overview: Internet Connection Sharing and Related Networking Features

The features for implementing and administering small networks are described as follows:

- Internet Connection Sharing (ICS)

  ICS provides Internet access for a home or small office network by using one common connection as the Internet gateway. The ICS host is the only computer that is directly connected to the Internet. Multiple ICS clients simultaneously use the common Internet connection and benefit from Internet services as if the clients were directly connected to the Internet service provider (ISP). Security is enhanced when ICS is enabled because only the ICS host computer is visible to the Internet. The addresses of ICS clients are hidden from the Internet rendering ICS clients invisible to the Internet. In addition, ICS simplifies the configuration of small networks by providing local private network services, such as name resolution and addressing.

  Note You should not use Internet Connection Sharing in an existing network with Windows 2000 Server domain controllers, Domain Name System (DNS) servers, gateways, Dynamic Host Configuration Protocol (DHCP) servers, or systems configured for static IP addresses.

- Internet Connection Firewall (ICF)

  With ICF, the firewall checks all communications that cross the connection between your network and the Internet and is selective about which responses from the Internet it allows. ICF protects only the computer on which it is enabled. If ICF is enabled on the Internet Connection Sharing (ICS) host computer, however, ICS clients that use the shared Internet connection for Internet connectivity are protected because they cannot be seen from outside your network. For this reason, you should always enable ICF on the ICS host computer. In addition, if there are clients on your network with direct Internet connections, or if you have a stand-alone computer that is connected to the Internet, then you should enable ICF on those Internet connections as well.

- Network Bridge

  Network Bridge removes the need for routing and bridging hardware in a home or small office network that consists of multiple LAN segments. With Network Bridge, multiple LAN segments become a single IP subnet, even if the LAN segments are of mixed network media types. Network Bridge automates the configuration and management of the address allocation, routing, and name resolution that is typically required in a network that consists of multiple LAN segments.

  Caution If neither ICF nor ICS is enabled on your network, do not set up Network Bridge between the public Internet connection and the private network connection. Setting up Network Bridge between the public Internet connection and the private network connection creates an unprotected link between your network and the Internet, leaving your network vulnerable to external attacks. When either ICF or ICS is enabled, this risk is mitigated.

Using Internet Connection Sharing and Related Features in a Managed Environment

Internet Connection Sharing, Internet Connection Firewall, and Network Bridge are not enabled by default, and Internet Connection Sharing (ICS) is available only on computers that have two or more network connections. An administrator or user with administrative credentials can enable ICS by clicking the **Advanced** tab on network connections (Control Panel\Network Connections). Also, when running the New Connection Wizard, administrators can choose to enable ICS. ICS lets administrators configure a computer as an Internet gateway for a small network, and it provides network services such as name resolution through Domain Name System (DNS). It also provides addressing through Dynamic Host Configuration Protocol (DHCP) to the local private network.

Using Internet Connection Firewall, an administrator can enable a firewall to protect the public connection of a small network or single computer that is connected to the Internet. ICF is considered a "stateful" firewall. A stateful firewall is one that monitors all aspects of the communications that cross its path and inspects the source and destination address of each message that it handles.

Any organization that uses domain controllers, DHCP, DNS, and other elements of network infrastructure should not use ICS and ICF, but can instead use a firewall designed for the entire organization.

The Network Bridge menu command **Bridge Connections** is available only when two or more network adapters are present. By default, Network Bridge is disabled, but administrators can use **Bridge Connections** to enable Network Bridge. In a domain environment you should not allow the capability to enable or configure these features. See the following subsection for information about how to disable them.

It is important to be aware of all the methods users and administrators have for connecting to your networked assets, and to review whether your security measures provide in-depth defense (as contrasted with a single layer of defense, more easily breached).

Controlling the Use of Internet Connection Sharing and Related Features

You can block administrators from accessing ICS, ICF, and Network Bridge by using answer files during initial installation and Group Policy post-deployment.

