Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 4.0 â (Checklist Format)

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

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 (IIS4.0) and associated services. The focus of these documents is security-relevant information pertaining to the installation and administration of Internet IIS4.0. 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 very familiar with Internet Information Server but would like a quick reference in checklist format to use when installing and configuring IIS4.0 in a secure manner. This document is a condensed form of the document entitled *"Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 4.0"*.

Table 1 Summary of IIS Documentation

Document	Contents	Target audience
Guide to the Secure Configuration and Administration of Internet Information Server 4.0	• A detailed look at the secure installation and configuration of IIS4.0 and it's associated services	• Experienced NT and IIS administrators who may need information on how to install IIS4.0 in a more secure manner.
Internet Information Server (IIS) – Secure Installation and Configuration Checklist (This document)	• 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.

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.

Internet Information Server Installation and Configuration

Internet Information Server (IIS) is a high-speed Web Server used to publish and distribute WWW-based content to standard browsers. 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, therefore, this service will not be addressed in this document. Three additional application services are commonly associated with IIS - the Certificate Server, the Index Server, and Microsoft Transaction Server. These services can be installed at the same time as IIS4.0 or later. Secure installation, configuration, and administration of these services will not be addressed in this document.

IIS4.0 Installation

Install IIS4.0 according to the manufacturer's instructions. Invoke the Windows NT Operating System security guidelines contained within the "*Guide to Secure Microsoft Windows NT Networks*." This can be done before or after IIS4.0 is installed.

- 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 by answering the following questions. 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?
  - Will the server permit anonymous or authenticated user access (or both)?
  - Will Secure Socket Layer (SSL) connections be supported?
  - 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.

  - Partition the server so that published content of each supported service (WWW, FTP, SMTP) is located on a separate partition. This will prevent attempts to traverse up the directory tree beyond the published content root.

  - Do not install the IIS4.0 on the same partition as the Operating system.

  - Enable audit and IIS logging and track the information.

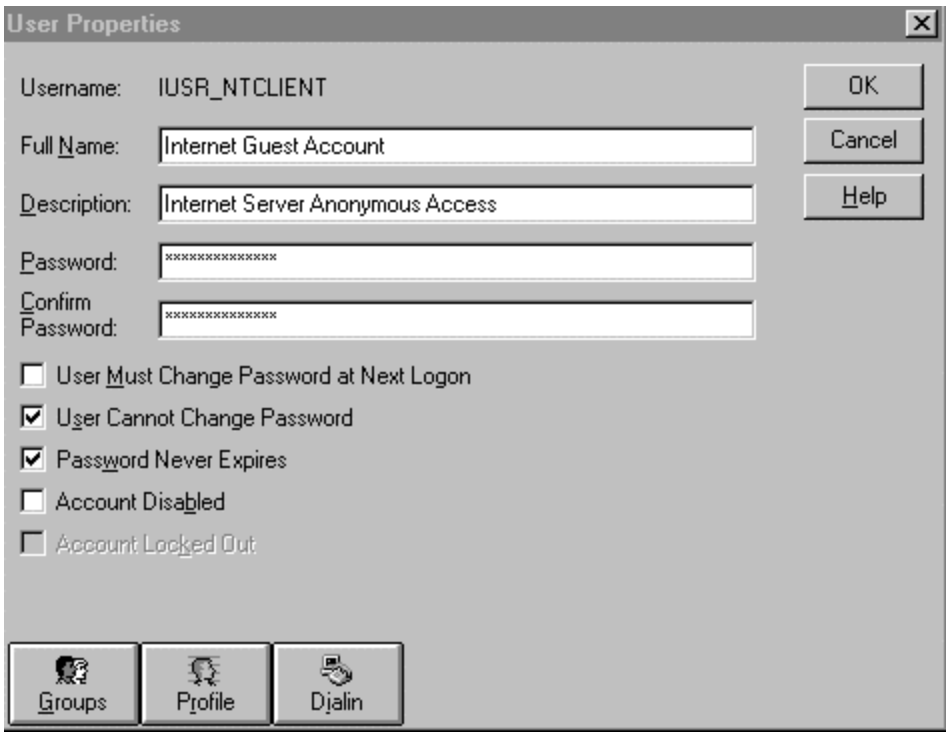
  - Remove all protocol stacks except TCP/IP, unless your Intranet requires another protocol stack.

  - 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.

  - Disable the following services, which are not required for most installations of IIS4.0:
    - Alerter
    - ClipBook Server
    - Computer Browser
    - DHCP Client
    - Messenger
    - Net Logon
    - 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 (This service is required to run User Manager)

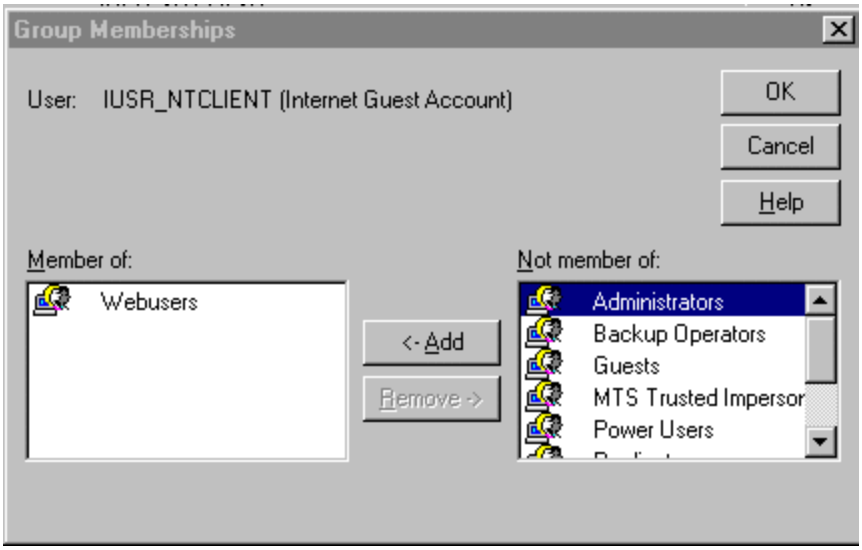
During the installation of IIS, a default account is created for anonymous logons. The default name for this account is IUSR_*computername,* where *computername* is the name of the machine hosting IIS. Configure this account as follows:

- Give this account the least amount of privileges possible.
- Select **User Cannot Change Password** and **Password Never Expires** options on the User Properties sheet for this account
- Ensure this is a local account, not a domain-wide account.
- Give this account the Right to **log on locally**. It does **NOT** require the Right to access this computer from the network.



User Properties Sheet for Anonymous Account

- Create new groups to be used with IIS. The “WebAdmins” group, for example, can be used to define users who will administer WWW content. If your sever hosts 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 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., the Users group.



IUSR_*computername* as a member of WebUsers group ONLY

- Change the access permissions on the IIS directories. It is particularly important to make certain that the groups “Everyone” and “Guest” are removed. The following chart outlines the recommended permissions for directories pertaining to IIS. Make sure you remove "Allow inheritable permissions from parent to propagate to this object" if it is selected for each directory to permit explicit ACL definition.

Note: IIS permissions complement the NTFS permissions. It is important to remember, however, that IIS web server permissions apply to all users accessing your site. Whereas, NTFS permissions are applied to individual users and groups with valid Windows NT accounts. 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, i.e., permissions that deny access will be enforced over those that grant access.

Type of Data	Example Directories	Data Examples	NTFS Permissions	IIS4.0 Permission
Default install directories	\inetpub \WINNT\system32\inetsrv	Top level IIS dir. System dir.	Administrators (Full Control) System (Full Control)	N/A
Metabase	\WINNT\system32\inetsrv	MetaBase.bin	Administrators (Full Control) System (Full Control)	N/A
Static Content	\wwwroot\images \wwwroot\home \ftproot\ftpfiles	HTML, images, FTP downloads, etc.	Administrators (Full Control) System (Full Control) WebAdmins (Modify) Authenticated Users (Read) Anonymous (Read)	Read and None
FTP Uploads (if required)	/ftproot/dropbox	Directory used by 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 and None
Script Files	\wwwroot\scripts	.ASP	Administrators (Full Control) System (Full Control) WebAdmins(Modify) Anonymous (Traverse Folder/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 (Modify) Anonymous (Traverse Folder/Execute)	Execute

- 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 Anonymous account (WebUsers group). Grant Modify 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 separate directory containing binary files that must be executed by the Web server. Script and Execute are additional access control permissions offered by IIS4.0.

- 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.

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

The Metabase File

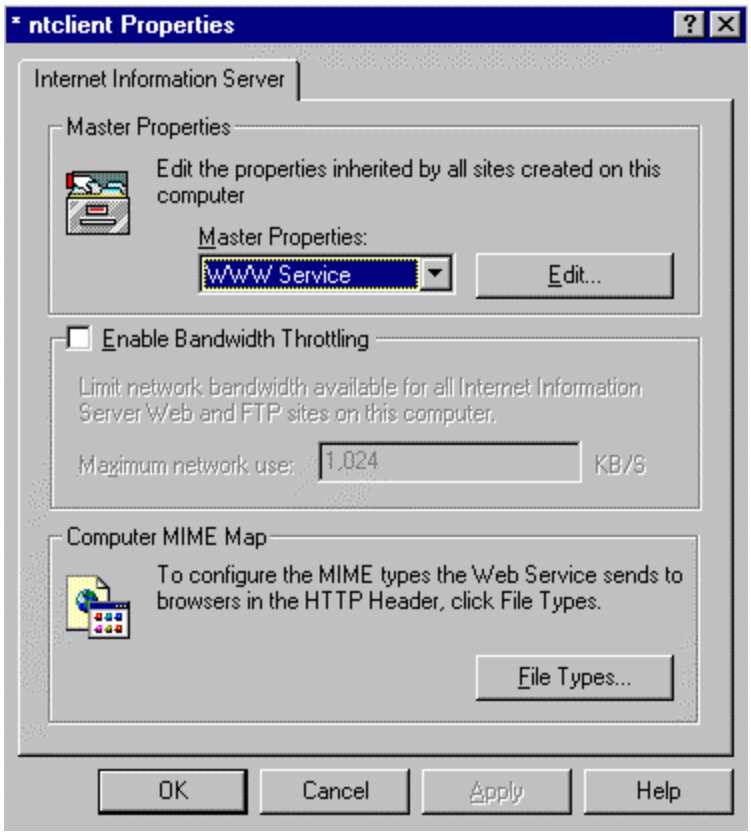
The Metabase is stored in a special format disk file, by default named Metabase.bin in the \WINNT\system32\inetsrv directory. This is the default installation directory for IIS. The Metabase loads from disk when IIS starts, stored to disk when IIS shuts down, and saved periodically while IIS is running. It is important to protect this file from unauthorized use, even though sensitive data is stored in a secure manner within the file.

