CHAPTER 3

Securing Web Sites and Applications

Because the day-to-day operations of your organization depend on the mission-critical applications that are running on Internet Information Services (IIS) 6.0 Web servers, your Web sites and applications need the highest possible security. When you install IIS 6.0, it is installed in a highly secure and locked configuration. Depending on your Web sites and applications, you might need to configure IIS to be less restrictive so that your Web sites and applications can operate correctly. Your Web sites and applications might also need increased security configuration to authenticate users or to restrict the Web sites, applications, and data that can be accessed by users.

In This Chapter

Related Information

- For information about ASP.NET-specific deployment considerations, see “Deploying ASP.NET Applications in IIS 6.0” in this book.
- For information about balancing application security and availability, see “Ensuring Application Availability” in this book.

Overview of the Securing Web Sites and Applications Process

To provide comprehensive security for your Web sites and applications, you must ensure that the entire Web server, including each Web site and application that the server hosts, is protected from unauthorized access. Also, you might have to ensure that the Web sites and applications are protected from other Web sites and applications that are hosted on the same server. Finally, you need to initiate practices to help ensure that your Web sites and applications remain secure.

For security reasons, IIS 6.0 is not installed by default on the Microsoft® Windows® Server 2003, Standard Edition; Windows® Server 2003, Enterprise Edition; and Windows® Server 2003, Datacenter Edition operating systems. When you install IIS 6.0, it is locked down — only request handling for static Web pages is enabled, and only the World Wide Web Publishing Service (WWW service) is installed. Features such as Active Server Pages (ASP), ASP.NET, Common Gateway Interface (CGI) scripting, FrontPage® 2002 Server Extensions from Microsoft, and Web Distributed Authoring and Versioning (WebDAV) do not work by default. You can serve dynamic content and enable these features in the Web Service Extensions node in IIS Manager.

Before you begin this process, complete the following steps:

- Install Windows Server 2003 with the default options.
- Install IIS 6.0 with the default settings in **Add or Remove Programs** in Control Panel.

If you use other methods for installing and configuring Windows Server 2003, such as unattended setup, or enabling IIS 6.0 by using Manage Your Server, then the default configuration settings might not be identical.

Upon completing the process outlined in this chapter, you will have a Web server running IIS 6.0 that fulfills your security requirements. However, to maintain the security of your server, you need to implement continuing security practices such as security monitoring, detection, and response. For more information about maintaining Web server security, see "Managing a Secure IIS Solution in *Internet Information Services (IIS) 6.0 Resource Guide* of the *Microsoft® Windows® Server 2003 Resource Kit*.

Note

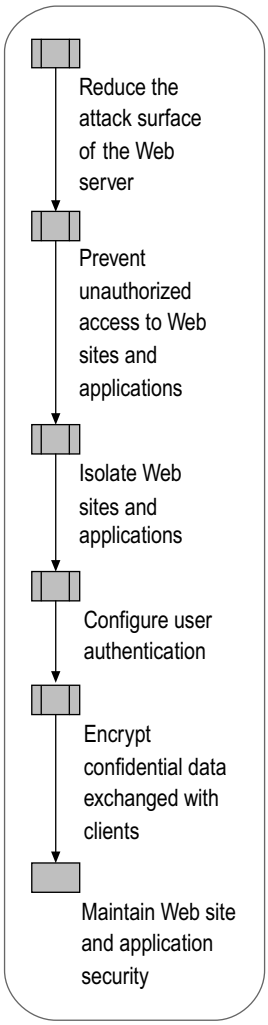
The security settings described in this chapter are appropriate for Web sites and applications that are hosted on Web servers on an intranet and the Internet, unless specifically noted.

Although not the focus of this chapter, you can apply many of the security recommendations described in this chapter to enhance the security of Web servers that have been upgraded from earlier versions of IIS.

Process for Securing Web Sites and Applications

To configure security for Web sites and applications that are hosted on a newly installed Web server, you need to follow certain security practices, such as enabling only the *Web service extensions* that you need. Web service extensions provide content and features beyond serving static Web pages. Any dynamic content that is served by the Web server is done by using Web service extensions, such as content and features that are provided by ASP, ASP.NET, or CGI. In addition, each Web site and application might have specific requirements for security settings. Figure 3.1 shows the process for securing your Web sites and applications.

Figure 3.1 Securing Web Sites and Applications



Securing the Web sites and applications requires that the Web server as a whole is secure. The process presented in this chapter assumes that the network infrastructure connecting the Web servers to the clients and to other servers is secure. The security of the network infrastructure is determined by the placement and configuration of the firewalls, routers, and switches in the network infrastructure.

Note

The process presented in this chapter includes all of the steps for securing your Web sites and applications in one of many possible sequences. You can complete these steps in the sequence that is recommended in this chapter, or in another sequence. Regardless of the sequence, it is recommended that you evaluate all of the steps in the process.

In addition to assuming that the network infrastructure is secure, the process presented here assumes that the server is a *dedicated Web server*. A dedicated Web server is a server that is only being used as a Web server and not for other purposes, such as a file server, print server, or database server running Microsoft SQL Server™.

For more information about securing IIS components other than Internet services, such as Simple Mail Transfer Protocol (SMTP) or Network News Transfer Protocol (NNTP), see "SMTP Administration" or "NNTP Administration" in IIS 6.0 Help, which is accessible from IIS Manager. For more information about securing other services on a multipurpose server, see "Planning a Secure Environment" in *Designing and Deploying Directory and Security Services* of the *Microsoft® Windows® Server 2003 Deployment Kit*.

Tip

To secure the Web sites and applications in a Web farm, use the process described in this chapter to configure security for each server in the Web farm.

The following quick-start guide provides a detailed overview of how to configure security for IIS 6.0. You can use this guide to help identify the steps of the security process that you need additional information to complete and skip the information with which you are already familiar. In addition, all of the procedures that are required to complete the security process are documented in "IIS Deployment Procedures in this book.

Reduce the Attack Surface of the Web Server

1. Enable only essential Windows Server 2003 components and services.
2. Enable only essential IIS 6.0 components and services.
3. Enable only essential Web service extensions.
4. Enable only essential Multipurpose Internet Mail Extensions (MIME) types.
5. Configure Windows Server 2003 security settings.

Prevent Unauthorized Access to Web Sites and Applications

1. Store content on a dedicated disk volume.
2. Set IIS Web site permissions.
3. Set IP address and domain name restrictions.
4. Set the NTFS file system permissions.

Isolate Web Sites and Applications

1. Evaluate the effects of impersonation on application compatibility:
   - Identify the impersonation behavior for ASP applications.
   - Select the impersonation behavior for ASP.NET applications.
2. Configure Web sites and applications for isolation.

Configure User Authentication

1. Configure Web site authentication.
   - Select the Web site authentication method.
   - Configure the Web site authentication method.
2. Configure File Transfer Protocol (FTP) site authentication.

Encrypt Confidential Data Exchanged with Clients

1. Use Secure Sockets Layer (SSL) to encrypt confidential data.
2. Use Internet Protocol security (IPSec) or virtual private network (VPN) with remote administration.

Maintain Web Site and Application Security

1. Obtain and apply current security patches.
2. Enable Windows Server 2003 security logs.
3. Enable file access auditing for Web site content.
4. Configure IIS logs.

5. Review security policies, processes, and procedures.

Reducing the Attack Surface of the Web Server

Immediately after installing Windows Server 2003 and IIS 6.0 with the default settings, the Web server is configured to serve only static content. If your Web sites consist of static content and you do not need any of the other IIS components, then the default configuration of IIS minimizes the attack surface of the server. When your Web sites and applications contain dynamic content, or you require one or more of the additional IIS components, you will need to enable additional features. However, you still want to ensure that you minimize the *attack surface* of the Web server. The attack surface of the Web server is the extent to which the server is exposed to a potential attacker.

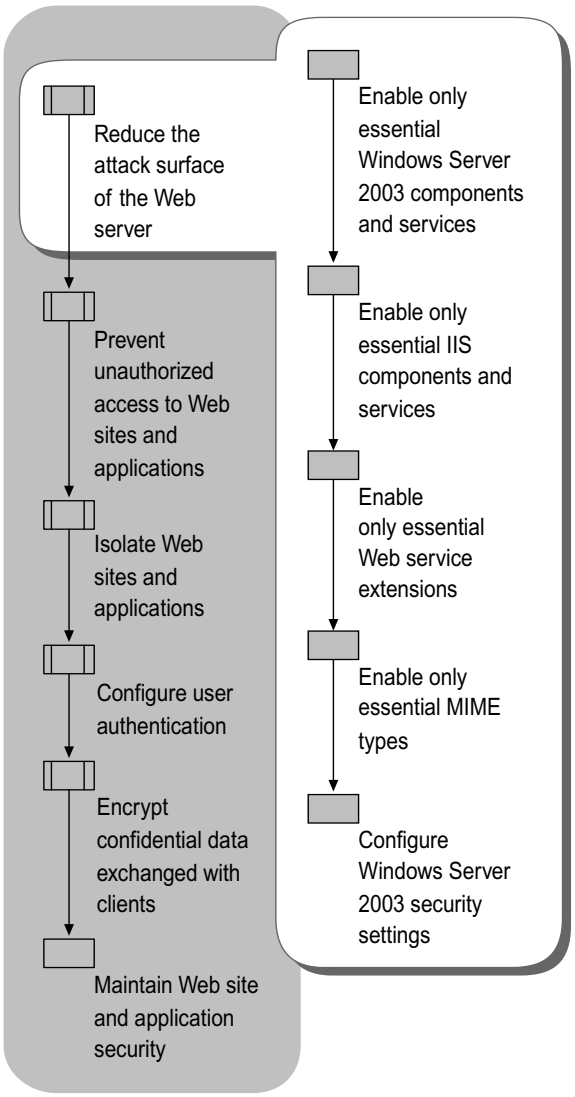
However, if you reduce the attack surface of the Web server too much, you can eliminate functionality that is required by the Web sites and applications that the server hosts. You need to ensure that only the functionality that is necessary to support your Web sites and applications is enabled on the server. This ensures that the Web sites and applications will run properly on your Web server, but that the attack surface is minimized.

Tip

In addition to new installations, you can use the information in this section to reduce the attack surface of existing Web servers.

Figure 3.2 illustrates the process for reducing the attack surface of the Web server.

Figure 3.2 Reducing the Attack Surface of the Web Server



Each additional Windows Server 2003 and IIS 6.0 component is configured with the most restrictive possible security that will allow the component to still function. However, in providing any functionality, there is still an opportunity for potential attackers to exploit any weakness of the component.

For example, enabling the Domain Name System (DNS) component in Windows Server 2003 with the default configuration settings would make the server susceptible to any of the standard attacks common to DNS on Windows, UNIX, Linux, or other operating systems. Additional configuration would be required to further secure DNS, such as requiring zones that are integrated with Microsoft Active Directory® directory service.

In addition, if your primary focus is Web server administration, you might not be familiar with DNS-related security attacks. So reducing the attack surface of the server helps eliminate potential attacks that you cannot predict because of your familiarity with other Windows Server 2003 and IIS 6.0 components.

Important

In addition to enabling only essential Windows Server 2003 and IIS 6.0 components, ensure that you configure the components to the highest possible security settings. By enabling nonessential components and services, you can increase the attack surface of your server because you have enabled these components and services without further configuring them to the most restrictive security settings.

Enabling Only Essential Windows Server 2003 Components and Services

The attack surface of the Web server is also affected by the other Windows components and services that are enabled in Windows Server 2003. When you install Windows Server 2003 as a dedicated Web server, the default components and services are configured to provide the smallest possible attack surface. In some cases, you might have installed Windows Server 2003 for other purposes, such as a file server, print server, or computer running SQL Server, so you are installing IIS 6.0 on an existing server. In this situation, you need to reevaluate the components and services that are currently running on the Web server to ensure that only the components and services that you need are enabled.

To enable and disable services, change the startup type of the service. You can configure the startup type of the service to one of the following:

- **Automatic.** The service starts automatically when the operating system starts.
- **Manual.** The service can be started by an administrator, a related operating system service, a system device driver, or an action in the user interface that is dependent on the manual service.
- **Disabled.** The service cannot be started automatically or manually; to start a disabled service, you must change the startup type to Automatic or Manual.

Table 3.1 lists the Windows Server 2003 services, as well as the default startup type, the recommended startup type, and comments about the services.

