

UNCLASSIFIED

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

The Network Applications Team
of the
Systems and Network Attack Center (SNAC)

By:
Sheila Christman
26 July 2001
Version 1.31



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

WIN2Kguides@nsa.gov

UNCLASSIFIED

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- Please keep track of the latest security patches and advisories at the Microsoft security bulletin page at <http://www.microsoft.com/technet/security/current.asp>.
- 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

Windows NT and Microsoft Internet Information Server are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

IIS4.0 INSTALLATION.....	1
WORLD WIDE WEB (WWW).....	12
FILE TRANSFER PROTOCOL (FTP).....	20
SIMPLE MAIL TRANSFER PROTOCOL (SMTP)	25
AUDITING.....	28
KNOWN VULNERABILITIES	30
UNCHECKED BUFFER IN INDEX SERVER ISAPI EXTENSION (MS01-033).....	30
SCRIPT MAPPINGS	31
MALFORMED EXTENSION DATA IN URL (MS00-30)	31
UNDELIMITED .HTR REQUEST AND FILE FRAGMENT READING VIA .HTR (MS00-031)	32
MALFORMED HTR REQUEST (MS99-019)	32
MALFORMED FTP LIST REQUEST VULNERABILITY (MS99-003).....	32
ALTERNATE DATA STREAMS	33
VARIATION OF THE “DOT” VULNERABILITY	33
DENIAL OF SERVICE VULNERABILITY WITH THE IIS FTP SERVICE	35
UNAUTHORIZED FILE MANIPULATION THROUGH SAMPLE WEB SITES AND SCRIPTS	36
POTENTIAL PROBLEM IN REMOTE DATA SERVICES (RDS) VERSION 1.5 (MS99-025)	39
MALFORMED HTTP REQUEST HEADER (MS99-029)	40
DOMAIN RESOLUTION AND FTP DOWNLOAD VULNERABILITIES (MS99-039).....	40
MULTITHREAD SSL ISAPI FILTER VULNERABILITY (MS99-53)	41
VIRTUAL DIRECTORY NAMING VULNERABILITY (MS99-058).....	41
ESCAPE CHARACTER PARSING VULNERABILITY (MS99-061)	41
BACKUPS	42
ANTIVIRAL PROGRAM.....	42

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

This document is one of three 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*".

For those who may not have the requisite level of familiarity with IIS, another complementary document, entitled "*Internet Information Server 4.0 – Security Assessment Report*", may be a better starting point. That document provides an overview of the Internet Information Server environment. It offers a description of the architecture of the Internet Information Server and associated services, introduces the Internet Information Server Administrator's tool, and describes, in general terms, the security features provided by Internet Information Server. The intended audience is those who are either unfamiliar with Internet Information Server or are interested in a refresher on these topics.

UNCLASSIFIED

Table 1 Summary of IIS Documentation

Document	Contents	Target audience
Guide to the Secure Configuration and Administration of Internet Information Server 4.0	<ul style="list-style-type: none">• A detailed look at the secure installation and configuration of IIS4.0 and it's associated services	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• A secure installation and configuration guide in checklist format with no detailed explanations	<ul style="list-style-type: none">• 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 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.

- 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?

UNCLASSIFIED

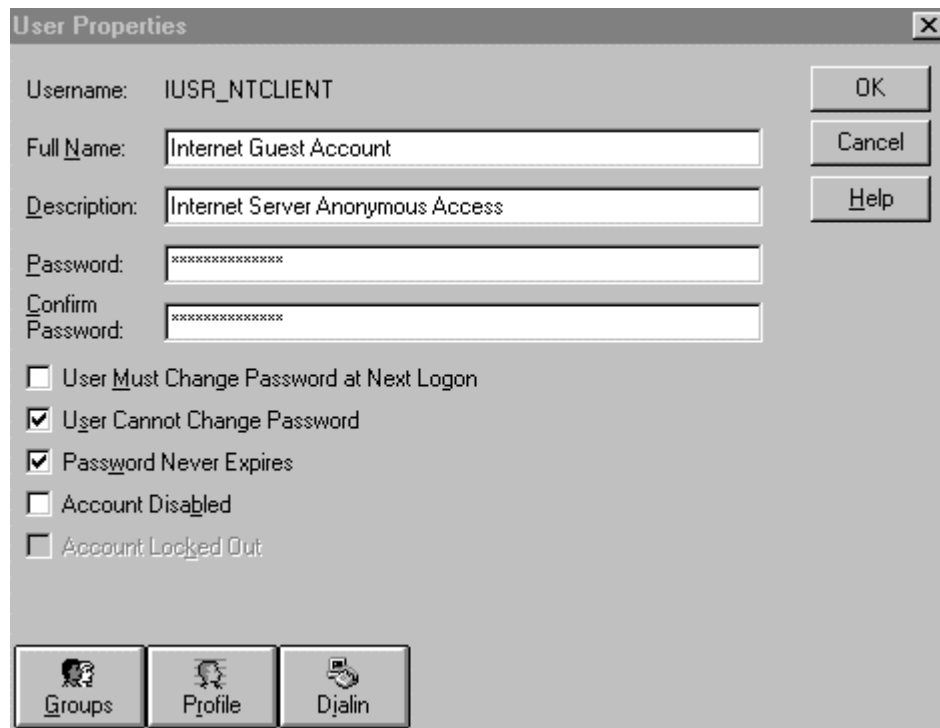
When installing IIS4.0, the following guidelines are recommended:

- 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)

UNCLASSIFIED

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:

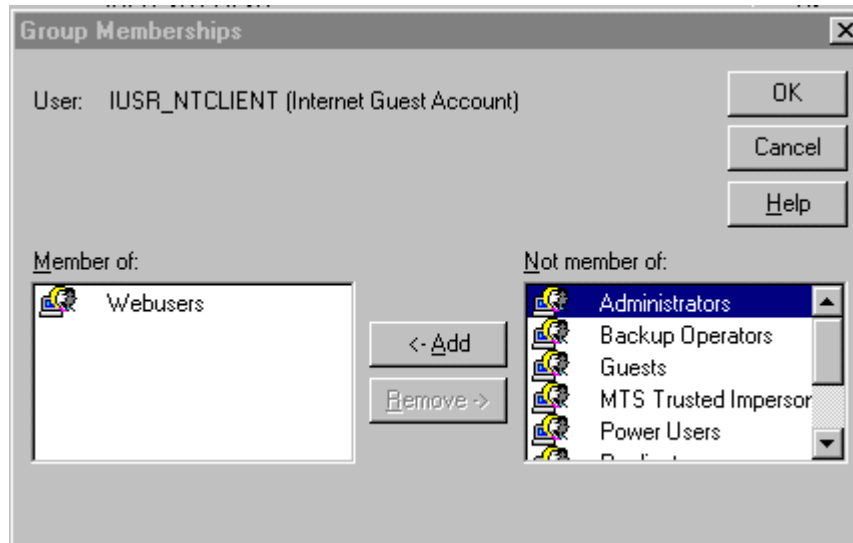
- ❑ Give this account the least amount of privileges possible.
- ❑ Select **User Cannot Change Password** and **Password Never Expires** options on the User Properties sheet for this account
- ❑ Ensure this is a local account, not a domain-wide account.
- ❑ Give this account the Right to **log on locally**.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



The screenshot shows the 'User Properties' dialog box for the user 'IUSR_NTCLIENT'. The 'Full Name' field is 'Internet Guest Account' and the 'Description' is 'Internet Server Anonymous Access'. The password fields are masked with asterisks. The 'User Cannot Change Password' and 'Password Never Expires' checkboxes are checked. The 'Account Disabled' and 'Account Locked Out' checkboxes are unchecked. At the bottom, there are three buttons: 'Groups', 'Profile', and 'Dialin'. On the right side, there are 'OK', 'Cancel', and 'Help' buttons.

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.

UNCLASSIFIED

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

UNCLASSIFIED

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

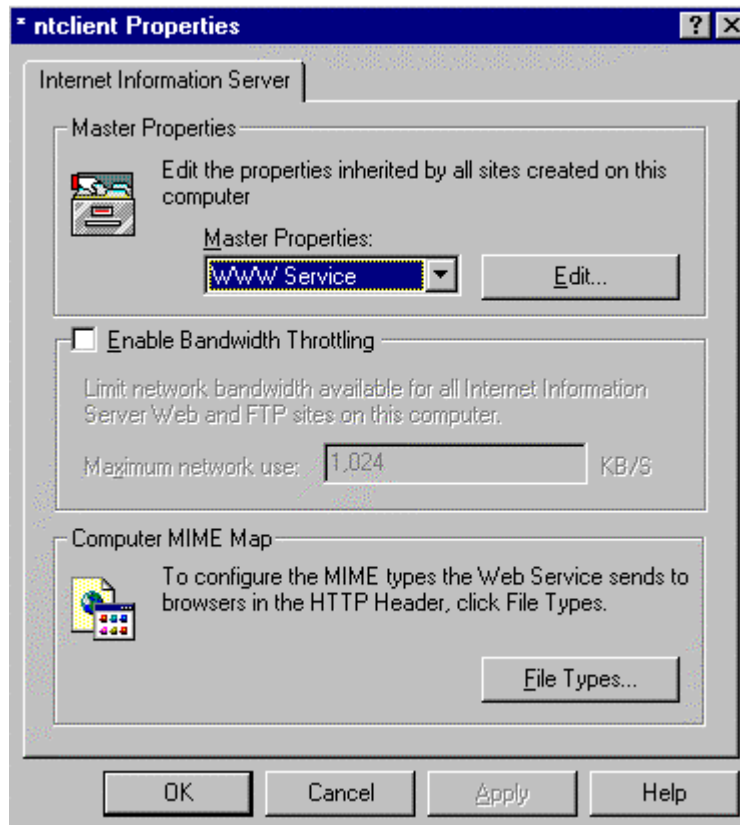
The Metabase File

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.

