Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 4.0 â

The Network Applications Team

Of the

Systems and Network Attack Center (SNAC)

By:
Sheila Christman
4 March 2002
Version 1.3.3

National Security Agency
9800 Savage Rd.
Ft. Meade, MD 20755-6704

WIN2KGuides@nsa.gov

Warning

Caution: This document contains possible recommended settings for the system Registry. You can severely impair or disable a Windows NT System Internet Information Server4.0 with incorrect changes or accidental deletions when using a Registry editor (Regedt32.exe or Regedit.exe) to change the system configuration.

Currently, there is no “undo” command for deletions within the Registry. Registry editor prompts you to confirm the deletions if “Confirm on Delete” is selected from the options menu. When you delete a key, the message does not include the name of the key you are deleting. Therefore, check your selection carefully before proceeding.

Trademark Information

Table of Contents

About the Guide to the Secure Configuration and Administration of IIS4.0

This document is one of two documents that describe how to securely install, configure, and administer the Internet Information Server4.0 (IIS) and associated services. The focus of these documents is security-relevant information pertaining to the installation and administration of Internet Information Server4.0. This includes the secure configuration of FTP, WWW, and SMTP services as they relate to IIS4.0.

This document is intended for the reader who is already familiar with Internet Information Server but needs to understand how to install, configure, and administer the product in a more secure manner. The information presented here is written in a direct and concise manner in deference to this intended audience.

While this document is intended as a complement to the *Guide to Secure Microsoft Windows NT Networks*, it presents the information a little differently. Some Internet Information Server security issues, and corresponding configuration and administrative actions are very specific to the way the product is being used. For this reason, it is difficult in some areas to recommend specific, concrete actions. Instead, a summary is offered which describes the concerns and recommends solutions that you must tailor to your environment.

Table 1 Summary of IIS Documentation

Document	Contents	Target audience
Guide to the Secure Configuration and Administration of Internet Information Server 4.0 (This document)	• A detailed look at the secure installation and configuration of IIS4.0 and it's associated services	• Experienced NT administrators who may be new to IIS
Internet Information Server (IIS) – Secure Installation and Configuration Checklist	• A secure installation and configuration guide in checklist format with no detailed explanations	• Experienced NT and IIS administrators

PLEASE NOTE THAT THESE DOCUMENTS ASSUME THAT THE READER IS A KNOWLEDGEABLE WINDOWS NT ADMINISTRATOR. A knowledgeable Windows NT administrator is defined as someone who can create and manage accounts and groups, understands how Windows NT performs access control, understands how to set account policies and user rights, is familiar with how to setup auditing and read audit logs, etc. These documents do not provide step-by-step instructions on how to perform these basic Windows NT administrative functions. It is assumed that the reader is capable of implementing basic instructions regarding Windows NT administration without the need for highly detailed instructions.

This document consists of the following chapters:

Chapter 1, "Internet Information Server Installation", provides an overview of the pertinent security issues related to the installation of the Internet Information Server4.0.

Chapter 2, "Administrative Tool-MMC" describes the Microsoft Management Console tool and Snap-ins used to manage IIS4.0.

Chapter 3, "Services Installation and Administration" describes configuration of the main functional components of IIS4.0 and details the pertinent security-related settings (WWW, FTP and SMTP)

Chapter 4, "Additional Security Issues" describes multiple administrator groups, IIS4.0 logging and a brief description of Certificates.

Chapter 5, "Final Thoughts**" –** Comments on backups and antiviral programs.

An Important Note About Operating System Security

IIS security is tightly coupled to the operating system. For example, IIS logon is coupled to the operating system logon so that a user does not have to log-on separately to manage or access IIS.

File permissions, Registry settings, password usage, user rights, and other issues associated with Windows NT security have a direct impact on IIS security.

The recommended source of information for how to securely configure the Windows NT 4.0 server and workstation is the *Guide to Secure Microsoft Windows NT Networks.* It is important to implement this guide on the IIS4.0 machine.

Chapter 1

Internet Information Server Installation

Internet Information Server (IIS) is a high-speed Web server used to publish and distribute WWW-based content to standard browsers. Install Version 4.0 from the Windows NT4.0 Option Pack CDROM. Version 2.0 can be installed during the installation of Windows NT4.0, however, this is not recommended. Version 4.0 provides the following publishing services: WWW, FTP, SMTP, and NNTP. Security issues relating to WWW, FTP and SMTP will be discussed in detail in this document. There are no unique security settings for NNTP in IIS4.0; therefore, this service will not be addressed. Three additional application services are commonly associated with IIS - the Certificate Server, the Index Server, and Microsoft Transaction Server. Although these services can be installed at the same time as IIS4.0 or later, the secure installation, configuration, and administration of these services will not be addressed in this document.

Operating System Security

Install IIS4.0 according to the manufacturer's instructions; however, prior to installing IIS4.0, invoke the Windows NT Operating System security guidelines contained within the *Guide to Secure Microsoft Windows NT Networks*. IIS4.0 security is tightly coupled to the operating system. File permissions, Registry settings, password usage, user rights, and other issues associated with Windows NT security have a direct impact on IIS4.0 security. The advantages gained by this tight coupling are: no increased complexity, and possibly security holes due to the addition of security layers; and better performance by eliminating unnecessary overhead caused by additional security and access control layers.

Visit Microsoft's Downloads web page for IIS 4.0 to install the latest security patches and hotfixes. The URL for obtaining this information is www.microsoft.com/Downloads. From this page, select the product IIS4.0 then download and install all required patches and hotfixes that address your particular security requirements.

Prior to configuring IIS4.0, determine how the server will be used. The configuration of IIS directories, files, user accounts and profiles, TCP/IP port connections, etc. will be based on your answers:

- Will the server be accessed from the Internet?
- Will the server be accessed from an Intranet?
- How many Web sites will this server host?
- Will the server permit anonymous or authenticated user access (or both)?
- Will Secure Socket Layer (SSL) connections be supported (HTTPS)?
- Will the server be used only for Web access via HTTP?
- Will the server support FTP services?
- Are there specific users that will need to copy, open, delete, and write files on your server?

When installing IIS4.0, the following guidelines are recommended:

Place your IIS machine where it will be physically secure; i.e., behind a locked door where only authorized personnel can gain physical access to it.

If possible, install IIS on a server with its own domain and no trust links to other domains.

Install IIS4.0 on a standalone server, where possible. If IIS4.0 is installed on a domain controller and the Web server is attacked, the entire server and sensitive domain information may be at risk. You should tighten up the security on this server as follows:

Install IIS4.0 on a server that is not required to support any other service. Neither application software nor development tools should be installed on the IIS4.0 server.

The IIS machine should be partitioned so that published content of each supported service (WWW, FTP, etc.) is located on a separate partition. This will prevent attempts to traverse up the directory tree beyond the published content root.

Do not install IIS4.0 on the same partition as the Operating system. The default permissions applied to the %SystemDrive%, typically C:\, by the *Guide to Secure Microsoft Windows NT Networks* may cause some services in IIS to not function properly if installed there.

Enable audit and IIS logging and track the information (described in Chapter 4).

Remove all protocol stacks except TCP/IP, unless your Intranet requires another protocol stack.

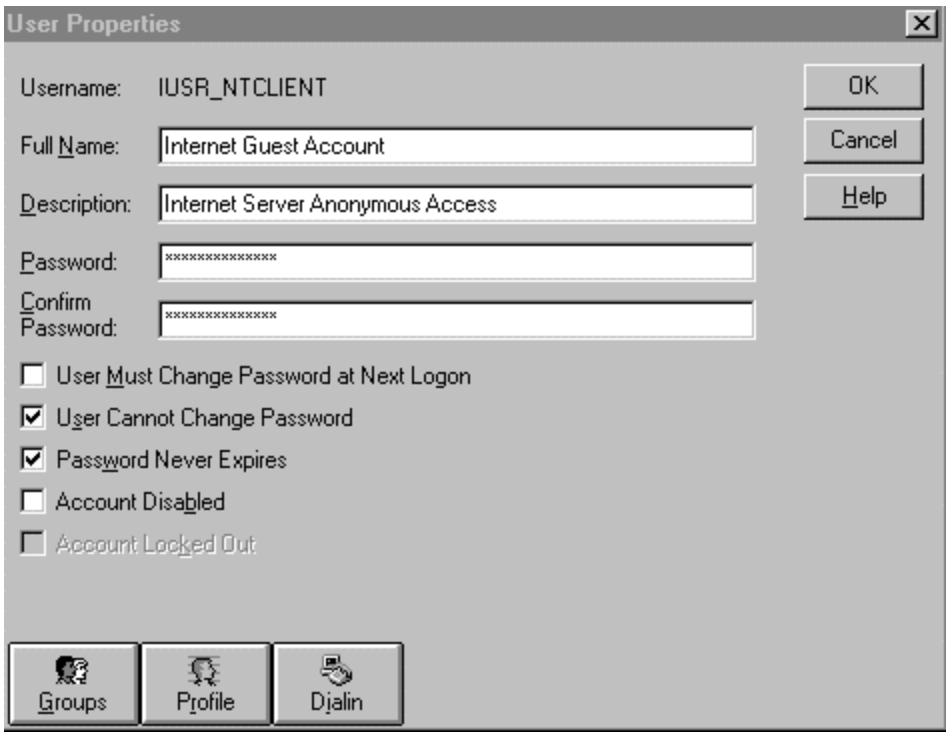
Disable IP Routing. If routing is enabled, it is possible to have data pass from your Intranet to the Internet. Open the **Network icon** in Control Panel, click the **Protocols** tab, select **TCP/IP Protocol**, and then click **Properties**. On the **Routing** tab, make sure the **Enable IP Forwarding** check box is clear.

The following is a list of services that are not required for most installations of IIS4.0 and should be disabled.

- Alerter
- ClipBook Server
- Computer Browser
- DHCP Client
- Messenger
- Net Logon (do not disable if domain users are required to logon to the server - this service is required to communicate with the domain controller)
- Network DDE & Network DDE DSDM
- Network Monitor Agent
- Simple TCP/IP Services
- Spooler
- NetBIOS Interface
- TCP/IP NetBIOS Helper
- WINS Client (TCP/IP)
- NWLink NetBIOS
- NWLink IPX/SPX Compatible Transport (not required unless you do not have TCP/IP or another transport)
- FTP Publishing Service (unless FTP services are required for your server)
- RPC Locator (only required if you are doing remote administration)
- Server Service (has to be started if you need to run User Manager)

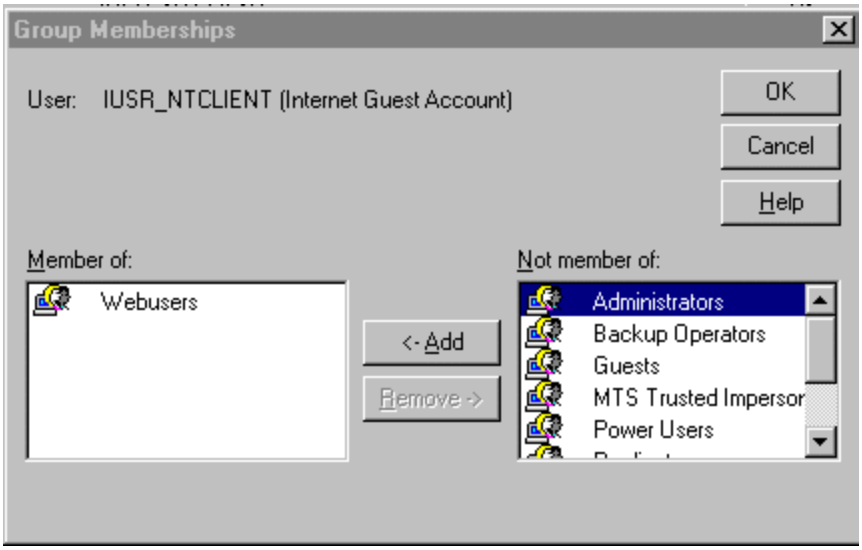
Post Installation

During the installation of IIS, a default account is created for anonymous logons. The default name for this account is IUSR_*computername,* where *computername* is the name of the machine hosting IIS. This account should be given the least amount of privileges possible. Review the security settings for the IUSR_*computername.* Make sure “User Cannot Change Password” and “Password Never Expires” options are selected. This account should be a local account, not a domain-wide account, and must have the Right to “log on locally”. It does not require the Right to “access this computer from the network”. If anonymous access to your Web site is prohibited, it is recommended that this account be disabled. All users would then be required to supply a valid username and password, using either Basic authentication or Windows NT Challenge/Response to access server resources. It is not necessary to use the default anonymous account name. This account can be disabled and another account created for this purpose. A description of these options, along with how to change the default account name, can be found in Chapter 3.



User Properties Sheet for Anonymous Account

Create at least two new groups to be used with IIS. The “WebAdmins” group, for example, to define users who will administer WWW content. If your sever will host several Web sites, create an administrative group for each site. A “WebUsers” group should be created as the primary group for the IUSR_*computername* account. The IUSR_*computername* account should not be a member of any other group. By default, the IUSR_*computername* account is a member of the Guests group. It is recommended that this account be removed from the Guests group and added to the “WebUsers” group. All accounts placed within the “WebUsers” group should ONLY be used for Web site access and should not be a member of any other group, i.e., "Users" group.



IUSR_*computername* as a member of WebUsers group ONLY

After installing IIS4.0, change the access permissions on the IIS install directories. It is particularly important to make certain that “Everyone”, “Guests”, and "Guest" are not granted access by highlighting them and selecting the "Remove" button. By default, the group "Everyone" is given Full Control of the default install directory (i.e., Inetpub). These group and user accounts are commonly used by malicious users to gain access to systems. Removing them will prevent such users from using your server for data storage or staging an attack by placing malicious code on the server. The following table shows the recommended NTFS and IIS permissions for the IIS-related directories. **Note**: IIS permissions complement the NTFS permissions. For a file to be sent to the client browser for rendering, IIS Read permission must be set for the Web directory, and the user in whose context the server is running must have NTFS Read access to that file. If they do not match, the most restrictive permission will be enforced. Chapter 3 will describe in detail IIS permissions and other security settings for WWW and FTP sites.

Table 2 Permission Settings

Type of Data	Example Directories	Data Examples	NTFS File Permissions	IIS4.0 Permissions
Static Content	\wwwroot\images \wwwroot\home \ftproot\ftpfiles	HTML, images, FTP downloads, etc.	Administrators (Full Control) System (Full Control) WebAdmins (Read,Write,Delete) Authenticated Users (Read) Anonymous (Read)	Read
FTP Uploads (if required)	/ftproot/dropbox	Directory used as a place for users to store documents for review prior to the Admin making them available to everyone	Administrators (Full Control) WebAdmins or FTPAdmins (Read,Write,Delete) Specified Users (Write)	Write
Script Files	\wwwroot\scripts	.ASP	Administrators (Full Control) System (Full Control) WebAdmins(Read,Write,Execute,Delete) Anonymous (Execute)	Script
Other Executable and Include Files	\wwwroot\executables \wwwroot\include	.exe, .dll, .cmd, .pl .inc, .shtml, .shtm	Administrators (Full Control) System (Full Control) WebAdmins (Read,Write,Execute,Delete) Authenticated Users (Read) Anonymous (Execute)	Execute
Metabase	\WINNT\system32\inetsrv	MetaBase.bin	Administrators (Full Control) System (Full Control)	N/A

Establish directories that contain read only files (HTML, images, files made available for FTP download, and other such files). Each type should have its own directory with ONLY Read (NTFS and IIS4.0) permission for file access allowed to the WebUsers group. Grant Read, Write, and Delete file access permissions to the group responsible for maintaining Web content (i.e., WebAdmins).