For each of the Windows Server 2003 services that are listed in Table 3.1, complete the following steps:

1. Review the recommended startup type to determine whether you need to change the default startup type.
2. Determine, based on the information provided in the comments, if the recommendation applies to your Web server.
3. Configure the startup type for the service based on the decisions made in the previous steps.

For more information about how to change the startup type of Windows Server 2003 services, see “Configure Windows Server 2003 Services” in “IIS Deployment Procedures” in this book.

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server

Service Name	Default Startup Type	Recommended Startup Type	Comment
Alerter	**Disabled**	**No change**	**Notifies selected users and computers of administrative alerts.**

Service Name	Default Startup Type	Recommended Startup Type	Comment
Application Layer Gateway Service	Manual	No change	Provides support for application-level plug-ins and enables network and protocol connectivity.
Application Management	Manual	See comment	Provides software installation services for applications that are deployed in Add or Remove Programs in Control Panel. On a dedicated Web server, this service can be disabled to prevent unauthorized installation of software.
Automatic Updates	Automatic	See comment	Provides the download and installation of critical Windows updates, such as security patches and hotfixes. This service can be disabled when automatic updates are not performed on the Web server.
Background Intelligent Transfer Service	Manual	See comment	Provides a background file-transfer mechanism and queue management, and it is used by Automatic Update to automatically download programs (such as security patches). This service can be disabled when automatic updates are not performed on the Web server.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
ClipBook	Disabled	See comment	Enables the Clipbook Viewer to create and share data that can be reviewed by remote users.
COM+ Event System	Manual	No change	Provides automatic distribution of events to COM+ components.
COM+ System Application	Manual	No change	Manages the configuration and tracking of COM+-based components.
Computer Browser	Automatic	No change	Maintains the list of computers on the network, and supplies the list to programs that request the list.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Cryptographic Services	Automatic	No change	Provides three management services: Catalog Database Service, which confirms the signatures of Windows files; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from the Web server; and Key Service, which helps in enrolling certificates.
DHCP Client	Automatic	No change	Required to automatically obtain IP configuration and to dynamically update records in DNS.
Distributed File System	Automatic	Disable	Manages logical volumes that are distributed across a local area network (LAN) or wide area network (WAN). On a dedicated Web server, disable Distributed File System.
Distributed Link Tracking Client	Automatic	Disabled	Maintains links between NTFS V5 file system files within the Web server and other servers in the domain. On a dedicated Web server, disable Distributed Link Tracking.
Distributed Link Tracking Server	Manual	Disabled	Tracks information about files that are moved between NTFS V5 volumes throughout a domain. On a dedicated Web server, disable Distributed Link Tracking.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
Distributed Transaction Coordinator	Automatic	No Change	Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems.
DNS Client	Automatic	No change	Allows resolution of DNS names.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Error Reporting Service	Automatic	See comment	Collects, stores, and reports unexpected application crashes to Microsoft. If this service is stopped, then Error Reporting will occur only for kernel faults. On a dedicated Web server, disable Error Reporting Service.
Event Log	Automatic	No change	Writes event log messages that are issued by Windows-based programs and components to the log files.
Fax Service	Manual	Disabled	Provides the ability to send and receive faxes through fax resources that are available on the Web server and network. On a dedicated Web server, this service can be disabled because sending and receiving faxes is not a typical function of a Web Server.
File Replication Service	Manual	No change	Enables files to be automatically copied and maintained simultaneously on multiple servers.
Help and Support	Automatic	No change	Enables Help and Support Center to run on the Web server.
HTTP SSL	Manual	No change	Implements the Secure Hypertext Transfer Protocol (HTTPS) for the HTTP service by using SSL. HTTP.sys automatically starts this service when any Web sites require SSL.
Human Interface Device Access	Disabled	No change	Enables generic input to Human Interface Devices (HIDs), which activates and maintains the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment

Service Name	Default Startup Type	Recommended Startup Type	Comment
IMAPI CD-Burning COM Service	Disabled	No change	Manages CD recording by using the Image Mastering API (IMAPI).
Indexing Service	Manual	See comment	Indexes content and properties of files on the Web server to provide rapid access to the file through a flexible query language. On a dedicated Web server, disable this service unless Web sites or applications specifically leverage the Indexing Service for searching site content.
Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS)	Disabled	No change	Provides network address translation (NAT), addressing and name resolution, and intrusion detection when connected through a dial-up or broadband connection. On a dedicated Web server, disable to prevent inadvertent enabling of NAT, which would prevent the Web server from communicating with the remainder of the network.
Intersite Messaging	Disabled	No changes	Required by Distributed File System (DFS).
IPSec Services	Automatic	No change	Provides management and coordination of Internet Protocol security (IPSec) policies with the IPSec driver.
Kerberos Key Distribution enter	Disabled	No change	Provides the ability for users to log on using the Kerberos V5 authentication protocol.
License Logging Service	Disabled	No change	Monitors and records client access licensing for portions of the operating system, such as IIS, Terminal Services, and file and print sharing, and for products that are not a part of the operating system, such as Microsoft SQL Server or Microsoft Exchange Server. On a dedicated Web server, this service can be disabled.
Logical Disk Manager	Automatic	No change	Required to ensure that dynamic disk information is up to date.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
Logical Disk Manager Administrative Service	Manual	No change	Required to perform disk administration.
Messenger	Disabled	No change	Transmits net sends and Alerter service messages between clients and servers.
Microsoft Software Shadow Copy	Manual	No change	Manages software-based volume shadow copies taken by the Volume Shadow Copy service. On a dedicated Web server, this service can be disabled when volume shadow copies are not used.
Net Logon	Manual	No change	Maintains a secure channel between the domain controller, other domain controllers, member servers, and workstations in the same domain and trusted domains.
NetMeeting Remote Desktop Sharing	Manual	Disabled	Eliminates potential security threats by allowing domain-controller remote administration through NetMeeting.
Network Connections	Manual	No change	Manages objects in the Network Connections directory.
Network DDE	Disabled	No change	Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the Web server. This service can be disabled when no DDE applications are running locally on the Web server.
Network DDE DSDM	Disabled	No change	Used by Network DDE. This service can be disabled when Network DDE is disabled.
Network Location Awareness (NLA)	Manual	No change	Collects and stores network configuration and location information, and notifies applications when this information changes.

Service Name	Default Startup Type	Recommended Startup Type	Comment
NTLM Security Support Provider	Manual	No change	Provides security to RPC programs that use transports other than named pipes, and enables users to log on using the NTLM authentication protocol.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
Performance Logs and Alerts	Manual	See comment	Collects performance data for the domain controller, writes the data to a log, or generates alerts. This service can be set to automatic when you want to log performance data or generate alerts without an administrator being logged on.
Plug and Play	Automatic	No change	Required to automatically recognize and adapt to changes in the Web server hardware with little or no user input.
Portable Media Serial Number Service	Manual	No change	Retrieves the serial number of any portable media player that is connected to the computer.
Print Spooler	Automatic	See comment	Manages all local and network print queues and controls all print jobs. On a dedicated Web server, this service can be disabled when no printing is required.
Protected Storage	Automatic	No change	Protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users. This service is used on a dedicated Web server for smart-card logon.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Remote Access Auto Connection Manager	Manual	See comment	Detects unsuccessful attempts to connect to a remote network or computer and provides alternative methods for connection. On a dedicated Web server, this service can be disabled when no VPN or dial-up connections are initiated.
Remote Access Connection Manager	Manual	See comment	Manages VPN and dial-up connection from the Web server to the Internet or other remote networks. On a dedicated Web server, this service can be disabled when no VPN or dial-up connections are initiated.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
Remote Desktop Help Sessions Manager	Manual	Disabled	Manages and controls Remote Assistance. On a dedicated Web server, this service can be disabled. Use Terminal Services instead.
Remote Procedure Call (RPC)	Automatic	No change	Serves as the RPC endpoint mapper for all applications and services that use RPC communications.
Remote Procedure Call (RPC) Locater	Manual	See comment	Enables RPC clients using the RpcNs* family of application programming interfaces (APIs) to locate RPC servers and manage the RPC name service database. This service can be disabled if no applications use the RpcNs* APIs.
Remote Registry Service	Automatic	No change	Enables remote users to modify registry settings on the Web server, provided the remote users have the required permissions. By default, only members of the Administrators and Backup Operators groups can access the registry remotely.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Removable Storage	Manual	See comment	Manages and catalogs removable media, and operates automated removable media devices, such as tape auto loaders or CD jukeboxes. This service can be disabled when removable media devices are directly connected to the Web server.
Resultant Set of Policy Provider	Manual	No change	Enables a user to connect to a remote computer, access the Windows Management Instrumentation (WMI) database for that Web server, and then either verify the current Group Policy settings or check the settings before they are applied.
Routing and Remote Access	Disabled	No change	Enables LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
Secondary Logon	Automatic	No change	Allows you to run specific tools and programs with different permissions and user rights than the default permissions and user rights of the account under which you logged on.
Security Accounts Manager	Automatic	No change	A protected subsystem that manages user and group account information.
Server	Automatic	No change	Provides RPC support, file sharing, print sharing, and named pipe sharing over the network.
Shell Hardware Detection	Automatic	No change	Provides notification for AutoPlay hardware events.
Smart Card	Manual	No change	Manages and controls access to a smart card that is inserted into a smart card reader attached to the Web server.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Special Administration Console Helper	Manual	No change	Allows administrators to remotely access a command prompt by using Emergency Management Services. This service can be disabled when Emergency Management Services is not being used to remotely manage the Web server.
System Event Notification	Automatic	No change	Monitors system events and notifies subscribers to the COM+ Event System of these events.
Task Scheduler	Automatic	No change	Provides the ability to schedule automated tasks on the Web server.
TCP/IP NetBIOS Helper Service	Automatic	No change	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients.
Telephony	Manual	See comment	Provides Telephony API (TAPI) support of client programs that control telephony devices and IP-based voice connections. On a dedicated Web server, this service can be disabled when TAPI is not used by applications.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
Telnet	Manual	Disabled	Enables a remote user to log on and run applications from a command line on the Web server. To reduce the attack surface, disable Telnet unless it is used for remote administration of branch offices or of Web servers that have no keyboard or monitor directly attached (also known as *headless* Web servers). Because Telnet traffic is plaintext, Terminal Services is the preferred method for remote administration.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Terminal Services	Manual	See comment	Allows multiple remote users to be connected interactively to the Web server, and provides display of desktops and run applications. To reduce the attack surface, disable Terminal Services unless it is used for remote administration of branch offices or headless Web servers.
Terminal Services Session Directory	Disabled	No change	Enables a user connection request to be routed to the appropriate terminal server in a cluster.
Themes	Disabled	No change	Provides user-experience theme management.
Uninterruptible Power Supply	Automatic	No change	Manages an uninterruptible power supply (UPS) that is connected to the Web server by a serial port.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
Upload Managers	Manual	See comment	Manages the synchronous and asynchronous file transfers between clients and servers on the network. Driver data is anonymously uploaded from these transfers and then used by Microsoft to help users find the drivers they need. The Driver Feedback Server asks for the permission of the client to upload the hardware profile of the Web server and then search the Internet for information about how to obtain the appropriate drivers or how to get support. To reduce the attack surface, disable this service on dedicated Web servers.
Virtual Disk Services	Manual	No change	Provides software volume and hardware volume management service.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Volume Shadow Copy	Manual	No change	Manages and implements volume shadow copies that are used for backup and other purposes. This service can be disabled when volume shadow copies are used on the Web server.
WebClient	Disabled	No change	Enables Windows-based programs to create, access, and modify Internet-based files.
Windows Audio	Disabled	No change	Manages audio devices for Windows-based programs.
Windows Image Acquisition (WIA)	Disabled	No change	Provides image acquisition services for scanners and cameras.
Windows Installer	Manual	No change	Adds, modifies, and removes applications that are provided as a Windows Installer (.msi) package.
Windows Management Instrumentation	Automatic	No change	Provides a common interface and object model to access management information about the Web server through the WMI interface.