- Store the Metabase.bin file on an NTFS partition and use Windows NT security to protect it. When IIS 4.0 is installed, the Administrators group and System are given Full Control to the Metabase.bin file. There is no need to modify this setting.

- To hide this file from unauthorized users, move or rename the file. To relocate or rename the Metabase file, 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.

Internet Service Manager

When you start the IIS4.0 Internet Service Manager (ISM), an MMC console begins running and automatically loads the Internet Service Manager 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 becomes very useful if you know that you will be creating a number of different sites on your server. These properties will be automatically inherited by all sites created on your server, which will save time when configuring each site. The common settings that can be established through the Master Properties dialog box to enhance security will be discussed. Access the Master Properties dialog box by highlighting the IIS server name in the ISM and selecting "**properties**" in the **Action** pull down menu. Click the **Edit** button to configure Master Properties for the selected server.

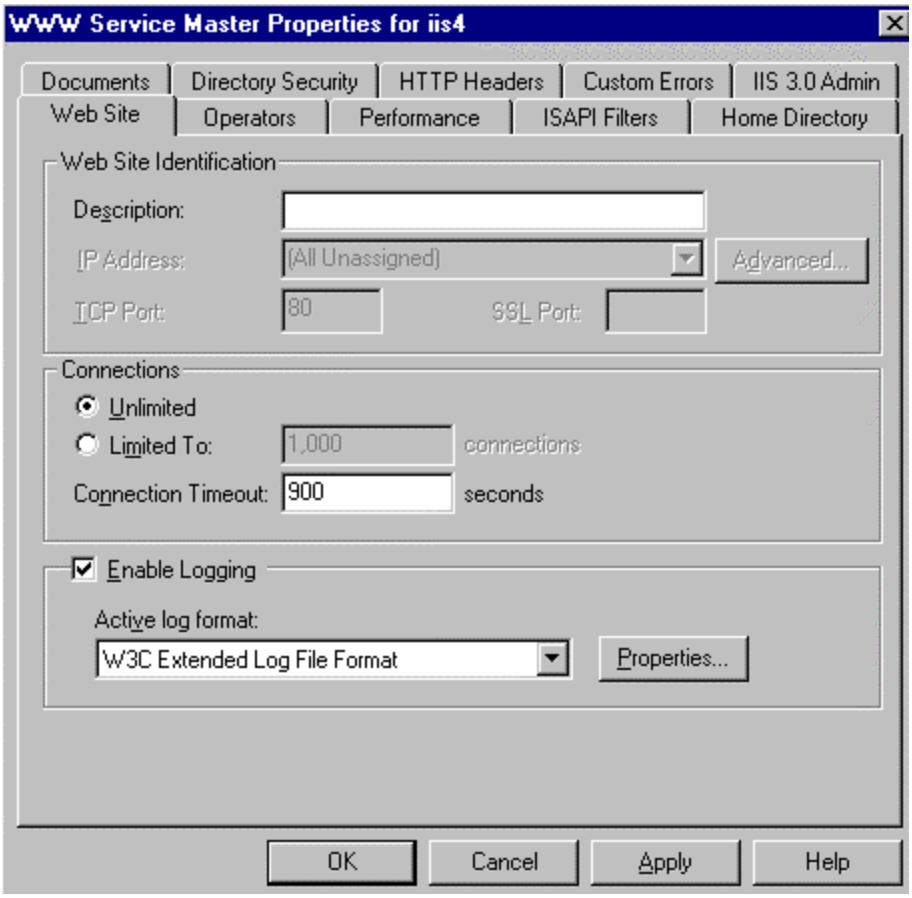


Master Property Dialog Box for IIS WWW Sites

Master Properties

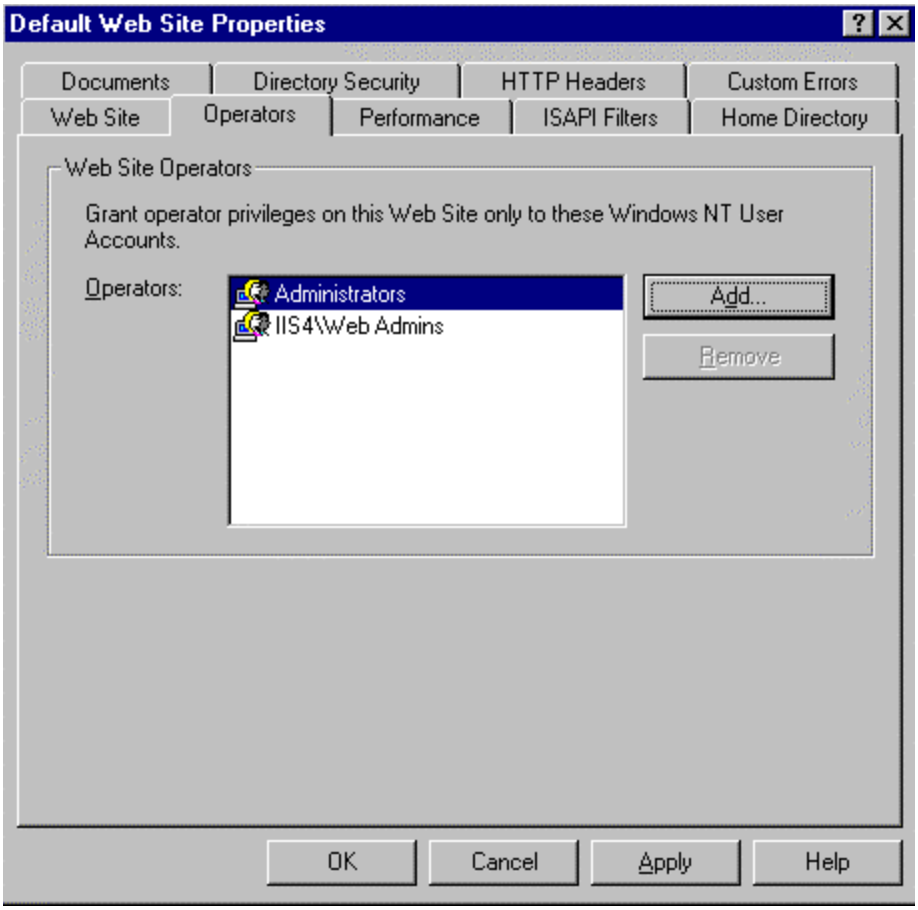
This property dialog box is used to set default values used by all current or new sites on this server. If a value for a specific web site will change as a result of the values set on the Master Properties dialog box, you will be prompted to select the items that should adopt the new settings. An item 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.



Master Web Site Properties dialog box

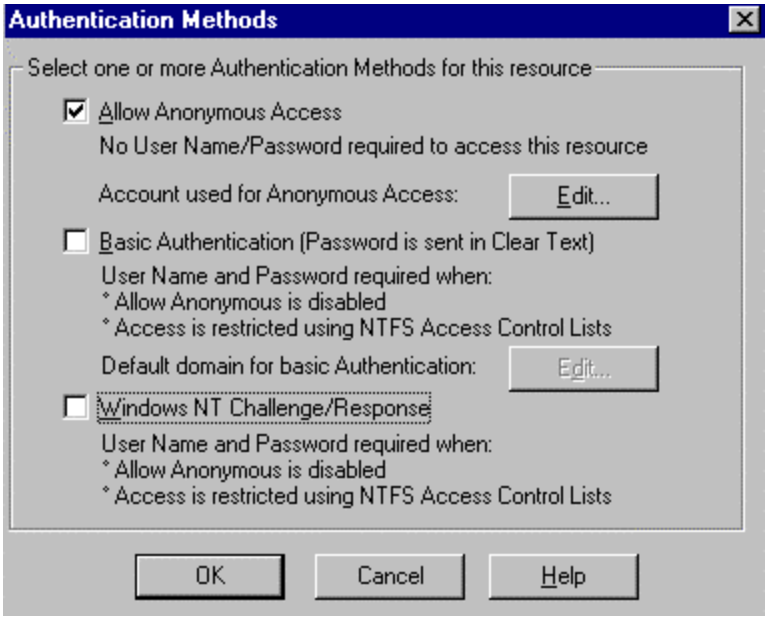
The following shows the dialog boxes for setting common security-related properties using the **Web Site** tab and **Operators** tab. Other tabs may have common settings as well, but will depend on how you setup your server. Note that these same settings can be applied individually to the WWW, FTP, and 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 sites.



Master WWW Operators dialog box

- Select **Add** to insert users or a group of users (recommended) who are responsible for maintaining web content for ALL sites created on the server. When you configure each site, these groups/accounts automatically appear and you 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. These specific groups are added to the above list during the configuration of each individual web site.)

Directory Security Tab - Authentication Methods



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.

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
- Require Secure Channel when accessing this resource
- Enable Basic Authentication and disable Anonymous and Challenge/Response for this site

Windows NT Challenge/Response (NTLM) – This is the most secure of the three options 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.

The following summarizes important 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. This directory will also be assigned IIS4.0 Read only permission during the WWW/FTP site setups. These directories are used to store data you wish to make available to client browsers for viewing/downloading only.

