Report Number: C4-057R-00

# Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0 â

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

Author:
William E. Walker IV

Updated: March 4, 2002
Version 1.3.1

National Security Agency
ATTN: C43 (Walker)
9800 Savage Rd.
Ft. Meade, MD 20755-6704

W2KGuides@nsa.gov

## Change Control

| Version | Date | Details |
|---|---|---|
| 1.1.4 | 19 June 2001 | Added this change control section to track version modifications. Updated MS 01-016 advisory information to add web link to patch. Added MS advisory MS 01-026, 01-033 to appendix C. Updated and added reference in the unattended installation section. |
| 1.1.5 | 17 July 2001 | Changed “Windows 2000 Security Guide” to “set of NSA Windows 2000 Security Guides”. This should curb further confusion by readers looking for a specific “Windows 2000 Security Guide” when it is the set of guides that is being referred to. Removed individual email address of author, added group email address to ensure questions are addressed efficiently. |
| 1.1.6 | 7 August 2001 | Corrected typo of issync.exe to iissync.exe on page 78. Modified table on pg 11 to remove execute perms from anonymous and authenticated user groups to further limit restrictions. Clarified wording on page 11 to reflect that the IIS binary files cannot be moved to a separate location even with an unattended install. Added MS01-037 bulletin to appendix C. |
| 1.2 | 20 August 2001 | Added warning on page 5 about IIS 5 installed on Windows 2000 Professional and not installing patches, especially security patches. Added bulletin 01-043, 01-044. |
| 1.2.1 | 2 October 2001 | Removed duplicate entry in table on page 8. |
| 1.3 | 17 December 2001 | Modified typo “Metadata File” to “Metadatafile” for the registry key entry required to move the Metabase on page 16. Added 5 executable files to page 79 for ACL’d and audited files. Added IUSR group info on page 10 and 79. Removed Appendix B (Known Vulnerabilities) and added a paragraph about patching the OS and IIS to page 11 along with a www link to the MS site for these updates. Added Certificate weakness information on page 75 and inserted as new Appendix B. Modified page 2 to reflect the revised appendices. |
| 1.3.1 | 4 March 2002 | Modified typo “Figure 3” to “Figure 57” on page 94. Page 91, Clarify use of name constraints for certificates. Page 99, put grid mark in table for ease or reading and added constraint support information in #4 footnote. |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## 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.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- This document contains possible recommended settings for the system Registry. Windows 2000 System Internet Information Services 5.0 can be severely impaired or disabled with incorrect changes or accidental deletions when using a Registry editor (`Regedt32.exe` or `Regedit.exe`) to change the system configuration. There is no "undo" command for deletions within the Registry. Registry editor prompts user to confirm the deletions if "Confirm on Delete" is selected from the options menu. When user deletes a key, the message does not include the name of the key being deleted. Check selection carefully before proceeding.
- 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.
- This document is current as of March 4, 2002. This is a living document and revisions will be constant, the change control area will state modifications. See Microsoft's web page for the latest changes or modifications to the Windows 2000 operating system and applications.

This Page Intentionally Left Blank

## Acknowledgements

Some parts of this document were drawn from Microsoft copyright materials with their permission.

## Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 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

**Change Control** ..... ii

**Warnings** ..... iii

**Acknowledgements** ..... v

**Trademark Information** ..... vi

*Table of Contents* ..... *vii*

**Table of Figures** ..... ix

**Table of Tables** ..... xi

**Introduction** ..... 1

*Getting the Most from this Guide* ..... *2*

*Commonly Used Names* ..... *2*

*About the Guide to Securing Configuration and Administration of Microsoft Internet Information Services 5.0* ..... *2*

*An Important Note About Operating System Security* ..... *3*

**Chapter 1 Internet Information Services Installation** ..... 5

*Operating System Security* ..... *5*

*Installation Guidelines* ..... *7*

*Post Installation* ..... *9*

*The Default Install Directory* ..... *11*

*IIS Services* ..... *15*

*Securing the Metabase* ..... *17*

*Recommendation Checklist for Chapter 1:* ..... *18*

**Chapter 2 Internet Services Manager – Master Properties** ..... 19

*Snap-Ins* ..... *19*

*Master Properties* ..... *20*

WWW Service ..... 21

FTP ..... 25

Server Property Server Extensions ..... 29

*Recommendation Checklist for Chapter 2:* ..... *31*

**Chapter 3 Services Installation and Administration** ..... 33

*Access Control Methods* ..... *33*

Secure Sockets Layer (SSL) ..... 33

Client and Server Digital Signatures ..... 33

Anonymous Access ..... 34

Basic Authentication ..... 35

Digest Authentication For Windows Domain Servers ..... 35
Integrated Windows Authentication ..... 36
*Summary of Web Server Configuration Issues* ..... *38*
*World Wide Web (WWW) Services* ..... *39*
*File Transfer Protocol (FTP)* ..... *49*
*Simple Mail Transfer Protocol (SMTP)* ..... *54*
*Network News Transfer Protocol (NNTP)* ..... *60*
*Recommendation Checklist for Chapter 3:* ..... *65*
**Chapter 4 Additional Security Services ..... 69**
*Auditing* ..... *69*
*Certificates* ..... *72*
*Script Mappings* ..... *77*
*IPSEC Filtering* ..... *77*
*IIS Default Samples and Printers* ..... *79*
*Operating System Directories and Executables* ..... *80*
*Recommendation Checklist for Chapter 4:* ..... *82*
**Chapter 5 Backup Procedures and Antiviral Precautions ..... 83**
*Backup Procedures* ..... *83*
*Antiviral Program* ..... *83*
**Appendix A IIS 5.0 Security Configuration Tools ..... 85**
*IISperms (“What If” Tool)* ..... *85*
*HISECWEB.INF (Policy Template)* ..... *86*
*IISLock (Windows 2000 Internet Server Security Configuration Tool)* ..... *88*
**Appendix B IIS 5.0 Many-to-One Certificate Mapping Weakness ..... 91**
*Implementing IIS 4.0 and 5.0 Many-to-One Certificate Mappings* ..... *91*
**Appendix C References ..... 100**

# Table of Figures



Figure 1 User Properties Sheet for Anonymous Account ..... 9
Figure 2 IUSR_computername as a member of WebUsers group ONLY ..... 10
Figure 3 Service Tool from Administrative Tools ..... 15
Figure 4 Sample Disabling of SMTP Service from Services Tool ..... 16
Figure 5 Microsoft Management Console with the Internet Service Manager Snap-in ..... 19
Figure 6 Master Property Dialog Box for IIS WWW/FTP Services ..... 21
Figure 7 Master Web Site Properties for WWW dialog box ..... 22
Figure 8 Master WWW Operators Dialog Box ..... 23
Figure 9 WWW Home Directory Master Properties ..... 24
Figure 10 Authentication Methods Properties from Directory Security Tab ..... 25
Figure 11 FTP Site Master Properties Sheet ..... 26
Figure 12 Security Accounts for FTP Master Properties ..... 27
Figure 13 Choosing *Log Visits* on Home Directory Tab for FTP Master Properties ..... 28
Figure 14 Directory Security for FTP Master Properties ..... 29
Figure 15 Server Extensions for Web Server ..... 30
Figure 16 Authentication Methods Dialog Box ..... 34
Figure 17 Web Site Identification Property Sheet ..... 40
Figure 18 Operators Tab for Default Web Site Properties ..... 41
Figure 19 Web Site Home Directory Default Properties ..... 42
Figure 20 Application Configuration App Options Tab ..... 44
Figure 21 Application Configuration Process Options Tab ..... 45
Figure 22 Documents Tab ..... 45
Figure 23 Directory Security Tab ..... 46
Figure 24 Authentication Methods Dialog Box ..... 47
Figure 25 IP Address and Domain Name Restrictions ..... 48
Figure 26 Server Extensions Tab ..... 49
Figure 27 FTP Site Tab ..... 50
Figure 28 FTP - Security Accounts Tab ..... 51
Figure 29 FTP - Messages Tab ..... 52
Figure 30 FTP - Home Directory Tab ..... 53
Figure 31 FTP - Directory Security Tab ..... 54
Figure 32 SMTP - General Tab ..... 55
Figure 33 SMTP - Authentication Dialog Box ..... 56
Figure 34 Security Dialog Box for SMTP ..... 56
Figure 35 Connection Dialog Box for SMTP ..... 57
Figure 36 Relay Restrictions for SMTP ..... 58
Figure 37 Outbound Security Dialog Box for SMTP ..... 59
Figure 38 SMTP - Security Tab ..... 60
Figure 39 NNTP - General Tab ..... 61
Figure 40 NNTP Authentication Methods ..... 62
Figure 41 NNTP - Connection (domain blocking) ..... 62
Figure 42 NNTP - Settings Tab ..... 63
Figure 43 NNTP - Security Tab ..... 64
Figure 44 IIS Logging Configuration Example ..... 70
Figure 45 General and Extended Properties ..... 71
Figure 46 Configuring Site to Require SSL ..... 73
Figure 47 1-to-1 Account Mapping Dialog Boxes ..... 74
Figure 48 Many-to-1 Account Mapping Dialog Box ..... 74
Figure 49 Web Interface to Certificate Request ..... 76
Figure 50 IP Security Policies on Local Machine ..... 78
Figure 51 IPSEC Filtering ..... 78
Figure 52 IISPerms "What If" Tool Interface ..... 86