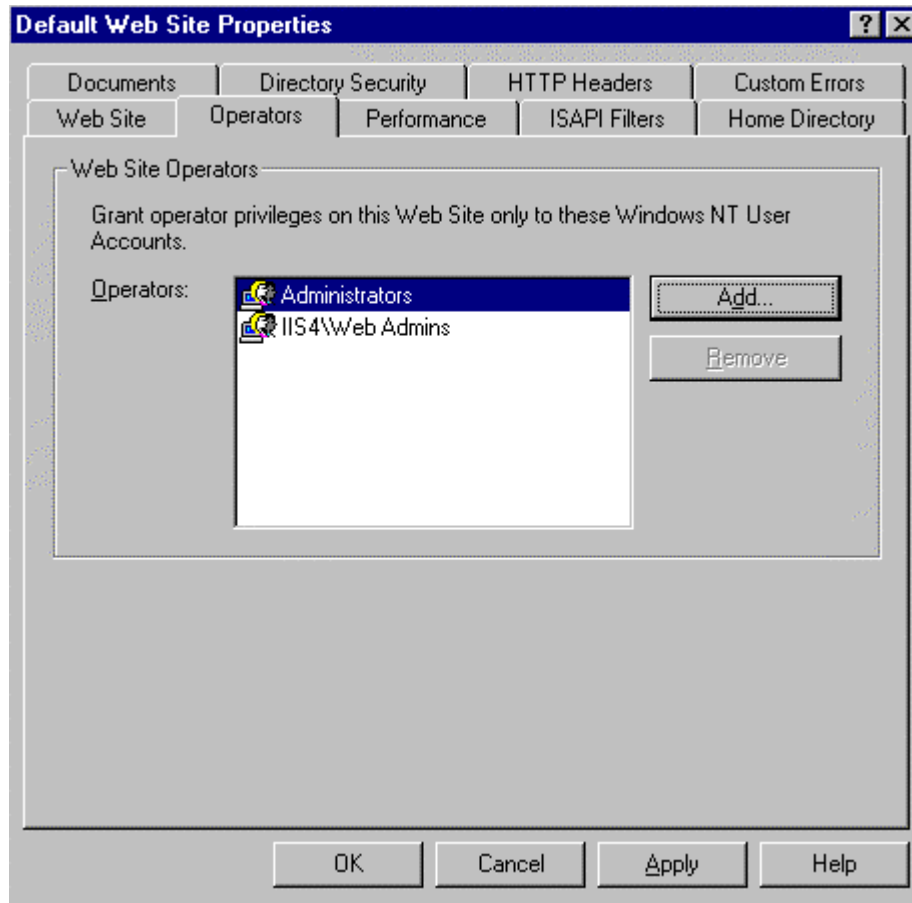
- ❑ Select **Edit** in Master Properties to configure common WWW site properties. Enable Logging is selected by default and is the only security related setting on this dialog box. Keeping the default setting will ensure logging is enabled for all web sites created on this server.

The screenshot shows the 'WWW Service Master Properties for iis4' dialog box. It features a tabbed interface with the following tabs: Documents, Directory Security, HTTP Headers, Custom Errors, IIS 3.0 Admin, Web Site, Operators, Performance, ISAPI Filters, and Home Directory. The 'Web Site' tab is selected. The dialog is divided into three main sections: 'Web Site Identification' with fields for Description, IP Address (set to '(All Unassigned)'), TCP Port (80), and SSL Port; 'Connections' with radio buttons for 'Unlimited' (selected) and 'Limited To: 1,000 connections', and a 'Connection Timeout: 900 seconds' field; and 'Enable Logging' which is checked, with a dropdown for 'Active log format' set to 'W3C Extended Log File Format'. At the bottom are buttons for OK, Cancel, Apply, and Help.

Master Web Site Properties dialog box

UNCLASSIFIED

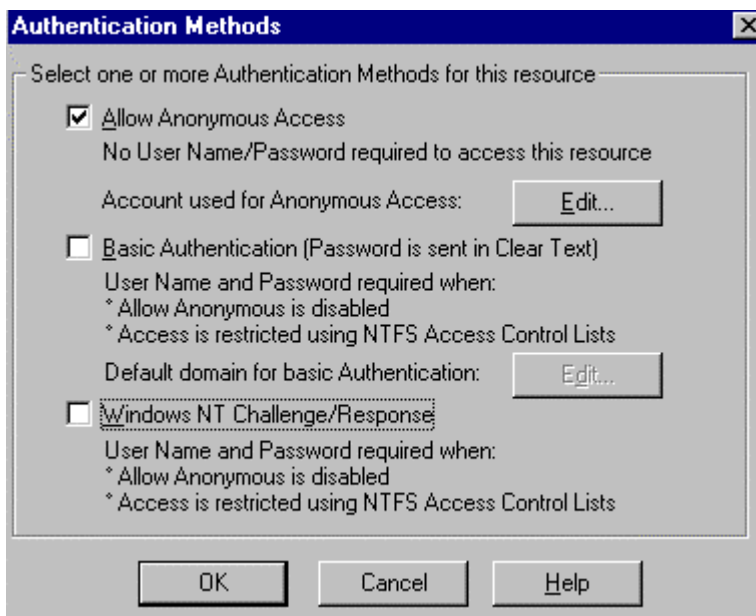
The following shows the dialog boxes for setting common security-related properties using the **Web Site** tab and **Operators** tab. Other tabs may have common settings as well, but will depend on how you setup your server. Note that these same settings can be applied individually to the WWW, FTP, and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

UNCLASSIFIED

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.

UNCLASSIFIED

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.

Default Web Site Properties

Documents | Directory Security | HTTP Headers | Custom Errors

Web Site | Operators | Performance | ISAPI Filters | Home Directory

Web Site Identification

Description: Default Web Site

IP Address: (All Unassigned) [Advanced...]

TCP Port: 80 | SSL Port: []

Connections

Unlimited

Limited To: 1,000 connections

Connection Timeout: 900 seconds

Enable Logging

Active log format: W3C Extended Log File Format [Properties...]

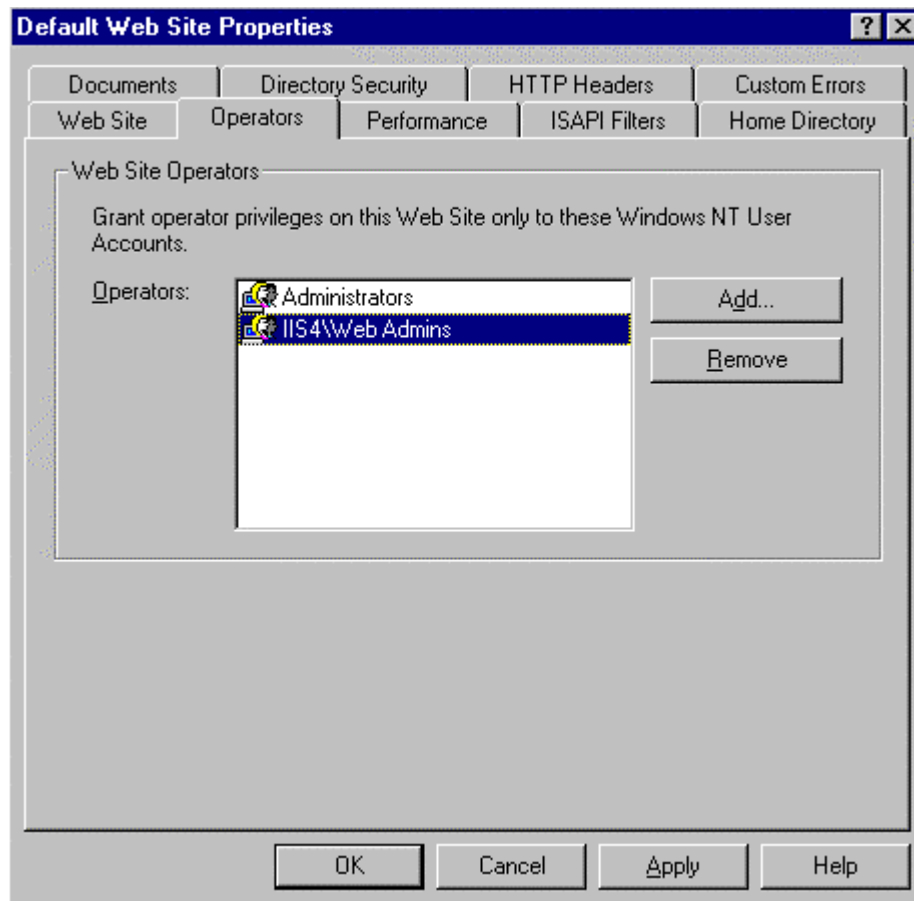
OK | Cancel | Apply | Help

Operators Property Dialog Box

Web Site Operators

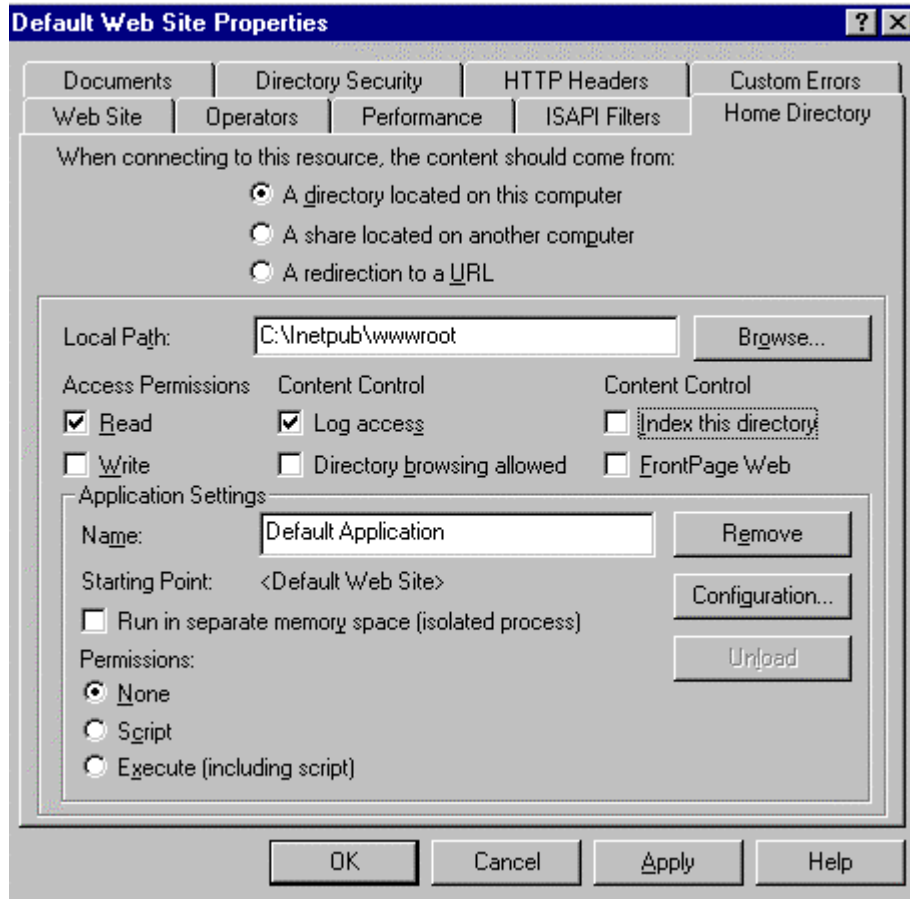
- Add users or a group of users (recommended) who are responsible for administering the data for your site by selecting the **Add** button on the **Web Site** property dialog box. Operators can work only with the properties that affect the web site for which they were created. They cannot access the 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

UNCLASSIFIED

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).