- Create directories with Execute NTFS permission only for the WebUsers group. These directories will be assigned IIS4.0 Script or Execute only permission during the WWW site setup. Script will be assigned to directories containing script files, such as .ASP. Execute will be assigned to directories containing all other types of executables, i.e., .exe/.cmd/.dll, etc.

- Make sure the Metabase file is protected by hiding it from unauthorized users.

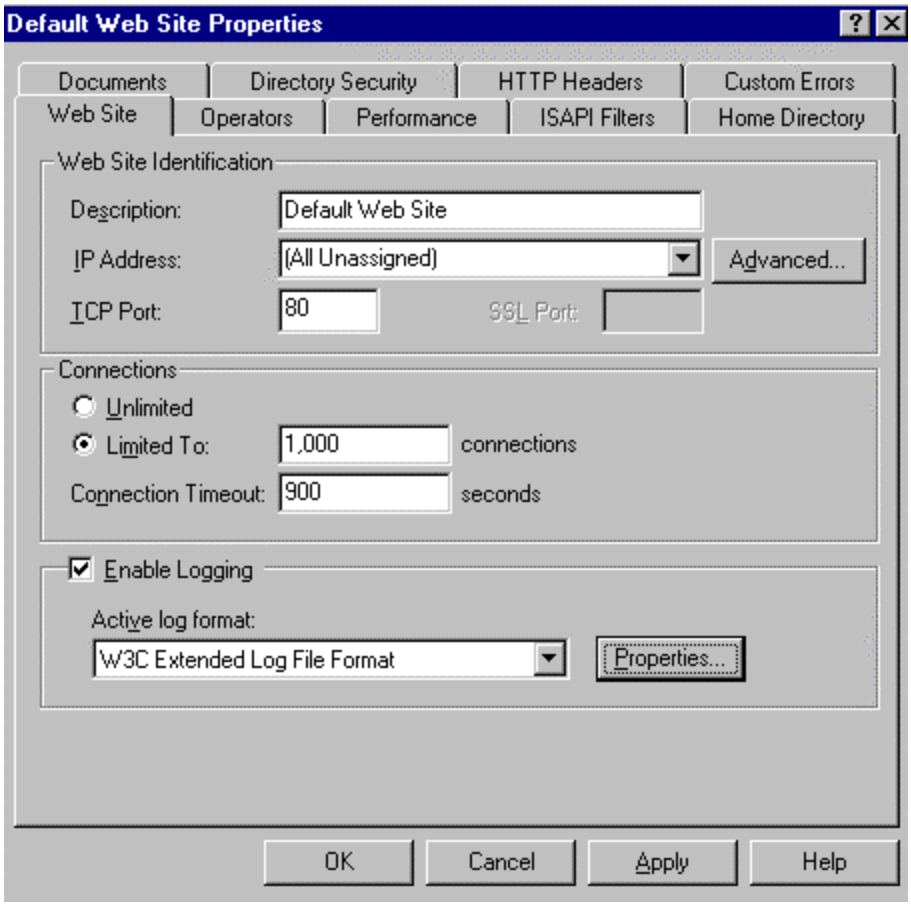
World Wide Web (WWW)

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 tree view to identify this web site; an IP address; a TCP Port and SSL Port (if you change these from their defaults, 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.

- **Connections** – Limit the number of simultaneous accesses to your web site and set a connection timeout. Timeout settings are recommended to prevent a possible denial of service attack.

- **Enable Logging** – Once IIS logging is enabled, you can configure how and when log files are created and saved.

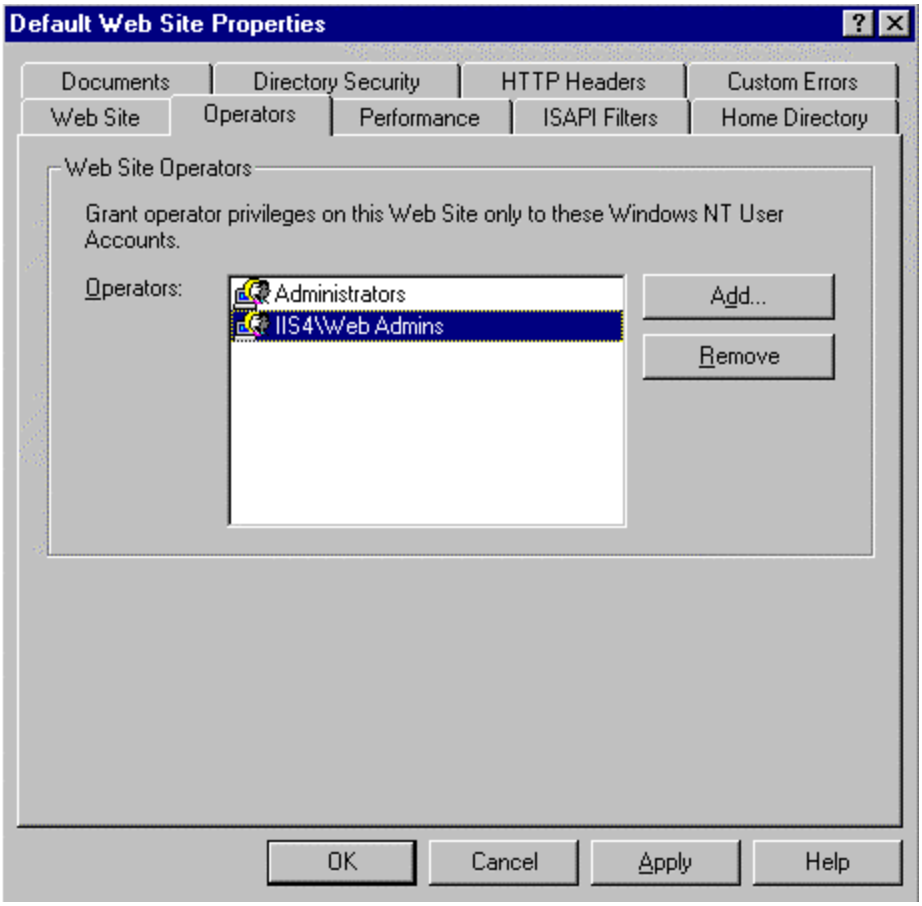


Operators Property Dialog Box

Web Site Operators

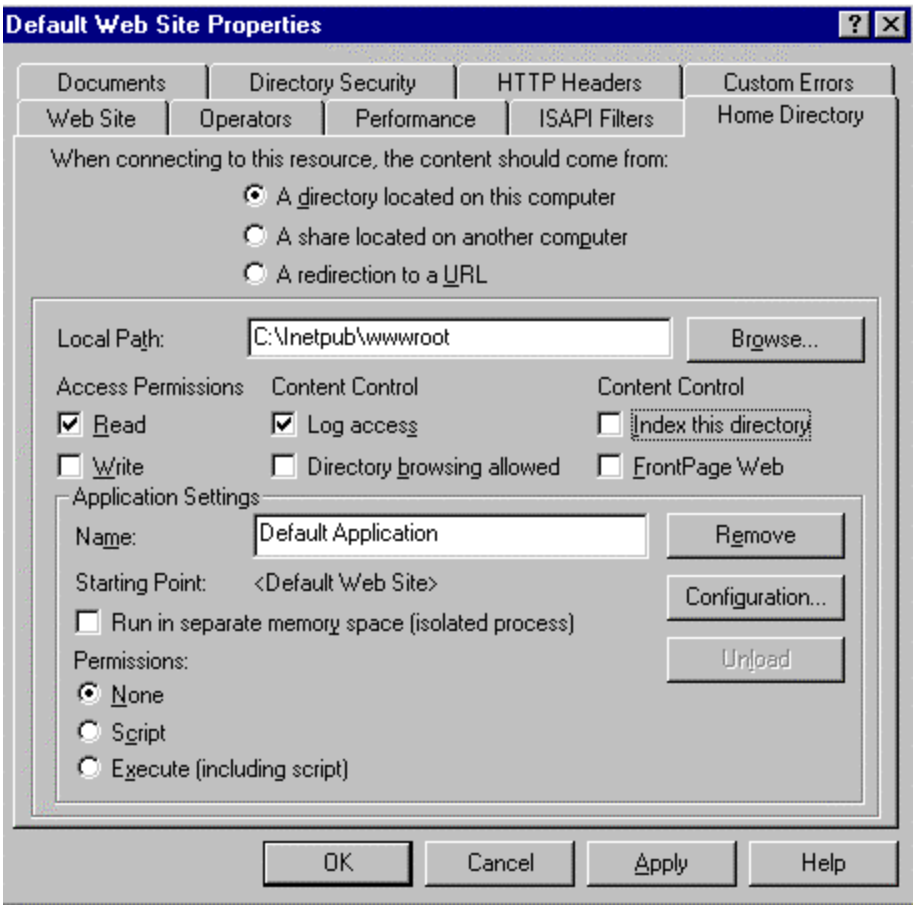
- Add users or a group of users (recommended) who are responsible for administering the data for your site by selecting the **Add** button on the **Web Site** property dialog box. Operators can work only with the properties that affect the web site for which they were created. They cannot access the properties that control overall IIS setup, the NT server operating system that hosts IIS, or the network on which the system runs.

NOTE: When selecting members for this group, make sure individuals are knowledgeable and trustworthy to minimize compromising your system's security.



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). Set **Read** only for directories created with downloadable content accessible by all users for browsing. Directories containing scripts or other executables should not have **Read** or **Write** permissions enabled.

Content Control

- Ensure **Log Access** is selected. This ensures that all visits to this directory are logged into the log file.

- Deselect **Directory Browsing Allowed** if it is selected. 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.

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.

- **Permissions** – These settings control the execution of applications contained within a directory. Carefully select the appropriate option. A directory containing scripts only should have only the **script** option enabled. Other executables should be maintained separately with only the **execute** option enabled. Make sure the read and write access permissions are not enabled when these options are selected.

Below is a description of the options available for Application Settings, permissions:

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).