(continued)

Table 3.1 Recommended Service Startup Types on a Dedicated Web Server *(continued)*

Service Name	Default Startup Type	Recommended Startup Type	Comment
Windows Management Instrumentation Driver Extensions	Manual	No change	Monitors all drivers and event trace providers that are configured to publish WMI or event trace information.
WinHTTP Web Proxy Auto-Discovery Service	Manual	See comment	Implements the Web Proxy Auto-Discovery (WPAD) protocol for Windows HTTP services (WinHTTP) and enables an HTTP client to automatically discover a proxy configuration. On dedicated Web servers, this service can be disabled

Service Name	Default Startup Type	Recommended Startup Type	Comment
Wireless Configuration	**Automatic**	**See comment**	**Enables automatic configuration for IEEE 802.11 adapters.** **On dedicated Web servers without wireless network adapters, this service can be disabled.**
WMI Performance Adapter	**Manual**	**See comment**	**Provides performance library information from WMI providers to clients on the network.** **On dedicated Web servers that do not use WMI to provide performance library information, this service can be disabled.**
Workstation	**Automatic**	**No change**	**Creates and maintains client network connections to remote servers.**

Enabling Only Essential IIS Components and Services

IIS 6.0 includes other components and services in addition to the WWW service, such as the File Transfer Protocol Service (FTP service) and the Simple Mail Transfer Protocol (SMTP) service. You can install and enable IIS components and services by using the **Application Server** subcomponent, which is found in **Add or Remove Windows Components** in **Add or Remove Programs** in Control Panel. After installing IIS, you need to enable the IIS 6.0 components and services that are required by the Web sites and applications running on your Web server.

Enable only the essential IIS 6.0 components and services that are required by your Web sites and applications. Enabling unnecessary components and services increases the attack surface of the Web server.

When a Web site or application does not function on the Web server and you suspect that an IIS 6.0 component or service might need to be enabled, complete the following steps:

1. Enable the individual IIS 6.0 component or service that you believe will allow the Web site or application to function.
2. Test the Web site or application for proper operation.
3. If the Web site or application functions correctly, further configure the IIS 6.0 component or service to the most restrictive security settings.
4. If enabling the IIS 6.0 component or service does not allow the Web site or application to function, disable the IIS 6.0 component or service and continue troubleshooting the problem.

The Web site or application might not function properly because of issues that are not security-related. For example, an Internet Server API (ISAPI) extension that is used by an application might not be installed properly. Although it might appear that the ISAPI extension is disabled, the problem might actually be caused by a faulty installation or configuration setting for the ISAPI extension. For more information about troubleshooting problems related to Web sites and applications that are not functioning, see “Troubleshooting” in IIS 6.0 Help, which is accessible from IIS Manager.

Important

When you are troubleshooting Web site- and application-related problems, do not enable all of the IIS 6.0 components and services. Enabling all of the IIS 6.0 components and services will unnecessarily increase the attack surface of the Web server.

For each of the subcomponents of the application server that are listed in Table 3.2 through Table 3.6, complete the following steps:

1. Review the recommended settings to determine whether you need to make changes to the default settings.
2. Determine, based on the information provided in the comments, if the recommendation applies to your server.
3. Enable or disable the component based on the decisions made in the previous steps.

   For more information about how to configure the IIS 6.0 protocols and services, see "Configure IIS Components and Services" in "IIS Deployment Procedures" in this book.

Table 3.2 Subcomponents of the Application Server

Subcomponent	Default Setting	Recommended Setting	Comment
Application Server Console	**Enabled**	**No change**	**Provides an MMC snap-in that includes administration for all of the Web Application Server (WAS) components.** **On a dedicated Web server, this component is not required because only IIS Manager is used.**
ASP.NET	**Disabled**	**See comment**	**Provides support for ASP.NET applications.** **Enable this component when you need to run ASP.NET applications on the Web server.**
Enable network COM+ access	**Enabled**	**See comment**	**Allows the Web server to host COM+ components for distributed applications.** **Disable this component unless it is required by your applications.**
Enable network DTC access	**Disabled**	**See comment**	**Allows the Web server to host applications that participate in network transactions through Distributed Transaction Coordinator (DTC).** **Disable this component unless it is required by**

			your applications.
Internet Information Services (IIS)	Enabled (See Table 3.3 for subcomponents)	No change	Provides basic Web and FTP services. This component is required on a dedicated Web server. Note: If this component is not enabled, then all subcomponents are not enabled.

(continued)

Table 3.2 Subcomponents of the Application Server *(continued)*

Subcomponent	Default Setting	Recommended Setting	Comment
Message Queuing	Disabled (See Table 3.4 for subcomponents)	See comment	Provides guaranteed messaging, security, and transactional support for applications that communicate through messaging services provided by Message Queuing (also known as MSMQ). This component is required when your Web sites and applications use Message Queuing. Note: If this component is not enabled, then all subcomponents are not enabled.

Table 3.3 Subcomponents of Internet Information Services (IIS)

Subcomponent	Default Setting	Recommended Setting	Comment
Background Intelligent Transfer Service (BITS) server extension	Disabled	See comment	BITS is a background file transfer mechanism used by applications such as Windows Updates and Automatic Updates. Enable this component when you have software that depends on it, such as Windows Updates or Automatic Updates to automatically apply service packs, hot fixes, or install other software on the Web server. For more information, see

			"Obtaining and Applying Current Security Patches" later in this chapter.
Common Files	Enabled	No change	On a dedicated Web server, these files are required by IIS and must always be enabled.

(continued)

Table 3.3 Subcomponents of Internet Information Services (IIS) *(continued)*

Subcomponent	Default Setting	Recommended Setting	Comment
File Transfer Protocol (FTP) Service	Disabled	No change	Allows the Web server to provide FTP services. This component is not required on a dedicated Web server. However, you might need to enable FTP on a server that is only used for posting content, to support software such as Microsoft FrontPage® 2002 without enabling FrontPage 2002 Server Extensions. Because the FTP credentials are always sent in plaintext, it is recommended you connect to FTP servers through a secured connection, such as those provided by IPSec or a VPN tunnel. For more information, see "Using IPSec or VPN with Remote Administration" later in this chapter.
FrontPage 2002 Server Extensions	Disabled	See comment	Provides FrontPage support for administering and publishing Web sites. On a dedicated Web server, disable when no Web sites are using FrontPage Server Extensions.
Internet Information Services Manager	Enabled	See comment	Administrative interface for IIS. Disable when you do not want to administer the Web server locally.
Internet Printing	Disabled	No change	Provides Web-based

			printer management and allows printers to be shared by using HTTP. This component is not required on a dedicated Web server.

(continued)

Table 3.3 Subcomponents of Internet Information Services (IIS) *(continued)*

Subcomponent	Default Setting	Recommended Setting	Comment
NNTP Service	Disabled	No change	Distributes, queries, retrieves, and posts Usenet news articles on the Internet. This component is not required on a dedicated Web server.
SMTP Service	Enabled	Disabled	Supports the transfer of electronic mail. This component is not required on a dedicated Web server.
World Wide Web Service	for subcomponents)	No change	Provides Internet services, such as static and dynamic content, to clients. This component is required on a dedicated Web server. Note: If this component is not enabled, then all subcomponents are not enabled.

Table 3.4 Subcomponents of Message Queuing

Subcomponent	Default Setting	Recommended Setting	Comment
Active Directory Integration	Disabled	See comment	Provides integration with Active Directory whenever the Web server belongs to a domain.
Common	Disabled	See comment	Required by Message Queuing.
Downlevel Client Support	Disabled	See comment	Provides access to Active Directory and site recognition for clients that are not Active

			Directory-aware.
MSMQ HTTP Support	Disabled	See comment	Provides the sending and receiving of messages over the HTTP transport.
Routing support	Disabled	See comment	Provides store-and-forward messaging as well as efficient routing services for Message Queuing.

(continued)

Table 3.4 Subcomponents of Message Queuing *(continued)*

Subcomponent	Default Setting	Recommended Setting	Comment
Triggers	Disabled	See comment	Provides support to associate the arrival of incoming messages at a queue with functionality in a COM component or stand-alone program. This component is required when your Web sites and applications use Message Queuing and use Message Queuing triggers.

Table 3.5 Subcomponents of the Background Intelligent Transfer Service (BITS) Server Extension

Subcomponent	Default Setting	Recommended Setting	Comment
BITS management console snap-in	Disabled	No change	Installs an MMC snap-in for administering BITS. Enable this component when you enable the BITS server extension ISAPI component.
BITS server extension ISAPI	Disabled	No change	Installs the BITS ISAPI so that the Web server can transfer data by using BITS. This component is required when you want to use Windows Updates or Automatic Updates to automatically apply service packs and hot fixes to the Web server. For more information,

			see "Obtaining and Applying Current Security Patches" later in this chapter.

Table 3.6 Subcomponents of the World Wide Web Service

Subcomponent	Default Setting	Recommended Setting	Comment
Active Server Pages	**Disabled**	**See comment**	**Provides support for Active Server Pages (ASP).** **Disable this component when none of the Web sites or applications on the Web server uses ASP. You can disable this component in** Add or Remove Windows Components**, which is accessible from** Add or Remove Programs **in Control Panel, or in the Web Service Extensions node in IIS Manager.** **For more information, see "Enabling Only Essential Web Service Extensions" later in this chapter.**
Internet Data Connector	**Disabled**	**See comment**	**Provides support for dynamic content provided through files with .idc extensions.** **Disable this component when none of the Web sites or applications on the Web server include files with .idc extensions. You can disable this component in** Add or Remove Windows Components**, which is accessible from** Add or Remove Programs **in Control Panel, or in the Web Service Extensions node in IIS Manager.** **For more information, see "Enabling Only Essential Web Service Extensions" later in this chapter.**

(continued)

Table 3.6 Subcomponents of the World Wide Web Service *(continued)*

Subcomponent	Default Setting	Recommended Setting	Comment
Remote Administration (HTML)	Disabled	No change	Provides an HTML interface for administering IIS. Use IIS Manager instead to provide easier administration and to reduce the attack surface of the Web server. This component is not required on a dedicated Web server.
Remote Desktop Web Connection	Disabled	No change	Includes Microsoft ActiveX® controls and sample pages for hosting Terminal Services client connections. Use IIS Manager instead to provide easier administration and to reduce the attack surface of the Web server. This component is not required on a dedicated Web server.
Server-Side Includes	Disabled	See comment	Provides support for .shtm, .shtml, and .stm files. Disable this component when none of the Web sites or applications on the Web server includes files with these extensions.

(continued)

Table 3.6 Subcomponents of the World Wide Web Service *(continued)*

Subcomponent	Default Setting	Recommended Setting	Comment
WebDav Publishing	Disabled	Disabled	Web Distributed Authoring and Versioning (WebDAV) extends the HTTP/1.1 protocol to allow clients to publish, lock, and manage resources on the Web.

			Disable this component on a dedicated Web server. You can disable this component in Add or Remove Windows Components**, which is accessible from** Add or Remove Programs **in Control Panel, or in the Web Service Extensions node in IIS Manager** **For more information, see "Enabling Only Essential Web Service Extensions" later in this chapter.**
World Wide Web Service	**Enabled**	**No change**	**Provides Internet services, such as static and dynamic content, to clients.** **This component is required on a dedicated Web server.**

Enabling Only Essential Web Service Extensions

If your Web sites and applications that are hosted on IIS 6.0 have extended functionality beyond static Web pages, including the generation of dynamic content, any dynamic content served or extended features provided by the Web server are done through Web service extensions.

For security reasons, you can enable or disable individual Web service extensions in IIS 6.0. After a new installation, IIS serves only static content. You can enable dynamic content capabilities, such as ASP.NET, Server-Side Includes, WebDAV publishing, and FrontPage 2002 Server Extensions, in the Web Service Extensions node in IIS Manager.

For example, one of your applications might use a custom ISAPI extension to provide access to a proprietary database. First, you need to add the custom ISAPI extension to the Web service extensions list. Then you can set the ISAPI extension that is used by the application to **Allowed**, explicitly granting it permission to run.

Enabling all of the Web service extensions ensures the highest possible compatibility with existing applications, regardless of whether you enable each of the Web service extensions individually or change the status of **All Unknown ISAPI Extensions** to **Allowed**. However, enabling all of the Web service extensions creates a security risk because it increases the attack surface of the Web server by enabling functionality that might be unnecessary for your server.

Web service extensions allow you to enable and disable the serving of dynamic content. MIME types allow you to enable and disable the serving of static content. For more information about enabling and disabling the serving of static content, see "Enabling Only Essential MIME Types" later in this chapter.