Establish directories that contain executable files only (scripts, batch files, and other executables). These directories should ONLY have NTFS Execute permission for users accessing your site (i.e., IUSR_*computername*, WebUsers) and IIS permission of Script ONLY. IIS4.0 Execute permission should only be allowed on directories where appropriate, i.e., a directory containing binary files that must be executed by the Web server. Script and Execute are additional access control permissions offered by IIS4.0. These options will be discussed in detail in Chapter 3.

Delete or move all directories that contain “samples” and any scripts used to execute the “samples”. The following is a list of directories created during the installation of IIS. It is recommended that these directories be deleted or relocated. If there is a requirement to maintain these directories at your site for training purposes, etc., have NTFS permissions set to only allow access to authorized users, i.e., “WebAdmins” and administrators. Also, to control access to these directories through WWW, require NTLM Challenge/Response authentication through the Web Site Properties dialog box (Chapter 3 describes how to configure this setting).

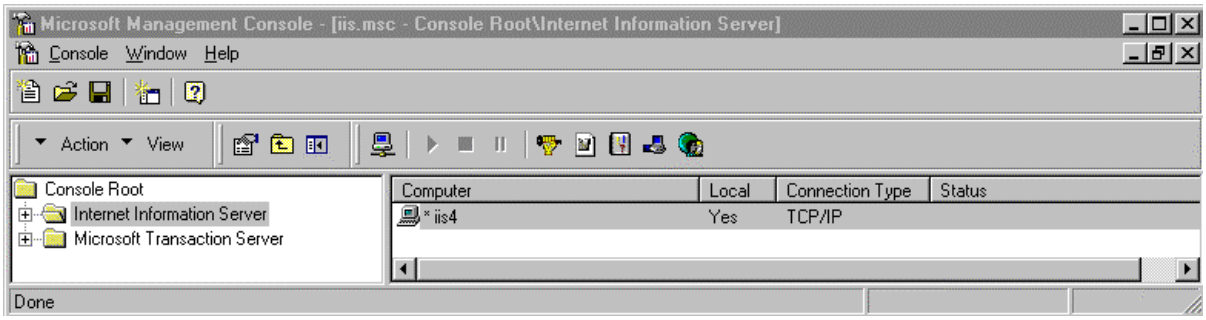
- \InetPub\ASPSamp
- \InetPub\iissamples
- \InetPub\scripts\tools
- \InetPub\scripts\samples
- \InetPub\wwwroot\samples
- InetPub\AdminScripts
- \Program Files\Common Files\System\msdac\Samples

Chapter

Administrative Tool – MMC

In earlier versions of the Windows NT Operating System, a collection of applications to manage the operating system and services were required. A single management function or group of similar functions was provided by one tool, while different tools provided other management functions. Understanding and locating the correct tool to run to access the desired management function was often a concern for new or inexperienced administrators. The Microsoft Management Console (MMC) partially addresses this concern by providing a user interface shell application, called a console. The objective is that all management functions are accessible by a subordinate process running within a console. These processes are known as Snap-ins. MMC itself does not provide any management behavior, but it offers a common environment for Snap-ins. The result is that management/administrative control of the platform is centralized. A Snap-in for IIS, Internet Service Manager (ISM), is provided during installation.

Each instance of a console and associated Snap-ins is commonly referred to as a tool. Any number of tools can be created. Once created, the console can be populated with existing Snap-ins or a new Snap-in may be created for a specific purpose. Administrators can create tools that host several Snap-ins and save these for later use or for sharing with subordinate administrators. You can take advantage of the customization features by preparing consoles that perform only one task and use them to delegate responsibility to other, perhaps less experienced administrators. You can tailor the console to present only the menu choices the user needs to get the job done. For example, an administrator could create a new MMC console with the IIS Snap-in for Web administrators to use to manage Web resources.

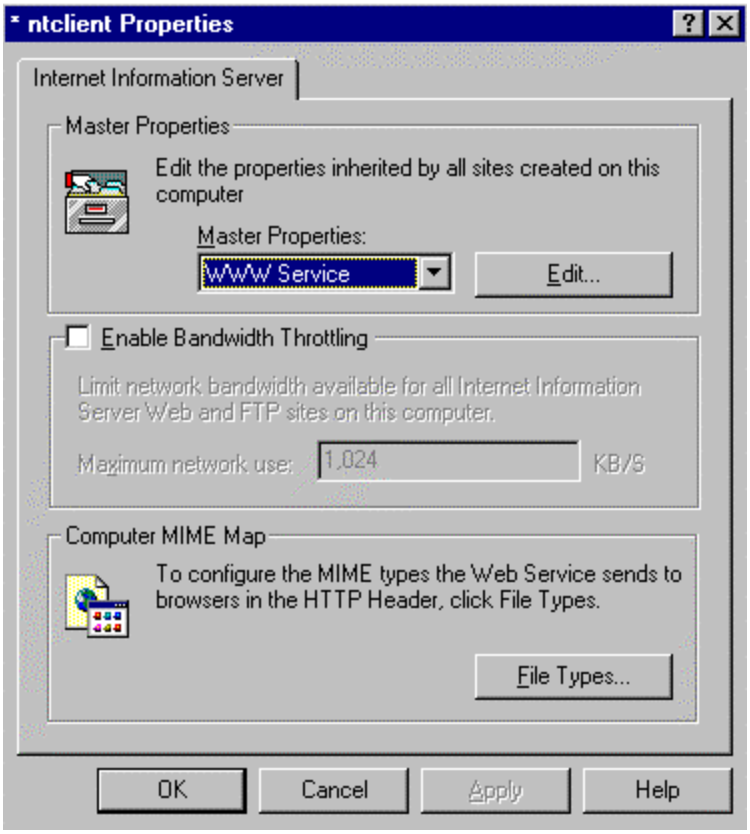


Microsoft Management Console with the Internet Service Manager Snap-In

NOTE: There is an HTML version of the ISM; however, several tasks cannot be performed using it. The HTML version is designed as a Web page and right-clicking is not supported. Some important IIS configuration options, such as changes to certificate mapping and starting other NT Server utilities, can only be performed using the ISM Snap-in.

Internet Service Manager

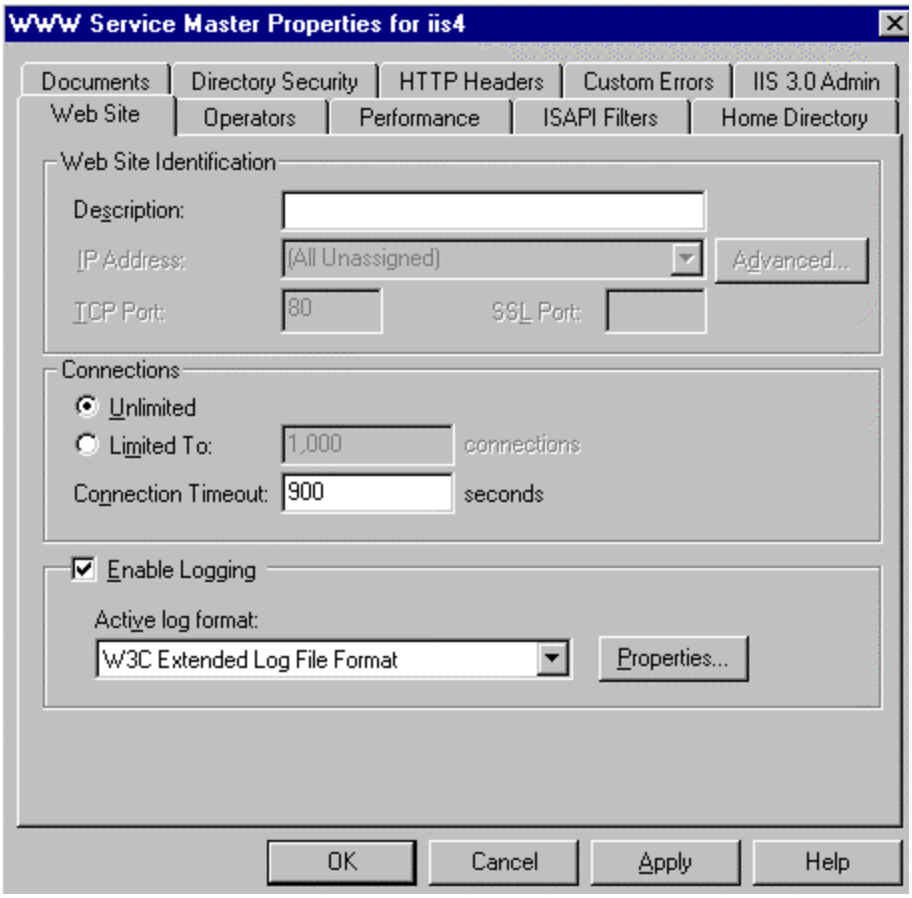
When you start the IIS4.0 Internet Service Manager (ISM), an MMC console begins running and automatically loads the Internet Information Server Snap-in. There are three main property dialog boxes general to IIS operation: Master Properties; Enable Bandwidth Throttling; and Computer MIME Map. Setting these general properties is very useful if you know that you will be creating a number of different Web sites on your server. These properties will be automatically inherited by all Web sites created on your server, which will save time when configuring each site. If some sites require different properties, these properties would be set during the configuration of each Web site. The common settings that can be established through the Master Properties dialog box to enhance security will be discussed here. The next chapter will describe the property dialog boxes for configuring individual security settings of the WWW, FTP and SMTP services using the ISM Snap-in. Access the Master Properties dialog box by highlighting the IIS server name in the ISM, then and select "**properties**" in the **Action** pull down menu. Click the **Edit** button to configure Master Properties for the selected server.



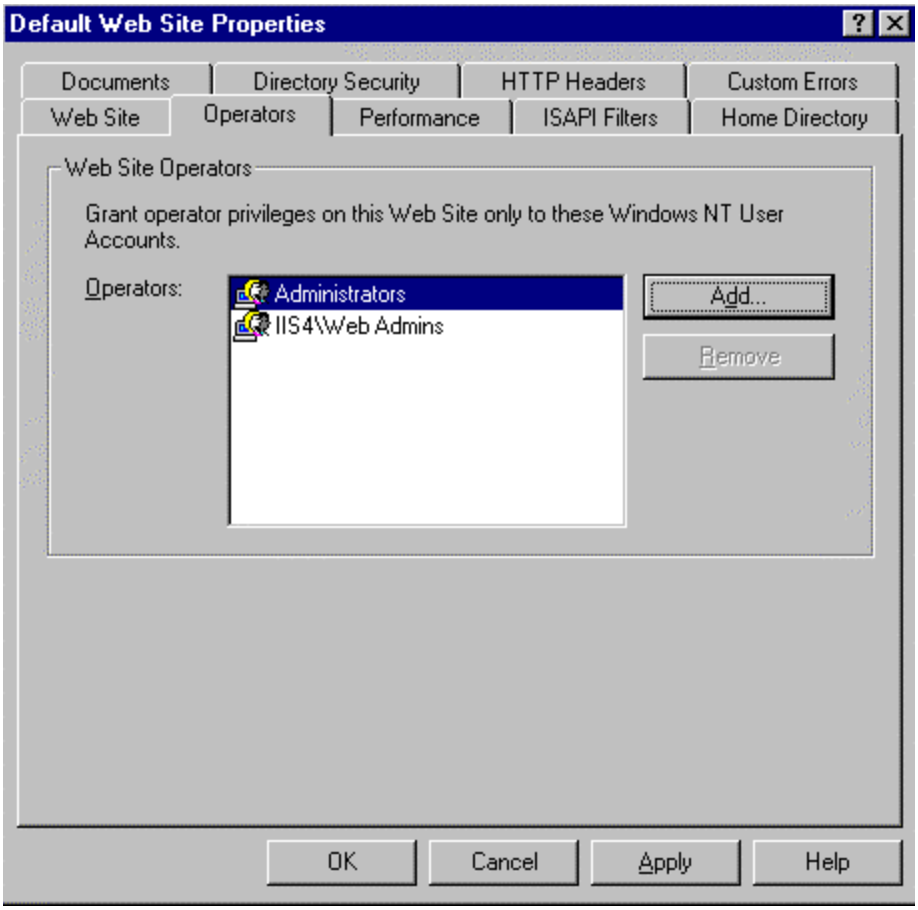
Master Property Dialog Box for IIS WWW Sites

Master Properties

This property dialog box is used to set default values used by all current or new sites on this server. If a value for a specific Web site will change as a result of the values set on the Master Properties dialog box, you will be prompted to select the items that should adopt the new settings. An item will remain unchanged if it is not selected. Changes made to a list-based property will replace the original setting, not merge with existing settings. Select **Edit** in Master Properties to configure common WWW site properties. Enable Logging is selected by default and is the only security-related setting on this dialog box. Keeping the default setting will ensure logging is enabled for all Web sites created on this server. The following shows the dialog boxes for setting common security-related properties using the Web Site tab and Operators tab. Other tabs may have common settings as well, but will depend on how you setup your server. Note that these same settings can be applied individually to the WWW, FTP, and SMTP services. Only the Web Site and Operators tabs are discussed here as they contain the settings that are most likely to be universally applicable to all of the services. Discussions of the remaining tabs can be found in Chapter 3.



Master Web Site Properties dialog box



Master WWW Operators dialog box

The Operators dialog box on the WWW Service Master Properties allows you to identify groups (recommended) or accounts with the permission to perform some administrative functions for all of the WWW sites created on this server. When you configure each site, these groups/accounts will automatically appear and you will have the option to remove them, as well as add other groups as appropriate for the site. If your server is responsible for maintaining several Web sites, create a separate group to manage WWW content for each site. As stated previously, These specific groups would be added to the above list during the configuration of each individual Web site.

Introduction of the Metabase

Purpose

The Metabase stores IIS configuration parameter values in a fast-access, memory-resident data store. The Metabase is specifically designed for use with IIS and is faster, more flexible, and more expandable than the Windows NT Registry.

Structure

Each node in the metabase structure is called a key, and may contain one or more IIS configuration values called *metabase properties*. The IIS metabase keys correspond to the components and capabilities of IIS, and each key contains properties that affect the configuration of its associated component or capability. The metabase is organized in a hierarchical structure that mirrors the structure of IIS as installed. Most of the IIS configuration keys and values stored in the system Registry for previous versions of IIS are now stored as properties in the metabase. New keys and values have been added for finer and more flexible control of IIS. An advantage of this metabase structure is that it facilitates assigning different settings of a property for different instances of the same key. For example, the MaxBandwidth property specifies how much of the total bandwidth available to a server can be committed to Web transactions. The metabase can now support a different MaxBandwidth setting for each Web site.