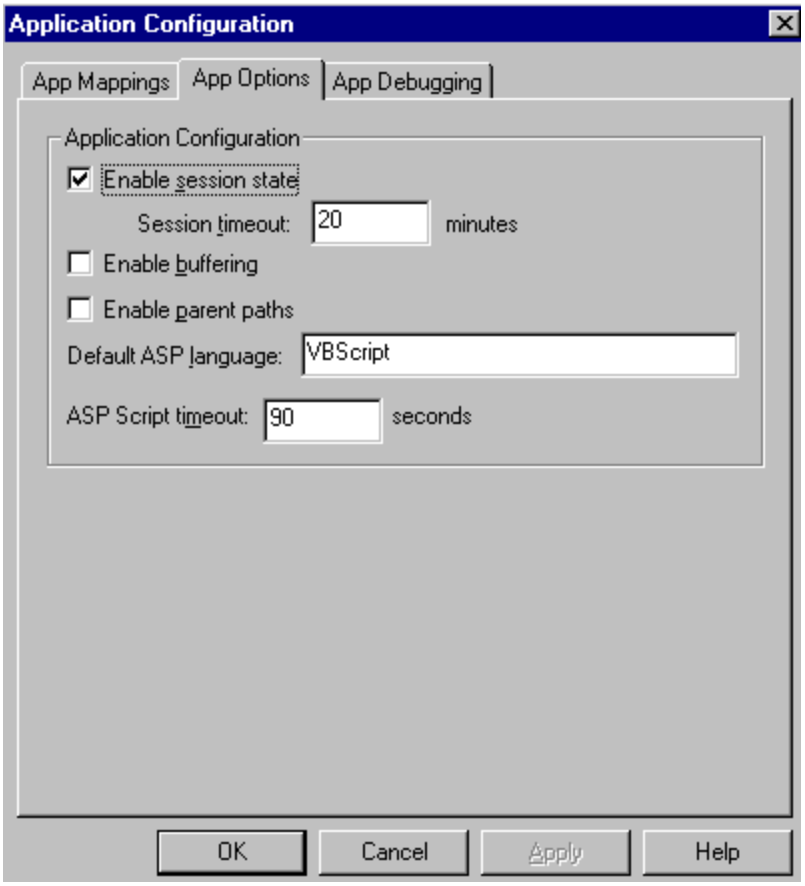
Applications can be configured in more detail by using the **Configuration** button. A separate dialog box is displayed with the following tab options: App Mappings; App Options; Process Options (if you select to run in separate memory space); and App Debugging. Discussions in this document focus on the security relevant settings, which are limited to the **App Options** and **Process Options** dialog boxes described below.

App Options

- Select **Enable session state** and set a **Session timeout** so that Active Server Pages (ASPs) creates 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.

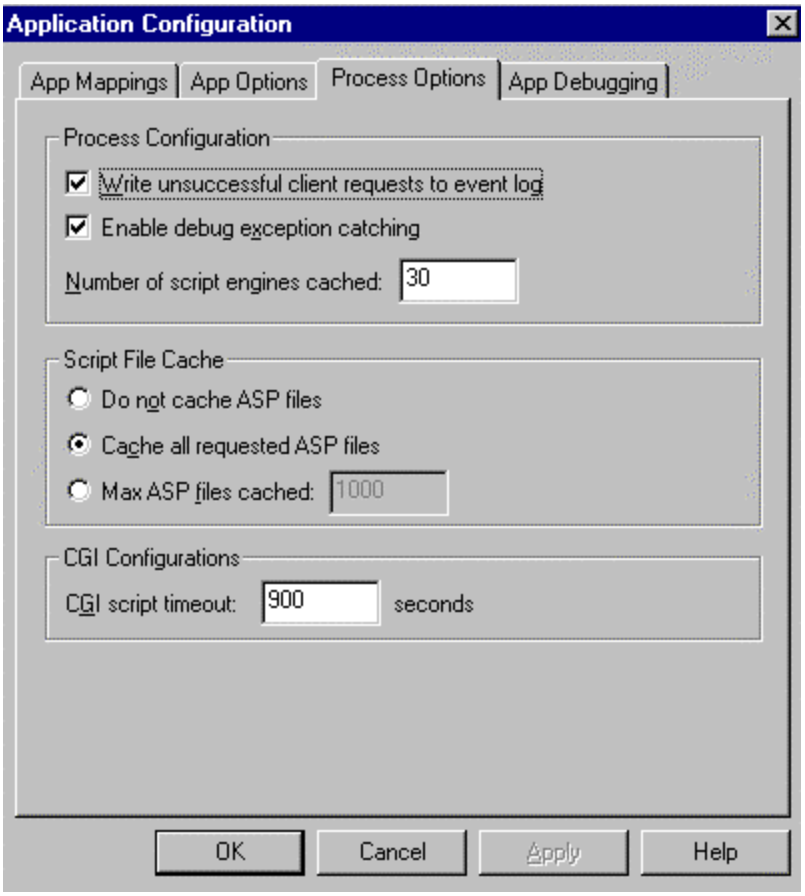
- Enter an **ASP Script timeout** value so that if a script does not complete execution within the allotted time, an entry will be made into the NT Server Event Log and execution of the script will stop. Setting timeout values will help prevent a denial of service attack.

- Deselect **Enable parent paths.** This option allows the use of ".." in calls to MapPath.



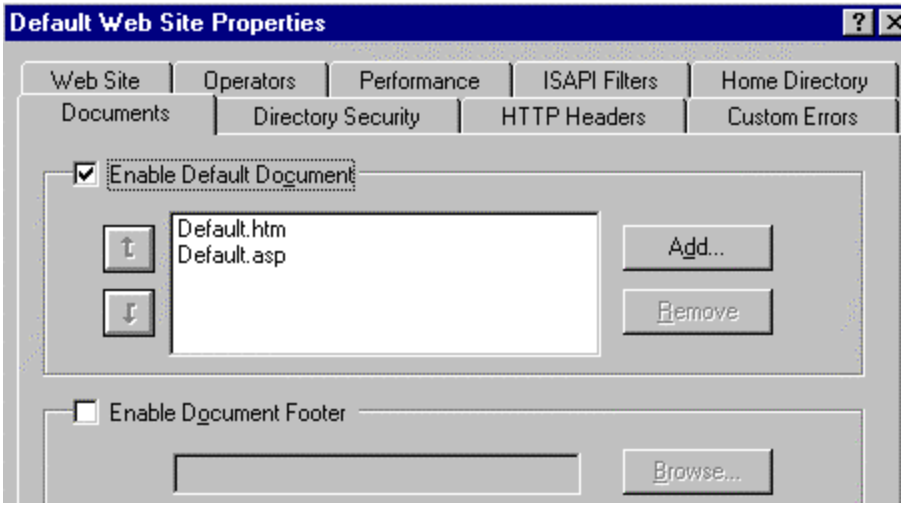
Process Options

- Select **Write unsuccessful client requests to event log**



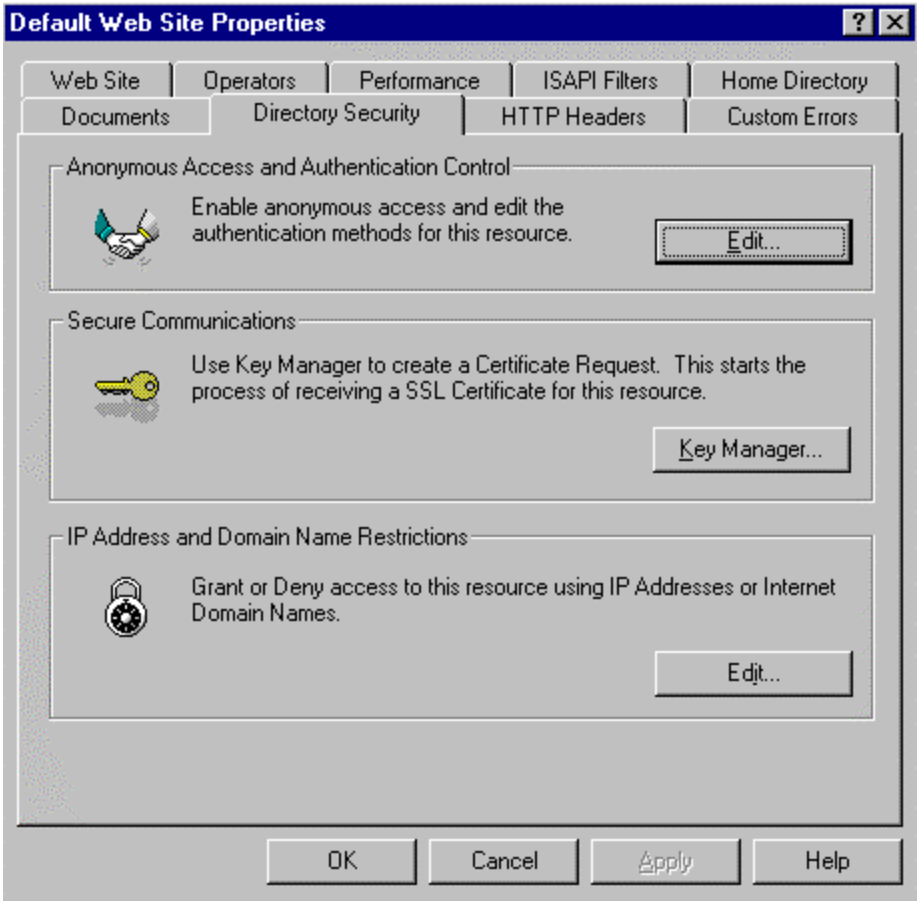
Documents Property Dialog Box

- Create and insert a default document. 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.