Tip

If the appropriate Web service extension is not enabled, the Web server returns a 404 error to the client when attempting to serve the dynamic content. When the 404 error is returned as a result of a Web service extension not being enabled, a 404.2 error entry is placed in the IIS log. For more information about troubleshooting IIS, see "Troubleshooting" in IIS 6.0 Help, which is accessible from IIS Manager.

Configure the Web service extensions by completing the following steps:

1. Enable the essential predefined Web service extensions based on the information in Table 3.1.

Table 3.7 Predefined Web Service Extensions

Web Service Extension	Description
Active Server Pages	**Enable this extension when one or more of the Web sites and applications contains ASP content.**
ASP.NET version 1.1.4322	**Enable this extension when one or more of the Web sites and applications contains ASP.NET content.**
FrontPage Server Extensions 2002	**Enable this extension when one or more of the Web sites use FrontPage Server Extensions.**
Internet Data Connector	**Enable this extension when one or more of the Web sites and applications uses the Internet Data Connector (IDC) to display database information (content includes .idc and .idx files).**
Server-Side Includes	**Enable this extension when one or more of the Web sites use server-side include (SSI) directives to instruct the Web server to insert various types of content into a Web page.**
WebDAV	**Enable this extension when you want to support WebDAV on the Web server. This Web service extension is not recommended on a dedicated Web server.**

2. For each Web service extension that is used by your Web sites and applications and that is not one of the default Web service extensions, add a new entry to the Web service extensions list and configure the status of the new entry to **Allowed**. For information about how to add a Web service extension to the list, see "Configure Web Service Extensions" in "IIS Deployment Procedures" in this book.
3. Use a Web browser on a client computer to verify that the Web sites and applications function properly on the server.

Enabling Only Essential MIME Types

IIS 6.0 serves only the static files with extensions that are registered in the Multipurpose Internet Mail Extensions (MIME) types list. IIS 6.0 is preconfigured to recognize a default set of global MIME types, which are recognized by all configured Web sites. You can define MIME types at the Web site and directory levels, independently of one another or the types defined globally. IIS also allows you to change, remove, or configure additional MIME types. For any static content file extensions used by the Web sites hosted by IIS that are not defined in the MIME types list, you must create a corresponding MIME type entry.

For example, a Web site or application might include static content with an extension that is not included in the default set of global MIME types. To allow the Web server to serve the new static content, you must add the extension to the MIME types list.

Tip

If the appropriate MIME type entries are not created in the MIME types list, the Web server returns a 404 error to the client when attempting to serve unknown static content types. When the 404 error is returned as a result of an unknown MIME type, a 404.3 error entry is placed in the IIS log. For more information about troubleshooting IIS, see "Troubleshooting" in IIS 6.0 Help, which is accessible from IIS Manager.

Configure the MIME types by completing the following steps:

1. For each static file type used by your Web sites and applications, ensure that an entry exists in the MIME types list.

   When your application uses the standard MIME types that are included in IIS 6.0, no new entry is required in the MIME types list. For information about how to add a MIME type to the MIME types list, see "Configure MIME Types" in "IIS Deployment Procedures" in this book.

2. Use a Web browser on a client computer to verify that the Web sites and applications function properly on the server.

Configuring Windows Server 2003 Security Settings

After installing Windows Server 2003, the security settings are configured so that the server is locked down. After installing IIS 6.0, evaluate the default security settings to determine whether they are sufficient for the Web sites and applications that your Web server hosts. You might need more stringent security requirements for Web sites and applications when the following is true:

- Users on the Internet access the Web sites and applications.
- The Web sites and applications contain confidential information.

Configure Windows Server 2003 to more restrictive security settings by completing the following steps:

1. Rename the Administrator account.

   The built-in account, Administrator, exists by default on every newly installed Web server. Potential attackers only have to guess the password for this well-known user account to exploit it. You can rename the Administrator user account to help protect your Web server from potential attackers. For more information about how to rename the Administrator user account, see "Secure Windows Server 2003 Built-in Accounts" in "IIS Deployment Procedures" in this book.

Important

During the default installation of Windows Server 2003, the Guest account is disabled. Ensure that the Guest account has not been enabled since the installation.

2. Format all disk volumes with the NTFS file system.

   From a security perspective, the primary reason for requiring that all disk volumes are formatted with NTFS is that NTFS is the only file system supported by Windows Server 2003 that allows you to secure files and folders. FAT or FAT32 partitions cannot be secured.

Because the Web sites and applications are stored as files and folders on the Web server, NTFS helps prevent unauthorized users from directly accessing or modifying the files and folders that make up your Web sites and applications. For more information about the benefits of formatting disk volumes as NTFS on Web servers, see "NTFS Permissions" in IIS 6.0 Help, which is accessible from IIS Manager.

If any existing disk volumes are FAT or FAT32, convert the disk volumes to NTFS. For more information about how to convert existing disk volumes to NTFS, see "Convert Existing Disk Volumes to NTFS" in "IIS Deployment Procedures" in this book.

3. Remove NTFS permissions that are granted to the Everyone group on the root folder of all disk volumes.

   By default, the Everyone group is granted Read and Execute permissions on the root folder of each disk volume. The default permissions can pose a potential security threat for any newly created folders on the volumes because, unless explicitly denied, these permissions are inherited in any new folders. To help prevent this potential security problem, remove all permissions that are granted to the Everyone group on the root folder of all disk volumes.

Important

The Administrators group still has full control on the root folder of each disk volume. In "Setting NTFS Permissions", later in this chapter, you will grant access to the Web site users by setting the appropriate NTFS permissions on the Web site content.

   For more information about how to remove the permissions that are granted to the Everyone group on the root folder of each disk volume, see "Secure the Root Folder of Each Disk Volume" in "IIS Deployment Procedures" in this book.

4. Remove any compilers or development environments.

   If compilers or development environments are installed on production Web servers, potential attackers can use them to upload source files to a malicious program and then use the Web server to compile the malicious program. In many instances, the source files might not be perceived as a threat, whereas an executable file would be. You can remove any compilers and development environments to help ensure that potential attackers cannot remotely compile a malicious program and then run that malicious program on the Web server.

   Consult the documentation of the compiler or development environment for information about how to remove them.

5. Disable NetBIOS over TCP/IP.

   To prevent attackers from executing the NetBIOS Adapter Status command on a server, and reveal the name of the user who is currently logged on, disable NetBIOS over TCP/IP on public connections of the server.

Important

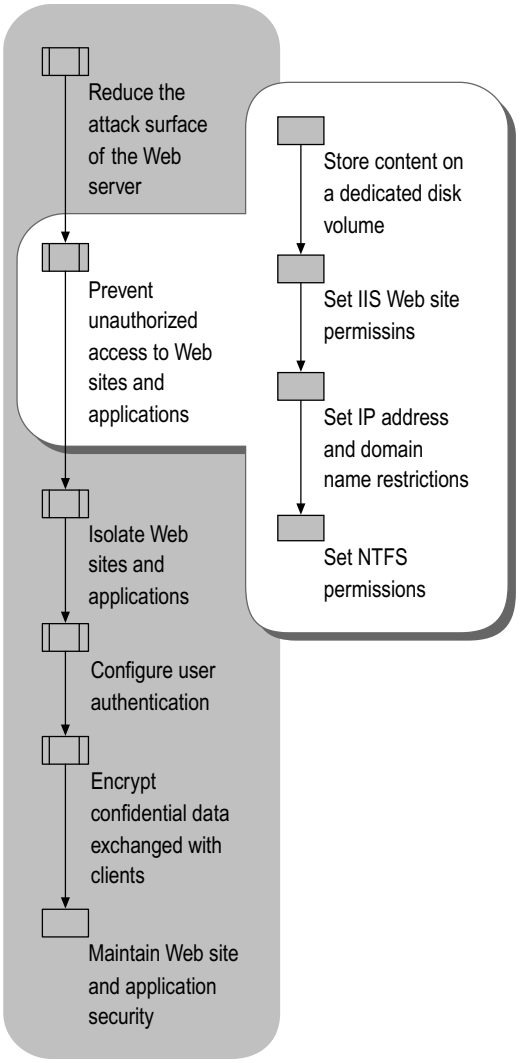
Before you disable NetBIOS over TCP/IP, make sure that it doesn't affect the management tools that you use to manage the server and other applications running on the server. You can do this by disabling NetBIOS over TCP/IP on a test server before disabling it on your production servers.

Preventing Unauthorized Access to Web Sites and Applications

Each Web site and application in IIS 6.0 and Windows Server 2003 is stored as a grouping of folders and files. Unauthorized access to, or modification of, these files and folders can present a serious breach of security. You must ensure that only authorized users can access or modify the Web sites and applications that are hosted on your Web server.

To help prevent unauthorized access to Web sites and applications on your Web server, use any combination of the steps illustrated in Figure 3.3. Based on the security requirements of your organization, you might perform a subset of the steps or all of the steps.

Figure 3.3 Preventing Unauthorized Access to Web Sites and Applications



Storing Content on a Dedicated Disk Volume

Store the files and folders that comprise the content of your Web sites and applications on a dedicated disk volume that does not contain the operating system. Doing this helps prevent *directory transversal attacks*.

Directory transversal attacks occur when an attacker attempts to send the Web server a request for a file that is located in another directory structure.

For example, Cmd.exe exists in the *systemroot*\System32 folder. Without the appropriate security settings, an attacker might be able to make a request to *systemroot*\System32\Cmd.exe and invoke the command prompt. If the Web site content is stored on a separate disk volume, such a directory transversal attack cannot work because Cmd.exe does not exist on the same disk volume. The default NTFS permissions for Windows Server 2003 prohibit anonymous users from executing or modifying any files in the systemroot folder and subfolders, so that only an unauthorized authenticated user can perform this type of attack.

In addition to security concerns, placing the content on a disk volume that is dedicated to Web site and application content makes administration tasks, such as backup and restore, easier. In cases where you store the content on a separate physical drive that is dedicated to the content, you will reduce the disk contention on the system volume and improve overall disk-access performance. Ensure that the dedicated disk volume is formatted as NTFS.

To help protect your Web sites and applications, store content on dedicated disk volumes by completing the following steps:

1. Create a disk volume, or designate an existing disk volume, where the Web sites and applications will be stored.
2. Configure the NTFS permissions on the root of the disk volume so that:
   - The Administrators group has full control.
   - All other permissions are removed.
3. Create a folder, or designate an existing folder, on the dedicated disk volume to hold the subfolders that will contain the Web sites and applications.
4. Beneath the folder that you created, or designated, in the previous step, create a subfolder for each Web site or application that will be installed on the Web server.
5. Install the Web sites and applications in the subfolders that you created in the previous step.

At this step in the deployment process, only members of the Administrators group have access to the content. You will grant access to the users who will access the Web sites and applications in "Setting NTFS Permissions" later in this chapter.

Setting IIS Web Site Permissions

In IIS 6.0, you can set Web site permissions, which allow you to control access to a Web site or virtual directory. IIS examines Web site permissions to determine which type of action can occur, such as accessing the source code of a script or browsing folders.

Use Web site permissions in conjunction with NTFS permissions, not in place of NTFS permissions. You can set Web site permissions for specific sites, directories, and files. Unlike NTFS permissions, Web site permissions affect everyone who tries to access your Web site.

Note

If Web site permissions conflict with NTFS permissions for a directory or file, the more restrictive settings are applied.

Table 3.8 lists and describes the Web site permissions that are supported by IIS 6.0.

Table 3.8 Web Site Permissions That Are Supported by IIS 6.0

Permission	Description
Read	**Users can view the content and properties of directories or**

	files. This permission is set by default. This permission is required for Web sites that have static content. If all of your content is scripted, such as a Web site that only uses ASP content, you can remove the Read permission.
Write	**Users can change content and properties of directories or files.**
Script Source Access	**Users can access source files. If the Read permission is set, then users can read source files; if the Write permission is set, then users can modify the content and properties of the source files. The Script Source Access permission also applies to the source code for scripts. This option is not available if both the Read and Write permissions are not set.** **Set this permission only when using WebDAV. In addition, make sure that you require authentication for this site and that your file permissions are set correctly.** Important **When you set the Script Source Access permission, users might be able to view sensitive information, such as a user name and password. Users might also be able to change source code that runs on your server, and seriously affect the security and performance of your server.**
Directory browsing	**Users can view file lists and collections.**
Log visits	**A log entry is created for each visit to the Web site. As an operational security practice, it is highly recommend that you enable logging.**
Index this resource	**Indexing Service can index this resource. This allows searches to be performed on the resource.**
Execute	**Users have the appropriate level of script execution:** • **None**. Does not allow scripts or executables to run on the server. • **Scripts only**. Allows only scripts to run on the server. • **Scripts and Executables**. Allows both scripts and executables to run on the server.