Figure 53 HISECWEB.inf MMC Policy Snap-In ..... 87
Figure 54 IISLock Web Interface Tool ..... 88
Figure 55 IIS 4.0's option for specifying a many-to-one mapping's CAs ..... 92
Figure 56IIS 4.0 Trusted Root Certification Authorities ..... 92
Figure 57 Many-to-one mapping rule for issuer attributes ..... 93
Figure 58 A many-to-one mapped account ..... 93
Figure 59 Certificates added to a CTL ..... 94
Figure 60 Naming a CTL ..... 95
Figure 61 An enabled CTL ..... 95
Figure 62 Trusted ns root certificate ..... 96
Figure 63. Masquerading ns subordinate CA ..... 97
Figure 64. Masquerading Brian Snort certificate and its chain ..... 98

# Table of Tables

Table 1 Permission Settings ..... 13
Table 2 Script Mapping - File Extensions and Uses ..... 77
Table 3 Directories and Utilities of Default Installation of IIS Samples ..... 79
Table 4 Directories and Files for Auditing and ACL's ..... 81

# Introduction

This document will describe how to securely install, configure, and administer the Internet Information Services 5.0 (IIS) and associated services. The focus of this document is security-relevant information pertaining to the installation and administration of Internet Information Services 5.0. This includes the secure configuration of FTP, WWW, SMTP and NNTP services as they relate to IIS 5.0.

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

While this document is intended as a complement to the set of *NSA Windows 2000 Security Guides*, it presents the information differently. Some Internet Information Services security issues, and corresponding configuration and administrative actions are very specific to the way the product is being used. For this reason, it is difficult in some areas to recommend specific, concrete actions. Instead, a summary is offered which describes the concerns and recommends solutions that a user must tailor to his/her own environment. Recommendations will be noted at the end of each section in a bulleted list for ease of reading and implementation.

**WARNING: This guide does not address security issues for the Microsoft Windows 2000 operating system that are not specifically related to the Microsoft Internet Information Services 5.0 and its implementation.**

## Summary of IIS Documentation

| Document | Contents | Target audience |
|---|---|---|
| Guide to the Secure Configuration and Administration of Internet Information Services 5.0 (This document) | • A detailed look at the secure installation and configuration of IIS 5.0 and it's associated services | • Experienced NT/2000 administrators who may be new to IIS |

PLEASE NOTE THAT THESE DOCUMENTS ASSUME THAT THE READER IS A KNOWLEDGEABLE WINDOWS 2000 ADMINISTRATOR. A knowledgeable Windows 2000 administrator is defined as someone who can create and manage accounts and groups, understands how Windows 2000 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 2000 administrative functions – it is assumed that the reader is capable of implementing basic instructions regarding Windows 2000 administration without the need for highly detailed instructions.

## Getting the Most from this Guide

The following list contains suggestions to successfully configure and administer Microsoft Internet Information Services 5.0:

**WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.**

- Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations:
  - Perform a complete backup of your system before implementing any of the recommendations in this guide
- Follow the security settings that are appropriate for your environment.

## Commonly Used Names

Throughout this guide the network subnet 192.168.0.0 will be used in the examples, screenshots, and listings.

**WARNING: It is extremely important to replace 192.168.0.0 with the appropriate network subnet for the networks being secured. These names are not real networks and have been used for demonstration purposes only.**

## About the Guide to Securing Configuration and Administration of Microsoft Internet Information Services 5.0

This document consists of the following chapters:

**Chapter 1**, "**Internet Information Services Installation,**" provides an overview of the pertinent security issues related to the installation of the Internet Information Services 5.0.

**Chapter 2**, "**Internet Services Manager – Master Properties,**" describes this IIS 5.0 management tool, which is a Microsoft Management Console tool Snap-in.

**Chapter 3**, "**Services Installation and Administration,**" describes configuration of the main functional components of IIS 5.0 and details the pertinent security-related settings (WWW, FTP, SMTP and NNTP).

**Chapter 4**, "**Additional Security Issues,**" describes multiple administrator groups, IIS 5.0 logging, a brief description of Certificates, and other miscellaneous items.

**Chapter 5**, "**Backup Procedures and Antiviral Precautions,**" comments on backups and antiviral programs.

**Appendix A, "IIS 5.0 Security Configuration Tools,"** contains information about the use of available tools to assisting in the configuration of IIS 5.0.

**Appendix B, "IIS 5.0 Many-to-One Certificate Mapping Weakness"** contains information about a weakness in the IIS 5.0 certificate mapping functionality.

**Appendix C, "References,"** contains a list of resources cited.

## An Important Note About Operating System Security

IIS security is tightly coupled to the operating system. For example, IIS logon can be 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 2000 security have a direct impact on IIS security.

The recommended sources of information for how to securely configure the Windows 2000 server and Professional are the set of *NSA Windows 2000 Security Guides*. It is important to implement the necessary guides on the IIS 5.0 machine.

This Page Left Intentionally Blank

Chapter

1



# Internet Information Services Installation

Internet Information Services (IIS) is a high-speed web server used to publish and distribute WWW-based content to standard browsers. IIS 5.0 is only available for the Windows 2000 platform. IIS 5.0 is primarily intended for installation on a Windows 2000 Server or Advanced Server and is not designed for use with any previous Mcrosoft operating system platforms. IIS 5.0 can run under the Windows 2000 Professional edition, however, it will be a scaled down version and functionality will be lost in the following areas: hosting multiple web sites, logging to an ODBC database, restricting access by IP address and process isolation.

**WARNING: Although IIS 5.0 is a scaled down version when installed on Windows 2000 Professional, it is still a computer security risk. This fact alone means that any IIS related patch that is released, especially security patches, MUST be installed. The code red worm had great help in spreading by Windows 2000 Professional systems and laptops that had IIS installed on them and were not patched.**

Version 5.0 provides the following publishing services: WWW, FTP, SMTP, and NNTP. Security issues relating to WWW, FTP, SMTP and NNTP will be discussed in detail in this document. Three additional application services are commonly associated with IIS - the certificate server, the index server, and Microsoft transaction server. Although these services can be installed at the same time as IIS 5.0 or later, the secure installation, configuration, and administration of these services will not be addressed in this document. Separate guidance is available for the certificate server on the same media containing this document.

## Operating System Security

Install IIS 5.0 according to the manufacturer's instructions; however, prior to implementing this guide, invoke the necessary Windows 2000 operating system security guidelines contained within the set of *NSA Windows 2000 Security Guides*. IIS 5.0 security is tightly coupled to the operating system. File permissions, registry settings, password usage, user rights, and other issues associated with Windows 2000 security have a direct impact on IIS 5.0 security. The advantages gained by this tight coupling are no increased complexity, possibly no security holes due to the addition of security layers, and better performance by eliminating unnecessary overhead caused by additional security and access control layers. The primary disadvantage is that poor OS security can often cause poor web security.

Prior to configuring IIS 5.0, determine how the server will be used. The configuration of IIS directories, files, user accounts and profiles, TCP/IP port connections, etc. will be based on your answers to the following questions:

- Will the server be accessed from the Internet?
- Will the server be accessed from an Intranet?