Using answer files for unattended or remote installation

Using standard methods for preparing an unattended or remote installation you can make entries in the [Homenet] section of the answer file. This section includes entries for installing home and small office networking settings for network adapters, Internet Connection Sharing, Internet Connection Firewall, and Network Bridge. For example, to prevents users and administrators from enabling Internet Connection Sharing by using an answer file, the entry is as follows:

```
[Homenet]
EnableICS = No
```

For additional configuration options for [Homenet] entries for the answer file, and for more information about unattended installation, see the references listed in Appendix A, "Resources for Learning About Automated Installation and Deployment." Be sure to review the information in the Deploy.chm file (whose location is provided in that appendix).

Using Group Policy

Group Policy settings for disabling small office networking features in your domain environment are described as follows:

- **Prohibit use of Internet Connection Sharing on your DNS domain network**

  This policy setting determines whether administrators can enable and configure the Internet Connection Sharing (ICS) feature on a connection. It also determines if ICS can run on a computer when the computer is connected to the DNS domain in which the policy setting is applied.

- **Prohibit use of Internet Connection Firewall on your DNS domain network**

  This policy setting determines whether administrators can enable and configure the Internet Connection Firewall feature on a connection.

- **Prohibit installation and configuration of Network Bridge on your DNS domain network**

  This policy setting determines whether administrators can enable and configure Network Bridge on your domain.

  Important These policy settings are dependent on the network context that the computer is in. They apply only when a computer is connected to the same DNS domain network it was connected to when the policy setting was refreshed on that computer. If a computer is connected to a DNS domain network other than the one it was connected to when the policy setting was refreshed, the policy setting does not apply.

These policy settings are located in Computer Configuration\Administrative Templates\Network\Network Connections. Configuration options are described in the following table.

Group Policy settings for controlling ICS, ICF, and Network Bridge

Policy setting	Description
Prohibit Use of Internet Connection Sharing on your DNS domain network (enabled)	If you enable this policy setting, ICS cannot be enabled or configured by administrators, and the ICS service cannot run on the computer. The Advanced tab in the Properties dialog box for a local area network (LAN) or remote access connection is removed. The Internet Connection Sharing page is removed from the New Connection Wizard. The Network

	Setup Wizard is disabled.
Prohibit Use of Internet Connection Sharing on your DNS domain network (disabled or not configured)	If you disable this policy setting or do not configure it and have two or more connections, administrators can enable ICS. The Advanced tab in the Properties dialog box for a LAN or remote access connection is available. In addition, the administrator is presented with the option to enable Internet Connection Sharing in the Network Setup Wizard and Make New Connection Wizard. (The Network Setup Wizard is available only in Windows XP Professional.)
Prohibit Use of Internet Connection Firewall on your DNS domain network (enabled)	If you enable this policy setting, Internet Connection Firewall cannot be enabled or configured by administrators, and the Internet Connection Firewall service cannot run on the computer. The option to enable the Internet Connection Firewall through the Advanced tab is removed. In addition, the Internet Connection Firewall is not enabled for remote access connections created through the Make New Connection Wizard. The Network Setup Wizard is disabled.
Prohibit Use of Internet Connection Firewall on your DNS domain network (disabled or not configured)	If you disable this policy setting or do not configure it, the Internet Connection Firewall is disabled when a LAN connection or virtual private network (VPN) connection is created, but administrators can use the Advanced tab in the connection properties to enable it. The Internet Connection Firewall is enabled by default on the connection for which Internet Connection Sharing is enabled. In addition, remote access connections created through the Make New Connection Wizard have Internet Connection Firewall enabled.
Prohibit installation and configuration of Network Bridge on your domain network (enabled)	When you enable this policy setting administrators cannot create a Network Bridge. Enabling this policy setting does not remove an existing Network Bridge from a computer.
Prohibit installation and configuration of Network Bridge on your domain network (disabled or not configured)	If you disable this policy setting or do not configure it, an administrator will be able to create and modify the configuration of a Network Bridge.