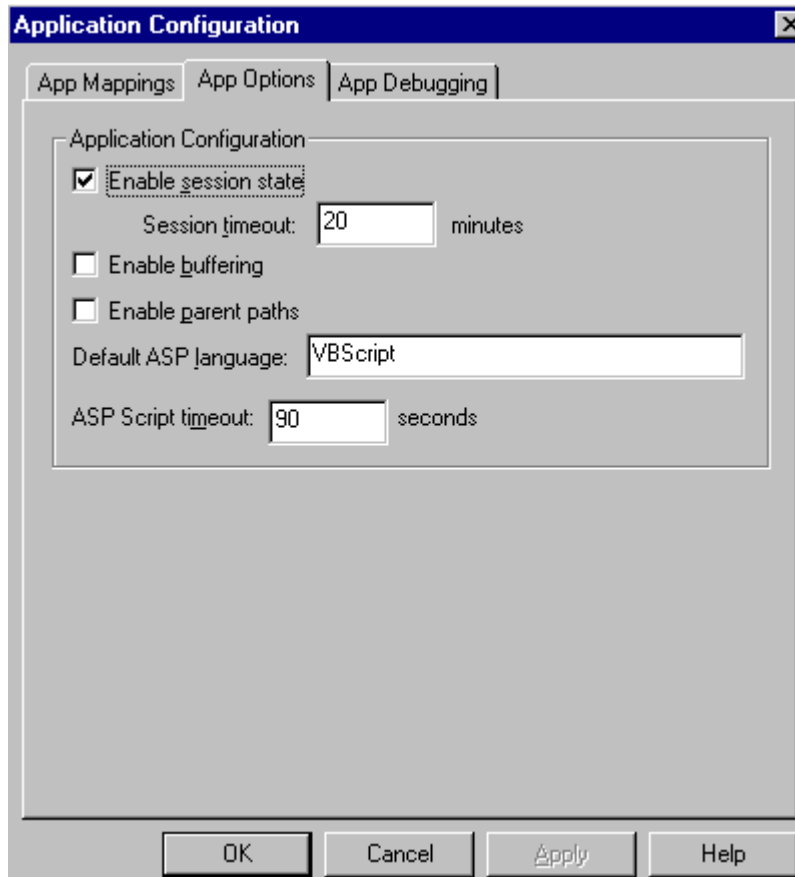
Applications can be configured in more detail by using the **Configuration** button. A separate dialog box is displayed with the following tab options: App Mappings; App Options; Process Options (if you select to run in separate memory space); and App Debugging. Discussions in this document focus on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

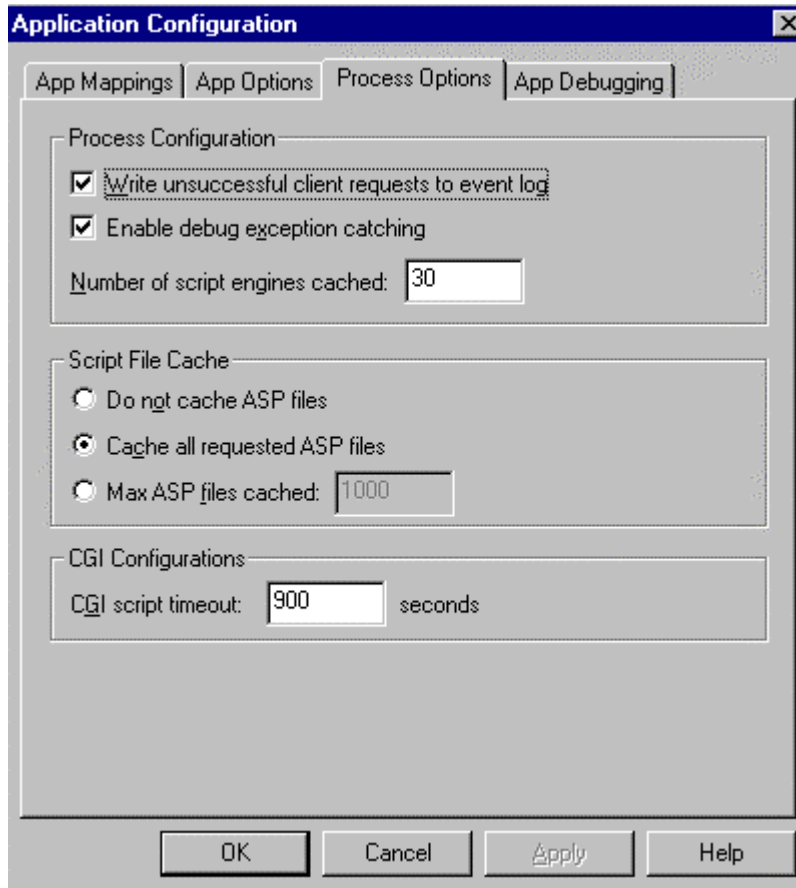
- ❑ Enter an **ASP Script timeout** value so that if a script does not complete execution within the allotted time, an entry will be made into the NT Server Event Log and execution of the script will stop. Setting timeout values will help prevent a denial of service attack.

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



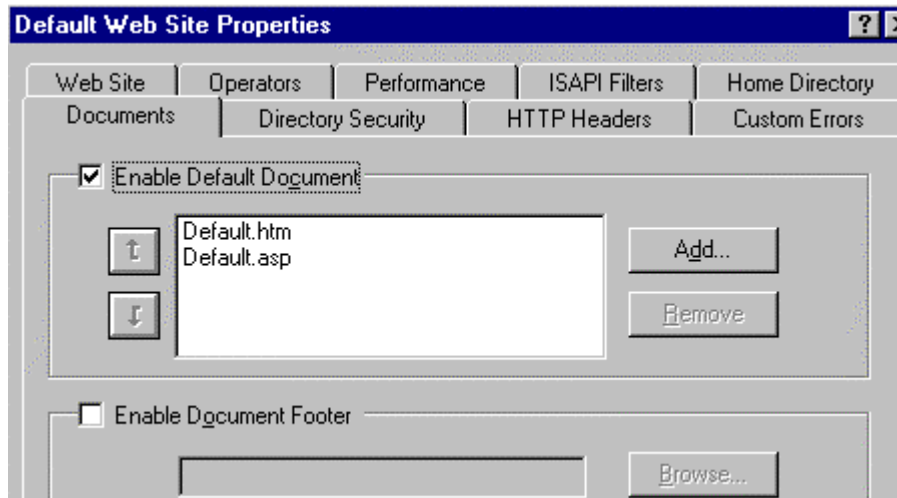
Process Options

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



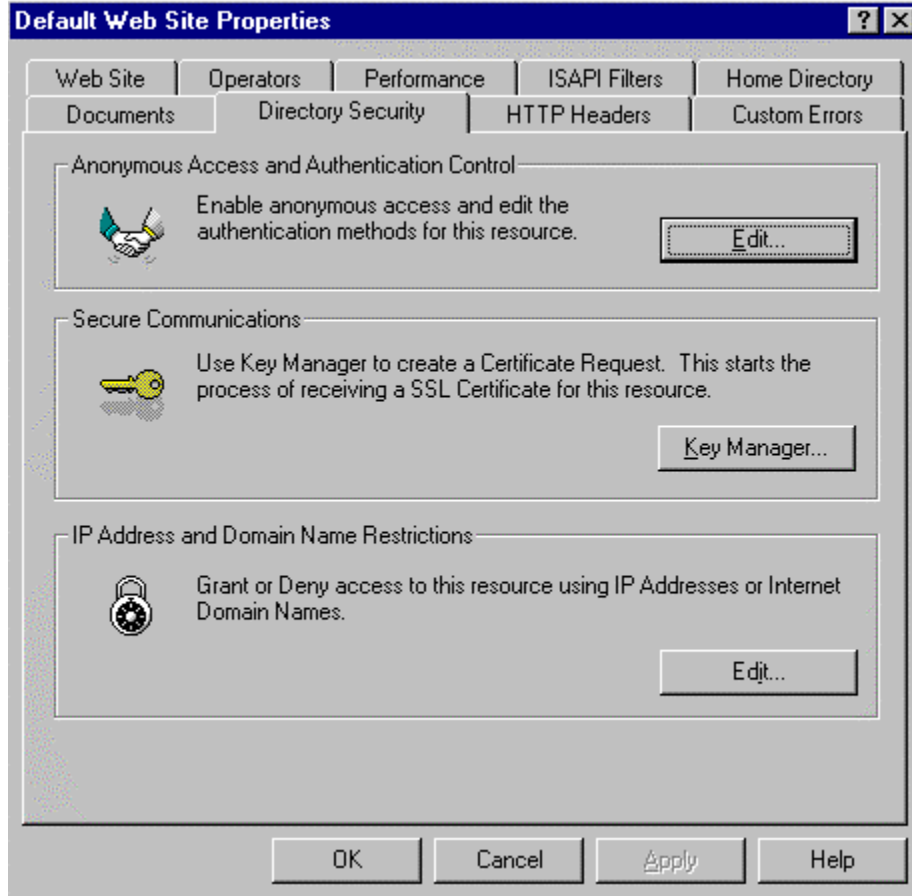
Documents Property Dialog Box

- 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

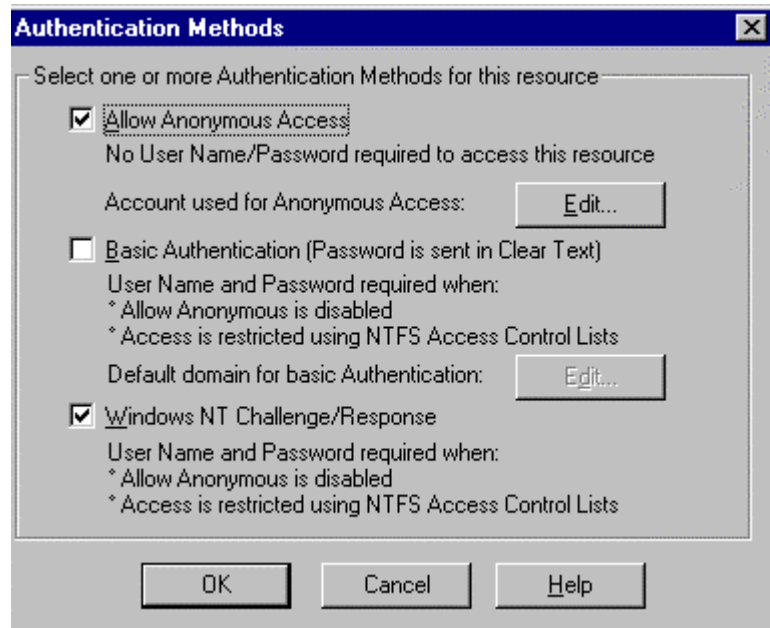
Security properties can be set at the web site, directory, virtual directory, or file level. Directory level will be used here to describe the settings, but apply to whichever level you are working with.