For information about how to set Web site permissions, see “Configure Web Site Permissions” in “IIS Deployment Procedures” in this book.

Setting IP Address and Domain Name Restrictions

One method of protecting the Web sites and applications that are hosted on your server is to restrict access from specific IP addresses or domain names. You can explicitly grant or deny access to any combination of IP address ranges or domain names.

By restricting access to Web sites and applications by using IP address ranges or domain names, you can grant or deny access to a specific set of computers or to an organization. The restrictions that you specify affect the entire Web site or application and cannot be configured for individual portions of the Web site or application.

Restrict access to a specific Web site for a specific IP address range or domain name by completing the following steps:

1. Specify the default access that will be given to the majority of users accessing the application by doing one of the following:
   - To allow the majority of users to access the application, enable default access.
   - To allow a limited number of users to access the application, disable default access.
2. For each computer, or group of computers, that you want to grant or deny access, specify the IP address range or domain name for the clients that are exceptions to the default access specified in Step 1.

   Unless you are unable to identify the IP address range for the computers, you must specify the domain name. From a performance perspective, specifying the IP address range is preferred. If you specify a domain name, DNS reverse lookups must be done each time a user accesses the application and the performance of your application is degraded.

   Specify the IP address range in the form of a single IP address or a network ID with a corresponding subnet mask.

For more information about setting IP address and domain name restrictions, see "Configure IP Address and Domain Name Restrictions" in "IIS Deployment Procedures" in this book.

Setting NTFS Permissions

NTFS permissions allow you to set permissions that are observed by IIS and by other Windows Server 2003 components. Windows Server 2003 examines NTFS permissions to determine the types of access a user, or a process, has on a specific file or folder.

Use NTFS permissions in conjunction with Web site permissions, not in place of Web site permissions. NTFS permissions affect only the accounts that have been granted or denied access to the Web site and application content. Web site permissions affect all of the users who access the Web site or application.

Note

If Web site permissions conflict with NTFS permissions for a directory or file, the more restrictive settings are applied.

You need to set NTFS permissions to allow the following situations:

- Administrators can manage the content of the Web sites and applications.
- Users can, at a minimum, read the content of the Web sites and applications.
- Application pool identities can, at a minimum, read the content of the Web sites and applications.

Web sites and applications can run under the identity of the following:

The user who is accessing the Web sites and applications

When you want to restrict access to resources, such as specific Web pages or database content that is stored in SQL Server, run your Web sites and applications under the identity of the user. For example, Basic authentication can allow Web sites and applications to pass through the identity of the user to other servers, such as a computer running SQL Server. By using this method, you can control the behavior of the Web site or application on a user-by-user basis.

The application pool identity that is used by the Web sites and applications

When you want to isolate Web sites or applications that are hosted on the same Web server from one another, run the Web sites or applications under the application pool identity. By using this method, you can prevent

Web sites and applications from interfering with one another independent of the users who are accessing the Web sites and applications. For more information about isolating Web sites and applications, see “Isolating Web Sites and Applications” later in this chapter.

Regardless of the identity that is used to run the Web site or application, you need to assign the appropriate NTFS permissions to the Web site or application so that it can run under the corresponding identity. Typically, these NTFS permissions are assigned to a group to which a number of users belong. Use this group when setting the permissions on the resources.

The primary disadvantage of restricting access by user accounts and NTFS permissions is that each user must have an account and must use that account to run the Web sites and applications. For your Internet-based Web sites and applications, requiring users to have accounts might be impractical. However, for intranet Web sites and applications you can use the existing accounts of users.

Explicitly deny access to anonymous accounts on Web sites and applications when you want to prevent anonymous access. *Anonymous access* occurs when a user who has no authenticated credentials accesses system resources. Anonymous accounts include the built-in Guest account, the group Guests, and the IIS anonymous accounts.

In addition to explicitly denying access to anonymous accounts, eliminate write access permissions for all users except members of the Administrators group.

Tip

If IIS denies access to content, you can enable object access auditing to find out the account that was used to access the content. The failed access event is recorded in the Security event log. The event log entry specifies the account that was used in the failed access. After you identify the account used in the failed access, grant the appropriate NTFS permissions to the account.

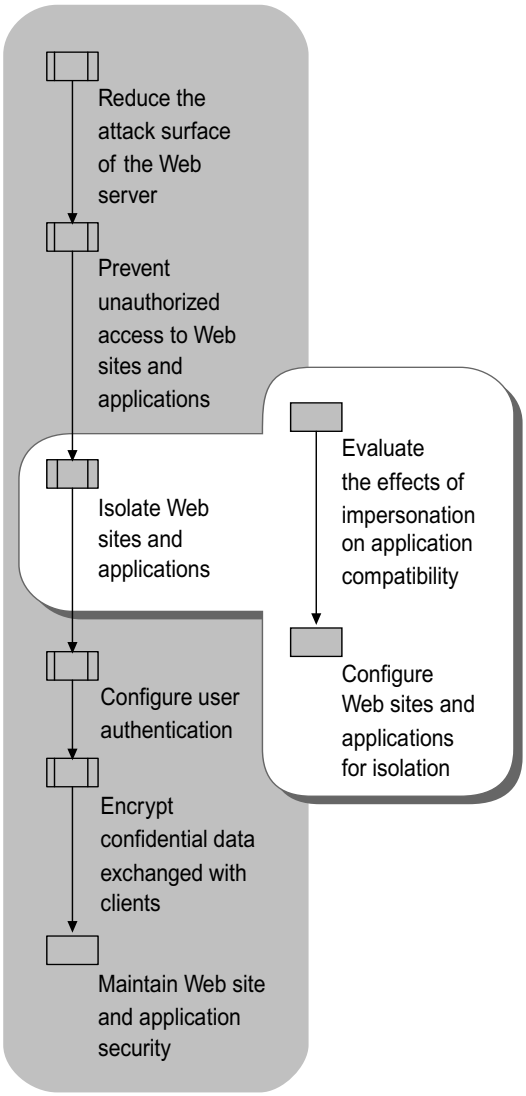
Isolating Web Sites and Applications

Although some of the Web servers that you deploy host only one Web site or application, you might also need to host multiple Web sites and applications on the same Web server. When a Web server hosts multiple Web sites and applications, each Web site and application requires a certain level of isolation.

For example, an Internet service provider (ISP) might host Web sites and applications for hundreds of organizations, each having a unique Web site. In this situation, the security requirements of each organization require a high degree of isolation between Web sites and applications.

Figure 3.4 illustrates the tasks involved in the process isolating your Web sites and applications.

Figure 3.4 Isolating Web Sites and Applications



You need to prevent multiple Web sites and applications that are hosted on the same Web sever from adversely interacting with one another. When IIS 6.0 is running in worker process isolation mode, you can isolate Web sites and applications hosted on the same Web server by specifying that the Web sites and applications belong to separate *application pools*. An application pool is a grouping of Web sites or applications served by the same worker process. Application pools can be used to help prevent the Web sites and applications running in one application pool from accessing the content contained in another application pool.

For each application pool, you can specify an *application pool identity*, which is a user account that is assigned to an application pool. After specifying the application pool identity, you assign permissions (such as NTFS permissions or SQL database permissions) for each application pool identity. Because individual application pools can use different identities, you can selectively grant or deny resource access to an application pool. The Web sites and applications running in an application pool have the same user rights and resource permissions assigned to the application pool identity.

For more information about setting NTFS permissions for Web sites and applications, see “Setting NTFS Permissions” earlier in this chapter.

Note

Web sites and applications that are running in the same application pool can affect the availability of other Web sites and applications in the same application pool. To enhance the availability of your Web sites and applications, isolate unstable Web sites and applications in a separate application pool. For more information about improving the availability of your Web server through application pools see, “Ensuring Application Availability in this book.

Evaluating the Effects of Impersonation on Application Compatibility

Securing your Web sites and applications by isolating them into separate application pools with unique identities can cause application compatibility problems when you are using anything but anonymous access. The application compatibility problems arise from the complexities of *impersonation*.

Impersonation allows a worker process to run under security credentials that are different from its base identity. Because the two are commonly confused, it is important to understand how the worker process identity that is established by the application pool identity is related to the impersonated user.

When a worker process is created by the WWW service, it is created with a process token that is associated with the application pool identity. This establishes the process identity of the worker process. By default, all of the actions taken by the worker process are completed in the context of this worker process identity account. However, when a client request is processed, the thread that processes the request uses a token associated with the client, which is also known as the *authenticated user’s token*, during the duration of the request.

Before IIS serves a URL, the authenticated user’s token is verified against the access control list (ACL) of the resource that is being requested. Additionally, if the request is for an ISAPI extension, such as ASP, the worker process applies the authenticated user’s token as an impersonation token to the thread that calls the ISAPI extension. When the ISAPI extension begins processing the request, this impersonation token applies to the actions it takes. Consequently, the actions taken by an ISAPI extension are associated with the authenticated user, not the process identity.

Evaluate the effects of impersonation behavior on compatibility for the following:

- ASP applications
- ASP.NET applications

Identifying the Impersonation Behavior for ASP Applications

For ASP applications, the type of authentication that is used by the user automatically determines impersonation behavior. Because the impersonation behavior is automatic, no configuration is required.

The impersonation behavior in an ASP application is as follows:

- If an anonymous user makes a request, the thread token is based on the user account that is configured as the anonymous user identity (by default, this is the IUSR_*machinename* user account).
- If an authenticated user makes a request, the thread token is based on the authenticated account of the user.

Selecting the Impersonation Behavior for ASP.NET Applications

Unlike ASP applications, you need to configure the impersonation behavior for ASP.NET applications. If you enable impersonation, ASP.NET receives the security token to impersonate from IIS. By specifying a value in the Web.config file of the application, you control the impersonation setting. You have the following three options when specifying this setting.

Impersonation is disabled

This is the default setting. In this instance, the ASP.NET thread runs using the process token of the application worker process regardless of which combination of IIS and ASP.NET authentication is used. By default, the process token of the application worker process is NetworkService.

Disable impersonation by modifying the Web.config file of the application to include the following setting:

```
<identity impersonate="false" />
```

Impersonation is enabled

In this instance, ASP.NET impersonates the token passed to it by IIS, which is either an authenticated user or the anonymous user account (IUSR_*machinename*). For backward compatibility with ASP, you must enable impersonation.

Enable impersonation by modifying the Web.config file of the application to include the following setting:

```
<identity impersonate="true" />
```

Impersonation is enabled and a specific impersonation identity is specified

In this instance, ASP.NET impersonates the token that is generated using the configured identity. In this case, ASP.NET does not use the token of the authenticated client, if applicable, except when performing access checks.

Enable impersonation and specify an impersonation identity by modifying the Web.config file of the application to include the following setting:

```
<identity impersonate="true" name="domain\user" password="password" />
```

Configuring Web Sites and Applications for Isolation

Complete the following steps to identify when Web sites and applications require isolation for security reasons:

Tip

Running worker processes under different identities can cause application compatibility problems, especially for Web sites that use user authentication. For more information, see “Web Application Isolation” in IIS 6.0 Help, which is accessible from IIS Manager.

1. Create a list of the Web sites and applications to be hosted on the Web server.
2. Group the Web sites and applications by organization (or business unit within an organization if all of the Web sites and applications hosted on the Web server are owned by one organization).
3. Subdivide each group created in the previous step into smaller groups of Web sites and applications that require the same user rights and resource access.
4. For each group created in the previous step, create a new application pool to be used by the Web sites and applications within the pool.

For information about how to create application pools, see “Isolate Applications in Worker Process Isolation Mode” in “IIS Deployment Procedures” in this book.

5. Assign the Web sites and applications within each group to the corresponding application pool.

   For information about how to assign the Web site to the new application, see “Isolate Applications in Worker Process Isolation Mode” in “IIS Deployment Procedures” in this book.

6. For each application pool, create a service account, to be used as the application pool identity.

   In IIS, the default identity for newly created application pools is NetworkService. To ensure that you can properly assign permissions to resources, create a new *service account*. A service account is a user account that is created explicitly for the purpose of providing a security context for services running on Windows Server 2003.