Security

The Metabase is stored in a specially formatted disk file named MetaBase.bin, and is located in the \Winnt\system32\inetsrv directory. The metabase loads from disk when IIS starts, is stored to disk when IIS shuts down, and is saved periodically while IIS is running. It is important to protect this file from unauthorized access, although sensitive data is stored in a secure manner within the file. If the file is replaced with a fraudulent file, the operation of the Web server can be compromised. If the file can be replaced while the server is not running, any changes implemented in the file will be effective the next time the server is started. The effects caused by these changes can range from denial of service through unauthorized service being provided by the Web server. It is recommended that you store this file on an NTFS partition and use Windows NT security to protect it. The default permission settings for this file are System and Administrators Full Access. Limiting the access to System and local Administrators provides good security; therefore, there is no need to change or add to these settings.

To reinforce access control to this file, it is recommended that this file be hidden from unauthorized users. This can be accomplished by moving or renaming the file. To relocate or rename the MetaBase file, you will need to stop IIS, move or rename the file, and modify the Registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InetMgr\Parameters. Add a new REG_SZ value to this key named MetadataFile to specify the new complete path of the Metabase file, including the drive letter and filename. This tells IIS where to find the file on startup.

Chapter

Services Installation and Administration

This chapter contains configuration and administration information pertaining to WWW, FTP, and SMTP services of IIS. Prior to detailing the installation and administration information for each service, a brief overview of the access control methods used by the services is provided.

Access Control Methods

IP address grant/deny restrictions

The first line of defense in the IIS security model is the ability to grant or deny access to the Web server based on IP address or Windows NT domain of the requesting client. A Windows NT domain or IP addresses of certain machines can be specified and either granted or denied access to the Web server. When any packet of data is received, its source IP address or domain name is checked against those defined in the "Advanced" tab of the WWW Service property dialog box, and the predefined actions for access are applied to it. When using IP address access control, note that some Web clients may be accessing your server through a proxy server of firewall. When this happens, the IP address of the incoming packets will be that of the proxy server or firewall itself, not of the actual user's client machine. Steps to configure this option for each service are described later in this chapter.

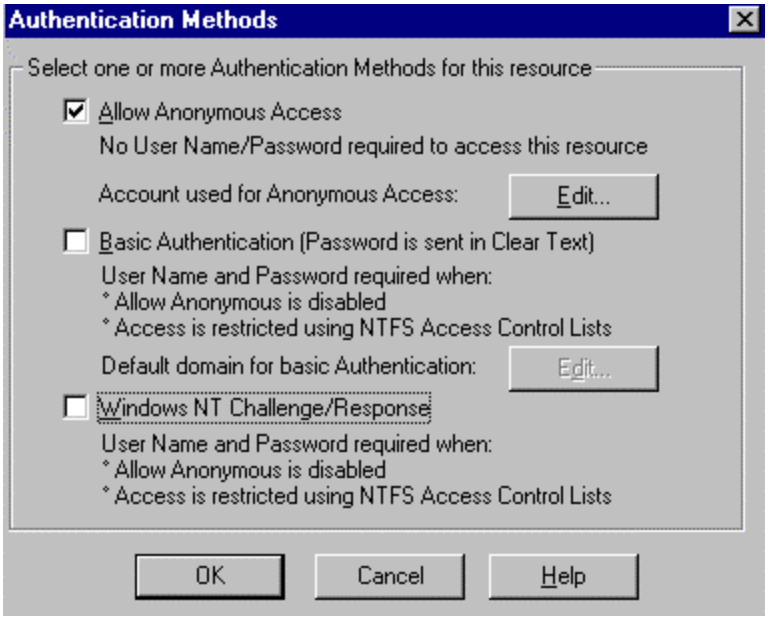
Secure Sockets Layer (SSL)

SSL provides a security handshake that is used to initiate a TCP/IP connection, such as the communication between a Web browser and a Web server. SSL provides privacy, integrity, and authentication in a private point-to-point communications channel. Chapter 4 provides a description for the use of certificates in this environment.

Client and server digital signatures

Digital signatures are used both to verify the identity of a user or server and to ensure that a message can be read only by the intended recipient. They are used by Web servers and browsers to provide mutual authentication, confidentiality of the pages transferred, and integrity of the information. More detail can be found in Chapter 4.

Identification and Authentication – Three options are available in IIS to identify and authenticate users:



Allow Anonymous Access – This is the method most often used when accessing a Web server. By default, IIS creates the account IUSR_*computername,* which is granted local logon user rights ("log on locally"). Whenever an attempt to access server resources over the Web is made, the user is automatically logged on using this account. The user can then only access resources based on the privileges granted to this anonymous account. The account name used for this purpose can be changed using the "Edit" button.

Basic Authentication – Is supported by almost every Web browser on the market. Basic Authentication sends the user name and password in clear text, which can be stolen by unauthenticated users. If your site requires the use of Basic Authentication, it is recommended you implement SSL as well. The combination will help you maintain tight access control to your sensitive data without risking logon information being intercepted.

To setup Basic Authentication with SSL, perform the following steps:

- Obtain a Server Certificate (Details in Chapter 4)
- Require Secure Channel when accessing this resource
- Enable Basic Authentication and disable Anonymous and Challenge/Response for this site

(Details on configuring these options can be found later in this chapter)

Windows NT Challenge/Response (NTLM) – This is the most secure of the three methods of authenticating users. A cryptographic technique is used to authenticate the password. The actual username and password are never sent across the network, so it is impossible for it to be captured by an unauthenticated source. Only clients with the Microsoft Internet Explorer browser can use this method of authentication. This option also does not work well on a secure extranet because it cannot operate over a proxy server or any other type of firewall application. It is, however, an excellent choice for secure intranets.

IIS can be configured to allow any combination of authentication scheme and anonymous access, allowing a Web site to contain both secure and nonsecure portions. When an authentication scheme is used in conjunction with anonymous access, the user is always initially logged on using the anonymous account (IUSR_*computername*). When a request fails because the account information doesn't specify proper authorization, a response is sent to the client Web browser indicating that the user doesn't have the required access. Returned with this information is a list of the various authentication schemes supported by the server. The client Web browser responds by prompting the user for a name and password. The browser then traverses the list until it finds an authentication scheme that it supports. It then resubmits the original request to the server, this time with the newly entered username and password using the selected authentication scheme. If Allow Anonymous Access is not selected as an option, one of the other two options must be selected.

Directory Management

In addition to the file and directory permissions established at the operating system level, described in Chapter 1, IIS4.0 introduces application level permissions. Read, Write, Execute, and Script are available access permissions for directories containing Web and FTP content. Read permission allows the contents to be viewed and passed to the client browser for rendering. Write enables clients with browsers that support the "PUT" feature of the HTTP 1.1 protocol standard to upload files to the server or to change the content in a write-enabled file. This is generally not granted unless you have a very specific need to make this type of access available. Make sure authorized users ONLY are granted this permission on your Web and FTP directories, if required. Script restricts execution to scripts. The file extensions for these scripts must be previously mapped to scripting applications (such as Perl and ASP). Execute allows any application to run, including binary files such as .exe and .dll; Execute includes Script. These permissions are set through the WWW and FTP site properties dialog boxes. Images of the Web site properties and FTP site properties are shown under the WWW and FTP headings.

NOTE: These access controls complement the NTFS access controls. For a file to be sent to the client browser for rendering, the Web directory has to permit IIS Read access and the user, in whose context the server is running, must have NTFS Read permission for the file. It is important to remember that NTFS access controls and IIS access controls are combined through a logical ***and*** to produce a composite set of permissions. For example, a user granted NTFS Read access to the ftproot directory, and Read and Write to the ftp home (ftproot) directory through IIS would result in the most restrictive set of permissions (Read ONLY access to the ftproot directory).

Ability to Implement Restrictions on Virtual Servers and Directories

Virtual servers allow you to configure one computer running IIS to support several domain names (or Web sites). When setting up a virtual server, an IP address is needed for the primary server and for each virtual server you wish to create. This makes your installation look like several Web servers when viewed from the Internet, when only one copy of IIS is actually running, with possibly only one network card.

Note: Virtual servers can only be setup for WWW sites; virtual servers are not available for FTP sites.

IIS allows you to supply an alias for directory paths that contain information to be published. This alias is commonly referred to as a virtual directory and is used in URLs. As far as visitors to your site are concerned, virtual directories are subdirectories branching from the main /wwwroot directory. Security is enhanced with virtual directories because it adds another level of abstraction to your site, altering the way in which Internet users access your information. Read, Script, Execute, Write, and Directory Browsing are IIS4.0 permissions which can be applied to a virtual directory and all of the files and folders contained within it. Read permission allows a client to download files stored in a virtual directory or subdirectory. Only directories that contain information to be published or downloaded should have Read permission set. To prevent clients from downloading executable files or scripts, it is recommended that they be located in separate directories without Read permission. Instead, these virtual directories should have Script or Execute permission so Web clients can run them. **Note:** If Read permission is also enabled, users may be able to look at the information contained within your scripts, some of which may be confidential (i.e., passwords).

Impersonation of Users When Running Applications

IIS accesses all files and runs all applications in the security context of the user requesting the file. This reduces the number of times a user is required to enter a name and password. In IIS4.0, impersonation can be used to restrict access to data that otherwise may be available to authenticated users. This means that an application or component in a user directory cannot access data or services restricted to other users or the server administrator. Impersonation allows Web-based applications to be run by users to perform administrator-like functions that require limited access with restrictions on what can be performed.

NOTE: Registry information is read from the profile of the user currently logged on the Windows NT machine. Applications often have problems when launched by IIS because the profile made available to an IIS application is that of the default user, i.e., IUSER_*computername.* This profile is generic to all users with minimal permissions. Therefore, a component may run as expected when User1 executes it on his/her desktop because the Registry is coming from User1's profile, and fail when User1 tries to execute it within IIS. This occurs because the default account does not have access to User1's profile. This is not true, however, if the user authenticates using NTLM Challenge/Response or Basic Authentication.

Summary

The following summarizes key areas to consider when configuring your Web server:

- Decide how you want access to be controlled on your Web site and set restrictions based on IP address.
- Determine if SSL and Certificates are required in your environment.
- Select an authentication method. Allow Anonymous is the most common method. Do not use Basic Authentication unless your site implements SSL (Certificates).
- Create directories with Read only NTFS permission for the WebUsers group. These directories will also be assigned IIS4.0 Read only permission during the WWW/FTP site setups. These directories will store data you wish to make available to client browsers for viewing or downloading only.
- Create a directory with Execute NTFS permission only for the WebUsers group. This directory will be assigned Script only permission during the WWW site setup. This directory will store executables, such as scripts.

World Wide Web (WWW)

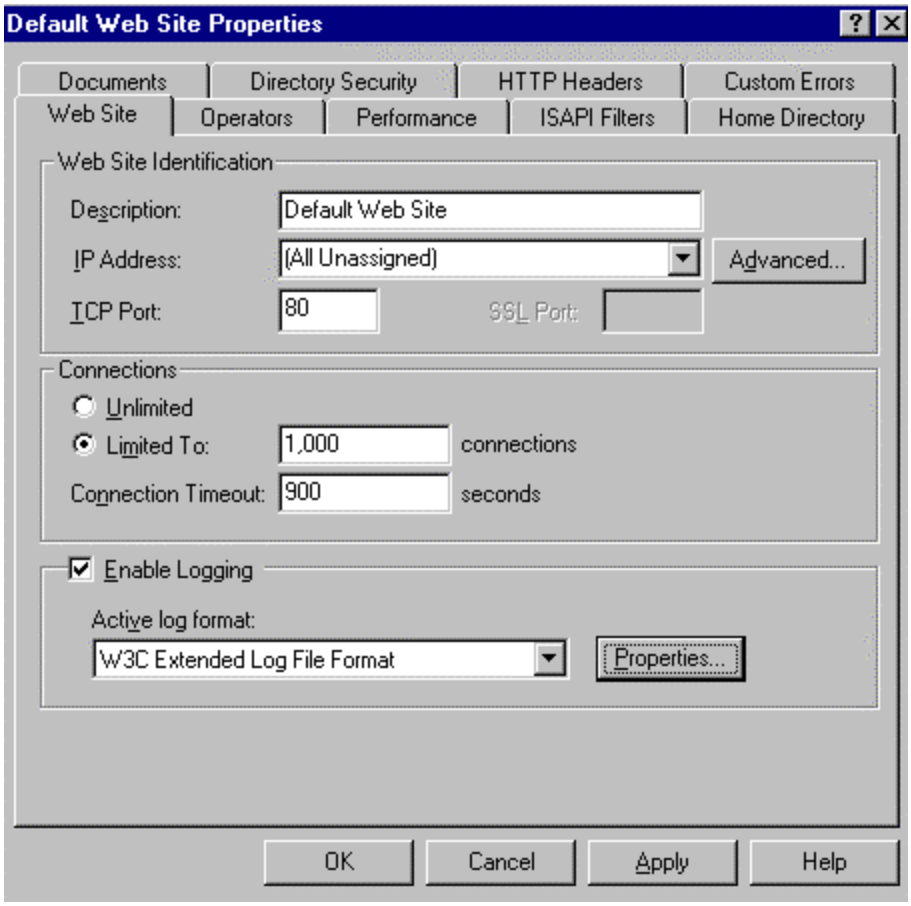
The following is a description of the property dialog boxes used in configuring your WWW site server securely:

Web Site Property Dialog Box – Highlight the Web site to be configured in the ISM, then select **properties** to access this dialog box.

Web Site Identification – Specify a Description - the name that you want to use in the ISM tree view to identify this Web site; an IP address; a TCP Port and SSL Port (if you change these from their defaults, you must notify your users or they will not be able to connect); and Advanced options, where you can map multiple domain names or host header names to a single IP address using the Host Header Name box. More information on this topic can be found in the IIS online documentation (Naming Web Sites).

Connections – Allows you to limit the number of simultaneous accesses to your Web site and to set a connection timeout. Timeout settings are recommended to prevent a possible denial of service attack.

Enable Logging – It is recommended that this option be turned on. Once IIS logging is enabled, you can configure how and when log files are created and saved. Details on logging will be covered in Chapter 4, Auditing.