UNCLASSIFIED

Anonymous Access and Authentication Control

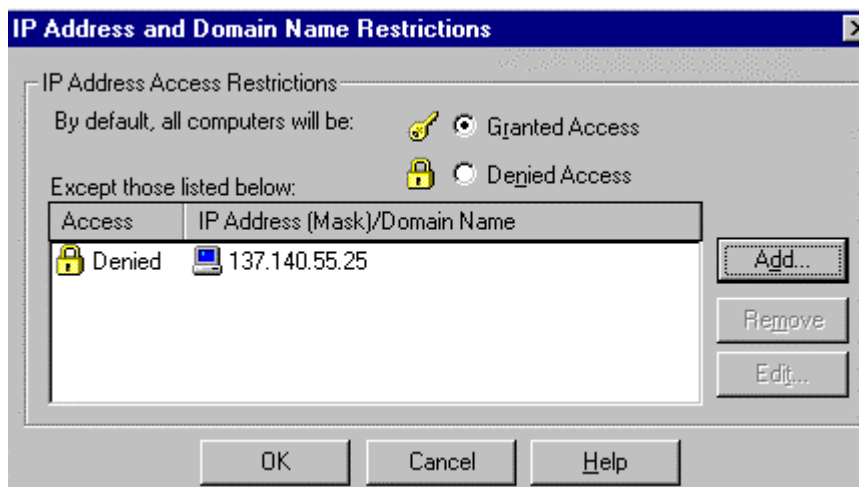
- ❑ Select the appropriate options for web sites, directories, and files as determined by the security policy of each site supported by the server.



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)

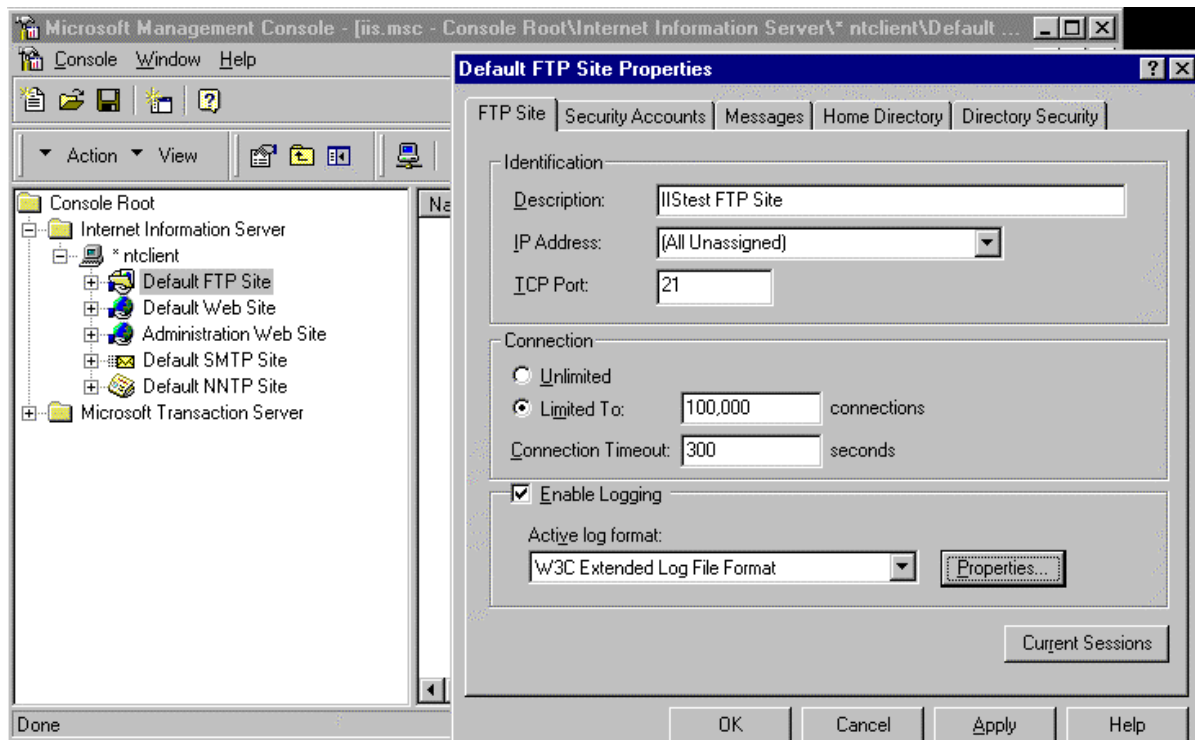
- ❑ Configure your FTP server so that uploading of files to the server **is prohibited**. If it is necessary to allow uploads, ensure users with this responsibility are explicitly specified on the directory permissions. This prevents intruders from stashing pirated software, cracking tools, and other 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.



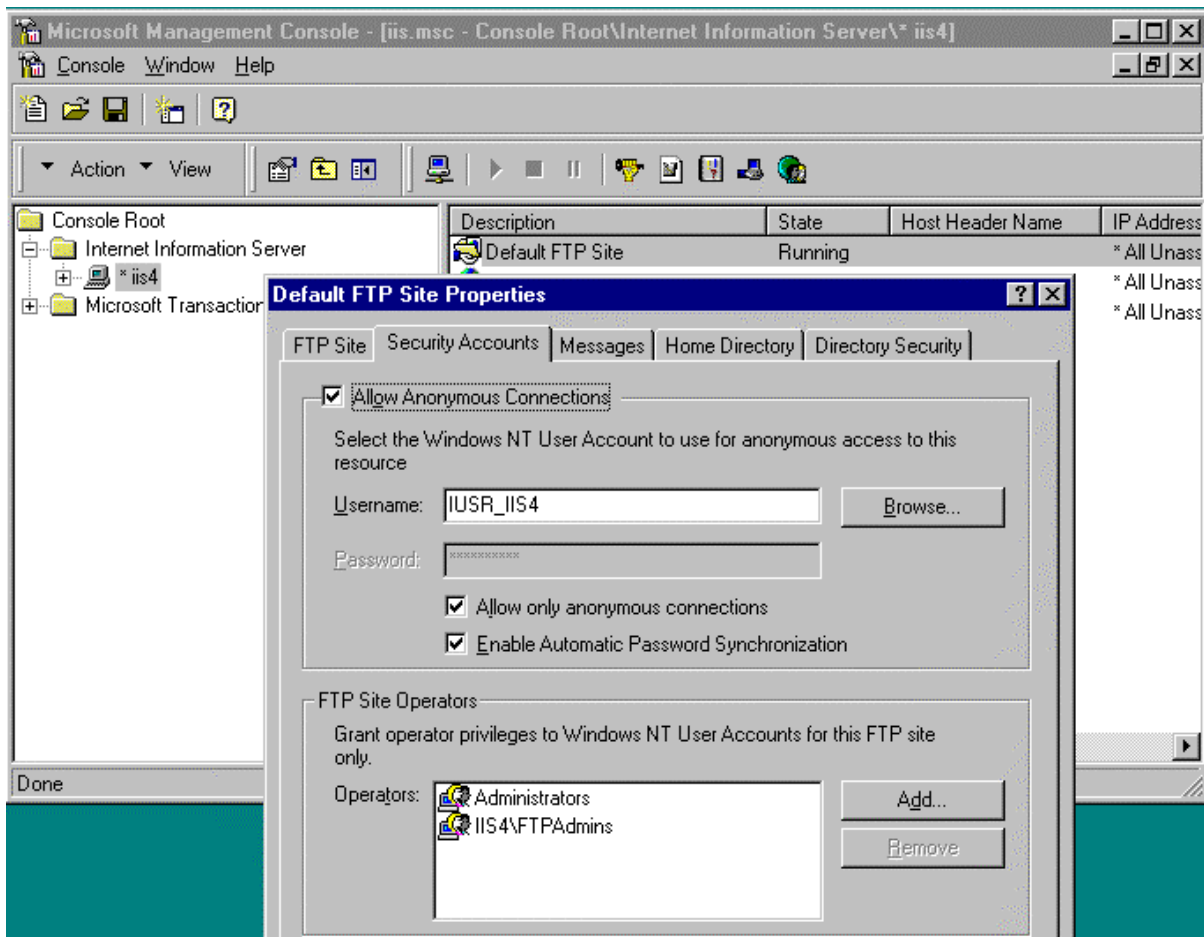
Security Accounts Property Dialog Box

- ❑ 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

UNCLASSIFIED

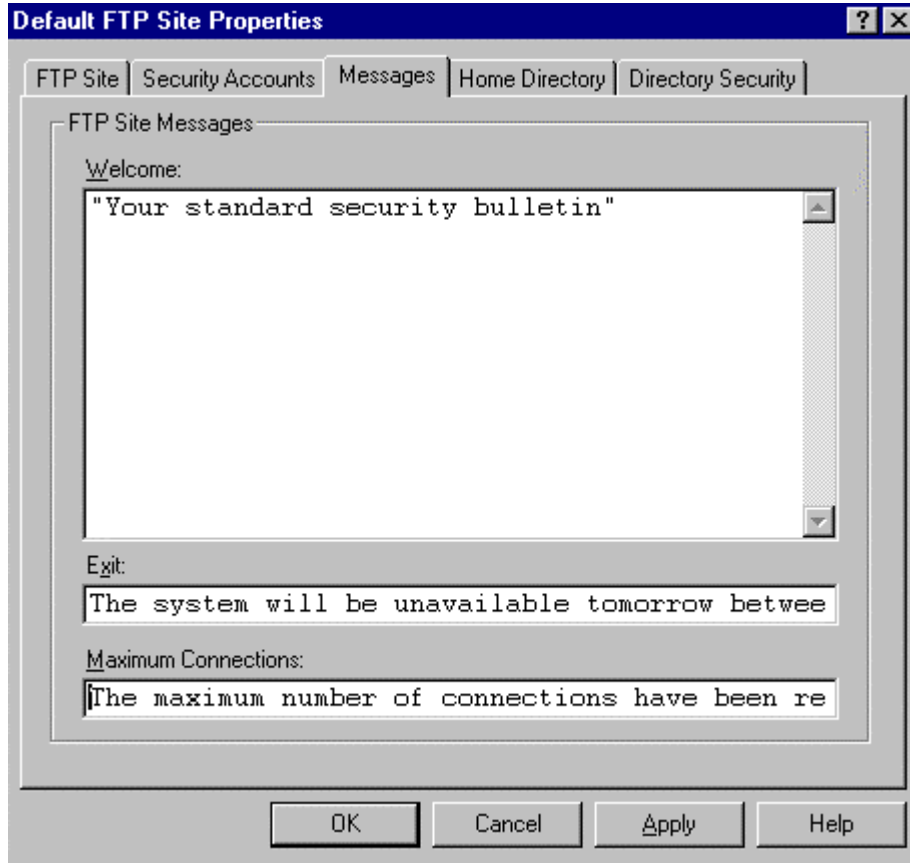
server then uses the `IUSR_computername` account as the logon account for permissions. NTLM (NT Challenge/Response) is not available for the FTP service.