- How many web sites will this server host?
- Will separate web sites share any content?
- 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?

## Installation Guidelines

When installing IIS 5.0, the following guidelines are recommended:

- Place the 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 IIS 5.0 on a standalone server, where possible. If IIS 5.0 is installed on a domain controller and the web server is attacked, the entire server and sensitive domain information may be at risk. Also, the added overhead of being a domain controller will also slow down the server's ability to provide web services efficiently.
- Install IIS 5.0 on a server that is not required to support any other service. Neither application software nor development tools should be installed on the IIS 5.0 server.
- Partition the IIS machine so that published content of each supported service (WWW, FTP, etc.) is located on a separate partition or disk. This will prevent attempts to traverse up the directory tree beyond the published content root.
- IIS 5.0 does not allow the user to install the application anywhere except in the C partition (unless using unattended installation). It is integrated into the operating system functionality. Because of this, the default permissions applied to the %systemdrive%, typically C:\, by the set of *NSA Windows 2000 Security Guides* may cause some services in IIS to not function properly. Care must be taken to ensure that operating system permissions do not interfere with the operation of the IIS Services.
- Remove all protocol stacks except TCP/IP, unless user's Intranet requires another protocol stack.
- IP routing is disabled by default and should be left that way. If routing is enabled, it is possible to have data pass from user's Intranet to the Internet.
- If access to the IIS 5.0 machine is required from the Internet, install it initially with all incoming traffic blocked at the router or firewall. After complete configuration, allow incoming traffic. This is recommended because once the main IIS installation has taken place, the services are active and connections can take place. This can cause a system compromise before there is time to configure the security of the web site(s).
- Installation of client for Microsoft networking is required for the HTTP, FTP, SMTP and NNTP services to run. If not installed the services will NOT be able to start automatically or manually.
- If SMTP of NNTP will be installed, the Server service will be required, thus, File and Print sharing for Microsoft networks must be installed. If it is not, the Server service will not show up in the available MS services.

The following is a list of services that are not required for most installations of IIS 5.0 and should be disabled. This list is not all inclusive of all possible services and will be dependant on the user's implementation of the IIS server and its environment.

| Service | Important Notes |
|---|---|
| Alerter | |
| ClipBook Server | |
| Computer Browser | |
| DHCP Client | |
| Distributed File System | |
| Distributed Link Tracking Systems Client | |
| FTP Publishing Service | Disabled unless user's require FTP services |
| IPSEC policy agent | Disabled unless IPSEC policies will be used |
| Licensing Logging Service | |
| Logical Disk Manager Administrator Service | |
| Messenger | |
| Net Logon | Disabled unless domain users are required to logon to the server, this service is required to communicate with the domain controller |
| Network DDE | |
| Network DDE DSDM | |
| Print Spooler | |
| Remote Registry Service | |
| Removable Storage | |
| RPC Locator | Required if user is doing remote administration |
| RunAS Service | |
| Server Service | Must be started if server will run the SMTP or NNTP service of IIS, for administration purposes |
| Task Scheduler | |
| TCP/IP NetBIOS Helper | |
| Telephony | |
| Windows Installer | |
| Windows Time | |
| Workstation Service | Must be started if the server will be part of a domain |

## Post Installation

During the installation of IIS, a default account is created for anonymous logons. The default name for this account is IUSR_*computername,* where *computername* is the name of the machine hosting IIS. This account should be given the least amount of privileges possible. Review the security settings for the IUSR_*computername.* Make sure **User Cannot Change Password** and **Password Never Expires** options are selected. This account should be a local account, not a domain-wide account, and must have the right to log on locally. It does not require the right to access this computer from the network, or log on as a batch job, which it does have by default. If anonymous access to the web site is prohibited, it is recommended that this account be disabled. All users would then be required to supply a valid username and password, using basic authentication, integrated Windows authentication or digest authentication for Windows domain servers to access server resources (discussed in more detail in Chapter 3). See **Figure 1**.

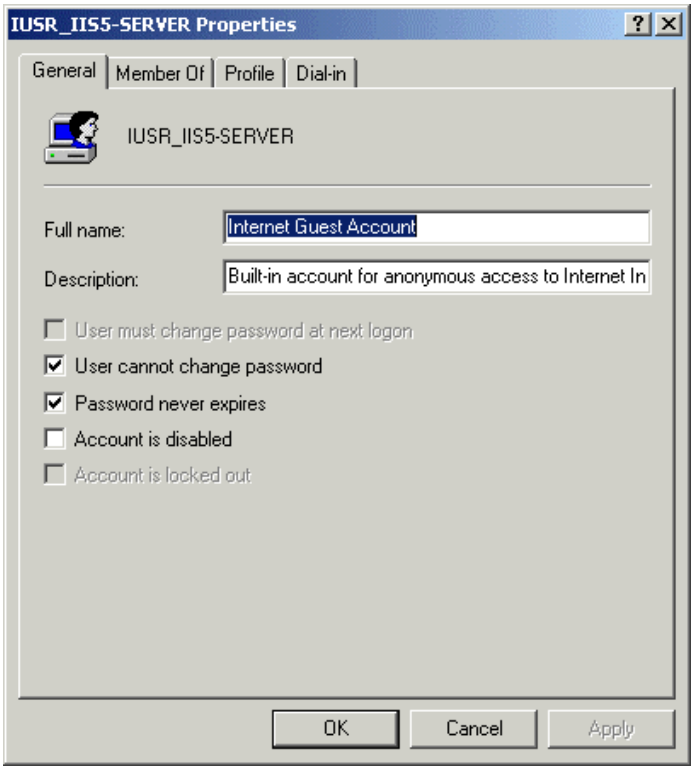



**Figure 1 User Properties Sheet for Anonymous Account**

**Note: The set of *NSA Windows 2000 Security Guides* does not take into account the need for the IUSR_*Computername* account to be included in the log on locally user rights. Please make sure to modify the user rights security template if applying after the installation of IIS 5.0.**

## Groups for file, directory, administration purposes

Create at least two new groups to be used with IIS. The “WebAdmins” group, for example, to define users who will administer WWW/FTP content. If the server will host several WWW/FTP sites, create an administrative group for each site. A “WebUsers” group should be created as the primary group for the IUSR_*computername* account. These groups will be used for setting NTFS permissions. 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, Everyone, Users and Authenticated Users group. It is recommended that this account be removed from the Guests group and added to the WebUsers group (it cannot be removed form the other built-in groups). 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, see **Figure 2**. You also may consider putting the IWAM_*computername* account in this group or creating another group for it.

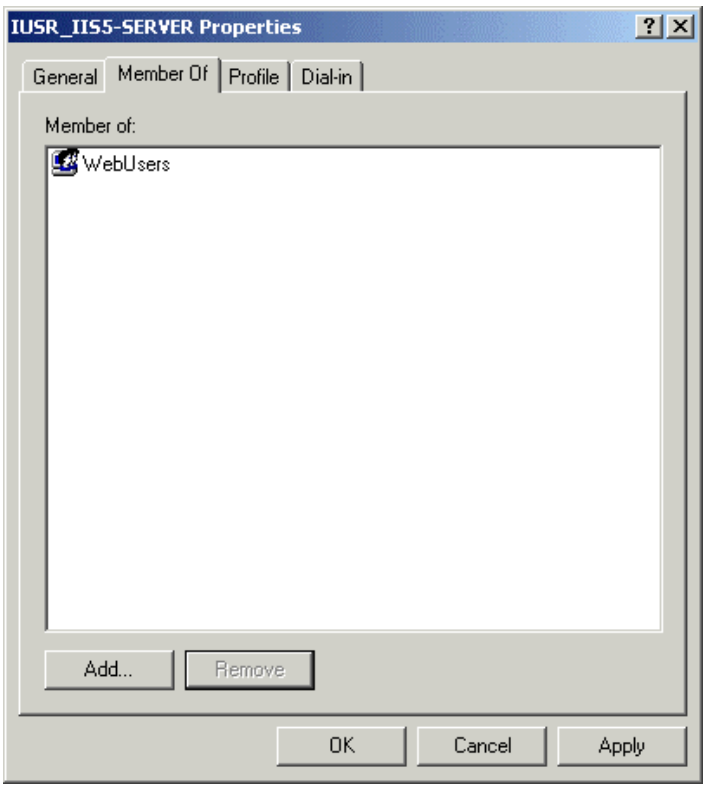



**Figure 2 IUSR_computername as a member of WebUsers group ONLY**

## Administering IIS with Multiple Groups

IIS 4.0 allowed the creation of local groups to setup different administrative groups for the IIS services. In IIS 5.0 this paradigm has changed. Local groups can and should be created for different administrative groups. However, the difference is that local groups for the WWW and FTP services will only be used for NTFS permissions. The SMTP and NNTP services will allow the ability to set local groups as administrative operators for the IIS service, and the next few paragraphs will describe the benefit of doing so. It must be noted that if the IIS 5.0 server will participate in a Windows 2000 domain, the domain

server's local, global, and universal groups can be created and used for both the administration and NTFS permissions identified below. Because of the difference in the local group functionality, user accounts should be used to identify administrative operators for the WWW and FTP services/sites unless utilizing domain groups. A public IIS server should not be a member of the internal domain and a segmented domain in the DMZ should not include a trust relationship to the internal domain.