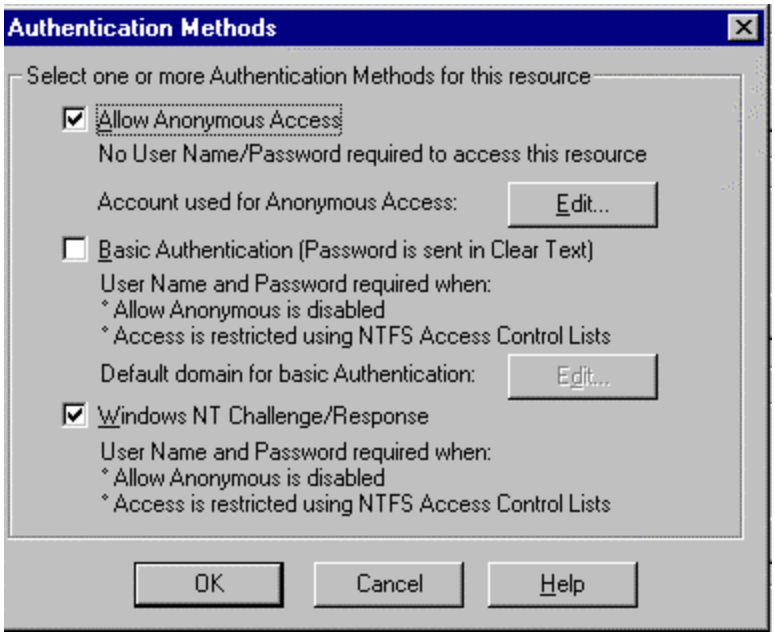
Directory Security Property Dialog Box

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

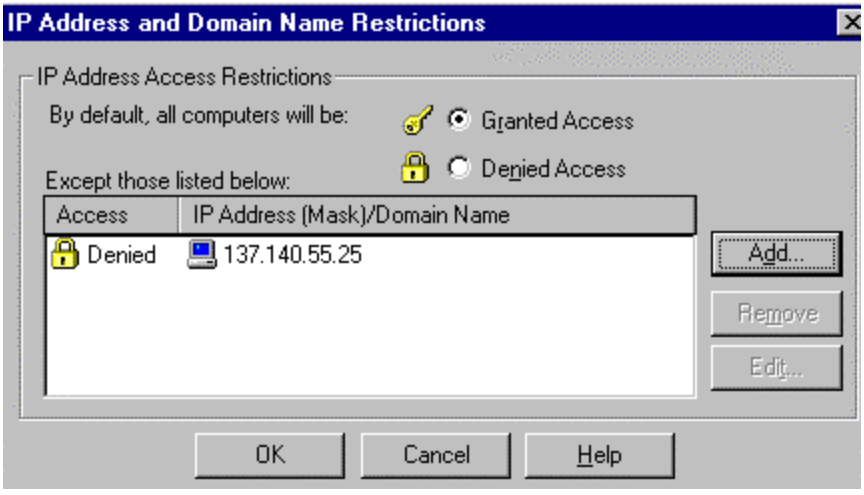
- Select the appropriate options for web sites, directories, and files as determined by the security policy of each site supported by the server.



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 setup, visitors to your web site must use a browser capable of supporting secure communications.

IP Address and Domain Name Restrictions

- 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** denies access to resources except to those computers with IP addresses specifically listed. Three options are available when specifying computer IP addresses: **single computer** - specify a single IP address**; group of computers** - specify the network ID and subnetmask; or an entire domain – specify a **Domain Name**.



File Transfer Protocol (FTP)

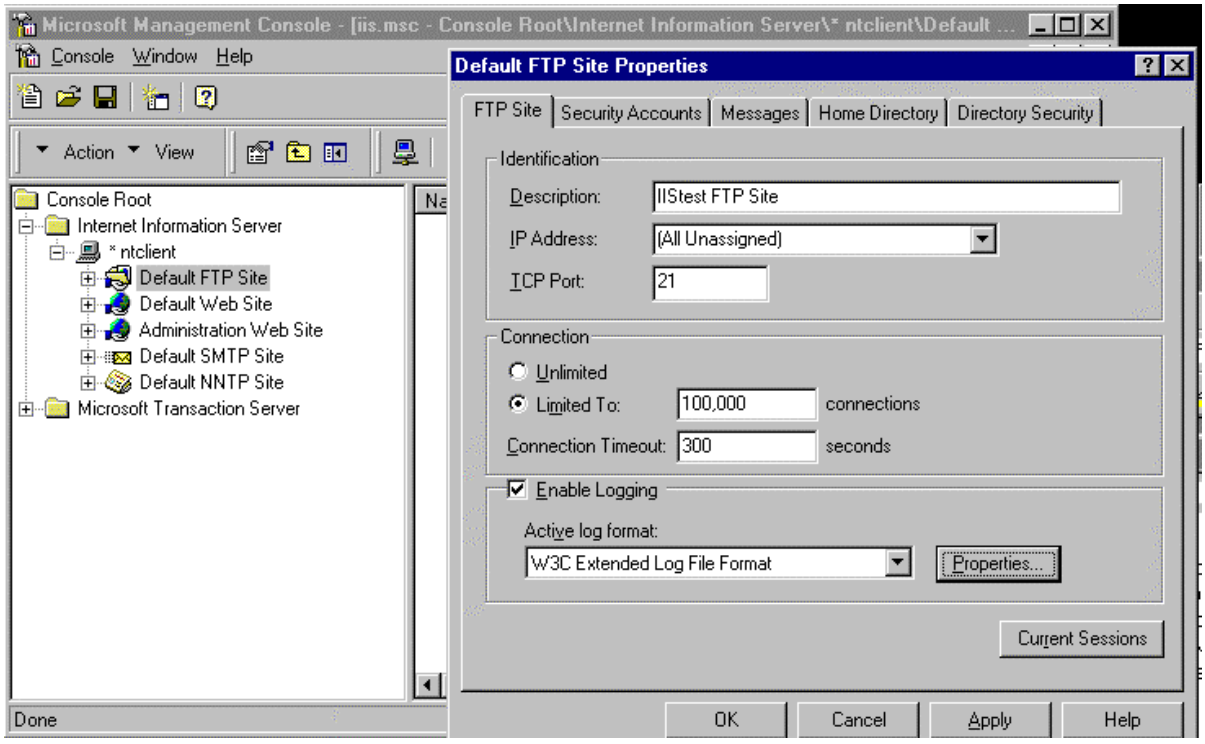
- Configure your FTP server so that uploading of files to the server **is prohibited**. If it is necessary to allow uploads, ensure users with this responsibility are explicitly specified on the directory permissions. This prevents intruders from stashing pirated software, cracking tools, and other illegal 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") to receive these files. Also, monitor this directory regularly as part of your security policy.

Organizing FTP Directories

- Organize FTP directories for your users. Make sure FTP download directories are configured for NTFS 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 NTFS Write permission for users granted permission to upload files to the FTP server. Conversely, the FTP directory configured for user downloads is set to Read ONLY. This will prevent users from altering or deleting files uploaded by others. 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

- Select the "Enable Logging" option and assign a connection timeout value to prevent a denial of service attack.



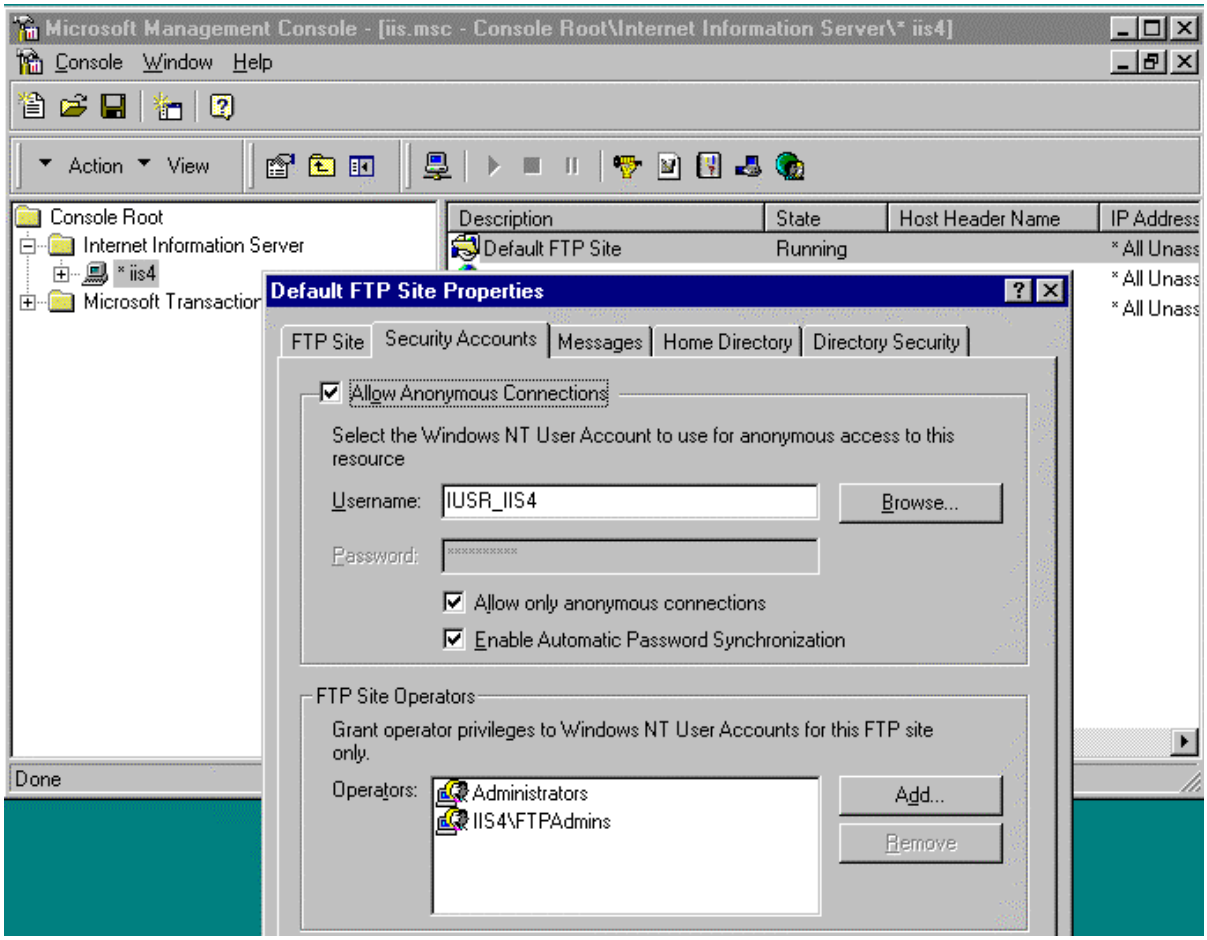
Security Accounts Property Dialog Box

- Select 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.