- ❑ 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

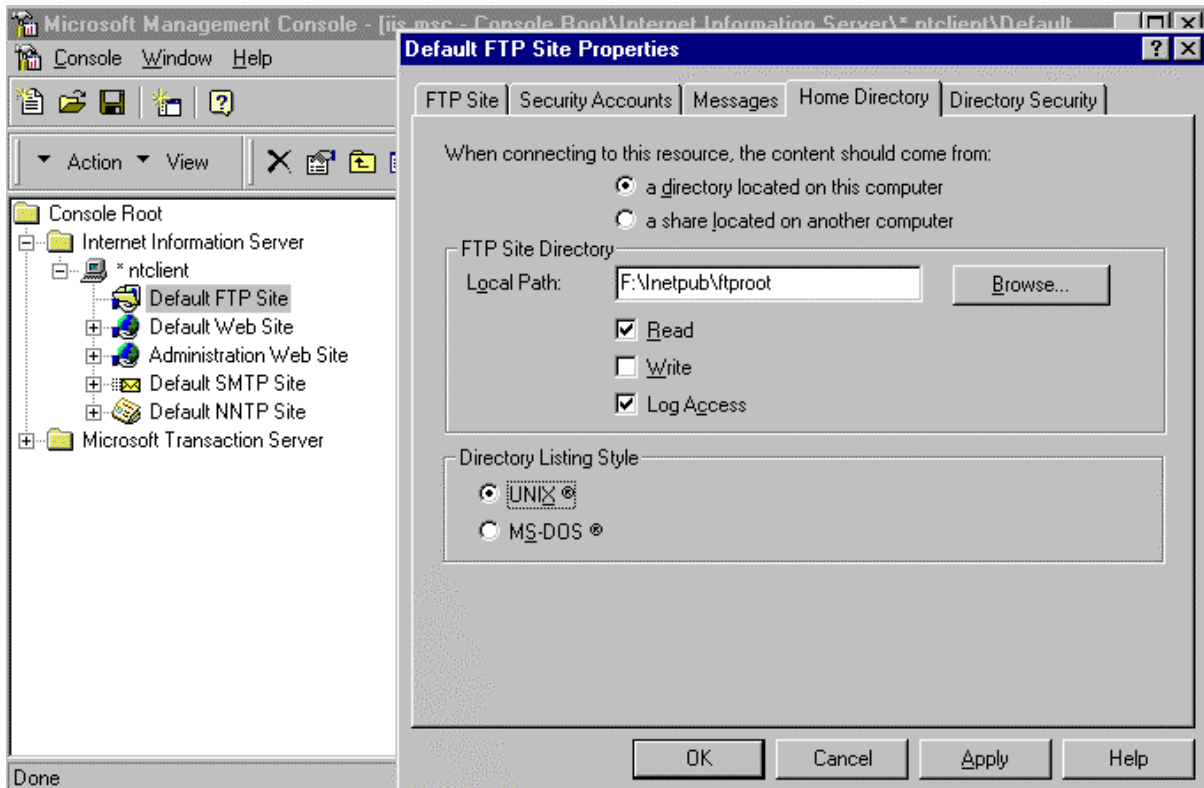
- Insert a Welcome message in the form of a Security Banner to be displayed to any user connecting to your FTP server. Exit messages can be used to display notices to users upon connection termination. A Maximum Connections message can be used to notify the user should the number of maximum connections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

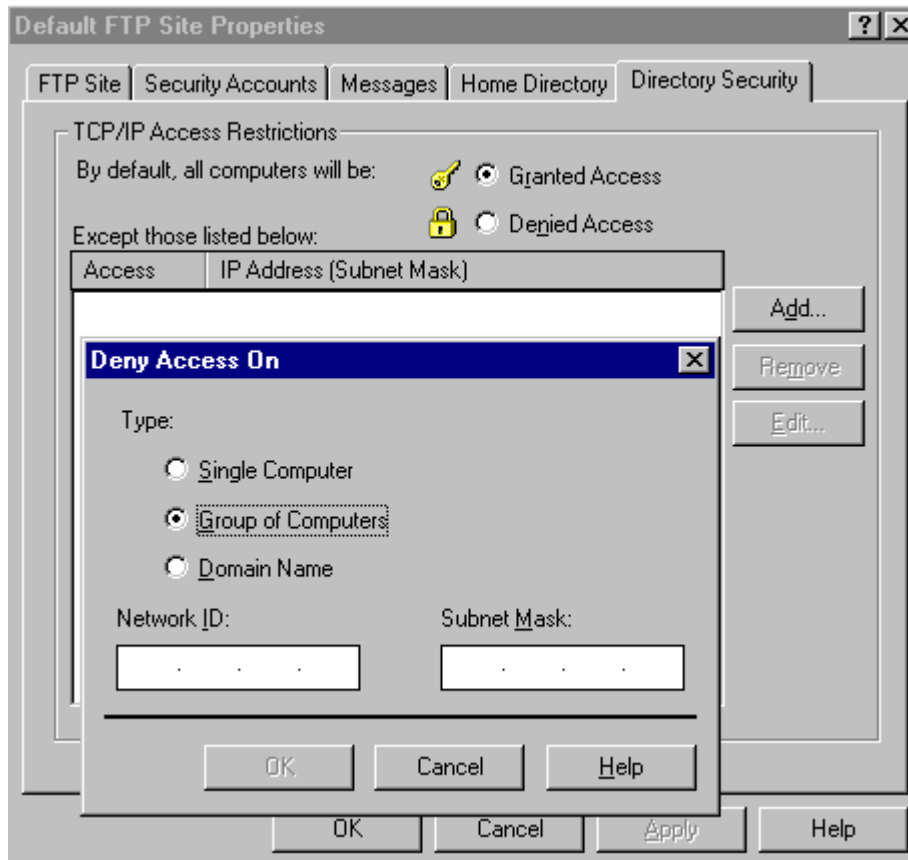
- ❑ Set Read access ONLY for the FTP Site Directory. If your site requires users to upload data, create two directories beneath the “ftproot” directory. One with Read ONLY access to store data made available to all users for download, and one with Write Only permission to be used as a “drop box” uploading 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 e-mail 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.

Default SMTP Site Properties

SMTP Site | Operators | Messages | Delivery | Directory Security

SMTP Site Identification

Description:

IP address:

Incoming Connections

TCP port:

Limited to connections

Connection time-out(seconds):

Outgoing Connections

TCP port:

Limited to connections

Connection time-out(seconds):

Limit connections per domain:

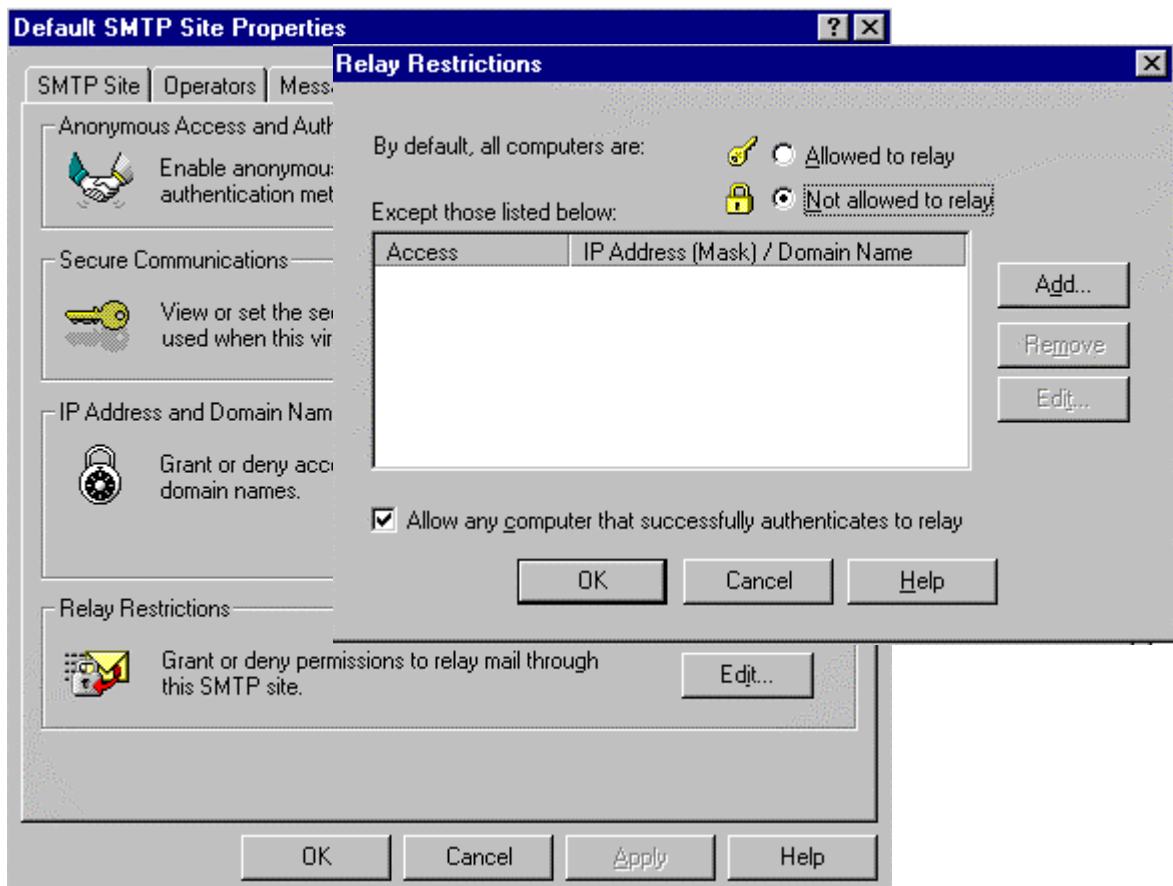
Enable Logging

Active log format:

UNCLASSIFIED

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**.



UNCLASSIFIED

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.

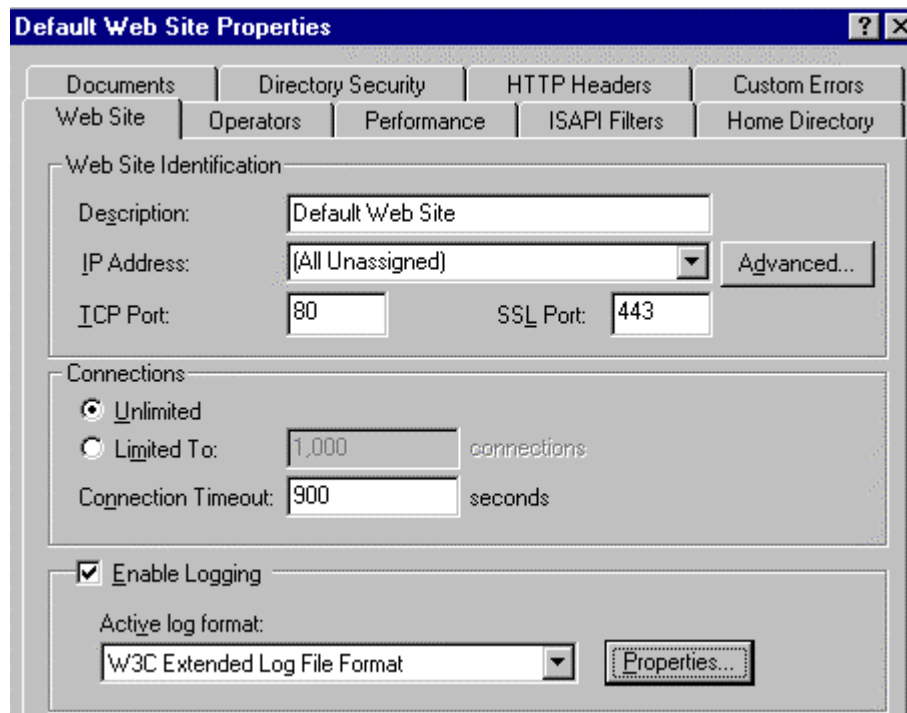


Auditing

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.