In order to simplify the assignment of administrative rights to the IIS Server, it is recommended that a separate Windows 2000 IIS Administrators Group(s)be established. It is **strongly** recommended that the user not use the Windows 2000 Administrator group, as it is not necessary to have Windows 2000 administrative rights to perform many IIS 5.0 administration functions. IIS administrative rights are assigned through the SMTP and NNTP (WWW and FTP if active in a domain) property dialog boxes by defining Service operators as described in Chapter 3.

Having a separate IIS administration group offers several benefits. First, it precludes the need for IIS administrators to logon unnecessarily as a Windows 2000 administrator – something that should be avoided for security reasons. Second, it will allow the partitioning of administrative rights. For example, the right to reconfigure the IIS server to a select few (Windows 2000 administrators) can be reserved, while allowing several individuals to manage WWW and FTP content. For instance, users who are members of a web operators group could be given access to control what is made available to visitors to the site through the WWW and FTP data directories. They would not have access to configure the web server, i.e., add users and groups, etc. Windows 2000 administrators would retain that right. Finally, having separate IIS administrator groups for each site maintained by the server would simplify the process of managing administrative rights – adding a new administrator for a site is as simple as making them part of the appropriate group.

This becomes very important when a server is used to manage several sites. As stated previously, an administrative group should be created for each web site. The members in these groups would be granted operator privileges to administer their own web site exclusively. This would allow the Windows 2000 administrators to maintain their server and manage their security risks more effectively by having as few Windows 2000 administrators as possible and not permitting any one group total control over all sites on the server.

### Install all patches for the Operating System and for IIS

IIS administrators should always check for hot fixes/patches and install them as necessary, along with the latest service pack available from Microsoft. Available patches can be found at the Microsoft Support Center at http://www.microsoft.com/security/ website. Follow the link Security Bulletins, then select Internet Information Services 5.0 from the product drop-down list.

## The Default Install Directory

After installing IIS 5.0, change the NTFS access permissions on the IIS install directories. It is particularly important to make certain that the "Everyone" and "Guests" group accounts, as well as the "Guest" user account, are not granted access by highlighting them and selecting the **Remove** button. By default, the group "Everyone" is given Full Control of the default publication directory (i.e., `C:\Inetpub`). These group and user accounts can be used by malicious users to gain access to systems. Removing them will prevent such users from using the server for data storage or staging an attack by placing

malicious code on the server. Also, the Inetpub directory is installed by default in the C:\ directory (or %systemdrive% if not C). A new directory or the existing structure should be moved to another partition or drive, separating the accessible sites from the operating system location. It is advisable to change the name from Inetpub to something less obvious.

The IIS 5.0 publishing directories can be installed in a custom location but only by utilizing an unattended installation, this is done by using an answer file. The answer file (ex. Iis5.txt) will need to consist of the following:

```
[Components]
iis_common = on
iis_inetmgr = on
iis_www = on
iis_ftp = on
iis_htmla = on
iis_doc = on
iis_pwmgr = on
iis_smtp = on
iis_smtp_docs = on
mts_core = on
msmq = off


[InternetServer]
PathFTPRoot={put your drive and install location here, i.e.
f:\FTPROOT}
PathWWWRoot={put your drive and install location here, i.e.
f:\WWWRoot}
```

Next the following command must be run to start the unattended installation from the command line (modify the drive and path to specify where you put the .txt file):

Sysocmgr/I:%windir%\inf\sysoc.inf /u:a:\iis5.txt

For further information pertaining to unattended installation and other options please see the Upgrading to IIS 5; Installing IIS 5 to a Custom Location reference.

**Note: There is no current way to install the IIS binary files to any other directory than the default, which is on C:\ (or %windir%).**

**Table 1** shows the recommended NTFS and IIS permissions for the IIS-related directories.

| Type of Data | Example Directories | Data Examples | NTFS File Permissions | IIS 5.0 Permissions |
|---|---|---|---|---|
| Static Content | \Inetpub\wwwroot\images<br>\Inetpub\wwwroot\home<br>\Inetpub\ftproot\ftpfiles | HTML, images, FTP downloads, etc. | Administrators (Full Control)<br>System (Full Control)<br>WebAdmins (Read & Execute ,Write, Modify)<br>Authenticated Users (Read)<br>Anonymous (Read) | Read |
| FTP Uploads (if required) | \Inetpub\ftproot\dropbox | Directory used as a place for users to store documents for review prior to the Admin making them available to everyone | Administrators (Full Control)<br>WebAdmins or FTPAdmins (Read & Execute, Write, Modify)<br>Specified Users (Write) | Write |
| Script Files | \Inetpub\wwwroot\scripts | .ASP | Administrators (Full Control)<br>System (Full Control)<br>WebAdmins(Read & Execute, Write, Modify)<br>Authenticated Users: special access (Execute)<br>Anonymous: special access (Execute) | Scripts only |
| Other Executable and Include Files | \WebScripts\executables<br>\WebScripts\include | .exe, .dll, .cmd, .pl<br>.inc, .shtml, .shtm | Administrators (Full Control)<br>System (Full Control)<br>WebAdmins (Read & Execute, Write, Modify)<br>Authenticated Users: special access (Execute)<br>Anonymous: special access (Execute) | Scripts only<br>Or<br>Scripts and Executables**<br><br>**(Depending on necessity) |
| Metabase | \WINNT\system32\inetsrv | MetaBase.bin | Administrators (Full Control)<br>System (Full Control) | N/A |

**Table 1 Permission Settings**

**Note: IIS permissions complement the NTFS permissions. For a file to be sent to the client browser for rendering, IIS Read permission must be set for the web directory, and the user in whose context the service is running must have NTFS Read access to that file. If they do not match, the most restrictive permission will be enforced.**

**WARNING: Advanced tab under the NTFS security property tab: granular access to all potential file permissions. Modifications to larger web sites using this method can cause difficult trouble shooting problems in the future.**

Chapter 3 will describe in detail IIS permissions and other security settings for the IIS services.

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 IIS 5.0) permission for file access allowed to the WebUsers group. Grant **Read & Execute**, **Write**, and **Modify** file access permissions to the group responsible for maintaining web content (i.e., WebAdmins).

Establish directories that contain executable files only (scripts, batch files, and other executables). These directories should ONLY have NTFS **Traverse Folder / Execute File** for users accessing your site (i.e., IUSR_*computername*, WebUsers) and IIS

permission of **Scripts Only**. IIS 5.0 **Scripts and Executables** permission should only be allowed on directories where appropriate, i.e., a directory containing binary files that must be executed by the web server. **Scripts and Executables** is additional access control permissions offered by IIS 5.0. These options will be discussed in detail in Chapter 3.

Delete or move all directories that contain “samples” and any scripts used to execute the “samples”. The following is a list of directories created during the installation of IIS. It is recommended that these directories be deleted or relocated. If there is a requirement to maintain these directories at the site for training purposes, etc., have NTFS permissions set to only allow access to authorized users, i.e., WebAdmins and administrators. See Chapter 4 for more complete information about samples. Also, to control access to these directories through WWW, require Integrated Windows authentication through the Web Site Properties dialog box (Chapter 3 describes how to configure this setting).