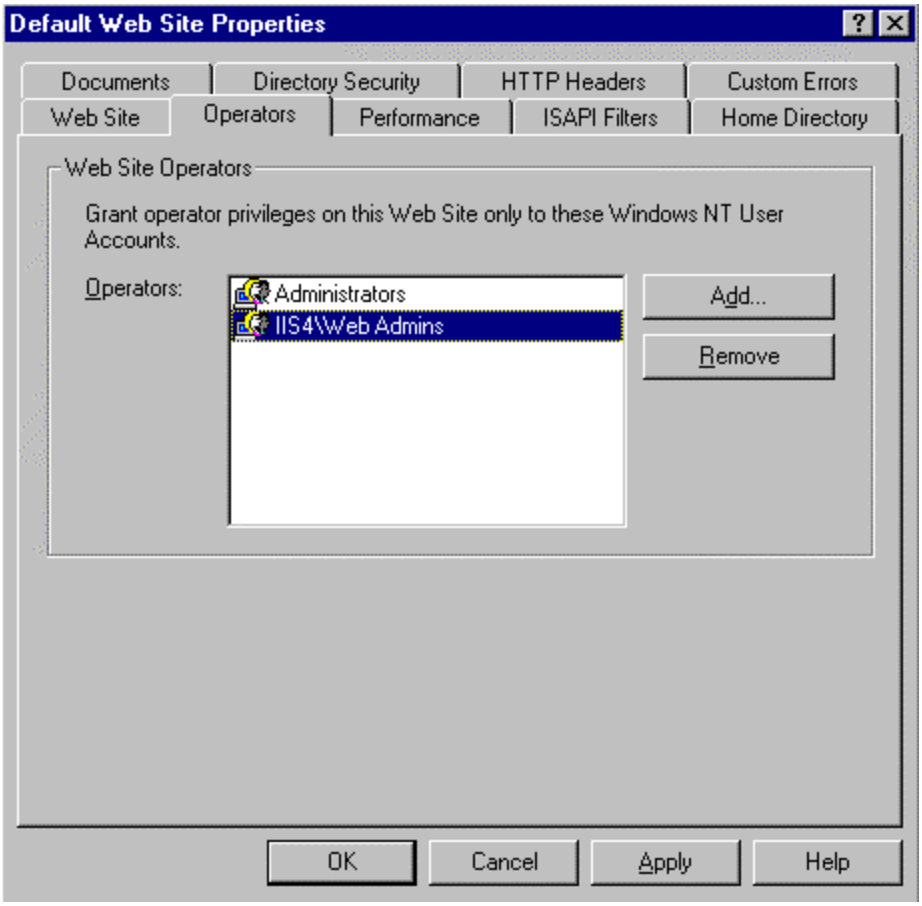
Operators Property Dialog Box

Web Site Operators – This is where you designate which NT Server user accounts you want to administer your Web site. This should be a group and the accounts within the group should not necessarily require NT Administrative permissions. Operators can work only with the properties that affect the Web site for which they were created. They cannot access the properties that control overall IIS setup, the NT server operating system that hosts IIS, or the network on which the system runs. The following are some functions that can be performed by Web Operators (members of the WebAdmins group in the example). **NOTE:** *When selecting members for this group, make sure individuals are knowledgeable and trustworthy to minimize compromising your system's security.

Manage Web content expiration dates and times.
Administer Web content (modify, add, delete)
Enable Logging
Change default Web documents.
***Set Web Server access permissions**.

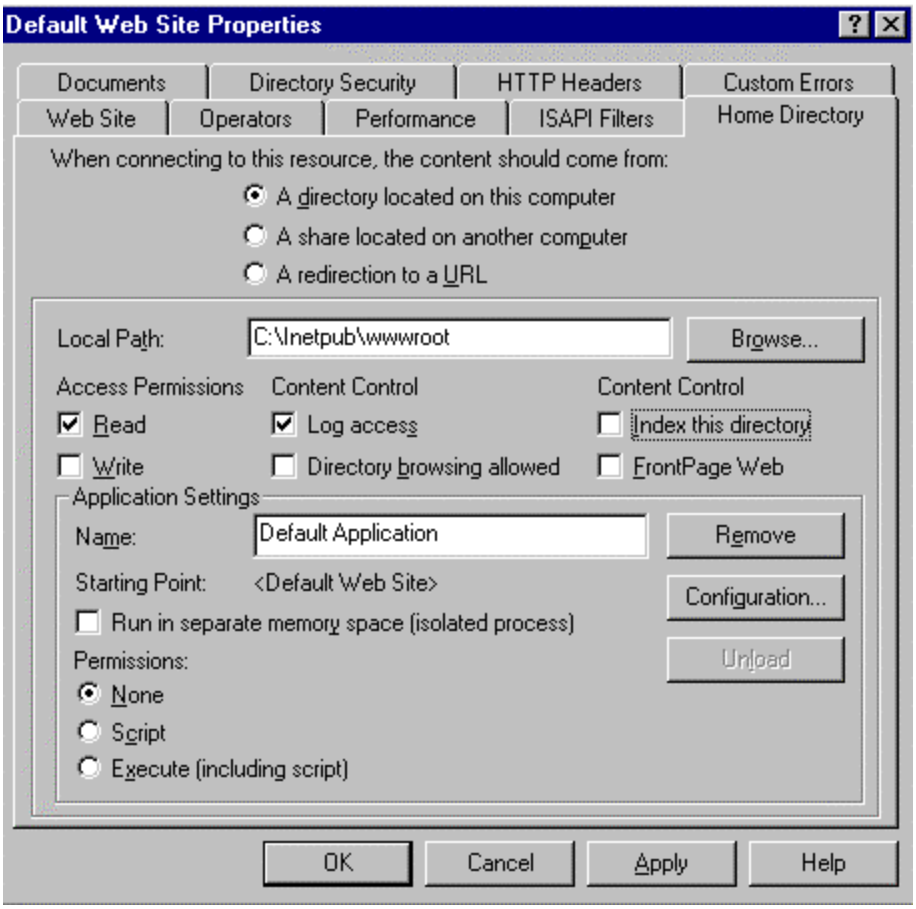
Only members of the NT Administrators group can perform the following tasks related to IIS:

Change application isolation
Create virtual directories or alter their paths
Change the Anonymous Username and Password
Alter the identification or configuration of your Web site.



Home Directory Property Dialog Box

The Home Directory property dialog box allows you to look at and change settings that control Web content delivery, access permissions, and Active Server Page configuration and debugging. Options that are available to you on this dialog box will vary based on the location of the content. However, all security-related settings can be covered under the "A directory located on this computer" option.



Access Permissions

Permissions set here need to match NTFS permissions. If they do not match, the most restrictive of the two will be enforced. Configure directories with appropriate permissions for your site(s), as described in the Post Installation section of Chapter 1, i.e., configure one directory with Read only permission and one with Script only (described below).

Content Control

Log Access – This option is selected by default. This ensures that all visits to this directory are logged into the log file.

Directory Browsing Allowed – This allows visitors to look at a hypertext listing of the directories and files on your system. This is NOT recommended. The issue here is that if no default document is sent to the client when the site is accessed, the unknown user will get a directory listing of your system instead. This exposes more of your system

to unknown users. There is a risk of exposing program files or other files to unauthorized access. Make sure this option is NOT selected.

Application Settings

An application is the directories and files contained within a directory marked as an application starting point.

Run in Separate Memory Space – This option enables you to isolate a Web-based application by having it run in a memory area that is separate from the Web server software. It is recommended that this be enabled so applications do not inadvertently cause problems with the Web server software. Server-side include (SSI) and Internet Database Connector applications cannot be run in a separate memory space from the Web server's memory space.

Permissions – These settings control the execution of applications contained within the directory. Permissions include:

NONE - prevents programs or scripts from executing.

SCRIPT – Restricts execution to scripts that have had file extensions previously mapped to scripting applications. Make sure the directory with this permission does not allow Read access to anonymous users. If Read permission is granted, it is possible that users may be able to look at the information contained within the scripts, some of which may be sensitive (i.e., passwords).

EXECUTE – Allows any application to execute, including scripts and NT binaries, such as .exe and .dll files. Use care when granting this permission. This permission should only be used for directories that contain binary files that must be executed by the Web server. If your site requires this permission for a directory, make sure it does not have NTFS write permissions allowed for anonymous users to your site (WebUsers, for example). Write with Execute permissions would allow a user to place executable code (possibly malicious code) on your server.

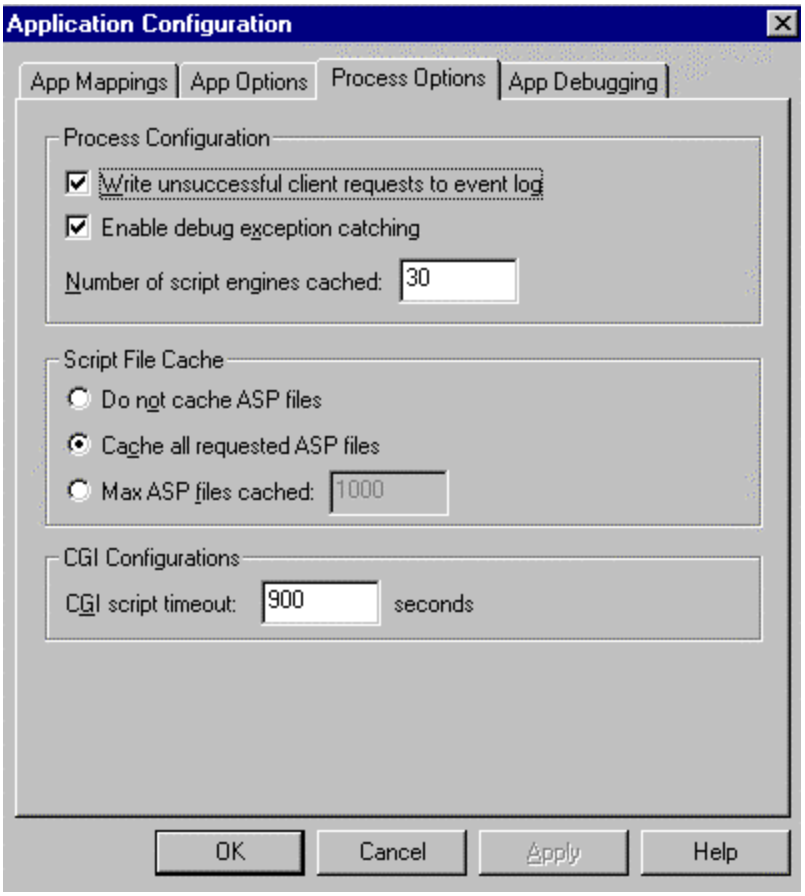
Applications can be configured in more detail by using the **Configuration** button. A separate dialog box is displayed with the following tab options: App Mappings; App Options; Process Options (if you select to run in separate memory space); and App Debugging. Discussions in this document focus on the security relevant settings, which are limited to the **App Options** and **Process Options** dialog boxes described below. Although there are no security settings in the App Mappings tab, these are of security concern and, therefore, are covered in Chapter 4, Additional Security Issues.

App Options -These options can be configured at the Web site, virtual directory, and directory level.

“Enable session state” and “Session timeout” – Check this option so that Active Server Pages (ASPs) create a new session for each user who accesses an ASP application. This lets you identify the user across several ASP pages in your application. If the user does not request a page or refresh within the session timeout, the session will end. Set an “ASP Script timeout” value so that if a script does not complete execution within the allotted time, an entry will be made into the NT Server Event Log and execution of the script will stop. Setting timeout values will help prevent a denial of service attack.

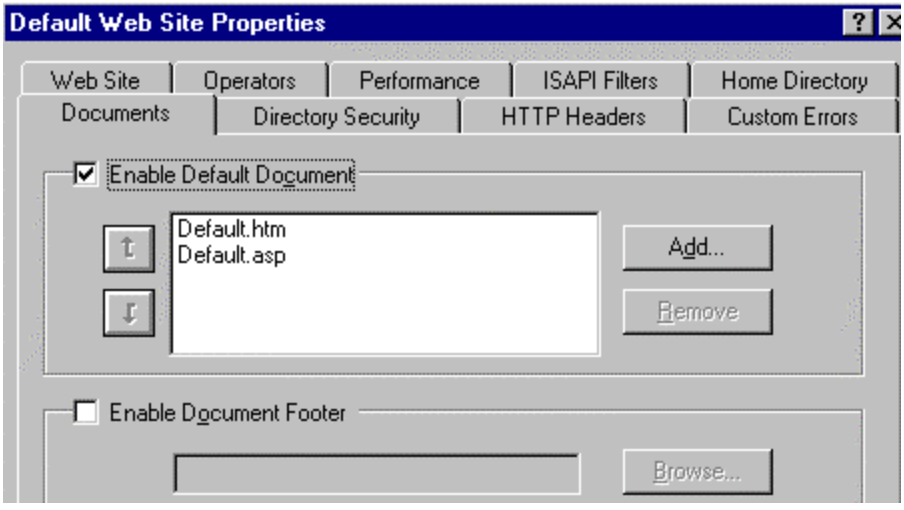
It is not recommended that "Enable parent paths" be selected. This allows ASP scripts to use relative paths to the parent directory of the current directory (".." syntax). If the parent directory permits Execute access, a script could attempt to run an unauthorized program in a parent directory.

Process Options – Enable "Write unsuccessful client requests to event log"



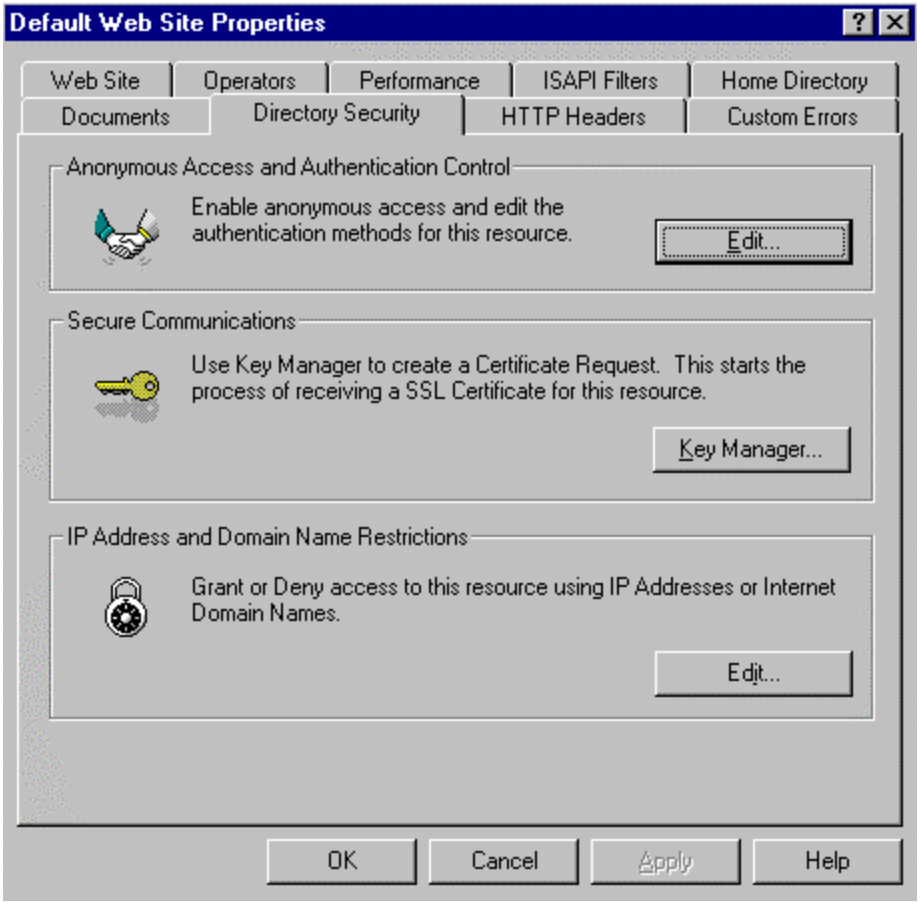
Documents Property Dialog Box

It is recommended that you always provide a default document that all users will see when accessing your site(s). This helps prevent displaying the directory structure of your site to a user unintentionally. This happens when the Directory Browsing Allowed option is left enabled.