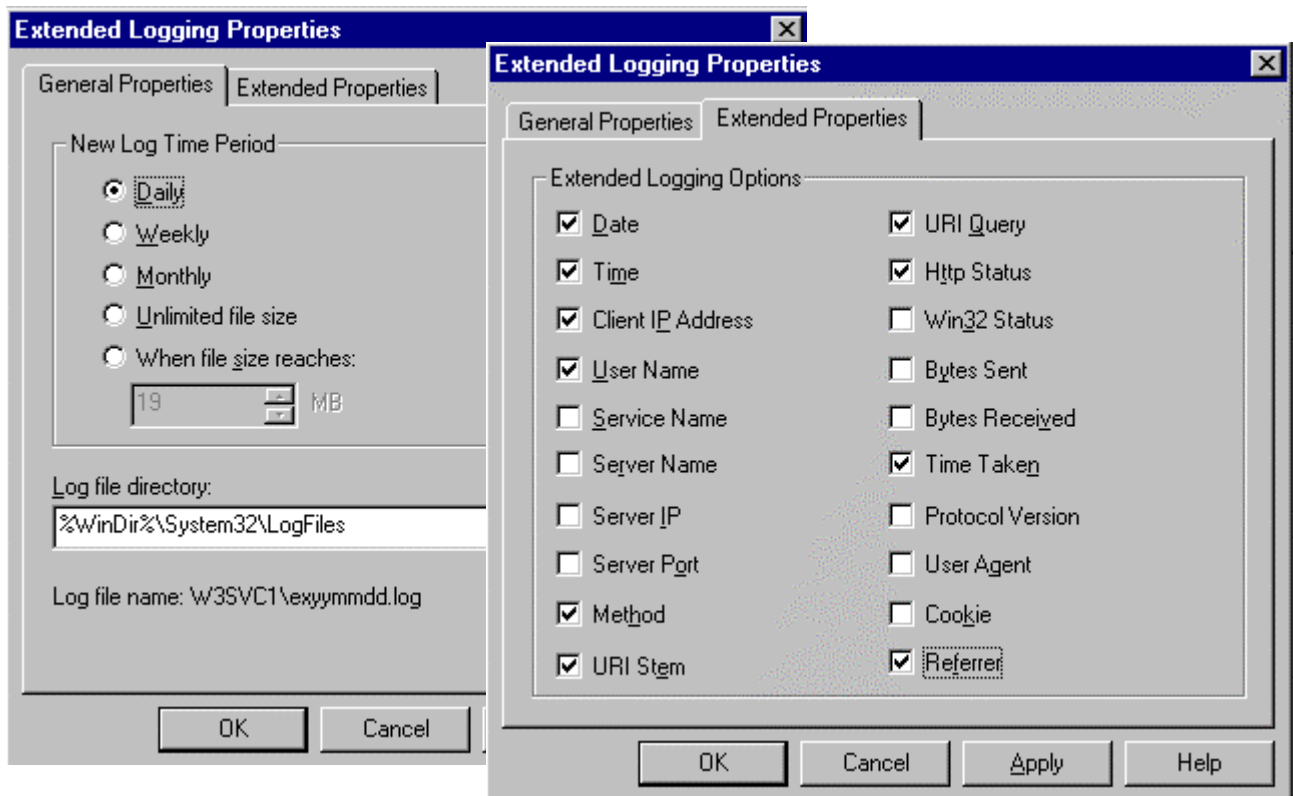
IIS logging is configured through the Services properties dialog boxes (WWW, FTP, and SMTP) by selecting the **properties** button.



- 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.

UNCLASSIFIED

- ❑ 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.



UNCLASSIFIED

Known Vulnerabilities

Some of the descriptions provided below were taken from various Microsoft Bulletins and are noted as such. Vulnerabilities eliminated in Service Packs (SP) are identified. IIS administrators should always check for hotfixes/patches and install them as necessary, along with the latest service pack available from Microsoft. Available patches can be found at the Microsoft Download Center at <http://www.microsoft.com/downloads/search.asp>.

Microsoft has issued a patch (**MS01-026 Superfluous Decoding Operation Could Allow Command Execution via IIS**) that serves as a roll-up patch that contains all previously issued IIS4.0 patches since Windows NT 4.0 Service Pack 5 and will be included in the next security roll-up for Windows NT 4.0. Three new vulnerabilities are eliminated with this patch:

A vulnerability that could enable a malicious user to run operating system commands on an affected server (see RFC 2396 for a description of how this vulnerability can be exploited).

A vulnerability that could allow a malicious user to enter a FTP command that causes IIS to fail. According to Microsoft, this is only a denial of service vulnerability and could not be used by an attacker to gain access to an IIS4.0 server.

A vulnerability that can permit a malicious user access to the guest account using the FTP service. If proper security procedures are followed, this vulnerability could not be exploited. The FTP server should only allow unauthenticated FTP and should not be a member of any domain. Also, the default Guest account should be disabled.

Although this is a roll-up patch, the following bulletins detail administrative actions that need to be taken to resolve issues discussed in them. In some cases, these actions cannot be performed programmatically by a hotfix, therefore, these issues still need to be addressed manually by the administrator:

- ❑ MS98-004 – Remote data service vulnerability
- ❑ MS99-013 – IIS sample files vulnerability
- ❑ MS99-025 – Same as MS98-004
- ❑ MS00-028 – Server-side image map component issue
- ❑ MS00-025 – Link view server-side component issue

For more information regarding this patch along with a list of patches superseded by this patch, go to <http://www.microsoft.com/technet/security/bulletin/ms01-026.asp>.

Unchecked Buffer in Index Server ISAPI Extension (MS01-033)

As a result of an unchecked buffer in a section of code within the idq.dll that handles input URLs, an attacker could conduct a buffer overrun attack and execute code on a web server that has idq.dll installed. As long as the script mapping for .idq or .ida files were present, and the attacker could setup a session with the web server, he could exploit this vulnerability. Microsoft strongly recommends installing the patch to eliminate the vulnerability. Removing the script mappings does not protect the web server entirely from a possible attack. This is because the script mappings are automatically reinstated when additional system components are added or removed. Microsoft has issued a patch to eliminate this vulnerability: (<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833>).

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. Some examples of this include .html, .asp, .shtml and .shhtml. 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.

- Remove unneeded script mappings.
- Install all available patches for extensions with known vulnerabilities.

Here are some references along with their uses:

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

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**.

Malformed Extension Data in URL (MS00-30)

A vulnerability exists in the way IIS processes URLs. The algorithm that processes URLs has flexibility built in to allow it to process any arbitrary sequence of file extensions or subresource identifiers. By providing an URL that contains specially-malformed file extension information, a malicious user could misuse this flexibility in order to arbitrarily increase the work factor associated with parsing the URL. This could consume much or all of the CPU availability on the server. The slowdown would only last until the URL had been processed, then service would return to normal. However, if such a request were sent over and over, a denial of service could result.

Microsoft has issued a patch to eliminate this vulnerability.
(<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20906>)

This patch limits the number of extensions that can be specified in a single URL, which can also be configured via a registry value.

UNCLASSIFIED

Administrators can limit the length of the URLs their servers will accept. This has the effect of limiting how complex the URLs can be. Set the following registry entry to the maximum length URL (including HTTP headers) you want to accept.

HIVE: HKEY_LOCAL_MACHINE\SYSTEM
KEY: CurrentControlSet\Services\W3SVC\Parameters
NAME: MaxClientRequestBuffer
VALUE TYPE: DWORD

For more information on this vulnerability, see Microsoft Knowledge Base Article Q260694.

Undelimited .HTR Request and File Fragment Reading via .HTR (MS00-031)

A denial of service vulnerability exists (undelimited .HTR Request) where a malicious user could provide a password change request that was missing an expected delimiter to cause the algorithm to conduct an outbounded search. This would prevent it from servicing additional .HTR requests, and could slow the overall response of the server.

The .HTR File Fragment Reading vulnerability could allow fragments of certain types of files to be read by providing a malformed request that would cause the .HTR processing to be applied to them.

Microsoft has issued a patch that eliminates these two vulnerabilities (<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20905>)

These vulnerabilities do not exist on servers where unneeded script mappings, specifically .HTR script mappings, have been removed. Although this is a good idea, keep in mind that script mappings are reinstated whenever system components are added or removed. Make sure the unwanted script mappings are removed if system components are added or removed.

For more information, please see Microsoft Knowledge Base Articles Q260838 and Q260069.

Malformed HTR Request (MS99-019)

A vulnerability exists in ISM.DLL, the filter that processes .HTR .STM and .IDC files. This vulnerability could allow denial of service attacks against an IIS server or, under certain conditions, allow arbitrary code to be run on the server.

The vulnerability involves an unchecked buffer in ISM.DLL. This poses two threats to safe operation of IIS. A malformed request for an .HTR, .STM, or .IDC file could overflow the buffer, causing IIS to crash – Denial of Service. The server would not need to be rebooted, but IIS would need to be restarted. The second threat would be more difficult to exploit. A carefully constructed file request could cause arbitrary code to execute on the server via a classic buffer overrun technique. Neither scenario could occur accidentally. Note: This vulnerability does not involve the functionality of the password administration features of .HTR files.

Microsoft has released a patch to eliminate this vulnerability. Install the patch or perform the following steps to disable the script mapping for .HTR files. From the ISM, Double-click "**Internet Information Server**"; Right-click on the computer name and select **properties**; On the **Master Properties** dialog box, select **WWW Service** then click **Edit**; on the **Home Directory** tab, click **Configuration**; Highlight the line in the extension mappings that contains “.HTR” and click **Remove**. Do the same for “.STM” and “.IDC”.

Malformed FTP List Request Vulnerability (MS99-003)

The FTP service in IIS has an unchecked buffer in a component that processes “list” commands. This results in a vulnerability that poses two threats to safe operation. The first is a denial

UNCLASSIFIED

of service threat; a malformed "list" request could overflow the buffer causing the server to crash. The second is more esoteric and would be far more difficult to exploit. A carefully constructed "list" request could cause arbitrary code to execute on the server via a classic buffer overrun technique. Neither variant could be exploited accidentally. The "list" command is only available to users after they have authenticated to the server. If the Guest account is not disabled, a malicious user could mount an attack on the server anonymously. Microsoft has posted the hotfixes to address this problem. This vulnerability is eliminated in SP5.

Alternate Data Streams

A problem was discovered with data streams that affects all versions of IIS through SP3. Web clients can read the contents of any NTFS file in an IIS directory to which they have been granted Read access, including ASP scripts. The problem is a result of the way IIS parses filenames. The main data stream, which stores the primary content, has an attribute called \$DATA. Accessing this NTFS stream via IIS from a browser may display the contents of a file. Normally, this type of file would be acted upon by an application. The application (e.g., asp.dll or perl.exe) knows to act upon the file because of mapping of the file extension of the file requested in the URL.