- \InetPub\iissamples
- \InetPub\AdminScripts

## IIS Services

There are four potential services that can be offered by installing IIS 5.0. Those four services are World Wide Web (WWW), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Network News Transfer Protocol (NNTP).

WWW – Service necessary to build a web server and serve web pages to clients.

FTP – Service necessary to allow users to FTP to the server to obtain or upload files.

SMTP – Service necessary to allow the web server to send and receive Email to clients in response to forms or perhaps shopping cart programs (if required).

NNTP – Service necessary to host a USENET style news server.

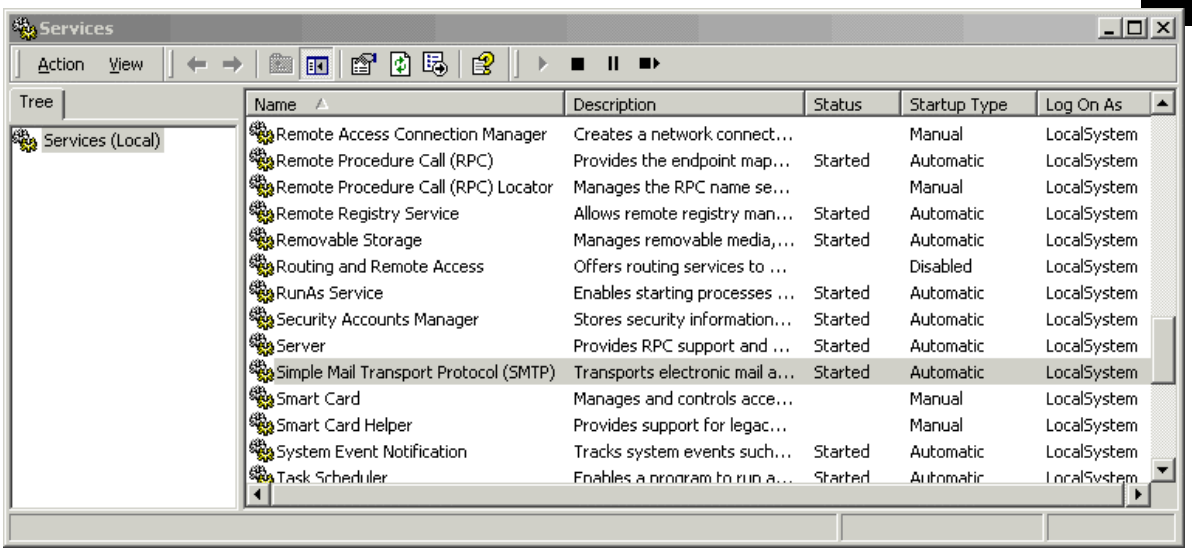



**Figure 3 Service Tool from Administrative Tools**

During the installation the administrator has the ability to turn off (deselect) the services that they do not wish to install. After installation, any of the services can be turned off in the case that they are no longer needed.

To deselect services:

- From the start menu, click **Programs** Þ **Administrative Tools** ⇒ **Services**
- Highlight the service that needs to be turned off, right-click mouse, choose **stop** to turn off the service
- To ensure that it will not restart upon rebooting, right-click the service and choose **Properties**. In the Startup type drop down menu change the service from "Automatic" to "Manual" or "Disabled". See **Figure 4**:

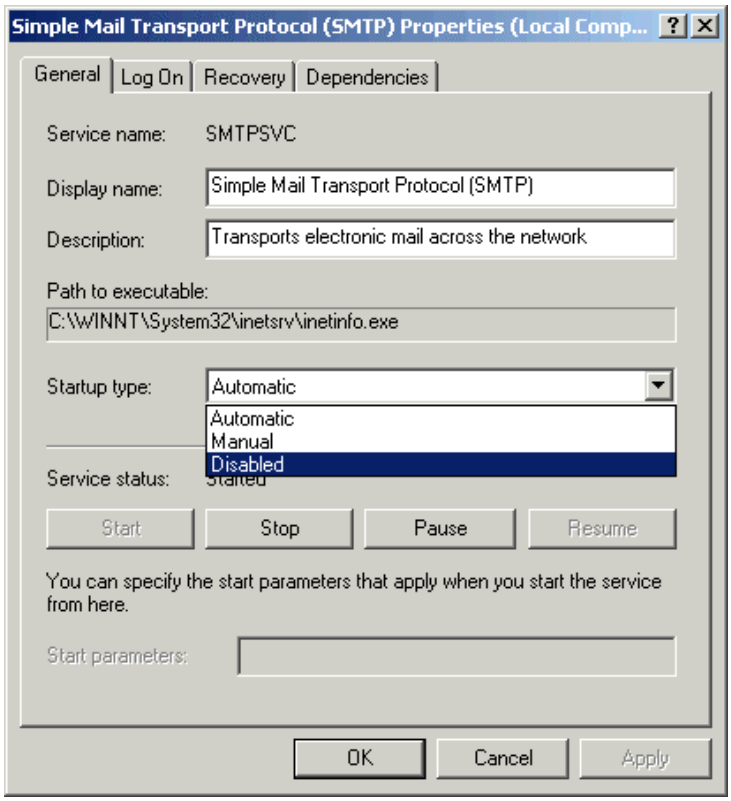



**Figure 4 Sample Disabling of SMTP Service from Services Tool**

## Securing the Metabase

This information is taken from the *Internet Information Server Version 4.0 Security Assessment* document written by Kenneth G. Jones of the MITRE Corporation. Refer to this document if a more detailed explanation is required.

### Purpose

The metabase stores IIS configuration parameter values in a fast-access, memory-resident data store. The Metabase is specifically designed for use with IIS and is faster, more flexible, and more expandable than the Windows 2000 Registry.

### Structure

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

### Security

The metabase is stored in a specially formatted disk file named `MetaBase.bin`, and is located in the `\Winnt\system32\inetsrv` directory. The metabase loads from disk when IIS starts, is stored to disk when IIS shuts down, and is saved periodically while IIS is running. It is important to protect this file from unauthorized access, although sensitive data is stored in a secure manner within the file. If the file is replaced with a fraudulent file, the operation of the web server can be compromised. If the file is replaced while the server is not running, any changes implemented in the file will be effective the next time the server is started. The effects caused by these changes can range from denial of service through unauthorized service being provided by the web server. It is recommended that this file be stored on an NTFS partition and use Windows 2000 security to protect it. The default permission settings for this file are System and Administrators Full Access. Limiting the access to System and local Administrators provides good security; therefore, there is no need to change or add to these settings.

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

## Recommendation Checklist for Chapter 1:

- ❑ Implement the necessary set of *NSA Windows 2000 Security Guides*
- ❑ Block all traffic to server before installation takes place (for Internet accessible server)
- ❑ Place IIS server in physically secure location
- ❑ Install IIS on stand alone system
- ❑ Install only OS and required IIS 5.0 components (no applications or development tools)
- ❑ Create a new Inetpub root directory on separate drive or partition from OS and other programs. Use a name other than Inetpub to help counter potential attacks
- ❑ Remove all protocol stacks except TCP/IP
- ❑ Disable all non-required services
- ❑ IUSR_*Computername* account privileges
    - o Select **User cannot change password**
    - o Select **Password Never Expires**
- ❑ User rights
    - o Grant **Log on locally**
    - o Remove **Log on as a batch service** and **Access this computer from the network**
- ❑ If non-anonymous access: disable the IUSR_*Computername* account
- ❑ Create local admin groups for each web site and populate with required accounts
- ❑ Create local group for WebUsers and include only the required accounts, including the IUSR_*Computername* account
- ❑ Remove IUSR_*Computername* from all other groups (i.e., guests, etc.)
- ❑ Remove all NTFS permissions from the Inetpub directory, and assign only required access groups and accounts (i.e., remove everyone, add WebUsers, WebAdmins, etc.)
- ❑ Establish logical directory structure (i.e., separate static content, html, asp, scripts, executables into different labeled directories)
- ❑ Set NTFS permission on directory structures as required
- ❑ Delete/move all sample directories and scripts that execute the samples

### Metabase

- ❑ Modify the metabase permissions and/or move it and change registry key

Chapter

2



# Internet Services Manager – Master Properties

## Snap-Ins

The Microsoft Management Console (MMC) provides a user interface shell application called a console. Microsoft's objective is for all management functions to be accessible as subordinates within the management console. These processes are known as Snap-ins. MMC itself does not provide any management behavior, but it offers a common environment for Snap-ins. The result is that management/administrative control of the platform is centralized. A Snap-in for IIS, Internet Service Manager (ISM), is provided during installation. The ISM will be discussed in more detail later in this chapter.