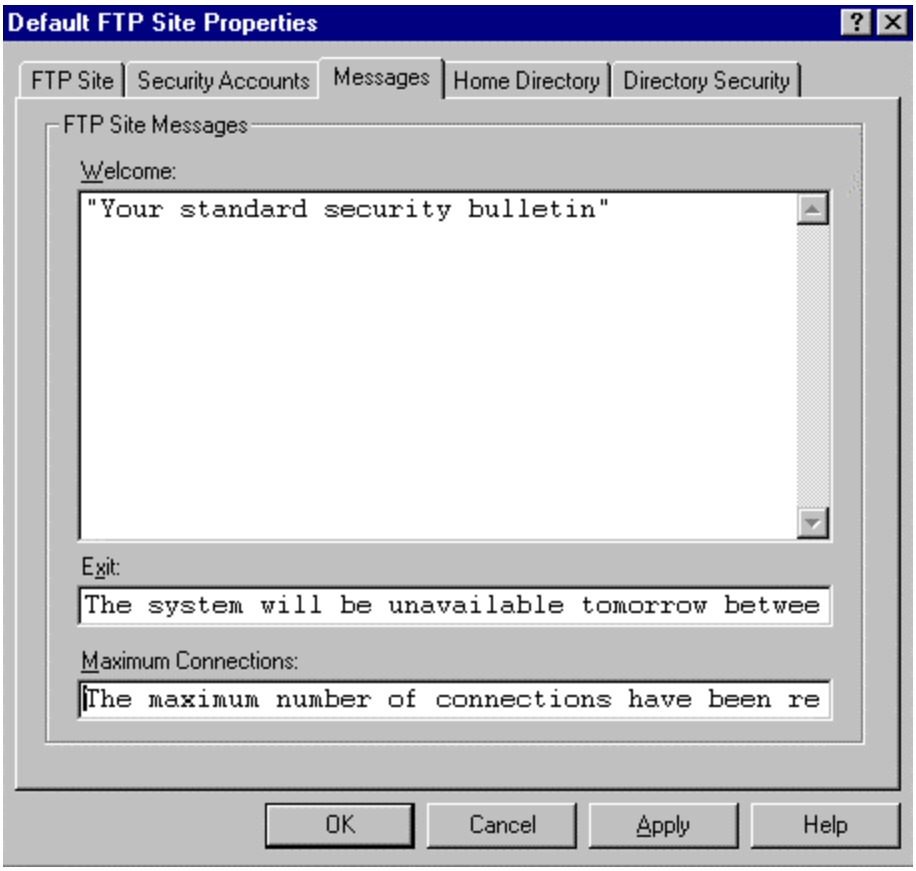
- Designate which user accounts you want to administer your FTP site. Place these accounts in a Group (i.e., FTPAdmins) then add this Group under the Security Accounts tab of the FTP site property sheet.

- 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. This eliminates the need to specify a password, avoiding a possible mismatch resulting in anonymous access failure. 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 anonymous accounts.



Message Property Dialog Box

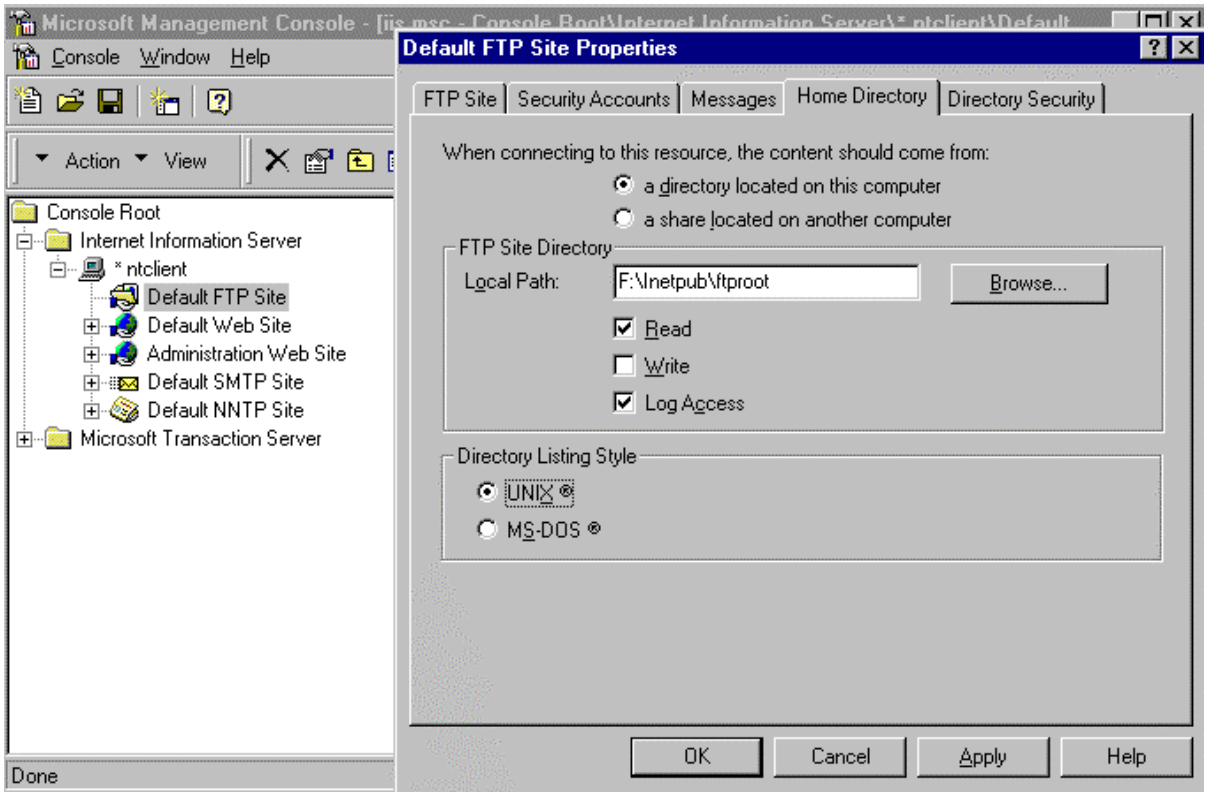
- Insert a Welcome message in the form of a Security Banner to be displayed to any user connecting to your FTP server. Exit messages can be used to display notices to users upon connection termination. A Maximum Connections message can be used to notify the user should the number of maximum connections is reached.



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.

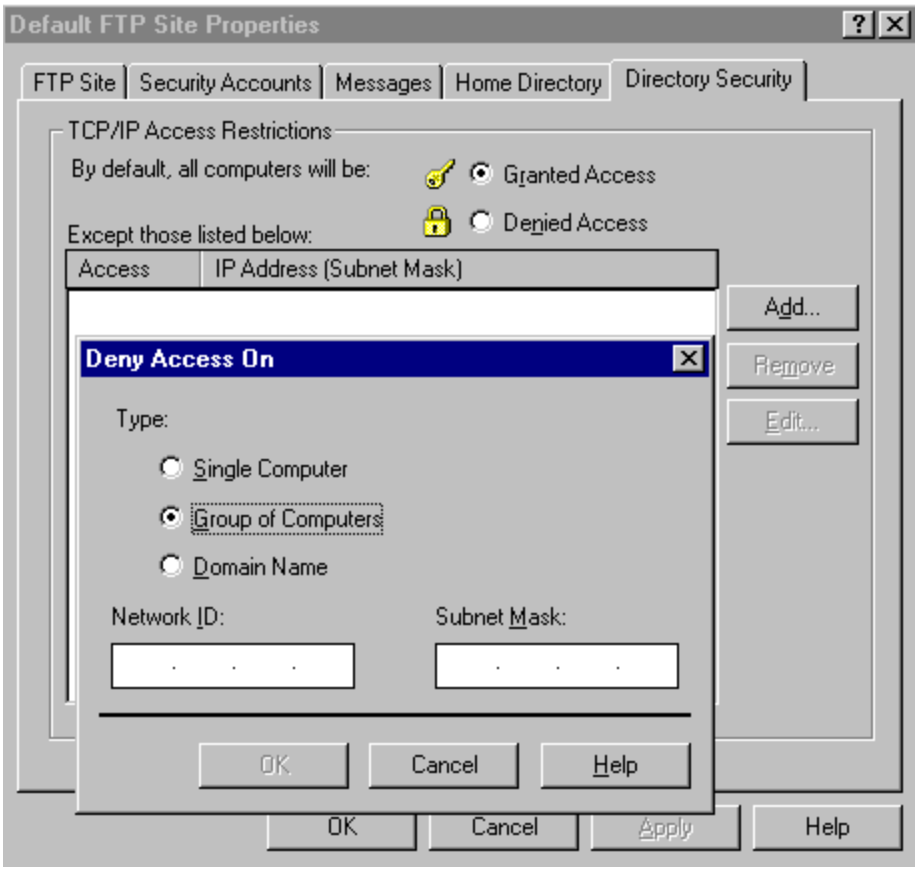
- Set Read access ONLY for the FTP Site Directory. If your site requires users to upload data, create two directories beneath the "ftproot" directory. One with Read ONLY access to store data made available to all users for download, and one with Write Only permission to be used as a "drop box" uploading data. FTPAdmins could then review 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 will allow ONLY those computers with listed IP addresses access to your resources, and will deny all other requests.