For more information about home and small office networking features, see Help and Support Center for the Windows Server 2003 family.

Appendix G: Add Network Place Wizard

In the Microsoft Windows Server 2003 family operating systems, users and administrators can use the Add Network Place Wizard to create shortcuts to shared folders and resources on the network or on Web or File Transfer Protocol (FTP) servers. If you don't have folders on a Web server already, the Add Network Place Wizard helps you create a new folder for storing files online.

The content in this appendix includes the following information:

- An overview of the Add Network Place Wizard
- How to control the use of the Add Network Place Wizard

Overview: Add Network Place Wizard

The Add Network Place Wizard is enabled by default for all users. In operating systems in the Windows Server 2003 family you access the wizard through Windows Explorer\My Network Places. After you click **My Network Places** and then double-click **Add Network Place**, the wizard appears.

You can use the wizard to sign up for a service that offers online storage space, or to create a shortcut to a Web site, an FTP site, or other local network connection. To add a shortcut in My Network Places to a folder on a Web server, the Web server must support network places. Support for network places requires the Web Extender Client (WEC) protocol and Microsoft FrontPage® Server Extensions, or the Web Distributed Authoring and Versioning (WebDAV) protocol and Internet Information Services (IIS). You must also have read and write access to the Web server.

In a highly managed network environment administrators might want to prevent users or administrators from storing or accessing folders on a Web server. You can remove access to the Add Network Place Wizard using Group Policy.

For more information about the WEC and WebDAV protocols, see Help and Support Center.

Controlling the Use of the Add Network Place Wizard

You can block users and administrators from accessing the Add Network Place Wizard in My Network Places by configuring a Group Policy setting.

Configure the following Group Policy setting in User Configuration\Administrative Templates\Windows Components\Windows Explorer: **Remove "Map Network Drive" and "Disconnect Network Drive."**

When you enable this policy setting, in addition to preventing users from using Windows Explorer or My Network Places to map or disconnect network drives, you also remove the Add Network Place option from My Network Places. Users can still connect to another computer on your intranet by typing the name of a shared folder in the Run dialog box.

> **Note** This policy setting was documented incorrectly on the Explain tab in Group Policy for Windows 2000. That Explain tab states incorrectly that this policy setting prevents users from connecting and disconnecting drives.

Appendix H: New Connection Wizard

In Microsoft Windows Server 2003 family operating systems you use the New Connection Wizard to create Internet and other types of network connections for home and small office networks. While this feature is designed for home and small office use, information about this feature is presented here so IT administrators can be aware of these potential capabilities within your organization's network.

The content in this appendix includes the following information:

- An overview of the New Connection Wizard
- How to control the use of the New Connection Wizard

Overview: New Connection Wizard

The New Connection Wizard in Windows Server 2003 family operating systems replaces the Windows 2000 Network Connection Wizard and Internet Connection Wizard. Administrators for a home or small office network can use the New Connection Wizard to create any type of network connection including Internet, incoming, dial-up, virtual private network (VPN), and direct connection.

Administrators can create a new connection through Control Panel\Network Connections. When you click **Create a new connection**, the wizard guides you through this process. In a highly managed network environment you might want to prevent administrators as well as users from creating new connections.

> **Note** The Internet Connection Wizard still appears when you first click any program that requires an Internet connection, such as Microsoft Internet Explorer. The Internet Connection Wizard can also be started from Outlook Express, if a link for **Set up a Mail account** or for **Set up a Newsgroups account** is visible and you click the link. You can disable the Internet Connection Wizard in Group Policy through User Configuration\Administrative Templates\Windows Components\Internet Explorer.

Controlling the Use of the New Connection Wizard

You can block administrators and users from using the New Connection Wizard by configuring Group Policy. The following two Group Policy settings are in User Configuration\Administrative Templates\Network\Network Connections:

- **Prohibit Access to the New Connection Wizard**

  This policy setting determines whether users, including administrators, can use the New Connection Wizard, which creates new Internet or intranet connections.