   In addition, you must add the service account to the IIS_WPG group to provide the appropriate access to the IIS metabase and content. The IIS_WPG group is granted the appropriate user rights and resource permissions to allow most Web sites and applications to run properly.

   For more information about how to create a service account to be used as an identity for an application pool and how to add the account to the IIS_WPG group, see “Create a Service Account” in “IIS Deployment Procedures” in this book.

7. Assign any additional *user rights* to the application pool identities.

   User rights authorize users to perform specific actions, such as logging on to a system interactively or backing up files and directories. User rights are different from permissions because user rights apply to user accounts, whereas permissions are attached to objects.

   The user rights granted to the IIS_WPG group are sufficient for most Web sites applications. When the user rights granted to the IIS_WPG group are insufficient, grant only the user rights to the user account, which is used as the identify for the application pool, that are necessary to ensure the appropriate operation and behavior of the application. Ensure that any nonessential user rights are removed to prevent the Web sites and applications from having elevated user rights.

   For more information about how to grant the appropriate user rights for an application pool identity, see “Grant User Rights to a Service Account” in “IIS Deployment Procedures” in this book.

8. Assign the service account identity to the corresponding application pool.

   For more information about how to assign the identity to the corresponding application pool, see “Configure Application Pool Identity” in “IIS Deployment Procedures” in this book.

9. Assign the appropriate resource permissions, such as NTFS or SQL database permissions, to the application pool identities.

   Assign only the NTFS file and folder permissions that are necessary to ensure the appropriate operation and behavior of the application. By default, grant only read permissions to the application pool identity to insure that the Web sites and applications in the application pool cannot modify the Web site content or other files on the Web server. If the applications require write access to any files and folders, consult the application developers to determine if the application can be modified so that write access is not required.

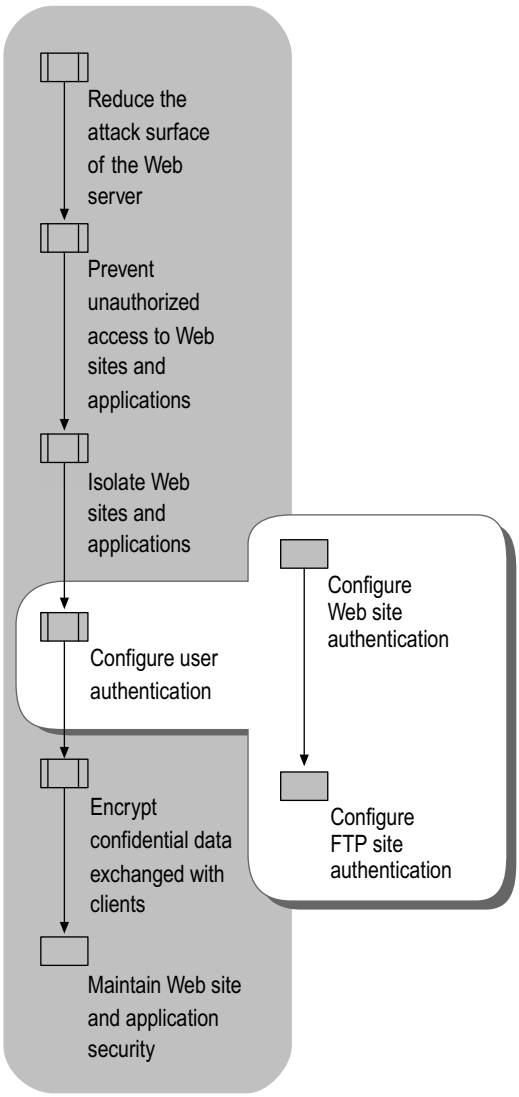
Configuring User Authentication

Authenticating users early in the connection process reduces the amount of information about that can be gained regarding your IIS 6.0 solution through anonymous access. In highly-secure Web sites and applications, you need to require authentication before the user can access any of the information. For other Web sites and

applications, you might require authentication only when the user is going to access portions of the Web site or application that contain confidential information.

Figure 3.5 illustrates the process for configuring user authentication.

Figure 3.5 Configuring User Authentication



Based on the types of services provided by the Web server, you might need to provide user authentication for Web sites or FTP sites. Web sites and FTP sites support different methods for authenticating users.

Configuring Web Site Authentication

The Web site authentication methods you chose are determined by whether you deploy your Web sites and applications on an intranet or the Internet and the relation of the users accessing the Web sites and applications to your organization.

Intranet -based Web sites and applications With intranet-based Web sites and applications, you can typically mandate the type of authentication that is used because the clients are controlled by your organization. In most instances, use Integrated Windows authentication to provide single sign on for users and the strongest possible protection of user credentials. If you are unable to use Integrated Windows authentication,

then select the next strongest authentication method from the authentication methods that are described in Table 3.9 in "Selecting a Web Site Authentication Method" later in this chapter.

Internet -based Web sites and applications With Internet-based Web sites and applications, you typically need to support a broad range of client operating systems and browsers because users outside your organization own the clients. Anonymous and Basic authentication are the most common authentication methods used for Internet-based Web sites and applications. For more information about these authentication methods, see "Selecting a Web Site Authentication Method" later in this chapter.

Configure Web site authentication by completing the following steps:

1. Select the authentication methods for each Web site.
2. Configure the authentication methods for each Web site.

Selecting a Web Site Authentication Method

The authentication method that you select varies based on the level of protection it provides for user credentials (user account and password information), and on the relationship of the user to your organization. Select the strongest authentication method possible to help ensure that the credentials of your users are protected.

Web site authentication methods can be divided into two categories:

- Methods that do not require or encrypt user credentials
- Methods that encrypt user credentials

Authentication Methods that Do Not Require or Encrypt User Credentials

For Internet-based Web sites and applications, the most commonly used authentication methods do not require or encrypt user credentials. Select one of these authentication methods when any combination of the following is true:

- Access to the Web sites and applications needs to be anonymous.
- Access to the Web sites and applications needs to be independent of the client configuration and relationship of the user to your organization.

Anonymous access

Anonymous access requires no authentication whatsoever. Anonymous access is used for intranet and Internet Web sites when you want unauthenticated users to be able to access the information provided by the Web sites and applications. The majority of Internet Web sites use anonymous access.

Authentication that is independent of the client configuration and user

Use Basic authentication when you want to require authentication to access a Web site or application, but need to use an authentication method that provides any combination of the following:

- No special configuration is required on the client. For example, the client can run any operating system or Web browser.
- The users have no close affiliation with your organization, and they are typically not employees or employees of partner organizations. As a result, you cannot require them to use an authentication method that encrypts user credentials.
- Your network infrastructure does not support encrypted authentication methods. For example, to use Windows Integrated authentication, you need the connection between requests to be maintained. Most proxy servers do not support such keep-alive connections.

Because Basic authentication does not encrypt user credentials, use a SSL-secured channel to encrypt user credentials. If you cannot encrypt Basic authentication traffic by using a SSL-secured channel, use one of the authentication methods that encrypt user credentials. These authentication methods are described in Table 3.9.

Authentication Methods That Encrypt User Credentials

Authentication methods that encrypt user credentials typically require some level of control over the client computer, and the user is usually an employee of your organization or a partner organization. Table 3.9 provides a comparison of the Web site authentication methods for Web sites and applications that encrypt user credentials.

Table 3.9 Web Site Authentication Methods That Encrypt User Credentials

Authentication Method	Advantages	Disadvantages
Digest	• Supports authentication through firewalls and proxies. • Encrypts user credentials. • Requires Active Directory running on Microsoft Windows® 2000 Server or later. • Provides medium security.	• Requires Microsoft Internet Explorer 5.0 or later. • Stores user password unencrypted in Active Directory. • Cannot be used to authenticate local accounts. • Requires the associated Application Pool identity to be configured as LocalSystem.

(continued)

Table 3.9 Web Site Authentication Methods That Encrypt User Credentials *(continued)*

Authentication Method	Advantages	Disadvantages
Advanced digest	• Supports authentication through firewalls and proxies. • Encrypts user credentials. • Stores hash of the user credentials in Active Directory. • Provides medium security.	• Requires Internet Explorer 5.0 or later. • Requires Active Directory running on Windows Server 2003. • Cannot be used to authenticate local accounts.
Integrated Windows	• Encrypts user credentials. • Provides high security. • Requires Internet Explorer 2.0 or later.	• Requires Microsoft clients.
Client Certificates	• For server authentication (certificates stored on the server), your organization obtains certificates from a trusted certification authority. • For client authentication, map certificates to users accounts stored in Active Directory running on Windows 2000 Server or later. • Provides high security.	• For client authentication (certificates stored on the clients), your organization has, or is willing to deploy, a public key infrastructure (PKI). • For client authentication, you have a method of securely distributing the certificates to the clients.
Microsoft .NET	• Supports authentication	• Requires Active Directory

Passport	through firewalls and proxies. • Encrypts user credentials. • Requires Internet Explorer 4.0 or later and Netscape Navigator 4.0 or later.	when account mapping is used. • Requires your organization to license the .NET Passport authentication service.

Configuring the Web Site Authentication Method

After you select the Web site authentication method for each Web site, you need to configure the Web site to use that method. For more information about how to configure Web server authentication, see "Configure Web Server Authentication" in "IIS Deployment Procedures" in this book.

Configuring FTP Site Authentication

Configure FTP site authentication for your FTP server by completing the following steps:

1. Select the FTP site authentication method that fulfills the security requirements of your organization, based on the information in Table 3.10.

   The authentication methods that you select vary, based on the ability of the method to protect user credentials (user account and password information). Select the strongest authentication method possible to help ensure that the credentials of your users are protected. Table 3.10 lists and describes these FTP site authentication methods.

   Table 3.10 FTP Site Authentication Methods

Authentication Method	Description
Anonymous FTP authentication	**For transferring any confidential information, avoid using Anonymous FTP authentication because no user authentication is performed with Anonymous FTP authentication, and anyone can transfer the information.**
Basic FTP authentication	**Basic FTP authentication sends the user name, password, and data in plaintext and can easily be discovered.**

2. Configure the FTP server to use the FTP site authentication method that you selected in the previous step.

When you are transferring confidential data:

- **Within your intranet by using FTP.** IPSec is required between the client computers and the FTP server to encrypt the user name, password, and any data transferred.
- **Outside your intranet (for remote users) by using FTP.** A VPN tunnel is required between the client computers and your intranet to encrypt the user name, password, and any data transferred.

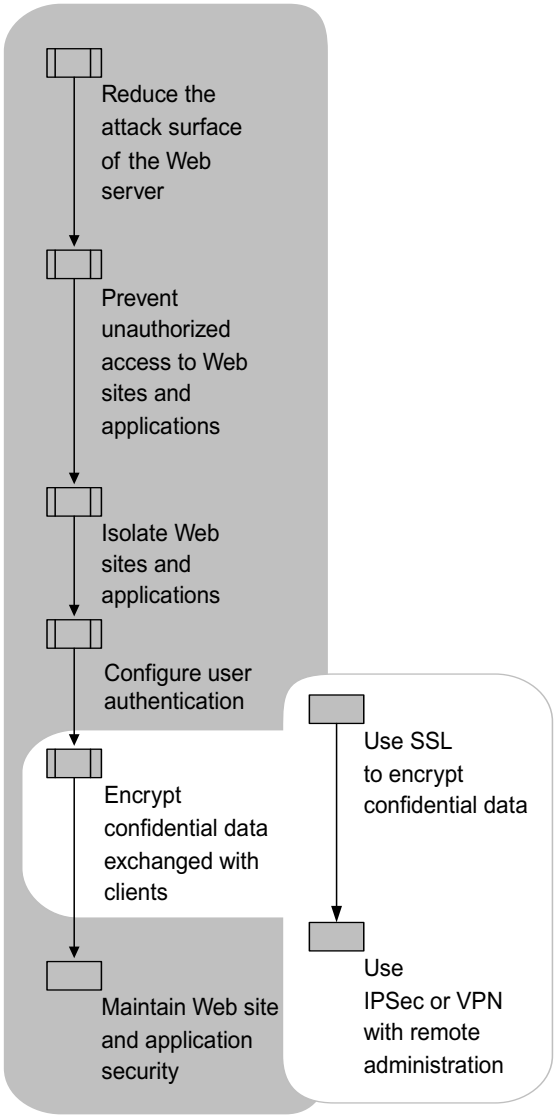
For information about how to configure FTP server authentication, see "Configure FTP Server Authentication" in "IIS Deployment Procedures" in this book.