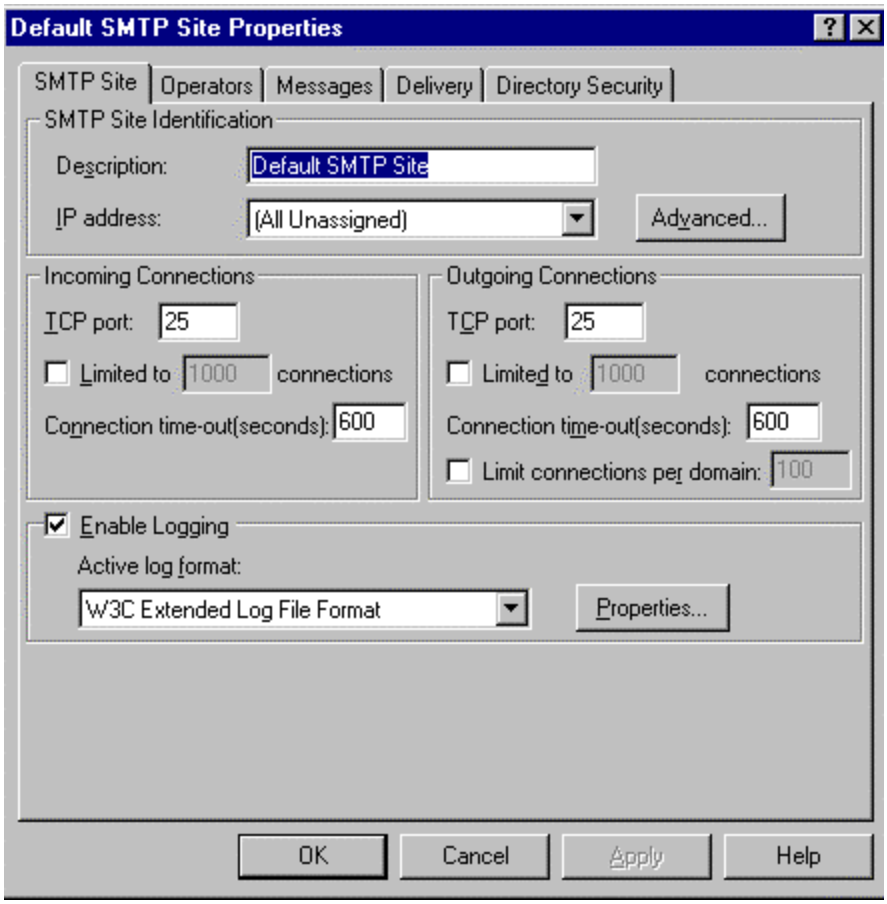
- Select the option that best fits your security policy. If access to FTP files is limited to users within your site, select "Denied Access" and specify computers or domains permitted access.



Simple Mail Transfer Protocol (SMTP)

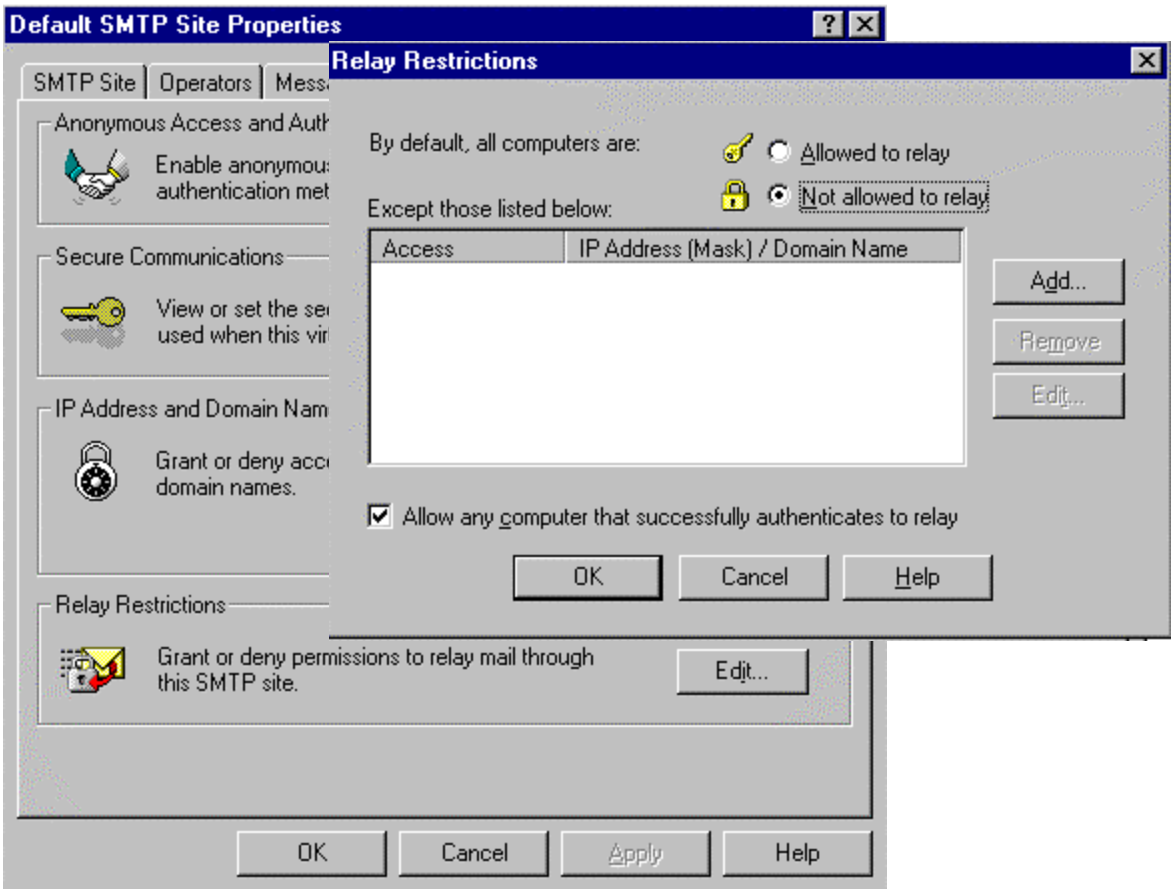
IIS4.0 includes an SMTP mail service used to transfer Internet messages between servers. However, this is not a full SMTP server. The SMTP service does not provide a POP server and is not intended for use by end-user programs (i.e., Netscape Mail or Outlook Express). This service is intended for use 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 pulldown 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.

- Select **Not allow 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.**



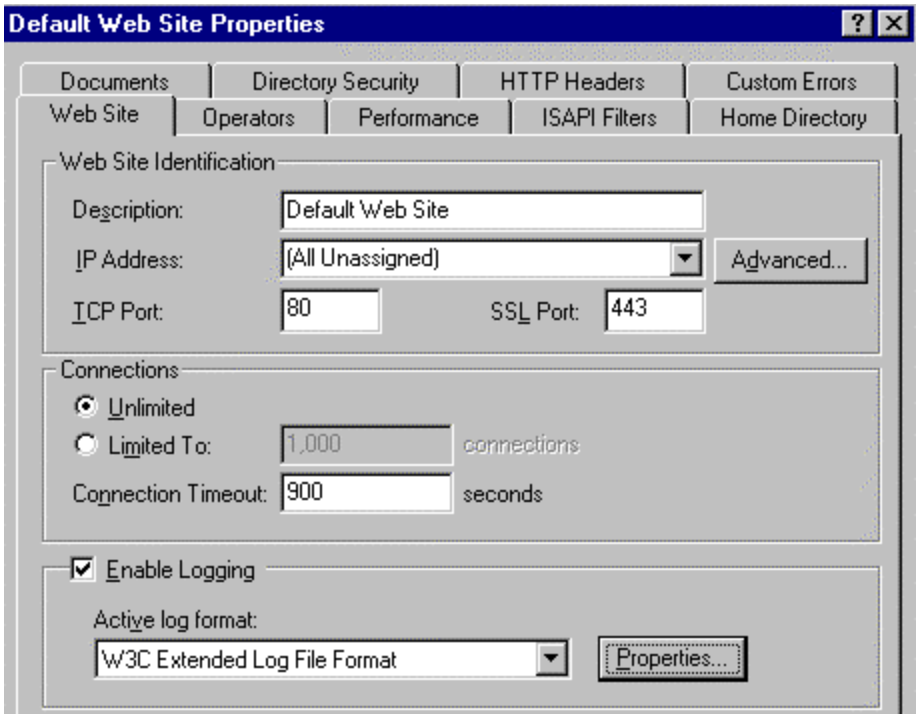
Microsoft SMTP Service supports the use of Transport Layer Security (TLS) for encrypting transmissions. You can require the use of TLS for all incoming connections through the Secure Communications dialog box from the Directory Security tab. To use TLS for the server, you must create key pairs and configure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

Auditing

In addition to the audit settings described in the "Guide to Secure Microsoft Windows NT Networks", enable IIS logging 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.