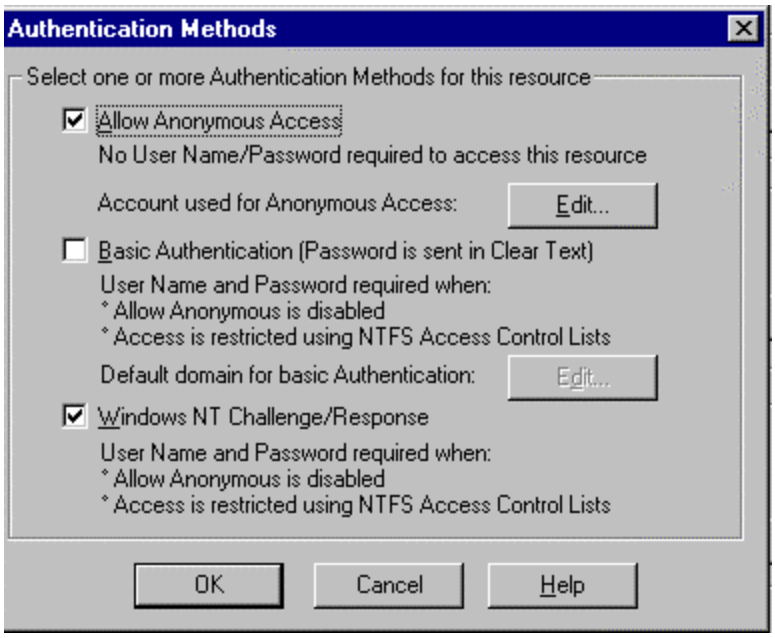


Directory Security Property Dialog Box

Security properties can be set at the Web site, directory, virtual directory, or file level. Directory level will be used here to describe the settings, but apply to whichever level you are working with.

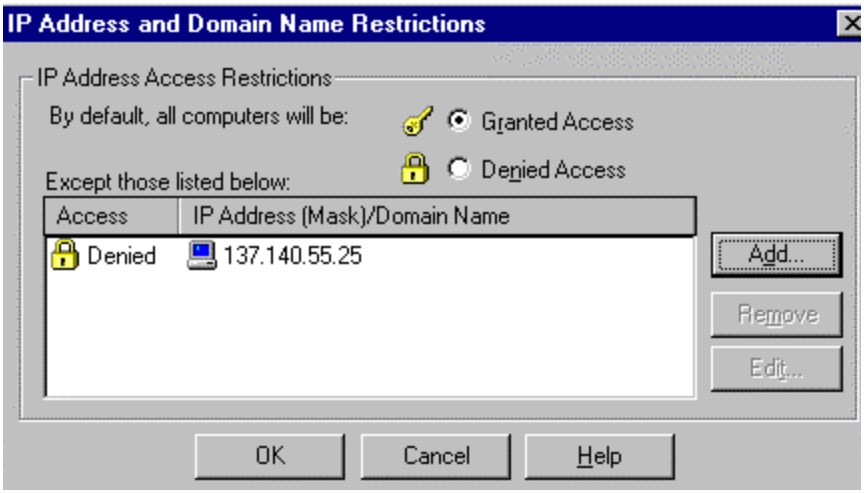


Anonymous Access and Authentication Control – The options presented on this property dialog box are described at the beginning of this chapter.



Secure Communications – This option is used to configure SSL features (use of certificates) available on your Web server. This enables the encryption of all traffic between the client and server. Once set up, visitors to your Web site must use a browser capable of supporting secure communications. Further detail on this topic can be found in Chapter 4.

IP Address and Domain Name Restrictions - This option allows you to specify who can access your WWW site based on IP address. There are two options on this property dialog box; "Granted Access" and "Denied Access". "Granted Access" allows all computers access to your resources except those specifically identified by IP address. "Denied Access" restricts access to resources to ONLY computers with IP addresses specifically listed. Requests from any other computer is denied. Three options are available when specifying computer IP addresses: **single computer**, where you specify a single IP address; **group of computers**, where you specify the network ID and subnetmask; or **Domain Name** (a warning message appears stating this option will cause a significant degradation in performance).



File Transfer Protocol (FTP)

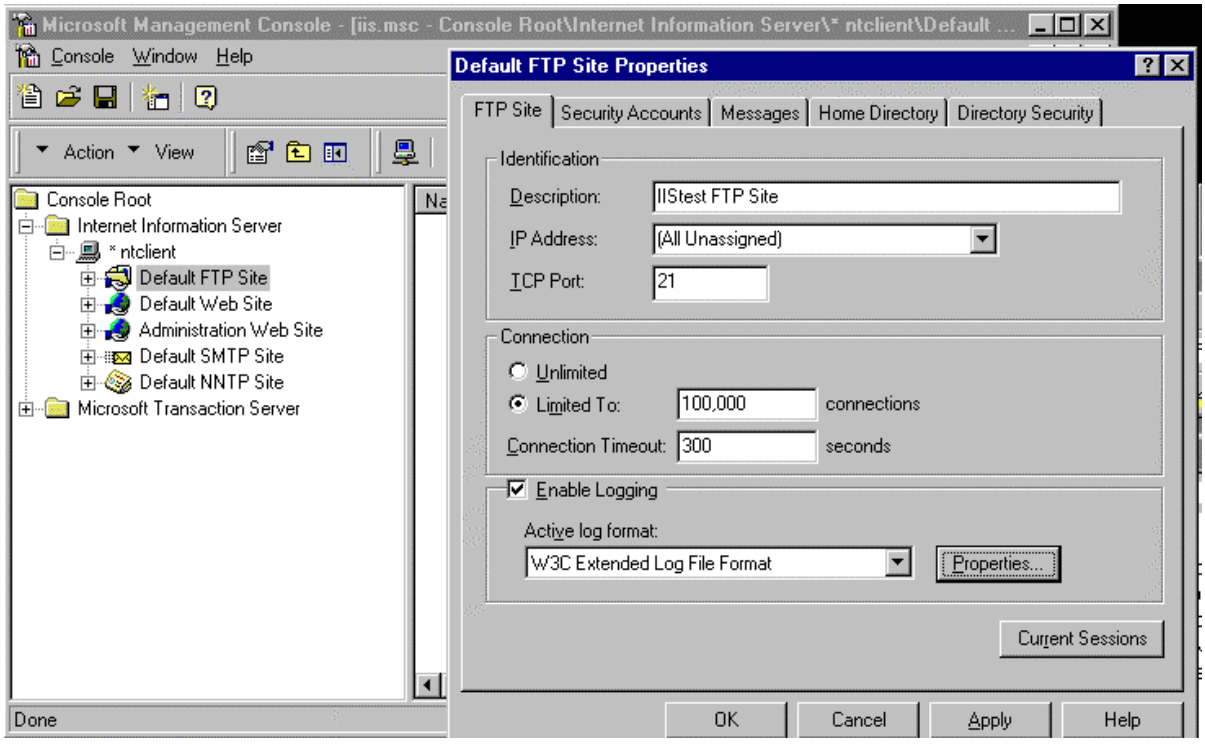
FTP allows clients to transfer files to and/or from an FTP server. Although much of the FTP functionality on the Internet is being replaced by the WWW service, FTP is still in common use. It is recommended that you configure your FTP server so that uploading of files to the server **is prohibited**. If it is necessary to allow uploads, set the directory permissions so that you have to explicitly specify who can upload files. This prevents intruders from stashing pirated software, cracking tools, and other illegal material that you do not want on your FTP server. If you have to allow uploads to your server, create a separate directory (a "drop box") called \INCOMING to receive these files. Also, monitor this directory regularly as part of your security policy.

Organizing FTP Directories

It is recommended that FTP directories be organized for your users. For FTP downloads, the directory names should reflect directory contents. For example, device drivers could be organized within directories with operating system names. Make sure FTP download directories are configured for Read ONLY permission. Create a "drop box" directory for temporary storage of files written to the FTP server. Files written to this directory should be examined for suitability and security risk then placed in the directory for downloading by others. Access to the "drop box" is limited to Write for the anonymous users account. Conversely, the FTP directory configured for user downloads is set to Read ONLY. This may be a little inconvenient because the anonymous users will not be able to look at files uploaded by others, but it will prevent them from altering or deleting those files. A Web site administrator could review files uploaded to the drop box and place them in the Read ONLY directory for downloading by others.

FTP Site Property Dialog Box

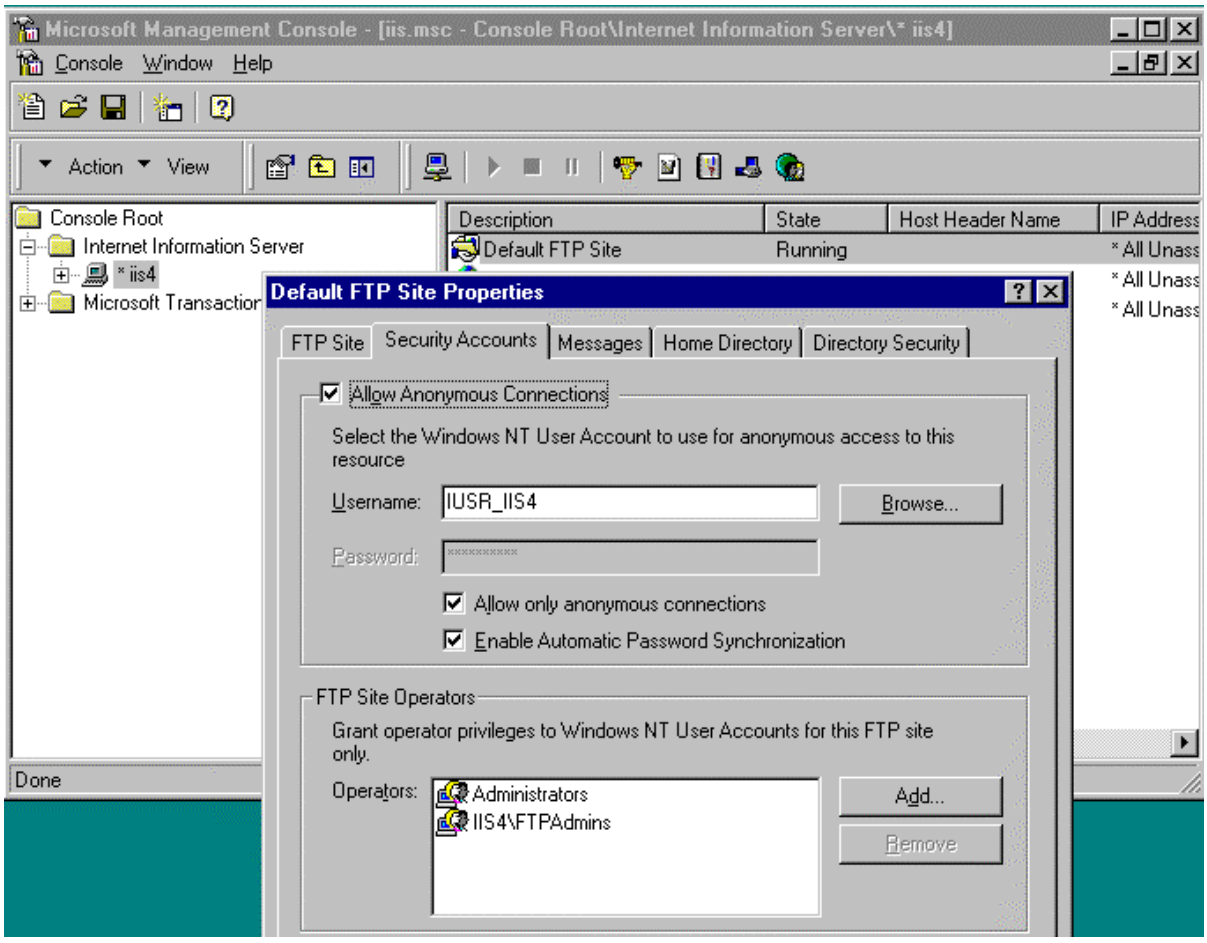
This property dialog box contains the same properties as the Web Site dialog box, but apply specifically to your FTP service. You can set the FTP site identification information, control the number of connections, and set a connection timeout. It is recommended that you select the "Enable Logging" option and assign a connection timeout value to prevent a denial of service attack.



Security Accounts Property Dialog Box

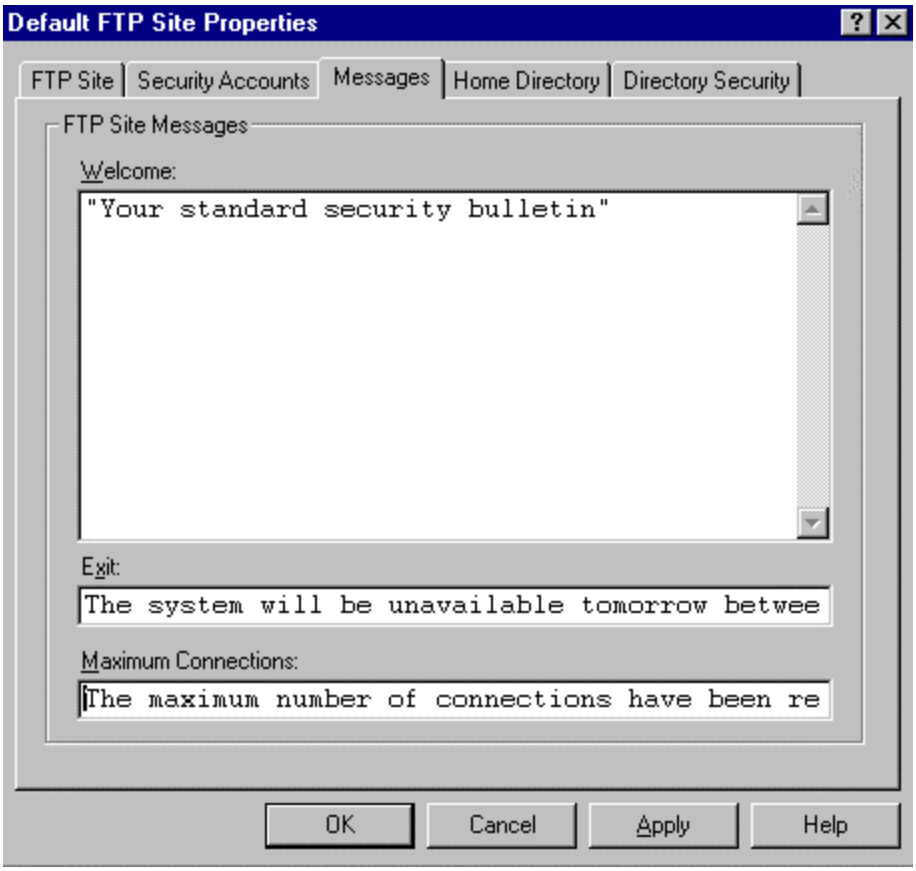
This property dialog box is used to configure anonymous FTP access and FTP site operators. It is recommended that you check the "**Allow only anonymous connections**" box to restrict access to ONLY anonymous connections. When this box is checked, users cannot log on with real usernames and passwords, which are sent in the clear, preventing a possible attack using the administrators account or another privileged account. Typically, FTP users log on using the username *anonymous* and their e-mail address as their password. The FTP server then uses the IUSR_*computername* account as the logon account for permissions. NTLM (NT Challenge/Response) is not available for the FTP service. The lower portion of the property dialog box is used to designate which user accounts you want to be able to administer your FTP site. It is recommended that groups be used instead of individual user accounts.

Select the **Enable Automatic Password Synchronization** option to match the anonymous FTP logon user name and password (typically IUSR_*computername*) with accounts created in the User Manager for Domains. If IUSR_*computername* is not the anonymous user account, make sure the anonymous user account defined is an account on the local computer. Password synchronization should not be used with non-local accounts.