  > **Important** If the policy setting **Enable Windows 2000 Network Connections settings for Administrators** is disabled or not configured, **Prohibit Access to the New Connection Wizard** will not apply to administrators on computers running Windows XP.

- **Enable Windows 2000 Network Connections settings for Administrators**

  This policy setting determines whether policy settings that exist in Windows 2000 will apply to administrators. The set of Network Connections policy settings that exists in Windows 2000 also exists in Windows XP. In Windows 2000, all of these policy settings have the ability to prohibit the use of certain features by administrators. By default,

Network Connections policy settings in Windows XP do not prohibit the use of features from administrators.

Note This policy setting is intended to be used in a situation in which the Group Policy object (GPO) contains computers running both Windows 2000 and Windows XP and identical Network Connections policy setting behavior is required between those computers.

Configuration options for these policy settings are presented in the following table.

Group Policy settings for controlling the use of the New Connection Wizard

Policy setting	Description
Prohibit Access to the New Connection Wizard (enabled)	If you enable this policy setting (and enable the **Enable Network Connections settings for Administrators** policy setting), the Make New Connection icon does not appear in the Start menu or in the Network Connections folder. As a result, users (including administrators) cannot start the New Connection Wizard.
Prohibit Access to the New Connection Wizard (disabled or not configured)	If you disable this policy setting or do not configure it, the Make New Connection icon appears in the Start menu and in the Network Connections folder for all users (except in a workgroup environment where only administrators can access this wizard). Clicking the Make New Connection icon starts the New Connection Wizard. Changing this policy setting from enabled to not configured does not restore the Make New Connection icon until the user logs off or on. When other changes to this policy setting are applied, the icon does not appear or disappear in the Network Connections folder until the folder is refreshed.
Enable Windows 2000 Network Connections settings for Administrators (enabled)	If you enable this policy setting, the Windows XP policy settings that exist in Windows 2000 can prohibit administrators from using certain features (see the policy settings in the Network Connections folder). With this policy setting enabled, policy settings that exist in both Windows 2000 and Windows XP behave the same for administrators.
Enable Windows 2000 Network Connections settings for Administrators (disabled or not configured)	If you disable this policy setting or do not configure it, Windows XP policy settings that exist in Windows 2000 will not apply to administrators.

For information about using Group Policy, see Appendix B, "Resources for Learning About Group Policy."

Related Links

This section contains a list of the Web sites found in other sections of this white paper, with some additional Web sites that provide general information about Microsoft products.

Links to product information, support information, TechNet, Microsoft Developer Network, and information in Resource Kits

The following sites provide information about products in the Windows Server 2003 family and other Microsoft products. The list includes sites containing product Help as well as other basic sites that provide information about Microsoft operating systems and other Microsoft products:

- Products in the Windows Server 2003 family:
  - http://www.microsoft.com/windowsserver2003/
  - http://www.microsoft.com/windowsserver2003/techinfo/
- Windows Server 2003 Help on the Web:

  http://www.microsoft.com/windowsserver2003/proddoc/

  For links to specific topics in Help, see the following sections of the white paper: "Hyperterminal"; Appendix A, "Resources for Learning About Automated Installation and Deployment"; and Appendix D, "Connection Manager."
- Windows Catalog:

  http://www.microsoft.com/windows/catalog/server/
- Microsoft Product Support Services:

  http://support.microsoft.com/
- Microsoft TechNet:

  http://www.microsoft.com/technet/
- Microsoft Developer Network:

  http://msdn.microsoft.com/
- Prescriptive Architecture Guides:

  http://www.microsoft.com/technet/itsolutions/idc/pag/pag.asp
- Windows Deployment and Resource Kits:

  http://www.microsoft.com/reskit/
- Internet Explorer Administration Kit:

  http://www.microsoft.com/windows/ieak/
- *Microsoft NetMeeting 3 Resource Kit* (the NetMeeting section in this white paper provides links to specific chapters in this kit):
  - http://www.microsoft.com/technet/prodtechnol/netmting/reskit/netmtg3/cover.asp
  - http://www.microsoft.com/windows/NetMeeting/Corp/ResKit/