Each instance of a console and associated Snap-ins is commonly referred to as a tool. Any number of tools can be created. Once created, the console can be populated with existing Snap-ins or a new Snap-in may be created for a specific purpose. Administrators can create tools that host several Snap-ins and save these for later use or for sharing with subordinate administrators. The administrator can take advantage of the customization features by preparing consoles that perform only one task and use them to delegate responsibility to other, perhaps less experienced administrators. The console can be tailored to present only the menu choices the user needs to get the job done. For example, an administrator could create a new MMC console with the IIS Snap-in for web administrators to use to manage web resources. See Figure 5:

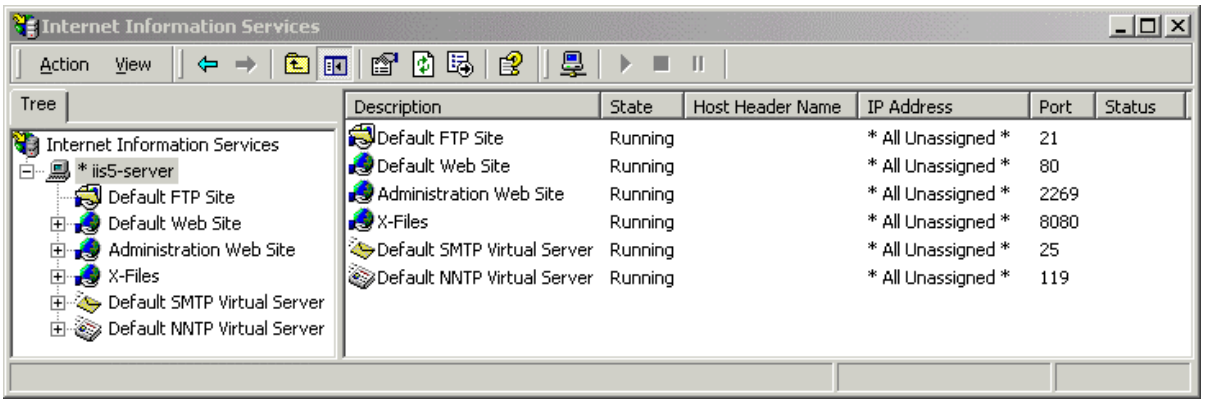



**Figure 5 Microsoft Management Console with the Internet Service Manager Snap-in**

In addition to the MMC, there is an HTML version of the ISM, which is capable of managing several aspects of IIS 5.0. The are also several areas not manageable with the HTML version which include server extensions for remote authoring, changes to

certificate mapping, and the SMTP and NNTP services. There are also some tasks that can more easily be performed using the ISM Snap-in. The HTML version is not easily customizable to allow delegated control over specific areas or sites.

Remote HTML administration should only be allowed if necessary. It should only be allowed for the IIS server administrator, using one specific IP address through IP Address and Domain Name Restrictions (Chapter 3) in conjunction with SSL (Chapter 4) client side certificates (Chapter 4) and putting the specific local username in the (later in this Chapter) area of the administration site properties. Beyond this, it is recommended to limit any server administration to the local host using the ISM. The ability to add administrative operators will be described in the master properties section of this chapter.

## Master Properties

In this section only the security related issues for the master properties of the services offered by IIS 5.0 will be discussed. Other security related features for all the services (WWW, FTP, SMTP and NNTP) will be identified and discussed in Chapter 3.

### Internet Service Manager

When the IIS 5.0 Internet Service Manager (ISM) is started, an MMC console begins running and automatically loads the Internet Service Manager Snap-in. Under the property page there are two main information sheets, **Internet Information Services** (which is active by default) and **Server Extensions**. Clicking the appropriate tab can access either. On the IIS sheet, there are three main property dialog boxes general to IIS operation - **Master Properties, Enable Bandwidth Throttling, and Computer MIME Map**. Setting these general properties is very useful if the user understands that they will be creating a number of different web sites on their server. These properties will be automatically inherited by all web sites created on the server, which will save time when configuring each site. If some sites require different properties, they can be set during the configuration of each web site.

Only the common settings that can be established through the Master Properties dialog box to enhance security will be discussed in this chapter. The next chapter will describe the property dialog boxes for configuring individual security settings of the WWW, FTP, SMTP and NNTP services using the ISM.

To access the Master Properties dialog box:

- Highlight the IIS server name in the ISM
- From the **Action** pull-down menu, select **Properties**
- Select the WWW or FTP service via the drop down menu and click the **Edit** button to configure Master Properties for the selected server. See **Figure 6**:

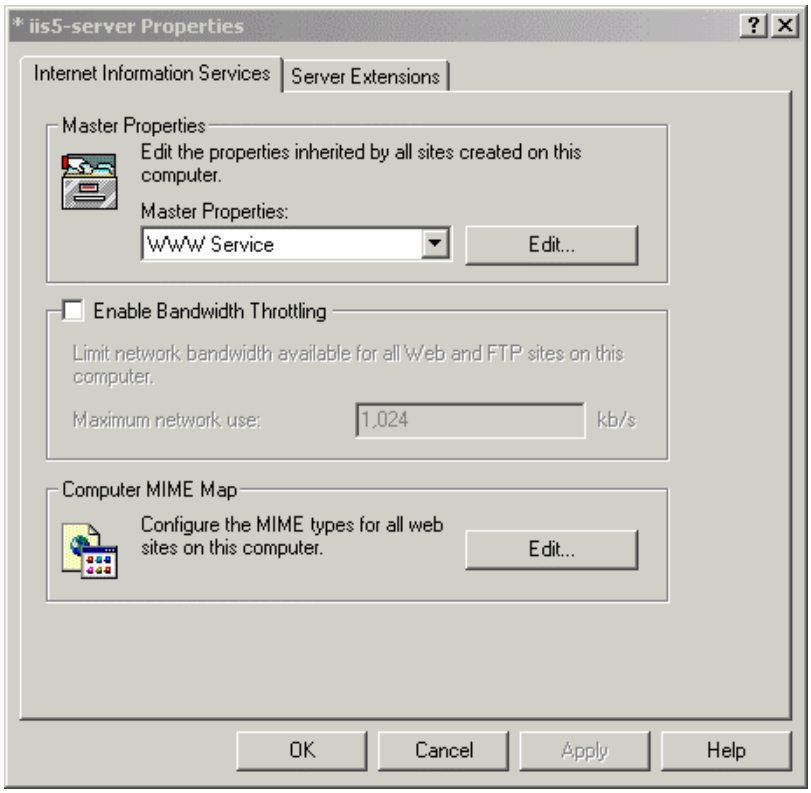



**Figure 6 Master Property Dialog Box for IIS WWW/FTP Services**

## WWW Service

This master 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, the user 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. The following shows the dialog boxes for setting common security-related properties using the **Web Site**, **Operators**, **Home Directory** and **Directory Security** tabs.

**NOTE: These same settings can be applied individually to the WWW, FTP, and SMTP services. Only the security related settings for the Master Web Site, FTP Site, Operators, Home Directory and Directory Security tabs are discussed here as they contain the settings that are most likely to be universally applicable to the WWW and FTP services.**

**Web Site Tab - Enable Logging** (See **Figure 7**) 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. This logging will keep track of many different information types, which will be discussed in Chapter 4.