Message Property Dialog Box

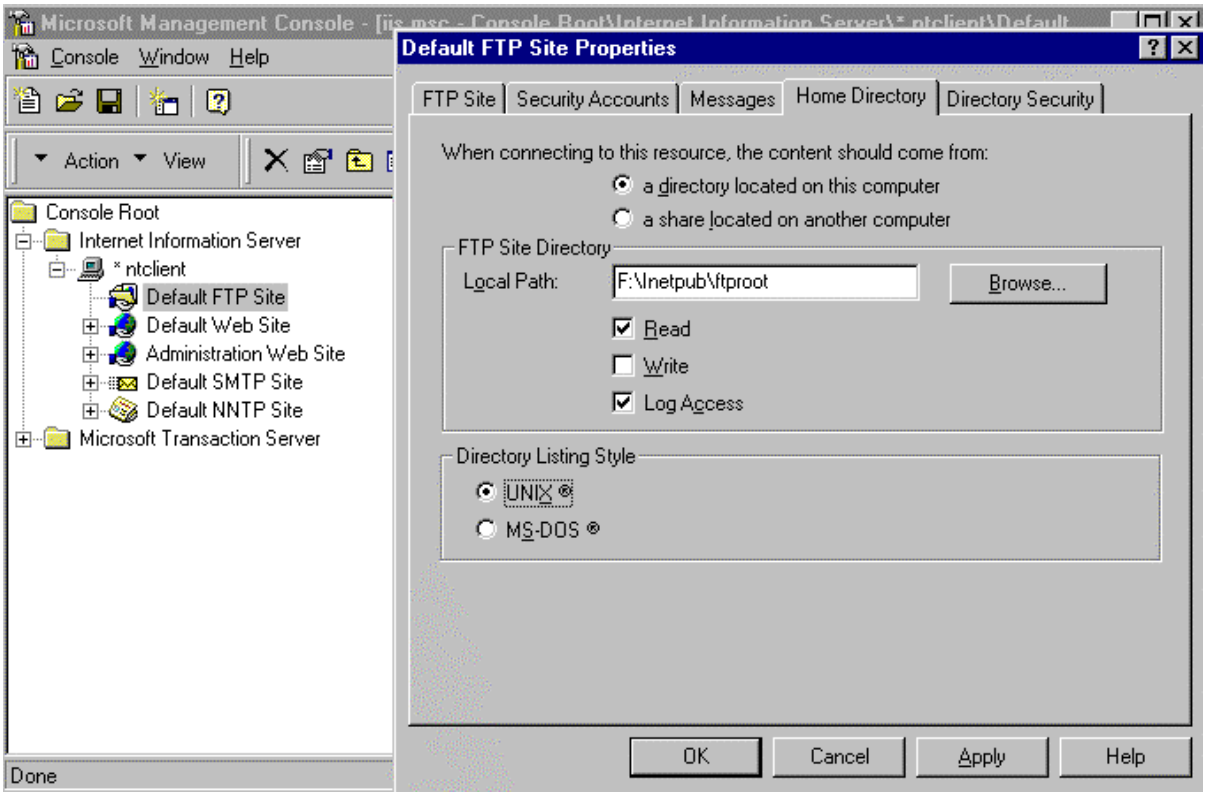
There are three types of messages that can be displayed to the user; Welcome, Exit, and Maximum Connections. It is recommended that a Welcome message in the form of a Security Banner be displayed to any user connecting to your FTP server. Exit messages can be used to display notices to users upon connection termination. In the event the maximum number of connections has been reached, the Maximum Connections message can be used to notify the user of this event.



Home Directory Property Dialog Box

This property dialog box is used to specify where the content comes from (either from a directory located on this computer or from a network share located on another computer-URL redirections cannot be specified). The local path to the directory, access permissions, and the style of the directory listings that IIS sends to the client can also be configured.

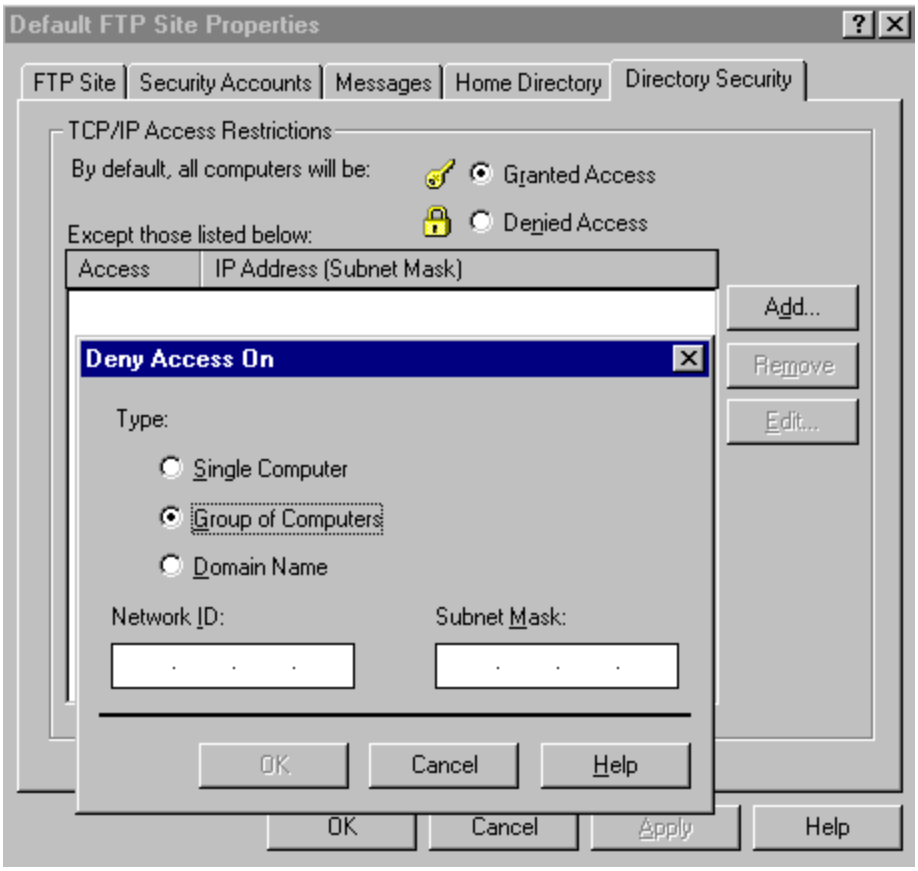
It is recommended that this directory have Read access ONLY. If your site requires users to upload data, create two directories beneath the “ftproot” directory. One with Read ONLY access to store data made available to all users for download, and one with Write Only permission to be used as a “drop box” for users to upload data into. A Web operator could then be responsible for reviewing the data in the “drop box” prior to making it available to all users in the Read ONLY directory.



Directory Security Property Dialog Box

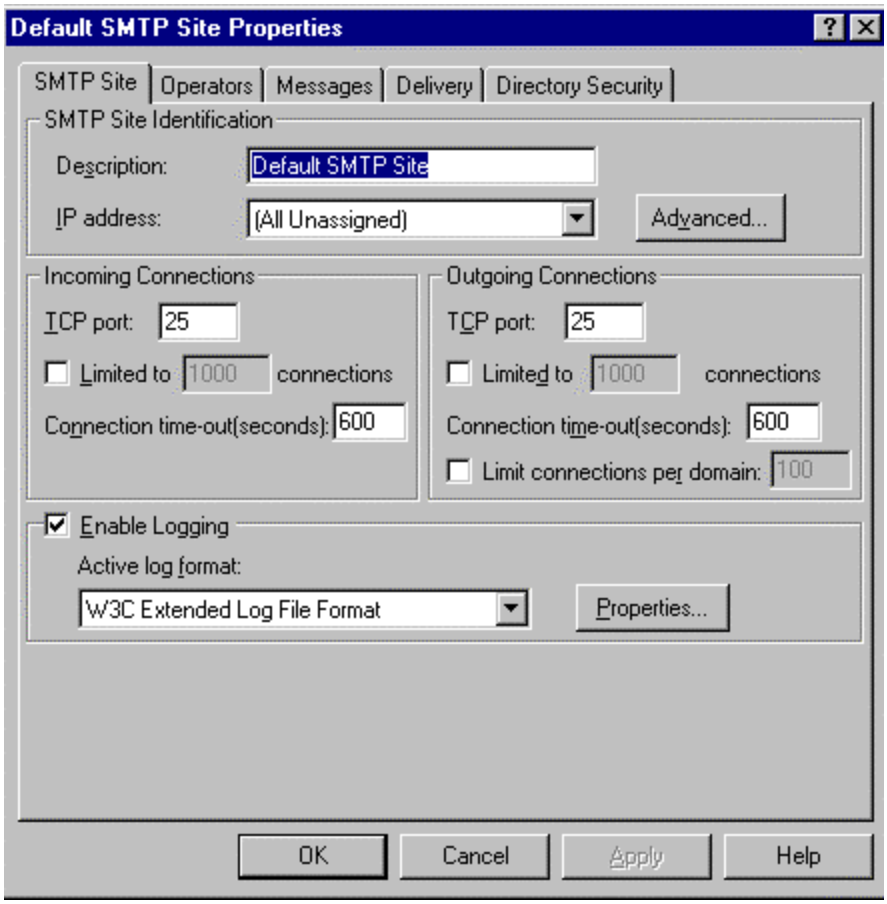
This property dialog box allows you to specify who can access your FTP site based on IP address. There are two options on this property dialog box; Granted Access and Denied Access. Granted Access allows all computers access to your resources except those specifically identified by IP address. Denied Access allows ONLY those computers with listed IP addresses access to your resources and denies all other requests. Three options are available when specifying computer IP addresses: single computer; group of computers (where you specify the network ID and subnetmask); or Domain Name (be careful when choosing this option, a warning message appears stating this option will cause a significant degradation in performance).

If you have a defined set of users that will be permitted to access the ftp directory, recommend selecting "Denied Access". This will permit only specified computers access to the data within the ftp directory and deny access to all others.

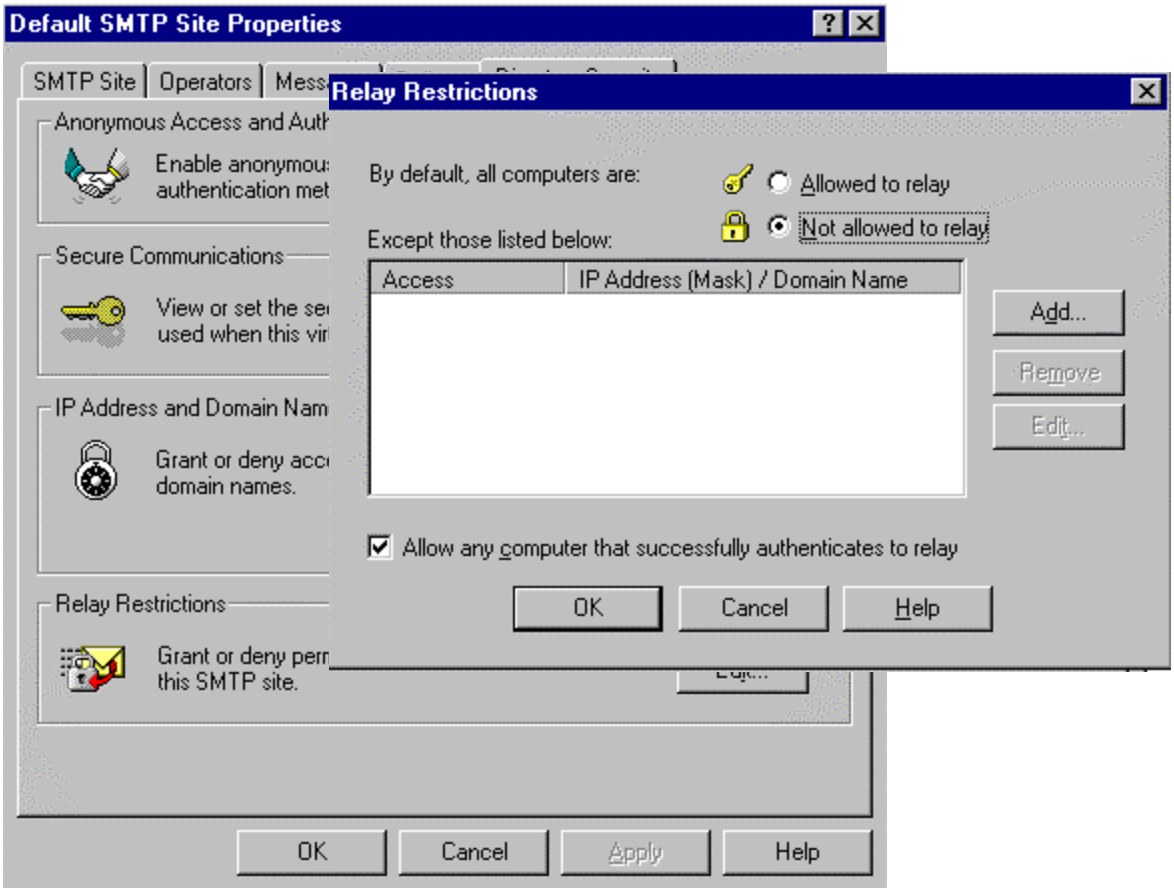


Simple Mail Transfer Protocol (SMTP)

IIS4.0 includes an SMTP mail service used to transfer Internet messages between servers. However, this is not a full SMTP server. The SMTP service does not provide a POP server and is not intended for use by end-user programs (i.e., Netscape Mail or Outlook Express). This service is intended for use by ASP applications and other applications that require the use of mail functions. Its interface is accessible under ASP, Visual Basic, and Visual C++ for sending and receiving messages. This allows, for example, the server to send a confirmation email message to a customer who submits a registration form. A Web server can also receive messages. This is useful in the event a mail message, sent by the server, could not be sent. The Web server could receive a non-delivery receipt notifying a Web administrator of the status of the message. A Web administrator could also setup a mailbox to collect customer feedback messages regarding a Web site. Below are images of dialog boxes available for configuring SMTP properties. Access the dialog boxes by highlighting the SMTP site on the Internet Service Manager and selecting properties on the Action pull down menu. On the SMTP Site tab, make sure Enable Logging is checked and configure the logging properties as you would the services discussed previously. The Operators tab allows you to define a user or group responsible for managing this service. It is not illustrated here, but is identical in concept to that defined for the WWW and FTP services.



The Directory Security tab provides the capability to configure the same options as the services discussed previously and offers one more, Relay Restrictions. Configuring this option is similar in concept to configuring the IP Address and Domain Name Restrictions property. Select either to allow all computers to relay through this service except those specifically defined, or deny all Mail Relay requests except those specifically defined. Be careful when configuring this option. Accepting a request to relay could possibly allow spammers to forward mail through your sever and have it appear as though that is where it originated. It is recommended that you select **Not allowed to relay**. If you choose to allow your server to become a Mail Relay, only allow authenticated computers by selecting the option **Allow any computer that successfully authenticates to relay.** Authentication is accomplished through NTLM Challenge/Response or Basic Authentication set on the SMTP mail directory.