For example, .asp files are mapped to be executed by the Active Server Pages scripting agent (asp.dll) on the server, rather than simply returning the contents of a file to the browser, as is done with standard .htm or .html files. .pl files are mapped to and executed by the Perl interpreter (perl.exe). This process is referred to as script mapping. Normally, the "raw" contents of these script-mapped files are not returned to the user. However, by requesting the file using the complete data stream name, a Web browser could obtain the "raw" contents of the script file. In some cases, the file might contain sensitive information such as embedded passwords or other sensitive "business logic" information. This is especially true for scripts that support Web-enabled databases.

The problem does not give the user who was able to access the script file the ability to alter the script on the server, or force the server to run any arbitrary code. Only the plain text or "raw" contents of the script file is exposed.

According to Microsoft, for the problem to occur:

- The user must know the name of the file
- The ACLs on the file must allow the user Read access (which is not recommended)
- The file must reside on an NTFS partition

The first requirement is relatively easy to obtain, especially for files that would normally be accessed through the browser, like Active Server Pages. For other files (non-HTML), this may be slightly more difficult, yet still possible to accomplish. The determining factors are directory browsing settings, file system sharing, and file system access control settings. The third requirement is actually a desired condition; if the partition is FAT opposed to NTFS, the files would be less secure. Of the three, only the second requirement is a condition where improper configuration could contribute to a vulnerability. Ensure directories have appropriate access controls set. Place executables in directories with only IIS Script or Execute permission set for anonymous access.

This vulnerability is eliminated in SP4. If you do not install SP4 or later, install the hotfix provided by Microsoft (iis3-datafix and iis4-datafix), after Service Pack 3 is applied. Those using IIS versions 3.0 and 4.0 are strongly recommended to apply the hotfix. Those running previous versions of IIS should upgrade to a more recent version and apply the latest service pack.

Variation of the "dot" vulnerability

Under certain conditions, Internet Information Server (IIS) might reveal Active Server Pages (ASP) code versus executing the script. The problem occurs when the URL path contains a period in

UNCLASSIFIED

part of the extended URL. The extended path is that portion after the DSN machine name or IP address and before the filename. For example, a URL such as <http://www.somesite.com/new.products/hello.asp> would display the code within hello.asp instead of executing it. The "new.products" portion of this URL causes the problem.

This problem is also related to the way IIS parses filenames. The problem occurs consistently on FAT partitions and happens on only NTFS partitions where the Everyone group has read access or IUSR_<computername> (anonymous account) has read access. On NTFS partitions that do not allow read access to Everyone or IUSR_<computername>, the system prompts the user for an ID and password. This problem is easily prevented by placing all .asp files in a "scripts" directory and disallowing read access to that directory. This recommendation is consistent with exercising good practices on IIS; any file with executable content should be placed in a directory with Script or Execute privilege and not allow the Read permission.

Denial of service vulnerability with the IIS FTP Service

The IIS FTP service supports passive mode (PASV) FTP connection. Passive mode (PASV) provides a firewall-friendly mechanism for FTP connections. FTP uses a secondary TCP connection for actual transmission of files. This data connection is set up from the FTP server to the FTP client. However, this does not work well when the client is behind a packet filter-based firewall. Packet filter-based firewalls, in general, do not permit incoming calls to random port numbers. If the client uses the PASV command, the data channel will be an outgoing call through the firewall. Such calls are more easily handled. A vulnerability in the PASV FTP connection mechanism can be a source of performance degradation and lead to denial of service attacks on the FTP and WWW services.

In such cases, the System Log will show errors that may look like the following:

FTP Server could not create a client worker thread for user at host <some IPAddress>. The connection to this user is terminated. The data is the error.

In addition, client systems may see error messages, such as:

Connection closed by remote host -or- The FTP session was terminated

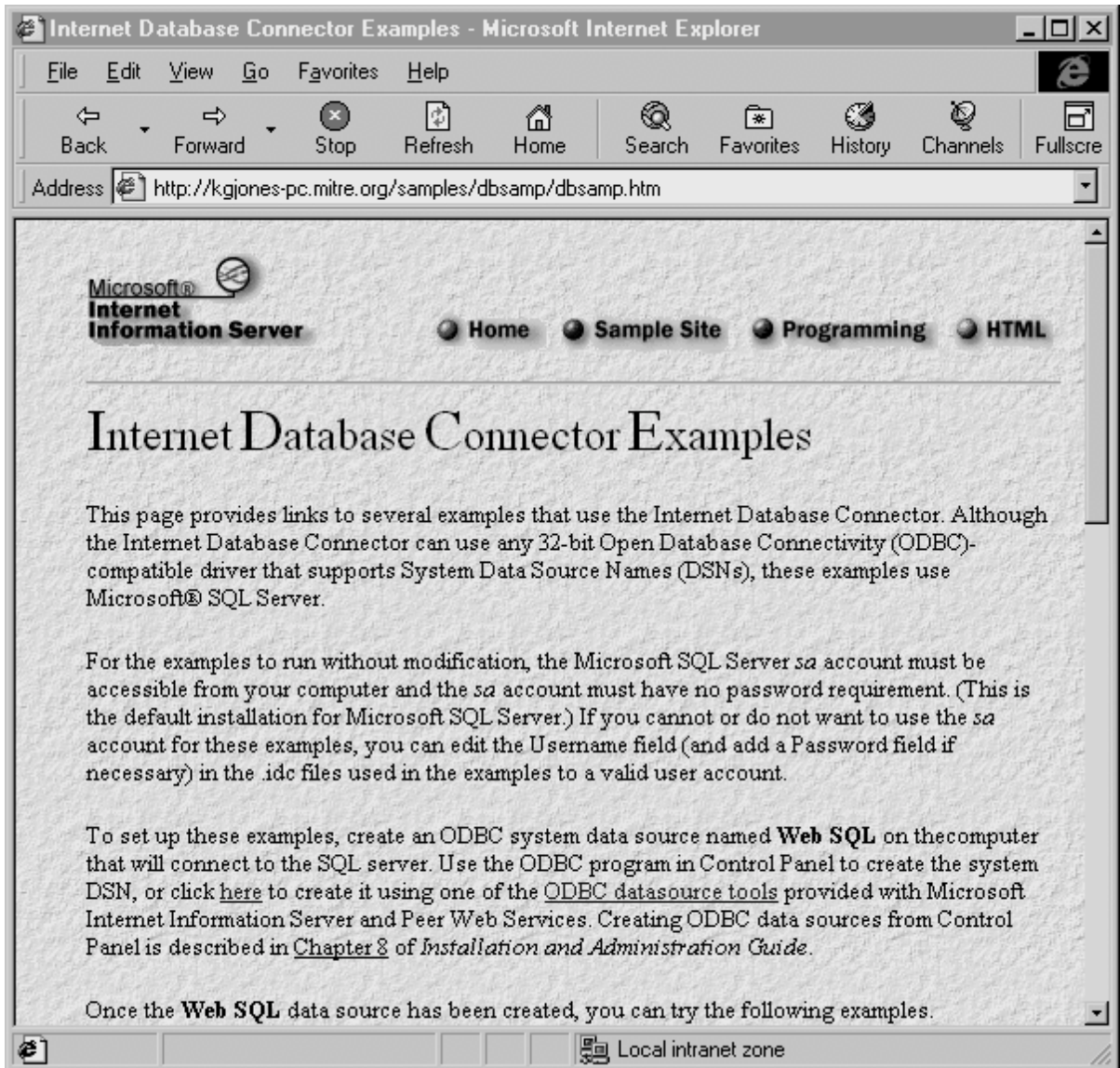
The problem may occur because it is possible to commit all available system threads for servicing clients, which leads to the above stated errors until threads are released. The vulnerability only causes a denial of service. It cannot crash the FTP service or any other services running on the targeted machine.

This vulnerability affects IIS versions 2.0, 3.0, and 4.0. This vulnerability is eliminated in SP4. If SP4 is not installed, install the hotfix provided by Microsoft for this vulnerability (ftpfix4i.exe) after SP3 is applied.

Unauthorized File Manipulation Through Sample Web Sites and Scripts

There are several directories and utilities in the default installation of IIS that are designed to highlight the capabilities of the server; however, in the process expose vulnerabilities in the system.

When executed, the default.asp script, which is part of the default installation, highlights IIS's database capabilities through a link titled **Database**. This Database link leads to a series of files in the InetPub\samples\dbsamp directory that demonstrate the database capabilities starting with InetPub\samples\dbsamp\dbsamp.htm, shown in the following image:



UNCLASSIFIED

From this point, it is possible to navigate to more capable files that can actually modify the file system of the server. These files are `getdrvrs.exe`, `dsnform.exe`, and `newdsn.exe` in the `scripts/tools` directory; `getdrvrs.exe` can be reached through the link labeled ODBC datasource. This file allows the user to select the type of driver for the Open Database Connectivity (ODBC) connection. This is normally the first step in creating an ODBC datasource.