Links to information about security, management, and deployment

The following sites provide information about security, management, and deployment topics:

- Managing mobile code:

  http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/mblcode.asp

- Best practices for enterprise security:

  http://www.microsoft.com/technet/security/bestprac/bpent/bpentsec.asp

- Links to a variety of security topics:

  http://www.microsoft.com/technet/security/

- *Microsoft Windows Server 2003 Deployment Kit*:

  http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx

  For deployment information in Resource Kits for other products, see the Windows Deployment and Resource Kits Web site:

  http://www.microsoft.com/reskit/

- Controlling communication with the Internet in an organization using Windows XP Professional with Service Pack 1:

  http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/xpmanaged/00_abstr.asp

- Controlling communication with the Internet in an organization using Windows 2000 with Service Pack 3:

  http://www.microsoft.com/technet/prodtechnol/windows2000pro/maintain/w2kmngd/00_abstr.asp

Links to information about components in Windows Server 2003 or tools you can use with Windows Server 2003

The following sites provide information about some of the components in the Windows Server 2003 family:

- Certificates, certificate status, and certificate revocation:
  - http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/WinXPPro/support/tshtcrl.asp
  - http://www.microsoft.com/technet/security/prodtech/pubkey/default.asp
- Driver Protection:

  http://www.microsoft.com/hwdev/driver/drv_protect.asp

- Dynamic Update:

  http://www.download.windowsupdate.com/msdownload/update/v3/static/DUProcedure/Dynamic Update.htm

- Hyperterminal:

  http://www.hilgraeve.com/support/faq/index.html

  (Web addresses can change, so you might be unable to connect to the Web site or sites mentioned here.)

- Internet Explorer:

  - http://www.microsoft.com/windows/ie/
  - http://www.microsoft.com/windowsserver2003/docs/IESecConfig.doc

  For additional information about Internet Explorer, see "Internet Explorer Administration Kit" in "Links to product information, support information, TechNet, Microsoft Developer Network, and information in Resource Kits," earlier in this section.

- Internet Explorer and File association Web service, language codes (relates to registry settings used for specifying language):

  http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wceielng/htm/cooriMLangRegistrySettings.asp

- Internet Information Services:
  - http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/iis.mspx
  - http://www.microsoft.com/windowsserver2003/techinfo/overview/iis.mspx
  - http://www.microsoft.com/technet/prodtechnol/iis/default.asp
- Internet Protocol version 6:

  http://www.microsoft.com/windowsserver2003/technologies/ipv6/

- Message Queuing and the Message Queuing SDK:
  - http://www.microsoft.com/msmq/
  - http://www.microsoft.com/msmq/developer.htm
  - http://www.microsoft.com/msmq/faq.htm
  - http://msdn.microsoft.com/library/en-us/msmq/msmq_overview_4ilh.asp

  For links to specific topics in the Message Queuing SDK, see "Appendix C: Message Queuing."

- NetMeeting, and also the Real-Time Communications (RTC) technology:
  - http://www.microsoft.com/rtc/
  - http://www.microsoft.com/windows/NetMeeting/
  - http://www.microsoft.com/technet/prodtechnol/netmting/evaluate/nm3feats.asp
  - http://support.microsoft.com/default.aspx?scid=KB;en-us;158623
  - http://support.microsoft.com/default.aspx?scid=/support/netmeeting/howto/default.asp

  For additional information about NetMeeting, see the *Microsoft NetMeeting 3 Resource Kit* in "Links to product information, support information, TechNet, Microsoft Developer Network, and information in Resource Kits," earlier in this section.