Encrypting Confidential Data Exchanged with Clients

Your business needs might require that confidential data be exchanged between the client computers and the Web server. You can help ensure that this information is safeguarded on the network by using *encryption*. Encryption is a cryptographic process that helps prevent unauthorized users from viewing the encrypted data.

Figure 3.6 illustrates the process for encrypting confidential data that is exchanged between client computers and the Web server.

Figure 3.6 Encrypting Confidential Data Exchanged with Clients



The method you select for encrypting the data exchanged between the client computers and the Web server is based on a number of factors. You can encrypt the data exchanged between clients by using:

- SSL for users accessing the Web sites and applications hosted on the Web server.

- IPSec or VPNs for administrators who remotely manage the Web sites and applications hosted on the Web server.

Using SSL to Encrypt Confidential Data

You can configure Secure Sockets Layer (SSL) security features on your Web server to encrypt network transmissions, which will help ensure the integrity of your data transmission, and to verify the identity of users. SSL can be configured to provide security for any portion of the Web sites or applications on the Web server.

Note

The process presented here describes how to configure SSL to use *server certificates*. Server certificates are installed on the Web server and typically require no additional configuration on the clients. Server certificates allow the clients to verify the identity of the server. Alternatively, some Web sites and applications might require *client certificates*. Client certificates are installed on the client and allow the server to authenticate the clients. For more information about configuring client certificates, see “Enabling Client Certificates” in IIS 6.0 Help, which is accessible from IIS Manager.

You can configure SSL to help protect confidential data on a URL-by-URL basis (individual portions of the Web site or application). One portion of the application might require encryption of data transmissions with SSL (by specifying HTTPS in the URL), while another portion of the application might allow unencrypted data transmission (by specifying HTTP in the URL). This flexibility in security configuration allows you to provide encryption of confidential data as required, which is unlike IPSec and VPNs because they require that you encrypt all traffic between the clients and the Web server.

As an example, consider a fictitious organization called Contoso Pharmaceuticals that has an e-commerce Web site on the Internet. The Web site contains both secured and unsecured content. The URL for the unsecured home page is http://www.contoso.com. The URL for the secured e-commerce portion of the Web site is https://purchase.contoso.com. Traffic between clients and the home page is unencrypted; whereas SSL encrypts traffic between clients and the e-commerce portion of the Web site.

To use SSL, you must install a valid server certificate on the Web server for each Web site that you want to use with SSL. Certificates are usually granted to organizations through trusted certification authorities. Part of the information that is contained in a certificate is information about the organization to which the certificate was granted, such as the registered domain name. Thus, Web sites with registered domain names need their own certificate.

Client browsers perform a number of verification checks on the SSL certificate. When a client browser detects an incorrect value in the certificate, the browser displays warning messages. The client browser can verify the following:

- Digital signature of the certificate
- Expiration date of the certificate
- Registered domain name to which the certificate was issued against the URL requested

To enable SSL, complete the following steps for each Web site and application:

1. Request a server certificate for the Web site from a certification authority.

   You can use the Web Server Certificate Wizard either to generate a certificate request file (Certreq.txt, by default) that you send to a certification authority, or to generate a request for an online certification authority, such as Microsoft Certificate Services in Windows Server 2003. Depending on the level of identification assurance offered by your server certificate, you can expect to wait several days to several months for the certification authority to approve your request and send you a certificate file.

For more information about requesting a server certificate by using the Web Server Certificate Wizard, see “Request a Server Certificate” in “IIS Deployment Procedures” in this book.

2. Install the server certificate to be used by the Web site on the Web server.

   For more information about installing the server certificate on the Web server by using the Certificate MMC snap-in, see “Install a Server Certificate” in “IIS Deployment Procedures” in this book.

3. Assign the server certificate to the Web site.

   For more information about assigning the server certificate to the Web site, see “Assign a Server Certificate to a Web Site” in “IIS Deployment Procedures” in this book.

Using IPSec or VPN with Remote Administration

You can use Internet Protocol security (IPSec) and virtual private networks (VPNs) to help secure traffic for Web server administration tasks performed over the network, such as uploading content by using FTP or managing the Web server. In addition to encrypting administrative traffic, IPSec and VPNs provide cryptographically strong authentication methods, such as computer certificates, smart cards, and strong password requirements, to provide improved *identity checking*.

Identity checking is the process of verifying the authenticity of the user credentials. Computer certificates, issued by your organization, ensure that remote administration is performed from specific computers and provides improved identity checking.

If your organization provides hosting of Web sites for other organizations, these organizations need to have a secure method for posting their Web site content to your Web servers. Because the organizations post their Web site content over the Internet, you need to encrypt the traffic and provide enhanced identity checking to help protect confidential information.

For example, you can use FTP to upload Web site content to be published on production Web servers. Because FTP exchanges content and user credentials in plaintext, you need to use IPSec or VPNs to encrypt the traffic.

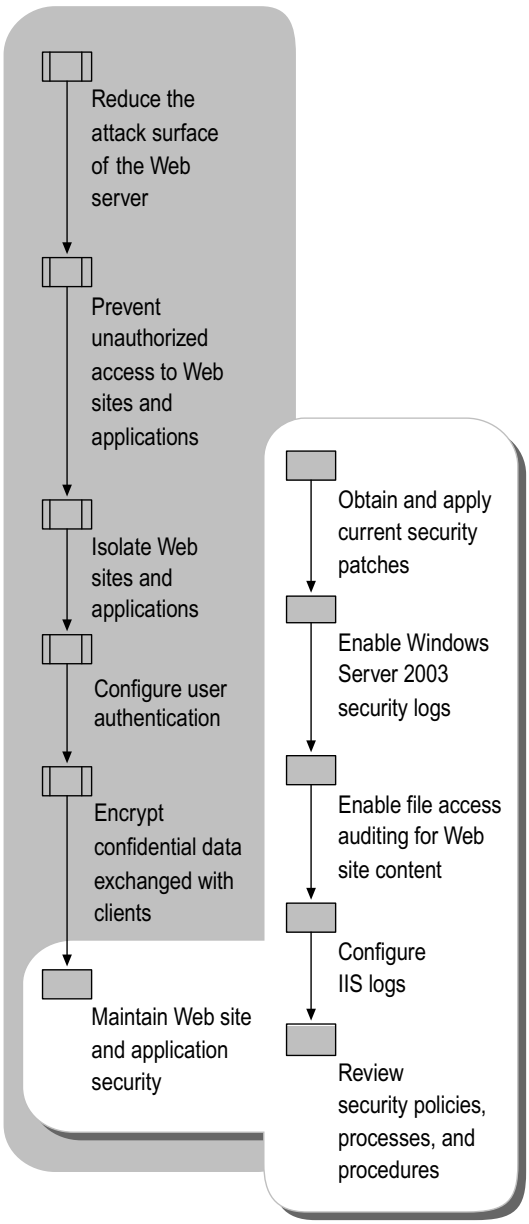
For more information about designing and deploying IPSec, see “Deploying IPSec” in *Deploying Network Services* of this kit. For more information about designing and deploying VPNs, see “Deploying Dial-up and VPN Remote Access Servers” in *Deploying Network Services* of this kit.

Maintaining Web Site and Application Security

After securing the Web sites and applications on your Web server, you need to help ensure that the Web sites and applications stay secure. You need to deploy Web servers that are easy to manage and operate. As you deploy the Web server, keep in mind the operations processes that must be performed after the Web server is deployed.

Figure 3.7 illustrates the process for maintaining the security of your Web sites and applications.

Figure 3.7 Maintaining Web Site and Application Security



For more detailed coverage of security operations processes, see "Managing a Secure IIS Solution" in *Internet Information Services (IIS) 6.0 Resource Guide*.

Obtaining and Applying Current Security Patches

You should always evaluate and apply the latest security updates to help ensure that your Web sites and applications remain secure. These security updates are published as service packs or hotfixes. As new security vulnerabilities are discovered, Microsoft publishes updates to help mitigate any security risks they might cause. You need to apply these security updates to help ensure that your Web server is protected from the most current security risks.

Stay current with security updates by completing the following steps:

1. Obtain the current security updates by using any combination of the following:

- **Subscribe to the Microsoft Security Notification Service newsletter.** The Microsoft Security Notification Service newsletter is a free subscription-based service that sends notification e-mails about available security updates to administrators.

  To subscribe to the Microsoft Security Notification Service newsletter, see the Microsoft.com Profile Center link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources. There is no charge for registering to receive the newsletters.

- **Run Windows Update on a regular basis.** Windows Update is a service that runs on Windows-based computers. Windows Update scans the local computer and identifies any updates that are applicable for the software installed on the computer. Windows Update is installed on Windows Server 2003 by default. You must manually start Windows Update on the Web server from Help and Support Center for Microsoft® Windows® Server 2003.

  For more information about running Windows Update, see "Windows Update" in Help and Support Center for Windows Server 2003.

- **Deploy Microsoft Software Update Services (SUS).** SUS is a service that acts as an intermediary between the Windows Update server on Microsoft.com and the Windows-based computers in your organization running Windows Update. By using SUS, you can download the latest updates to a server on your intranet, test the updates on test servers, select the updates that you want to deploy, and then deploy the updates to computers within your organization.

  For more information about deploying SUS, see "Deploying Software Update Services" in *Designing a Managed Environment* of this kit.

Table 3.11 lists the options for obtaining security updates, and describes the advantages and disadvantages of each option.

Table 3.11 Options to Obtain Security Updates

Option	Advantages	Disadvantages
Microsoft Security Notification Service Newsletter	• Does not require Web servers to be directly connected to the Internet • Does not require a dedicated server • Free	• Is not specific to a particular technology, such as IIS • Is not specific to a particular operating system version • Requires administrators to manually review newsletters for recommended updates
Windows Update	• Provides automatic notification of available updates • Free	• Requires the Web server to have Internet access.
SUS	• Provides automatic notification of available updates	• Requires a dedicated server to run properly • Requires the SUS server be able to access the Internet • Requires separate purchase of SUS

2. Test the security updates on a Web server in a test environment.

Before deploying the security updates on your production Web server, use one of the options described in Step 1 to test the security updates on a test Web server that is configured identically to your production Web server. Table 3.12 lists the methods for deploying the security updates on a Web server in a test environment.

Table 3.12 Methods for Deploying Security Updates

Method	Deployment
Microsoft Security Notification Service Newsletter	**Manually download the updates and then deploy them manually or automatically by using a software distribution program, such as Microsoft System Management Server.**
Windows Update	**Configure Windows Update to do one of the following:** • Inform an administrator that is logged on to the Web server that updates are available and then allow the administrator to install the updates • Automatically install the updates.
SUS	**Configure the SUS to provide updates to the Web server through an updated version of Windows Update called Automatic Updates.**

You can configure Windows Update and Automatic Updates in SUS to install updates automatically, with or without confirmation, based on the security rating of the update. Table 3.13 lists the security ratings used by Windows Update and Automatic Updates, and provides a description of each rating.

Table 3.13 Security Ratings Used by Windows Update and Automatic Updates

Rating	Description
Critical	**A vulnerability that, if exploited, might allow the propagation of an Internet worm without user action.**
Important	**A vulnerability that, if exploited, might result in a compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources.**
Moderate	**A vulnerability risk that can be mitigated by factors such as default configuration, auditing, or difficulty to exploit.**
Low	**A vulnerability that is extremely difficult to exploit, or that has minimal impact.**

3. Deploy the security updates to your production Web server by using the same option that you tested on the test Web server.

Enabling Windows Server 2003 Security Logs

Collecting information about the security aspects of the Web server is required to help ensure that the Web server stays secure. Windows Server 2003 uses security and system logs to store collected security events. The security and system logs are repositories for all events recorded on the Web server. Many management systems, such as Microsoft Operations Manager, periodically scan these logs and can report security problems to your operations staff.