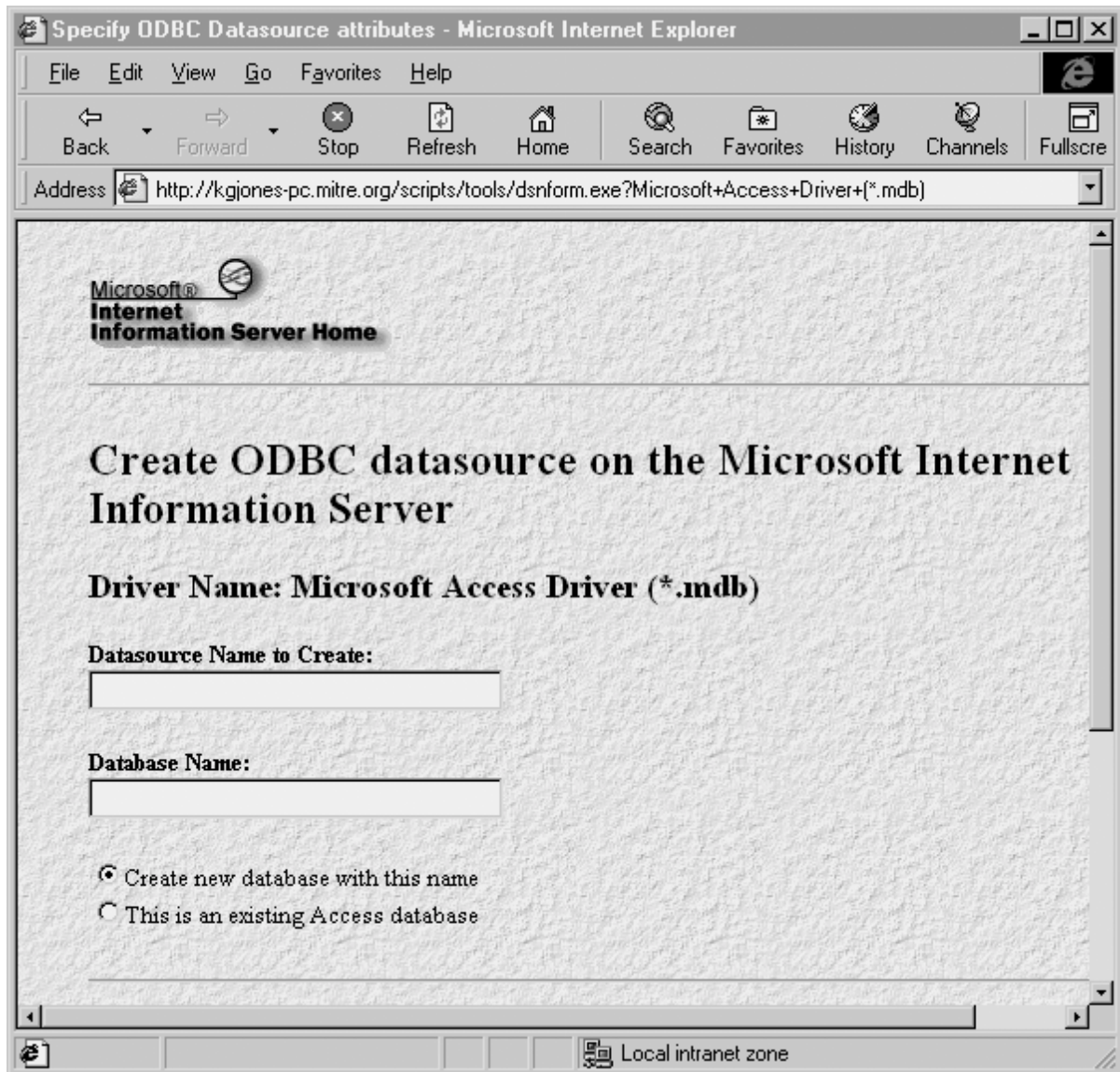
ODBC is a database-independent technology for accessing data. An ODBC datasource is the structure which links the physical database and database engine to the Data Source Name (DSN). A DSN is a local reference to the datasource that allows a script to pass SQL commands to the database engine. The datasource is the set of parameters established to access a specific database. These parameters include the name/path to the database file and the type of ODBC driver; there is a unique ODBC driver for each database application/engine. The ODBC driver converts the SQL query statements in the script to the proprietary commands of the database. The datasource also has a scope, whether it is global or restrictive (there are three type of datasources). The datasource is not a separate file but appears to be a data entry in another file.

The next step in this process will call a file entitled `dsnform.exe` to the browser/client that the user can fill out to create a new ODBC datasource on the Web server. When the form in `dsnform.exe` is completed and submitted, `newdsn.exe` is called and this program actually creates the datasource.

Datasources are normally created from the Control Panel applet titled ODBC. Access to specific Control Panel applets is controlled and, therefore, users without sufficient authority cannot execute these applets.

One of the samples in IIS that can take advantage of these database tools is a form to create a database table to support a guestbook. Individual entries for the guestbook can also be generated through the sample scripts. Without much difficulty, an unauthorized user could create a database, create the necessary table in that database, and then populate the table with guestbook entries. Most systems have directories where all users are allowed to create and maintain files, such as temporary directories. These directories could be used to host the database file.

The principle concern is that these sample directories and the enclosed scripts are accessible to the group Everyone. The impact, if the `default.asp` script is left on the server and not replaced or deleted, any browser/client that can access the Web server can execute these scripts and write information to the file system of the server.



Screen Capture of dsnform.exe

It is recommended the directories that have samples and scripts to execute the samples be deleted.

If it is desired to maintain these directories for instructional use, re-locate them, require NTLM authentication when accessing them through the WWW service, and change the NTFS permissions to allow access only to system and Web administrators.

Potential Problem in Remote Data Services (RDS) Version 1.5 (MS99-025)

According to the notice issued by Microsoft, "a Web client connecting to an IIS server can use the RDS DataFactory object (installed with NT Option Pack) to direct that server to access data using an installed OLE DB provider. This includes executing SQL calls to ODBC-compliant databases using the ODBC drivers installed on the server."

Description of RDS Datafactory

Remote Data Service (RDS) is a component of Microsoft Data Access Components (MDAC), which is installed by default when IIS4.0 is installed via the Windows NT Option Pack. The goal of the RDS component is to enable controlled Internet access to remote data resources through the Internet Information Server. For example, this provides the ability for Web clients to issue client-based SQL queries to OLE DB data sources hosted on the Web server.

The DataFactory object allows you to connect to a specified data source (such as a SQL Server database), using a specified UserID and password, and execute a query against that server and then return the results back to the client. The data source, UserID, password, and SQL statement are passed as parameters to the method exposed on the DataFactory object. If the Registry keys that will be specified shortly are removed, the user will be unable to create the object, therefore removing any possibility of abuse.

A Web client connecting to an IIS server can use the RDS Datafactory object to direct that server to access data using an installed OLE DB provider. This includes executing SQL calls to ODBC-compliant databases using the ODBC drivers installed on the server.

For example, a Web client could issue a SQL command along with the name or IP address of a remote SQL server, a SQL account and password, database name, and a SQL query string. If the request is valid (remote server is reachable by the IIS server, user account and password are correct, and database name is valid), the query results will be sent via HTTP back to the client. While it is true that this requires significant inside information, the potential accessibility of this information should not be underestimated. Many organizations still don't practice good computing practices and have unprotected databases and/or blank or easy to guess passwords on their database administrator accounts. The RDS Datafactory object, along with other installed ODBC drivers, opens other possibilities, including possible access to non-published files on the IIS server.

The problem is compounded by using other software, such as Microsoft DataShape Provider and Microsoft JET OLE DB provider (included with MDAC 2.0 in Visual Studio 98) because they allow shell commands to be executed.

It is recommended that the all RDS functionality be disabled. To do so, remove the following Registry keys:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\
Parameters\ADCLaunch\AdvancedDataFactory

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\
Parameters\ADCLaunch\VbBusObj.VbBusObjCls

UNCLASSIFIED

These keys can be removed using the Registry Editor (REGEDT32.EXE), or other tools for manipulating the registry. Additionally, the NT Resource Kit includes the utility REGDEL.EXE, which can be used to remove the above mentioned keys. REGDEL.EXE is a command line utility available as part of the Windows NT Resource Kit utilities that can be used to delete registry entries from the command line.

Copy the following text into a .BAT file (e.g. c:\dfremove.bat) and run the batch file on machines on which you want to remove the RDS components.

```
@ECHO OFF
REM Batch file to remove RDS components
REM Make sure that REGDEL.EXE from the Resource Kit is in your PATH
set rkey=HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC
REGDEL %rkey%\Parameters\ADCLaunch\RDS\Server.DataFactory
REGDEL %rkey%\Parameters\ADCLaunch\AdvancedDataFactory
REGDEL %rkey%\Parameters\ADCLaunch\VbBusObj.VbBusObjCls
Echo RDS Keys Removed
```

The following recommendations, taken from Microsoft's Knowledge Base article Q184375, should be followed by all Web developers who are publishing data in Active Server Pages:

- Remove all nonessential ODBC drivers, especially the Microsoft Text Driver
- Tighten NTFS permissions (ACLs) to restrict access to only trusted users
- If using SQL Server, enforce strong security measures, such as:
 - Run SQL Server as a low-privileged user account
 - Do not allow extended stored procedures

Malformed HTTP Request Header (MS99-029)

Microsoft has released a patch that eliminates a vulnerability in web server products that use IIS4.0 as their web engine. The vulnerability could be used to mount denial of service attacks against the web server. If multiple HTTP requests containing specially-malformed headers are sent to an affected server, IIS may consume all memory on the server. If this happens, IIS would be unable to service requests until either the clients that issued the requests were closed, or the IIS service were stopped and restarted. Once either of these actions have occurred, normal service would be restored. Please see Microsoft Knowledge Base (KB) article Q238349 for more information on this vulnerability. The patch is available at <ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/HDBRK-fix>. This vulnerability is eliminated in Windows NT4.0 Service Pack 6.

Domain Resolution and FTP Download Vulnerabilities (MS99-039)

IIS4.0 provides the ability to restrict access to a web site based on the user's domain. However, if IIS cannot resolve a user's IP address to a domain, it will grant the user's first request for a session. It will correctly deny them thereafter.

A user who accesses an FTP site via a browser will be able to download files even if they are marked No Access. This vulnerability is due to a regression error that was introduced in hotfixes released after Windows NT 4.0 Service Pack 5; it does not exist in SP5 or in previous versions.

Neither vulnerability provides a means to usurp control of the server. A patch is available that eliminates both vulnerabilities.

Multithread SSL ISAPI Filter Vulnerability (MS99-53)

The SSL ISAPI filter provided as part of IIS supports concurrent use. When used in this mode, a synchronization problem could induce a race condition and cause a single buffer of plaintext to be leaked. The conditions under which this could happen are very rare, and could only occur when a single user's session was multi-threaded and traffic volumes were extremely high.

The scope of this vulnerability is very limited. The leaked plaintext would always be sent to its owner, never another user. Also, because the leaked data would fail its integrity check, the effect of the leak would be to cause the SSL session to immediately collapse. The condition could not be induced by a hostile user, and would offer at best a target of opportunity. Finally, it is worth noting that this vulnerability only affects the SSL ISAPI filter, not the secure communications capability provided by Windows NT via Schannel. A patch is available to eliminate this vulnerability.

Virtual Directory Naming Vulnerability (MS99-058)

If a file on one of the affected web server products resides in a virtual directory whose name contains a legal file extension, the normal server-side processing of the file can be bypassed. The vulnerability would manifest itself in different ways, depending on the specific file type requested, the specific file extension in the virtual directory name, and the permissions that the requester has in the directory. In most cases, an error would result and the requested file would not be served. In the worse case, the source code of the .ASP or other files could be sent to the browser.

This vulnerability would be most likely to occur due to administrator error, or if a product generated an affected virtual directory name by default. (Front Page Server Extensions is one such product). Recommended security practices militate against including sensitive information in .ASP and other files that require server-side processing, and if this recommendation is observed, there would be no sensitive information divulged even if this vulnerability occurred. In any event, an affected virtual directory could be identified during routine testing of the server. For more information on this vulnerability, please see Microsoft Knowledge Base article Q238606 and Q186803. Microsoft has released a patch to eliminate this vulnerability which is available at the Microsoft Download Center.

Escape Character Parsing Vulnerability (MS99-061)

RFC 1738 specifies that web servers must allow hexadecimal digits to be input in URLs by preceding them with the "escape" character, a percent sign. IIS complies with this specification, but also accepts characters after the percent sign that are not hexadecimal digits. Some of these translate to printable ASCII characters, and this could provide an alternate means of specifying files in URLs.

The vulnerability does not affect IIS; even specifying a filename via this alternate method does not bypass IIS' access controls. However, third-party software that runs atop IIS but does not perform canonicalization is affected by it. For more information on this vulnerability, see Microsoft Knowledge Base article Q246401. Microsoft has released a patch for this vulnerability which can be downloaded from the Microsoft Download Center.

UNCLASSIFIED

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.

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.
- 26 July 2001, Version 1.31 – expanded the [warnings](#) page.