- Passport Manager Administration:
  - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/passport25/NET_Passport_VBScript_Documentation/NET_Passport_Fundamentals/Passport_Manager_Administration_Utility.asp
  - http://msdn.microsoft.com/library/default.asp?url=/downloads/list/websrvpass.asp
- Remote Assistance:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;300692

- Search Companion:

http://sa.windows.com/privacy/

- Terminal Server Licensing (and Terminal Server):
  - https://activate.microsoft.com/prpolicy.asp
  - http://www.microsoft.com/windowsserver2003/howtobuy/licensing/overview.mspx
  - http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx
- Windows Error Reporting:
  - http://watson.microsoft.com/dw/1033/dcp.asp
  - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/windows_error_reporting.asp
  - http://oca.microsoft.com/en/cerintro.asp
- Windows Media Player:
  - http://www.microsoft.com/windows/windowsmedia/
  - http://www.microsoft.com/Windows/WindowsMedia/enterprise/TechResources/default.aspx
  - http://www.microsoft.com/Windows/WindowsMedia/howto/articles/intranet.aspx
- Windows Media Services:
  - http://www.microsoft.com/windows/windowsmedia/
  - http://www.microsoft.com/MSPress/books/6280.asp
  - http://www.microsoft.com/Windows/WindowsMedia/enterprise/TechResources/default.aspx
  - http://www.microsoft.com/Windows/WindowsMedia/howto/articles/intranet.aspx
  - http://www.microsoft.com/windows/windowsmedia/9series/server.aspx
  - http://www.microsoft.com/windows/windowsmedia/distribute.aspx
  - http://msdn.microsoft.com/library/en-us/dnwmt/html/RedisWMedC.asp
  - http://msdn.microsoft.com/downloads/list/winmedia.asp
- Windows Time Service. For more information about configuring Windows Time Service during deployment of products in the Windows Server 2003 family, see *Designing and Deploying Directory and Security Services* and *Designing a Managed Environment* in the *Microsoft Windows Server 2003 Deployment Kit* at:

  http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx
- Windows Update:
  - http://windowsupdate.microsoft.com/
  - http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp

The following site provides information about using tools that work with the Windows Server 2003 family:

- Windows Application Compatibility Toolkit:

  http://www.microsoft.com/windows/appexperience/

Links to information about licensing, product activation, and registration

The following sites provide information about licensing, product activation, and registration:

- http://www.microsoft.com/licensing/
- http://www.microsoft.com/piracy/basics/activation/
- http://www.microsoft.com/piracy/basics/activation/apolicy.asp
- http://www.microsoft.com/piracy/basics/activation/prvcyms.asp

Links to sites maintained by task forces and other organizations

The following sites are maintained by the Internet Engineering Task Force:

- http://www.ietf.org/html.charters/ngtrans-charter.html
- http://www.ietf.org/rfc/rfc2373.txt?number=2373/
- http://www.ietf.org/rfc/rfc3056.txt?number=3056/

The following sites are maintained by the International Multimedia Telecommunications Consortium:

- http://www.imtc.org/
- http://www.imtc.org/h323.htm

The following site is maintained by the International Telecommunication Union:

- http://www.itu.int/home/index.html

(Web addresses can change, so you might be unable to connect to the Web sites mentioned here.)

Links to information about Group Policy

The following sites provide information about topics related to Group Policy:

- General information about Group Policy:
  - http://www.microsoft.com/grouppolicy/
  - http://www.microsoft.com/technet/grouppolicy
- Group Policy Management Console:
  - http://www.microsoft.com/windowsserver2003/gpmc/
  - http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx
- Group Policy Object settings spreadsheet:
  http://www.microsoft.com/WindowsXP/pro/techinfo/productdoc/gpss.asp
- Using Group Policy to manage desktops:
  http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/prda_dcm_jplq.asp
- Implementing Registry-Based Group Policy:
  http://www.microsoft.com/windows2000/techinfo/howitworks/management/rbppaper.asp