If you audit or log too many events, the log files might become unmanageable and contain superfluous data. Before enabling the system and security logs, you need to enable auditing for the system log and establish the number of events that you want recorded in the security log. You cannot change the information that is logged in the system log: These events are preprogrammed into Windows Server 2003 services and applications. You can customize system log events by configuring *auditing*. Auditing is the process that tracks the activities of users and processes by recording selected types of events in the security log of the Web server. You can enable auditing based on categories of security events. At a minimum, enable auditing on the following categories of events:

- Any changes to user account and resource permissions
- Any failed attempts for user logon
- Any failed attempts for resource access
- Any modification to the system files

You can customize which types of events are recorded in the security log. The most common security events recorded by the Web server are associated with user accounts and resource permissions.

For more information about how to enable security auditing, see “Enable Security Auditing” in “IIS Deployment Procedures” in this book.

Enabling File Access Auditing for Web Site Content

In addition to enabling Windows Server 2003 security logs, enable file access auditing for your Web site content. This is a separate step that must be completed to monitor any changes to the files and directories that contain your application and content.

You can enable auditing on a user-by-user basis for each file and directory. However, at a minimum, enable auditing for all users for any successful or failed attempts to do the following:

- Modify or delete existing content
- Create new content

Tip

Beyond these minimal events, you can audit content for other purposes, such as forensic analysis of intruder detection.

For more information about how to enable file auditing on Web site content and files, see “Enable Web Site Content Auditing” in “IIS Deployment Procedures” in this book.

Configuring IIS Logs

In addition to the Windows Server 2003 system and security logs, you should configure IIS to log site visits. When users access your server running IIS 6.0, IIS logs the information. The logs provide valuable information that you can use to identify any unauthorized attempts to compromise your Web server.

Depending on the amount of traffic to your Web site, the size of your log file (or the number of log files) can consume valuable disk space, memory resources, and CPU cycles. You might need to balance the gathering of detailed data with the need to limit files to a manageable size and number. If you are planning to put thousands of Web sites on one Web server with high traffic volumes and disk writes, you might want to use centralized binary logging to preserve server resources. Also, consider limiting log size by changing the frequency of log

file creation. For more information, see “Saving Log Files” in IIS 6.0 Help, which is accessible from IIS Manager.

The IIS logs allow you to record events for each application and Web site on the Web server. You can create separate logs for each of your applications and Web sites. Logging information in IIS 6.0 goes beyond the scope of the event logging or performance monitoring features provided by Windows. The IIS logs can include information, such as who has visited your site, what the visitor viewed, and when the information was last viewed. You can use the IIS logs to identify any attempts to gain unauthorized access to your Web server.

IIS 6.0 supports different log formats for the IIS logs that you enable. IIS 6.0 supports the following log formats.

W3C Extended log file format

World Wide Web Consortium (W3C) Extended format is a customizable ASCII format with a variety of different properties. You can log properties that are important to you, while limiting log size by omitting unwanted property fields. Properties are separated by spaces. Time is recorded as Universal Time Coordinate (UTC).

For information about customizing this format, see “Customizing W3C Extended Logging” in IIS 6.0 Help, which is accessible from IIS Manager. For more information about the W3C Extended format specification, see the W3C World Wide Web Consortium link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources.

IIS log file format

IIS log file format is a *fixed* (meaning that it cannot be customized) ASCII format. This file format records more information than other log file formats, including basic items, such as the IP address of the user, user name, request date and time, service status code, and number of bytes received. In addition, IIS log file format includes detailed items, such as the elapsed time, number of bytes sent, action (for example, a download carried out by a **GET** command), and target file. The IIS log file is an easier format to read than the other ASCII formats because the information is separated by commas, while most other ASCII log file formats use spaces for separators. Time is recorded as local time.

For more information about the IIS log file format, see “About Logging Site Activity” in IIS 6.0 Help, which is accessible from IIS Manager.

NCSA Common log file format

National Center for Supercomputing Applications (NCSA) Common log file format is a fixed ASCII format that is available for Web sites, but not for FTP sites. This log file format records basic information about user requests, such as remote host name, user name, date, time, request type, HTTP status code, and the number of bytes sent by the server. Items are separated by spaces. Time is recorded as local time.

For more information about the NCSA Common log file format, see “About Logging Site Activity” in IIS 6.0 Help, which is accessible from IIS Manager.

ODBC logging

Open Database Connectivity (ODBC) logging format is a record of a fixed set of data properties in a database that complies with ODBC, such as Microsoft Access or Microsoft SQL Server. Some of the items logged include the IP address of the user, user name, request date and time (recorded as local time), HTTP status code, bytes received, bytes sent, action carried out (for example, a download carried out by a **GET** command), and the target file. With ODBC logging, you must both specify the database to be logged to, and set up the database to receive the data.

Note

When ODBC logging is enabled, IIS disables the kernel-mode cache. As a result, overall server performance can be degraded.

For more information about ODBC logging, see “About Logging Site Activity” in IIS 6.0 Help, which is accessible from IIS Manager.

Centralized binary logging

Centralized binary logging is the process of multiple Web sites writing binary, unformatted log data to a single log file. Each Web server running IIS creates one log file for all of the Web sites on that server. Centralized binary logging preserves valuable memory resources. Depending on your configuration, you can see dramatic performance and scalability gains with centralized binary logging.

For more information about centralized binary logging, see "Centralized Binary Logging" in IIS 6.0 Help, which is accessible from IIS Manager.

For more information about how to configure IIS logs, see "Enable Logging" in "IIS Deployment Procedures" in this book. For more information about logging Web site activity, see "Logging Site Activity" in IIS 6.0 Help. For more information about managing IIS logs, see "Analyzing Log Files" in *Internet Information Services (IIS) 6.0 Resource Guide* of the *Windows Server 2003 Resource Kit*.

Reviewing Security Policies, Processes, and Procedures

As a part of maintaining the security of your Web server, you must perform periodic reviews of the security policies, processes, and procedures in use by your organization. Review your security practices for any changes that might affect the security of the Web server. These changes in security practices can include the following:

Ensuring that any recent security risks are mitigated As new security risks are identified, such as new viruses, you need to ensure that your security practices help mitigate these risks. If your current security practices do not address the new risks, then modify them to help mitigate the risks.

Identifying changes in Web server configuration that can compromise security Through the course of normal administration of the Web server, configuration changes are made. During this process, security settings might have been inadvertently changed. You need to periodically review the configuration of the Web server to ensure that it complies with the security requirements of your organization.

You can categorize these Web server security practices by their function, such as operating system security, security policies, firewall security, and router security. In addition, the frequency with which these processes and procedures are completed varies. Some security practices need to be completed continuously while others might be completed monthly.

Table 3.14, Table 3.15, Table 3.16, and Table 3.17 list examples of security policies, processes, and procedures for an ISP, grouped by categories. These examples are representative of the types of security practices that are required to maintain the security of your Web server. For more information about the security policies, processes, and procedures for your Web server, see "Managing a Secure IIS Solution" in *Internet Information Services (IIS) 6.0 Resource Guide* of the *Windows Server 2003 Resource Kit*.

Table 3.14 Windows Server 2003 Operating System Security

Security Policy, Process, or Procedure	Frequency
Limit user rights to only those that are required.	Constant
Limit any windows for vulnerabilities that can be exploited when deploying new servers.	Constant
Limit Terminal Services access to only necessary accounts.	Constant
Run a two-tier DNS structure to protect the identity of internal servers.	Constant
Run an intrusion detection system.	Constant
Scan the ports in use on your server addresses and addresses	Daily

assigned to remote users.	
Review event and IIS logs.	**Weekly**
Test firewalls from inside and outside by using port scanners and other appropriate tools.	**Weekly**

Table 3.15 Windows Server 2003 Policy Security

Security Policy, Process, or Procedure	Frequency
Explicitly deny interactive logon user right to all nonadministrative accounts.	**Constant**
Explicitly deny "Allow logon through Terminal Services" user right to all nonadministrative accounts.	**Constant**
Enable FULL (Success/Failure) auditing on domain Group Policy objects.	**Constant**
Send event notification when events like "User added to Domain Administrators" occur.	**Constant**

(continued)

Table 3.15 Windows Server 2003 Policy Security *(continued)*

Security Policy, Process, or Procedure	Frequency
Allow only Administrators to have write permissions on all content servers.	**Constant**
Require strong passwords for all users.	**Constant**
Require smart cards for all administrators.	**Constant**
Allow administrators to log on only to specific workstations.	**Constant**
Enable account lockout policies for failed logon attempts.	**Constant**
Audit the domain Group Policy object.	**Monthly**
Audit Active Directory user rights.	**Monthly**
Audit all servers to determine if nonessential services are running.	**Monthly**

Table 3.16 Firewall and Router Security

Security Policy, Process, or Procedure	Frequency
Restrict the network segments where management traffic is allowed.	**Constant**
By default, deny IP traffic and log any failed attempts.	**Constant**

Ensure that the minimal firewall rules are enforced, including:
• Explicitly deny all traffic to the following:
  • TCP and UDP ports 135-139, 455 (NetBIOS/SMB)
  • TCP and UDP ports 3389 (Terminal Services)
  • Domain controllers
  • Internal DNS servers
	Constant

• Permit traffic to TCP and UDP port 53 (DNS) to external DNS servers.	

Table 3.17 Miscellaneous Security

Security Policy, Process, or Procedure	Frequency
Run virus scans on all servers.	**Constant**
Monitor security distribution lists and newsgroups for potential security issues.	**Constant**
During virus outbreaks, block any suspicious content (such as e-mail attachments).	**Constant**
Monitor the number of Non-Delivery mail reports generated (indicates e-mail spamming).	**Weekly**
Monitor SMTP relay attempts that are not valid (indicates e-mail spamming).	**Weekly**
Audit accounts to determine the users who are no longer employed at the organization, partner organizations, or customer organizations.	**Monthly**

Additional Resources

These resources contain additional information and tools related to this chapter.

Related Information

- "Deploying ASP.NET Applications in IIS 6.0" in this book for information about ASP.NET-specific deployment considerations.
- "Ensuring Application Availability" in this book for information about balancing application security and availability.
- "IIS Deployment Procedures in this book for information about specific procedures for securing Web sites and applications.
- "Deploying Dial-up and VPN Remote Access Servers" in *Deploying Network Services* of the *Microsoft® Windows® Server 2003 Deployment Kit* for information about designing and deploying VPN.
- "Deploying IPSec" in *Deploying Network Services* of this kit for information about designing and deploying IPSec.
- "Deploying Software Update Services" in *Designing a Managed Environment* of this kit for information about deploying SUS.
- "Planning a Secure Environment" in *Designing and Deploying Directory and Security Services* of this kit for information about securing other services on a multipurpose server.
- "Analyzing Log Files" in *Internet Information Services (IIS) 6.0 Resource Guide* of the *Windows Server 2003 Resource Kit* for information about managing IIS logs.
- "Managing a Secure IIS Solution in *Internet Information Services (IIS) 6.0 Resource Guide* of the *Windows Server 2003 Resource Kit* for information about maintaining Web server security.

- The Microsoft.com Profile Center.link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources for information about how to subscribe to the Microsoft Security Notification Service newsletter.
- The W3C World Wide Web Consortium link on the Web Resources page at http://www.microsoft.com/windows/reskits/webresources for information about the W3C Extended format specification.

Related IIS 6.0 Help Topics

- "About Logging Site Activity" in IIS 6.0 Help, which is accessible from IIS Manager, for information about log file formats.
- "Enabling Client Certificates" in IIS 6.0 Help, which is accessible from IIS Manager, for information about configuring client certificates.
- "NTFS Permissions" in IIS 6.0 Help, which is accessible from IIS Manager, for information about the benefits of formatting disk volumes as NTFS on Web servers.
- "Saving Log Files" in IIS 6.0 Help, which is accessible from IIS Manager, for information about balancing the gathering of detailed data with the need to limit files to a manageable size and number.
- "SMTP Administration" or "NNTP Administration" in IIS 6.0 Help, which is accessible from IIS Manager, for information about securing SMTP or NNTP.
- "Troubleshooting" in IIS 6.0 Help, which is accessible from IIS Manager, for information about troubleshooting problems related to Web sites and applications that are not functioning.
- "Web Application Isolation" in IIS 6.0 Help, which is accessible from IIS Manager, for information about potential application compatibility problems that can occur when running worker processes under different identities, especially for Web sites that use user authentication.

Related Windows Server 2003 Help topics

For best results in identifying Help topics by title, in Help and Support Center, under the **Search** box, click **Set search options**. Under **Help Topics**, select the **Search in title only** check box.

- "Windows Update" in Help and Support Center for Windows Server 2003 for information about using Windows Update.