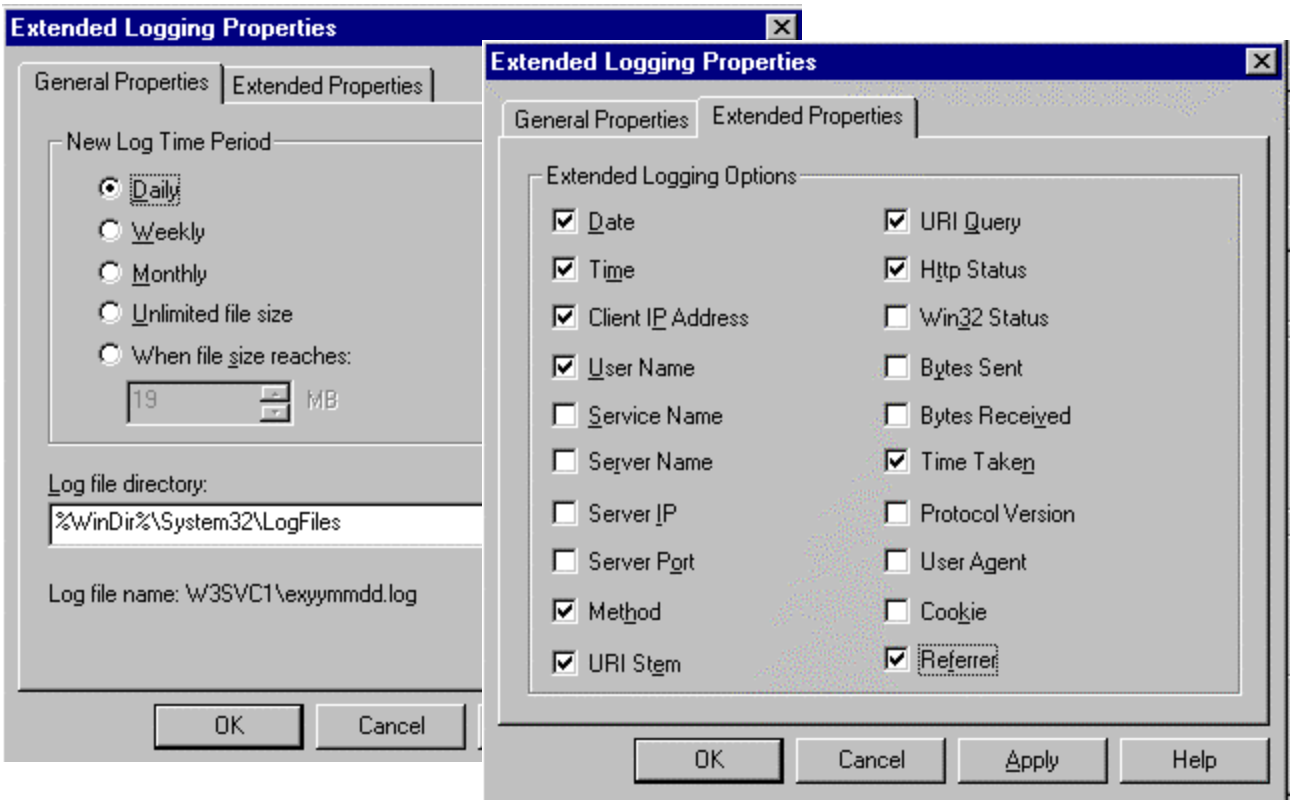


- Move and rename the IIS LogFiles directory. This can increase the difficulty unauthorized users experience while trying to "cover their tracks."
- Limit Full Control access on the IIS LogFiles directory to SYSTEM and Administrators ONLY (or whichever group is created to manage auditing on your system). 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. Audit for success and failure in the Windows NT audit facility.

- Extended Logging Options - Some settings that should be included in 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

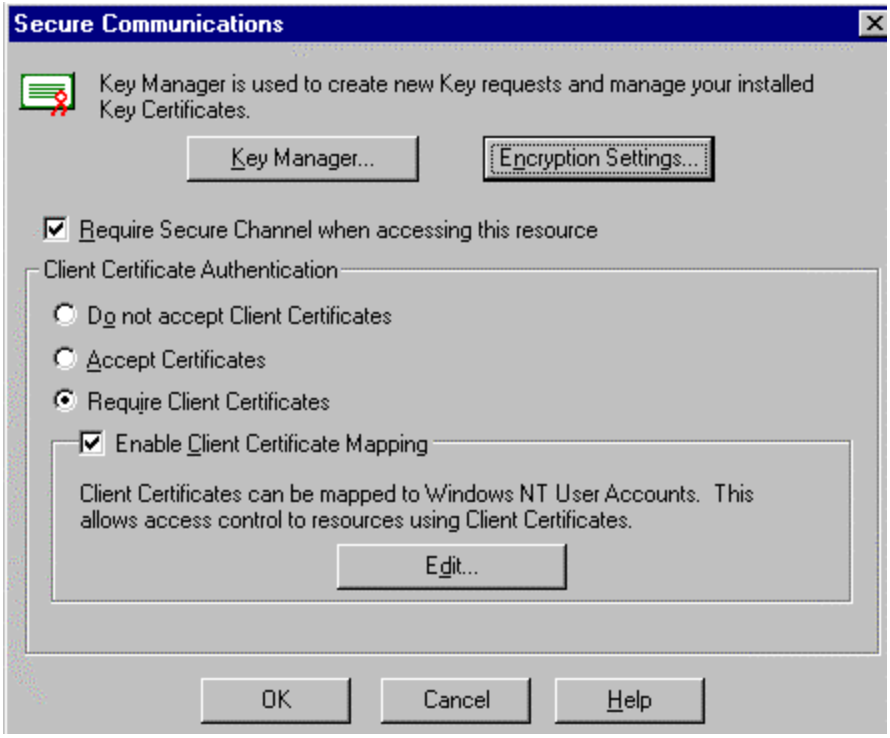
A good description of how to administer the certificate manager and client certificates within your IIS environment can be found in the book entitled Mastering Internet Information Server 4.0. This document provides a brief description.

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

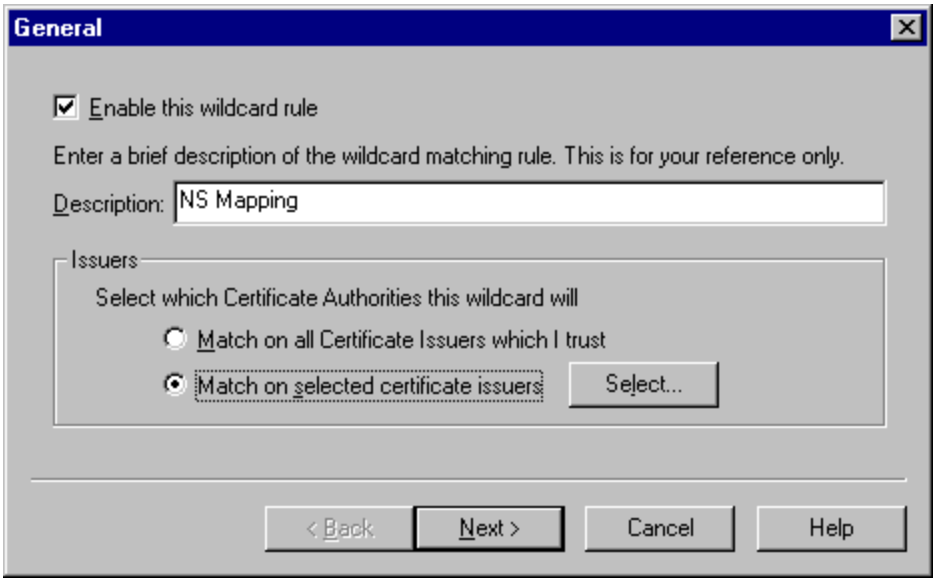
Once you have configured your site to use certificates, activate the SSL security on your server using the ISM for the directories that require secure access.

Two options are available when mapping certificates to user accounts in IIS4 – a one-to-one mapping and a many-to-one mapping. One-to-one mapping is pretty simple, one certificate maps to one NT account. The comparison performed is a certificate-to-certificate comparison of the presented certificate to the certificate defined in the one-to-one mapping rule. However, 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 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.

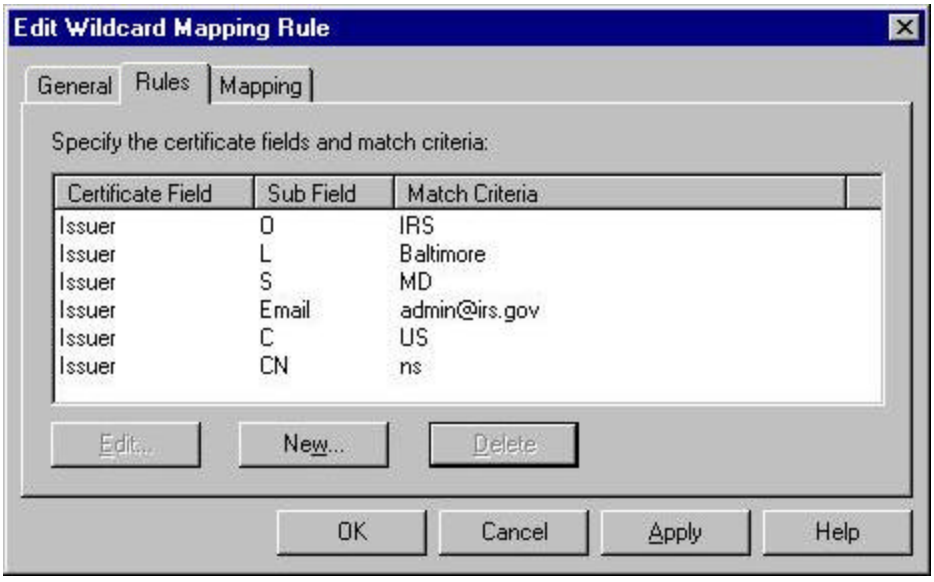


- Click the **Edit** button in the Secure Communications window to configure a wildcard rule for the many-to-one certificate mappings.

- Select the **Match on selected certificate issuers** option and click the **Select** button to define the CA(s) (or certificate issuers) to be applied in the many-to-one certificate mapping rule. Do NOT select **Match on all Certificate Issuers which I trust** 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 criteria 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.

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.

Backups

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.
- 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:

- Mastering Microsoft Internet Information Server 4, Peter Dyson
- Microsoft Internet Information Server ResourceKit, Microsoft Press
- Mastering Windows NT 4, Fifth Edition, Mark Minasi
- Windows NT 4 Unleashed, Server-Workstation, Robert Cowart
- Microsoft IIS & MSP Configuration Guidelines, Steve Sutton, Trusted Systems Services, Inc.
- Windows NT Server, Internet Information Server Security Overview White Paper, Microsoft
- Internet Information Server Version 4.0-Security Assessment Report, Kenneth G. Jones, MITRE Corporation
- Making Sure Your Server's Secure, Frank Redmond III, Microsoft
- Untangling Web Security: Getting the Most from IIS Security, James Morey, 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 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 section on mapping certificates (this problem was identified by Captain James Hayes, USAF, during testing of certificate mappings in IIS4 and IIS5)

4 March 2002 – slight modification regarding the mapping of certificates