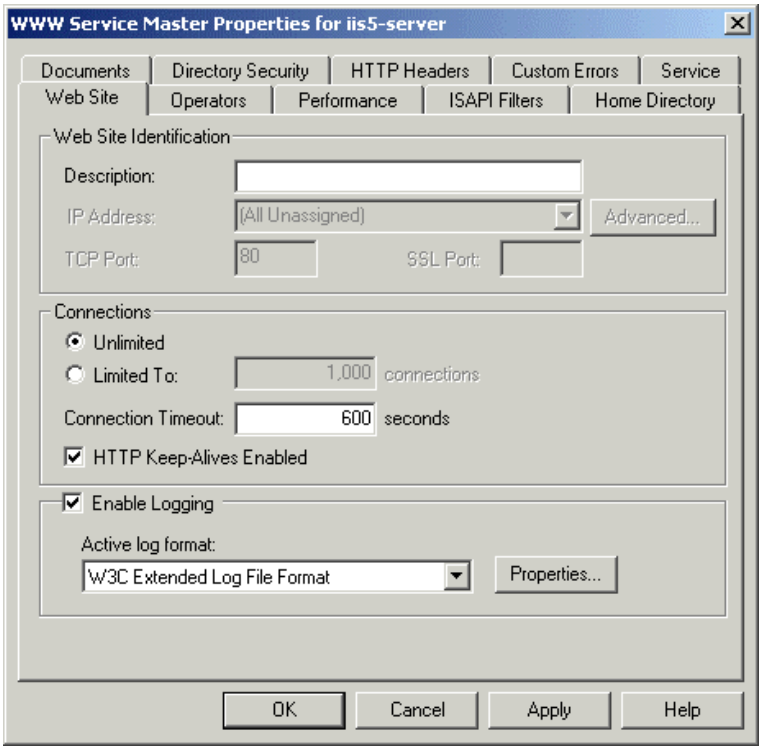



**Figure 7 Master Web Site Properties for WWW dialog box**

**Operators Tab –** See **Figure 8.** The WWW Service Master Properties Sheet allows the user to identify groups or accounts with the permission to perform some administrative functions for all of the WWW sites created on this server. When each site is configured, these groups/accounts will automatically be included and the user will have the option to remove them, as well as add other groups/accounts as appropriate for the site. If the server is responsible for maintaining several web sites, create a separate group to manage WWW content for each site. IIS 5.0 does not allow user created local groups to be included in the Operators sheet for WWW or FTP sites. This rule also applies to the specific WWW/FTP site properties, not just the master sheet.

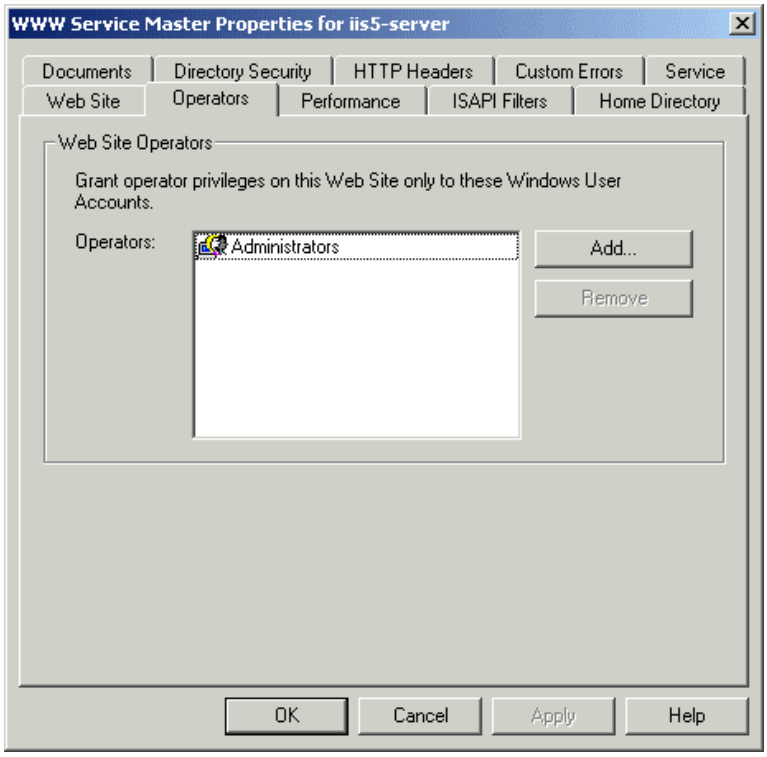



**Figure 8 Master WWW Operators Dialog Box**

**Home Directory Tab –** See **Figure 9**. The master properties of the WWW server is a good place to set all the sites to log visits. The logging will ensure that all sites, which are added later, will, by default, be logging the visits to the site. Logging is the baseline for detecting intrusive behavior on target systems. By setting this here, the administrator will not need to set it for each site that is created during the life of the server. The Read, Write and Directory browsing permissions should be left unset. For each site that is created, these options can be set as required.

- Read setting - gives permissions for visitors to see the sites.
- Write setting - gives permissions to write to the directories where the sites were installed.
- Directory browsing setting - gives the user the ability to see a listing of all the files in a particular directory.

The recommendation here is to disable the Read, Write and Directory browsing permissions in the master properties, by NOT selecting them. This will be addressed further in Chapter 3 with the site settings.

Finally, on the Home Directory tab is the execute permissions drop down box. The recommended setting is "**None**" which will preclude visitors from being able to run scripts or executables by default. These settings can be modified as necessary for each individual site, but using "None" as the default will help preclude unintentionally assigning execute permissions where they were not intended.

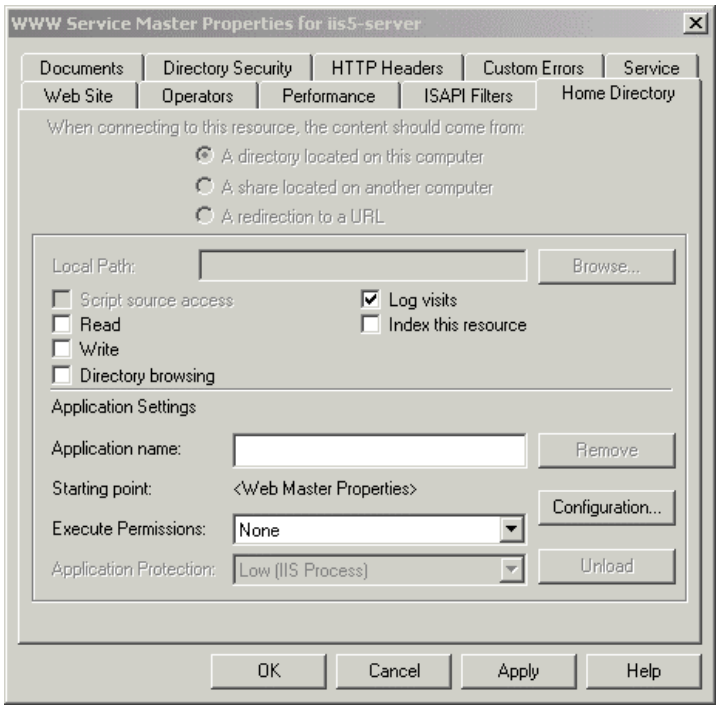



**Figure 9 WWW Home Directory Master Properties**

**Directory Security Tab –** See **Figure 10**. The authentication methods used on the web site(s) are very important in identifying the users and controlling access to specific files, directories, and scripts or executables. The authentication will depend on whether the site is used in an intranet or on the Internet. To get to the **Authentication Methods** sheet, select **Edit** from the "Anonymous access and authentications control" area of the **Directory Security** tab of the WWW master properties sheet. The **Anonymous Access** option will either grant or deny access to all sites on the server by default. If this site will be used in an intranet and the internal network is a Windows based network, anonymous access should be disabled. This will allow logging and access control by specific user accounts. If a specific web site needs anonymous access it can be enabled during individual web site setup. If this server will be accessible to the Internet and most of the hosted web sites will allow anonymous access, then enabling anonymous access here makes sense.

In addition to anonymous access, three other authentication mechanisms are available:

- Basic authentication allows the username and password to traverse the Internet/network in cleartext. This can allow an intruder to capture valid accounts to attempt to break into the site. (Use of basic authentication with SSL will protect against this threat as discussed in Chapter 4)
- Digest authentication for Windows domain servers is similar to Basic authentication, except, instead of using cleartext usernames and passwords, it passes a hash of the password in order to provide more secure authentication. Digest authentication is only usable with HTTP 1.1 compliant browsers (currently only IE5). The IIS 5.0 server must be in a Windows 2000 domain and the user passwords must be stored in plain text files on the domain controller (There is an option in user account properties for managing user accounts in a domain on the domain controller). Therefore, the

domain controller must be secured (Refer to the set of *NSA Windows 2000 Security Guides*).