Microsoft SMTP Service supports the use of Transport Layer Security (TLS) for encrypting transmissions. You can require the use of TLS for all incoming connections through the Secure Communications dialog box from the Directory Security tab. To use TLS for the server, you must create key pairs and configure key certificates. You do this by selecting the Key Manager button.

Chapter 4

Additional Security Issues

This chapter reiterates the importance of creating groups to manage WWW and FTP content on an IIS server, describes how to configure auditing in IIS4.0, and gives a brief description of the installation and use of Certificates.

Administering IIS with Multiple Groups

In order to simplify the assignment of administrative rights to the Internet Information Server, it is recommended that a separate Windows NT IIS Administrators Group – or Groups - be established. It is **strongly** recommended that you do not use the Windows NT Administrator group, as it is not necessary to have Windows NT administrative rights to perform many IIS4.0 administration functions. IIS administrative rights are assigned through the MMC WWW and FTP property dialog boxes by defining Service operators as described in Chapter 3.

Having a separate IIS administration group offers several benefits. First, it precludes the need for IIS administrators to logon unnecessarily as a Windows NT administrator -- something that should be avoided for security reasons. Second, it will allow you to partition administrative rights. For example, you may reserve the right to reconfigure the IIS server to a select few (NT administrators), while allowing several individuals to manage WWW and FTP content. For instance, users that are members of a Web operators group could be given access to control what is made available to visitors to your site through the WWW and FTP data directories. They would not have access to configure your Web server, i.e., add users and groups, etc. NT administrators would retain that right. Finally, having separate IIS administrator groups for each site maintained by your server would simplify the process of managing administrative rights -- adding a new administrator for a site is as simple as making them part of the appropriate IIS group.

This becomes very important when a server is used to manage several sites. As stated previously, an administrative group should be created for each Web site. The members in these groups would be granted operator privileges to administer their own Web site exclusively. This would allow the NT administrators to maintain their server and manage their security risks more effectively by having as few NT administrators as possible and not permitting any one group total control over all sites on the server.

Script Mappings

The IIS web server is configured to support many different common filename extensions, which allows it to serve pages using a variety of different application `.dll` files (See **Table 3**). Some examples of this include `.html, .asp, .shtml and .shtm`. Many web servers are used only for static pages, such as `.html`, so there is no need to implement these other mappings. The mappings that the server is not required to utilize should be removed. This will prevent any potential vulnerability in those `.dll` files, such as buffer overflows, from affecting the security of your web server.

If a need arises in the future to add some functionality, the mapping can always be added.

Here are some references along with their uses:

Extension	Use
`.htr`	Web-based password resets
`.idc`	Internet Database Connector
`.stm, .shtm, .shtml`	Server-side Includes
`.printer`	Internet Printing
`.cer`	Represents a certificate
`.cdx`	Active Channel Definition File
`.asa`	Active Server Application
`.htw, ida, .idq`	Index Server

Table 3 Script Mapping - File Extensions and Uses

To access the script-mapping screen, open the ISM, right-click the web server and choose **properties**. Select the WWW service, click **edit**, go to the **Home Directory Tab** and click on **Configuration**.

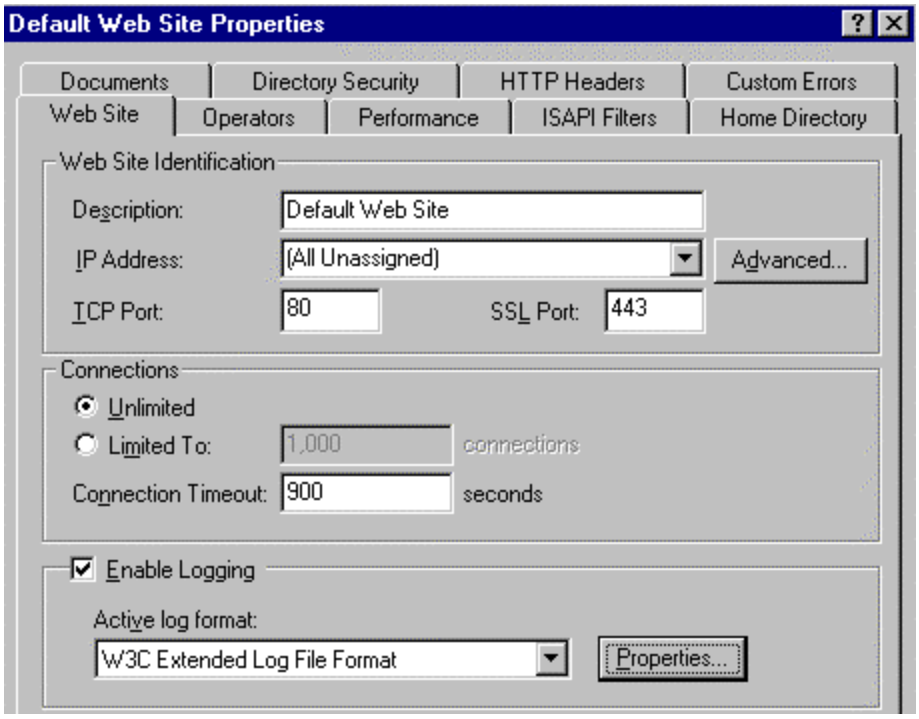
Auditing

In addition to the audit settings described in the *Guide to Secure Microsoft Windows NT Networks*, IIS logging should be enabled to enhance security auditing of the IIS environment. IIS logging tracks IIS-specific events related primarily to HTTP traffic in and out of the server. Included in the log is IP address information that is not available through Windows NT logging and auditing mechanisms. The following suspicious activity can be tracked using the IIS logs:

- Multiple failed commands, especially to directories configured for executable content.
- Attempts to upload files to directories configured for executable content.
- Attempts to access .bat or .cmd files and subvert their purpose.
- Attempts to send .bat or .cmd commands to directories configured for executable content.

- Excessive requests from a single IP address, attempting to cause a denial of service attack.

IIS logging is configured through the Services properties dialog boxes (WWW, FTP, and SMTP) by selecting the **properties** button.



Below are some suggestions for configuring auditing as it pertains to IIS data:

- Move and rename the IIS LogFiles directory. This can increase the difficulty unauthorized users experience while trying to "cover their tracks."

- Full Control access to the IIS LogFiles directory should be limited to SYSTEM and Administrators ONLY (or whichever group is created to manage auditing on your system). Make sure "Replace Permissions on Existing Files" is checked when making these changes on your system.

- Write, Delete, Change Permissions, and Take Ownership are critical events for WWW content directories, and should be audited for success and failure in the Windows NT audit facility.

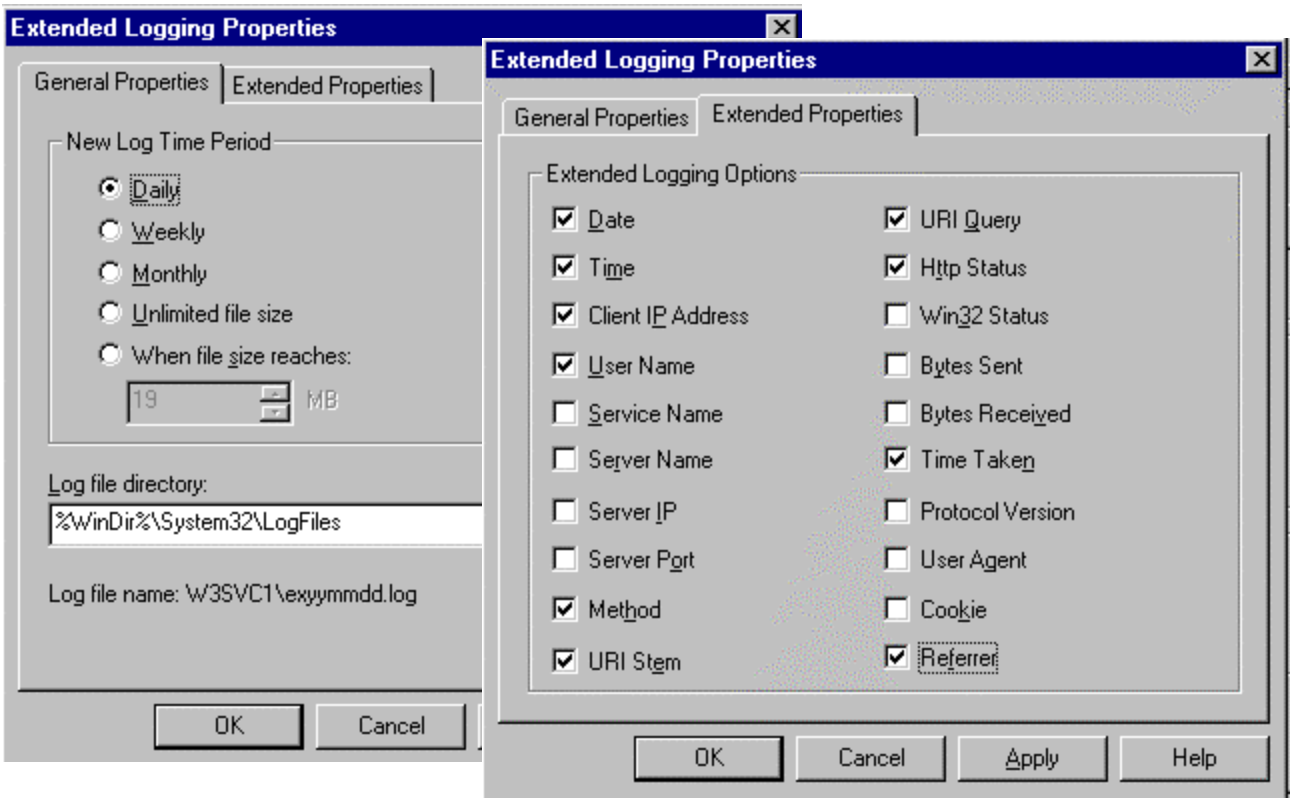
- Extended Logging Options - The following settings can be altered according to your site's audit policy:

    - Date and Time event occurred;

    - IP Address of the client and username (this is likely to be IUSR_*machinename)* accessing your site – this is very useful because this data does not appear in the NT log files;

    - HTTP method used to access your site;

- URI Stem - the resource accessed by the client (HTML page, script, or ISAPI application);
- URI Query - the query the client was making;
- Status of the request;
- Time taken to process the request; and
- URL of the last site visited by the client.



Certificates

A good description of how to administer the certificate manager and client certificates within your IIS environment can be found in the book entitled Mastering Internet Information Server 4.0. This document provides a brief description.

If your system requires the use of SSL for secure communications between your clients and server, you must install a server certificate and the client must have a browser that can support secure communications. Authentication, confidentiality, and data integrity are all obtained with the use of digital certificates and SSL. A certificate authority (CA) creates a certificate, which is made up of a public key for cryptographic use, an expiration date, serial number, name, and certificate class.

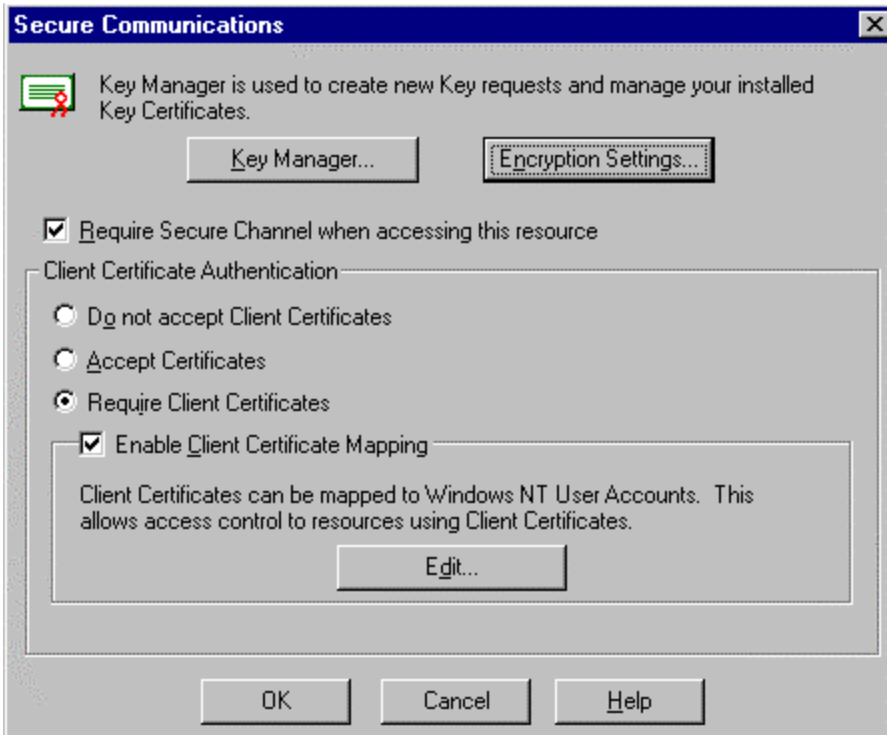
The Key Manager is used to request a digital certificate from a trusted third-party certificate authority and manage installed Key Certificates. It is used to configure background information that will be needed to apply for a digital certificate and create the required files. The Key Manager can be accessed through the Secure Communications **Edit** button of the **Directory Security** tab of the Server and Web Site Properties dialog boxes. The following tasks are performed through the Key Manager:

- generate a key pair file and a request file
- request a digital certificate from a CA online
- install the digital certificate on your server

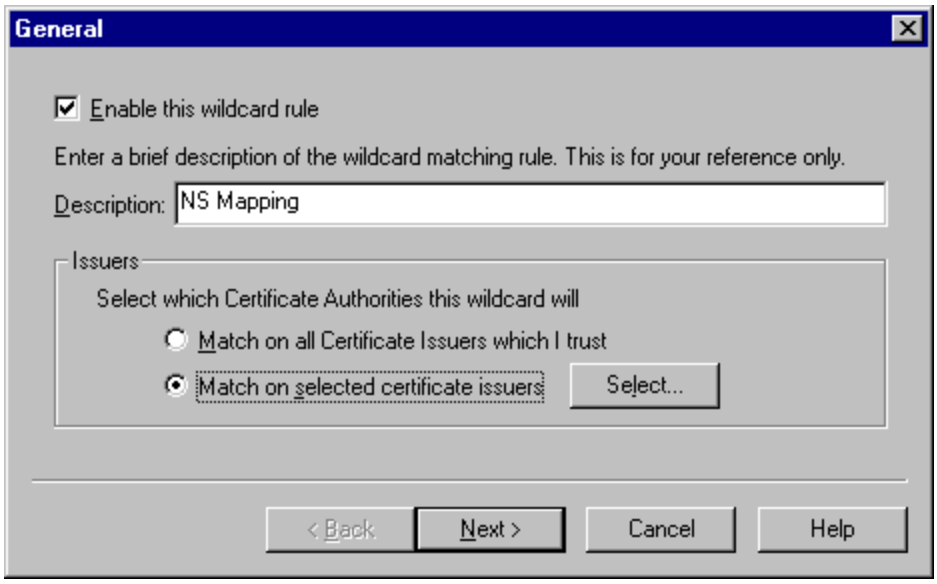
Once you have configured your site to use certificates, activate the SSL security on your server using the ISM for the directories that require secure access.

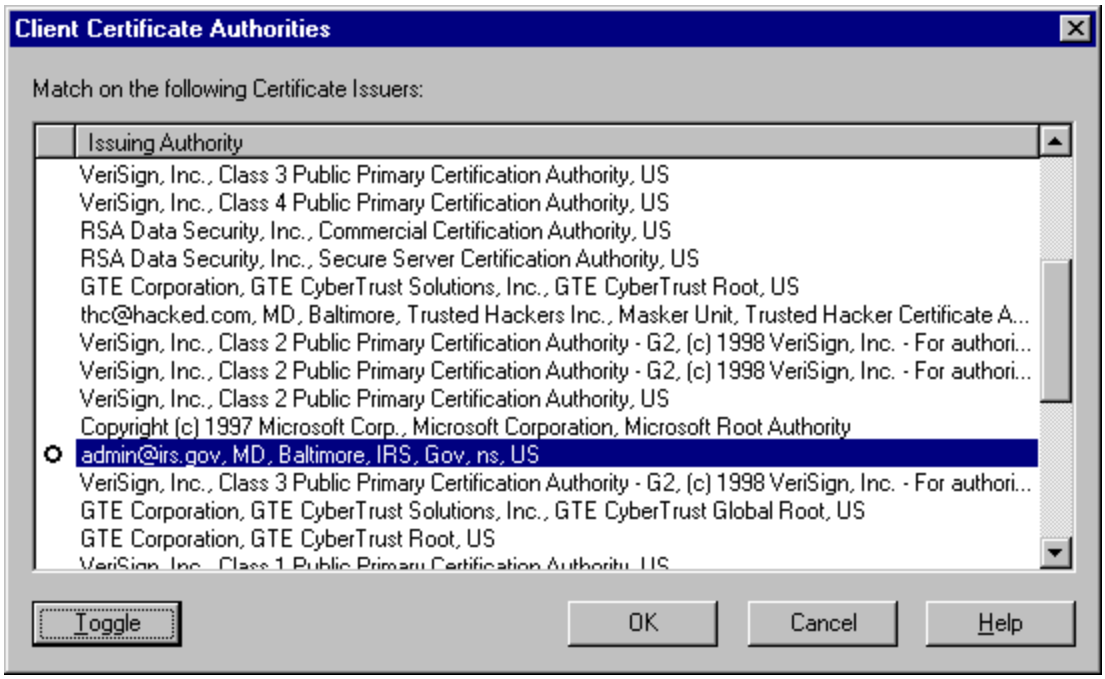
Web site developers can use scripts and client certificates to control access to the site. IIS supports the mapping of client certificates to specific Windows NT user accounts. This allows more control over published content on the Web. Organizations can authenticate users who logon with a client certificate by creating mappings that relate information contained in the certificate to a Windows NT user account. Using the IIS certificate-mapping feature, web site developers can either map a specific user's client certificate to a Windows NT account (a one-to-one mapping) or map multiple certificates to a single Windows NT user account (a many-to-one mapping). In one-to-one mappings, each individual certificate is mapped to a specific NT account. IIS also supports wildcard mapping. To map multiple certificates to a single Windows NT user account (many-to-one mapping), administrators define wildcard-matching rules that create a mapping by verifying whether a certificate contains certain items of information. For example, an administrator could define a matching rule that automatically maps any certificate issued by a particular organization to a user account, rather than creating a separate mapping for each client certificate. If an environment requires one-to-one certificate mappings due to varying attributes in customer certificates, for example, a many-to-one certificate mapping could be accomplished by creating a separate mapping to one account for each required certificate. In a one-to-one mapping scenario, it is important to note the comparison that takes place between the client certificates used during the SSL 3.0 session and the copies loaded into IIS is a certificate-to-certificate comparison. In the many-to-one scenario, certificate attributes (such as "subject" and "issuer") contained within the client certificate are compared with the attributes defined in the many-to-one mapping rule. There is no binary comparison in the many-to-one mapping; therefore, the potential for masquerading exists to possibly gain access to restricted information on a web site.

It is very important to understand how the many-to-one mapping and certificate matching rules are used in granting access to protected web information. If not configured correctly, unauthorized access can inadvertently be granted. The comparison of certificates in a many-to-one mapping is not binary and is performed irrespective of the length of the certificate chain. In this case, "subject" and/or "issuer" attributes from client certificates are extracted and compared to the defined attributes in a many-to-one mapping rule. Since the comparison is not binary, it is possible for a root CA's subordinate CA to create a CA certificate with the same name as a peer CA. This certificate could then be used to masquerade as the peer CA to possibly gain access to restricted resources on a web site. In order for this to happen, both the legitimate issuer of the peer CA certificate and the issuer of the rogue CA certificate must be in the physical store for Trusted Root Certification Authorities of the Local Computer. The risk of this actually occurring is low, as the exploitation of this vulnerability can only be accomplished from within the root CA's hierarchy.

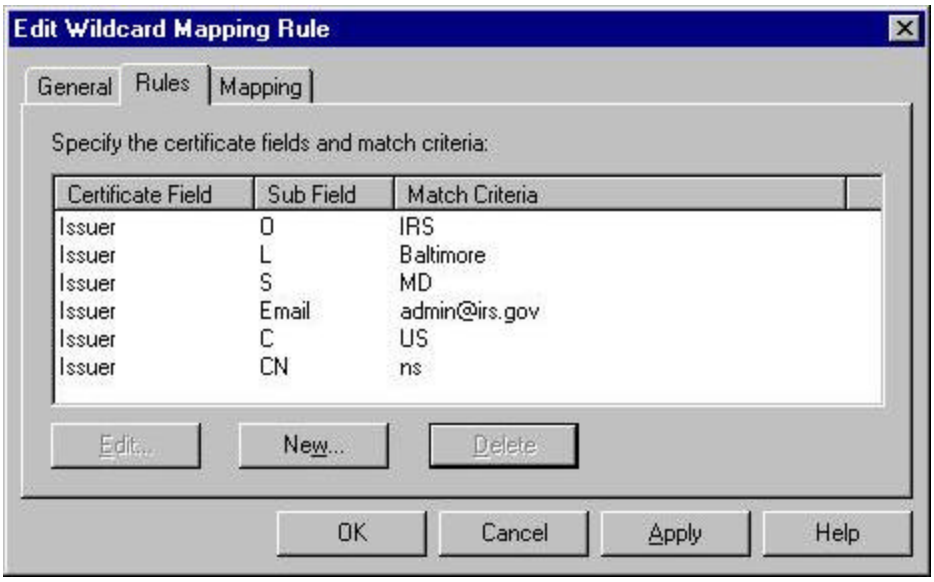


By clicking the **Edit** button in the Secure Communications window, an administrator can configure a wildcard rule for the many-to-one certificate mappings. The **Match on selected certificate issuers** option enables the administrator to define the CA(s) (or certificate issuers) to be applied in the many-to-one certificate mapping rule by clicking the **Select** button. Do NOT select **Match on all Certificate Issuers which I trust** option unless all default CAs have been deleted and you are sure that users with certificates created by those CAs, which you have carefully selected to put in the Trusted Root Certificate store of the Local Computer, apply to the created rule.





Select the CA(s) to apply to the many-to-one mapping rule. If the rule definition requires issuer attributes, or is intended to only use client certificates issued by a specific root CA or one of its subordinates, select ONLY that CA from the list of trusted CAs. If subject attributes are required, select ONLY those CAs that apply to the defined rule.



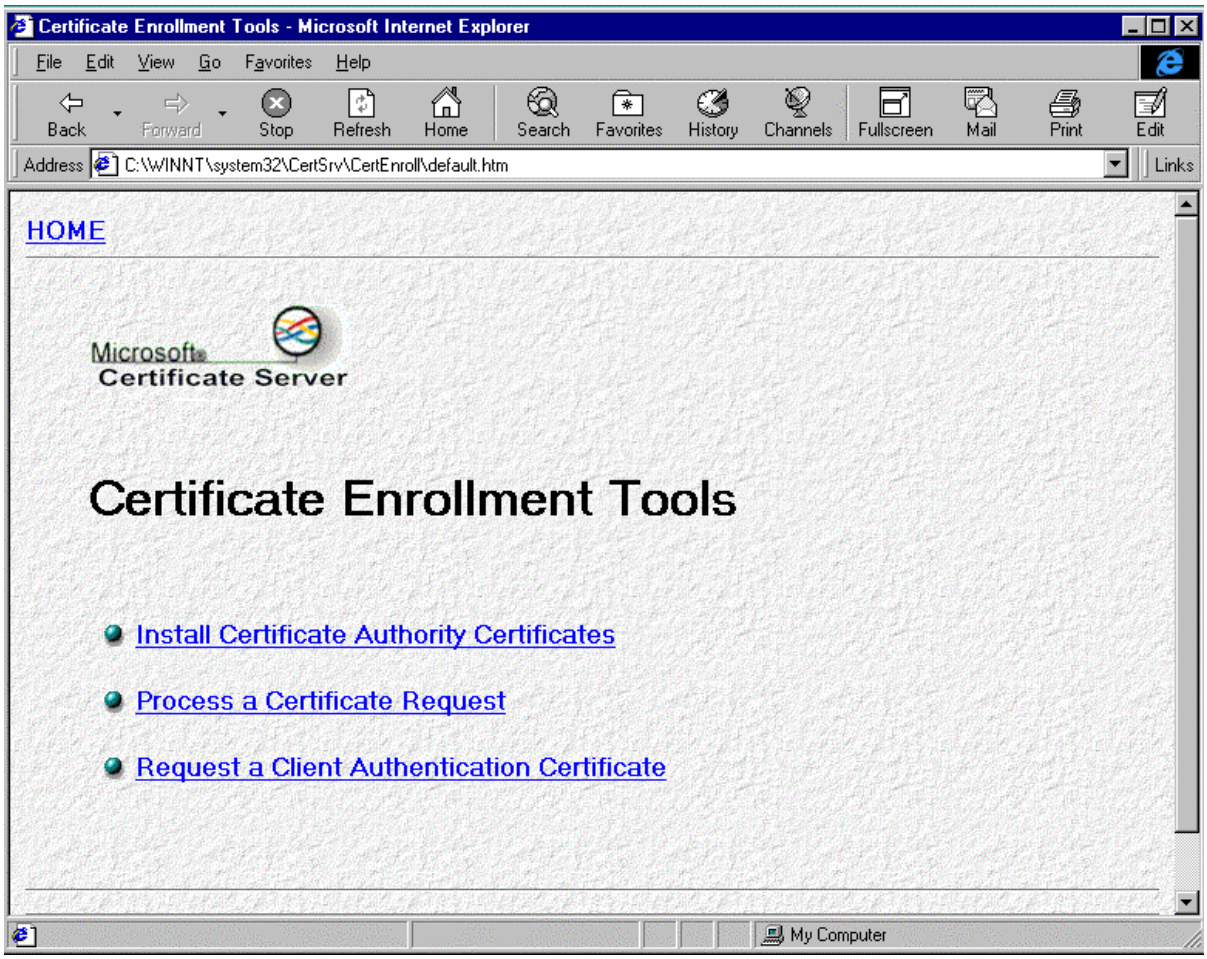
Define the matching rule to be applied to the selected CA(s). Apply all subject attributes as required. On the **Mapping** tab, define the logon account to use when the presented certificate matches the rules defined under the **Rules** tab. Access can also be refused based on certificates presented that match specified criteria by configuring a matching rule and selecting the **Refuse Access** option under the **Mapping** tab.

A Certificate Server can be setup at your site as a CA to generate its own digital certificates that you can then use for client and server authentication under the SSL protocol. The IIS setup program installs the Certificate Server files and the Web-based administration tools. Certificate Server runs as a Windows NT service and is configured by default to run automatically under the System account when the NT Server system boots. A few steps need to be taken to allow your server to perform client authentication and for clients to perform server authentication.

- Certify the server – The process of becoming certified takes place between your server and a CA.

- Client certificate enrollment – A client submits a request to the server for a certificate and then installs it in the client application.

These steps are accomplished by using the Certificate Server Certificate Enrollment Tools dialog box. Open the Certificate Server Certificate Enrollment Tools dialog box by opening Internet Explorer on **C:\WINNT\System32\CertSrv\CertEnroll\default.htm** (or the appropriate URL if accessing a certificate server over the network). It is a Web-based enrollment control used to perform the tasks listed.



NOTE: Once SSL and the use of certificates are configured for your site, clients must access the secure content using HTTPS. HTTPS servers can communicate with both secure and nonsecure HTTP servers. However, files and directories configured to require SSL would not be passed to clients not using HTTPS.

Chapter

Final Thoughts

This final chapter of the *Guide to the Secure Configuration and Administration of Microsoft Internet Information Server4.0*" deals with backup procedures and antiviral precautions.

Backup Procedures

It is very important to include a disaster recovery policy in your site's security plan. There are several ways to backup the data provided to clients from your server. Automatic backups, such as disk mirroring or disk duplexing, where you have a complete copy of the server's hard drive that can go online in the event the primary drive goes down, and manual backups. It is recommended that you do not rely on disk mirroring or duplexing exclusively. This strategy only protects against a single drive failure. In the event of a multiple disk failure, you must have other backups to recover. Here are some things to consider when implementing your backup strategy:

- How often does the server content change?
- How long can your site go without providing services to clients?
- Members of the Backup Operators group should have special logon accounts when performing backups. Backup privileges should not be assigned to regular user accounts.
- Consider keeping a set of backups offsite in the event of a natural disaster.
- Make a set of backups before and after any maintenance to the Web server. This includes any software/hardware changes to the system.
- It is very important that you make and TEST your backups regularly.
- Make sure that NTFS permissions are intact when a restore is done from a backup.

Antiviral Program

There are numerous public sector sources for information on antiviral products. A suggested starting point is the International Computer Security Association at http://www.ncsa.com. This Web page contains a lot of generic information about viral solutions and hot links to the major vendors.

Implement a robust anti-viral program as part of the security policy for the IIS environment.

References:

- Peter Dyson, Mastering Microsoft Internet Information Server 4
- Microsoft Press, Microsoft Internet Information Server ResourceKit
- Mark Minasi, Mastering Windows NT 4, Fifth Edition
- Robert Cowart, Windows NT 4 Unleashed, Server-Workstation
- Steve Sutton, Microsoft IIS & MSP Configuration Guidelines, Trusted Systems Services, Inc.
- Windows NT Server, Internet Information Server Security Overview White Paper, Microsoft
- Kenneth G. Jones, Internet Information Server Version 4.0-Security Assessment Report, MITRE Corporation
- Frank Redmond III, Making Sure Your Server's Secure, Microsoft
- James Morey, Untangling Web Security: Getting the Most from IIS Security, Microsoft Corp.
- James Hayes, Implementing IIS 4.0 and 5.0 Many-to-One Certificate Mappings

Revisions:

1 November 1999 - incorporate comments from Julie Connolly of the Mitre Corporation

10 January 2000 - included table of permission settings and added recent vulnerability announcements

5 September 2000 – added recent vulnerability announcements

19 June 2001 – added recent vulnerability announcements and inserted a section in Chapter 4 regarding problems with script mapping

14 September 2001 – removed vulnerability section and added a reference to Microsoft's IIS 4.0 downloads page; removed references to old documents

16 December 2001 – added a description of a possible weakness in many-to-one certificate mappings (this problem was identified by Captain James Hayes during testing of certificate mappings in IIS4 and IIS5)

4 March 2002 – slight modification to Certificates section