- The integrated windows authentication option is the same as Windows NT Challenge/Response in IIS 4.0. Integrated Windows authentication can only be used with the MS Internet Explorer (IE) web browser.

See Chapter 3 for a more detailed explanation of the authentication methods. The recommendation is to use the authentication method that will meet the needs of your site policy. Because of the wide variety of uses a more explicit recommendation is not possible.

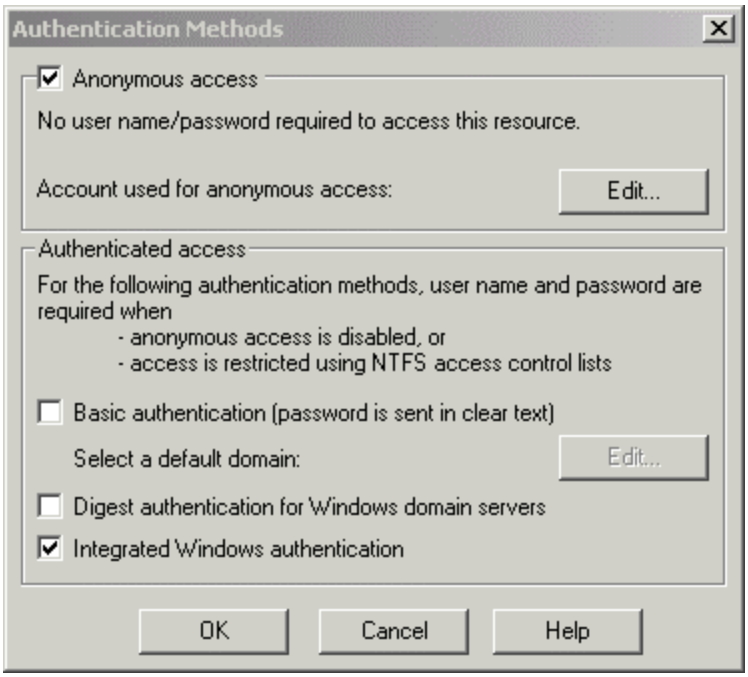



**Figure 10 Authentication Methods Properties from Directory Security Tab**

## FTP

The FTP master property sheet has fewer options to offer than for the WWW service. To get to the FTP master property sheet, simply use the drop down box on the **IIS-Server Properties** sheet to select FTP Service and click **Edit**.

**FTP Site Tab –** See **Figure 11**. It is recommended that logging be enabled in this section of the property sheets for ease of administration later and to ensure that logging is not forgotten as sites are added. Depending on the type of FTP service allowed, the number of connections allowed and inactivity timeout can be set in this section. This will allow better control of potential Denial of Service (DoS) attacks and server resource consumption.

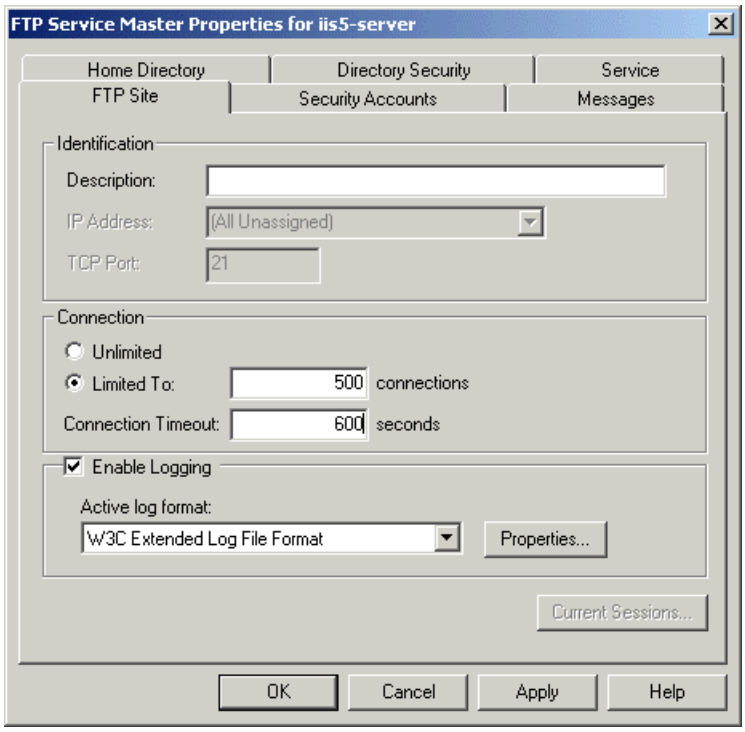



**Figure 11 FTP Site Master Properties Sheet**

**Security Accounts Tab –** See **Figure 12**. Similar to that of the WWW service properties, anonymous access to the FTP service can be set here. Again, if this FTP server will be accessible by the Internet and anonymous access will be allowed, it is recommended to set that here. Also remember that the individual sites can override this setting, this is just blanket coverage for adding sites or changing all existing sites for a security or policy reason.

**WARNING: FTP passwords are sent in cleartext if a user logs in with their Windows 2000 account.**

It is recommended to select the **Allow only anonymous connections** option here to preclude password compromise. The **Allow IIS to control password** option is the same as the **Enable automatic password synchronization** option in IIS 4.0. This will allow synchronization of the password in this property sheet with that in the Computer Management snap-in to control user and group accounts. However, the IUSR_*computername* account should be on the local machine with which IIS is installed. This is the default and should not be changed. A Windows domain username and password should never be used for FTP. The second section of the sheet allows the identification of FTP site operators. The identification of groups or accounts with the permission to perform some administrative functions for all of the FTP sites created on this server is specified here. When each site is configured, these groups/accounts will automatically be included. The user will have the option to remove them, as well as add other groups/accounts as appropriate for the site. If the server is responsible for maintaining several FTP sites, create a separate group to manage FTP content for each

site. IIS 5.0 does not allow user created local groups to be included in the operators sheet for WWW or FTP sites. This rule also applies to the specific WWW/FTP site properties, not just the master sheet.

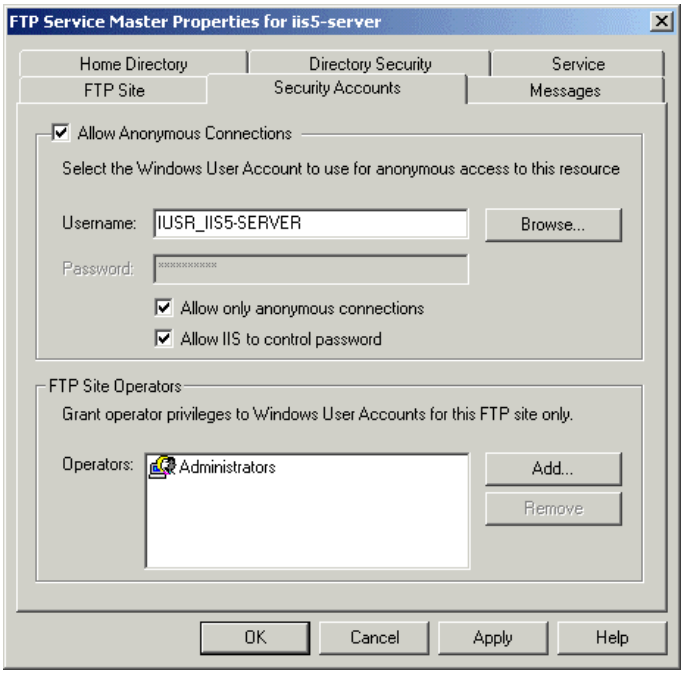



**Figure 12 Security Accounts for FTP Master Properties**

**Home Directory Tab –** See **Figure 13**. This area only has one security related option, **Log visits**. Unlike some of the other options that depend on the server implementations, this option should always be enabled from a security standpoint. It is recommended that the **Log visits** option be enabled on this master property sheet. Logging is essential in identifying intrusive behavior, in reconstructing the attack, identifying the extent of the damage done, as well as collecting valuable information to prosecute if legal proceedings may occur. **Log visits**, along with the logging feature identified on the **FTP Site** tab, should always be selected.

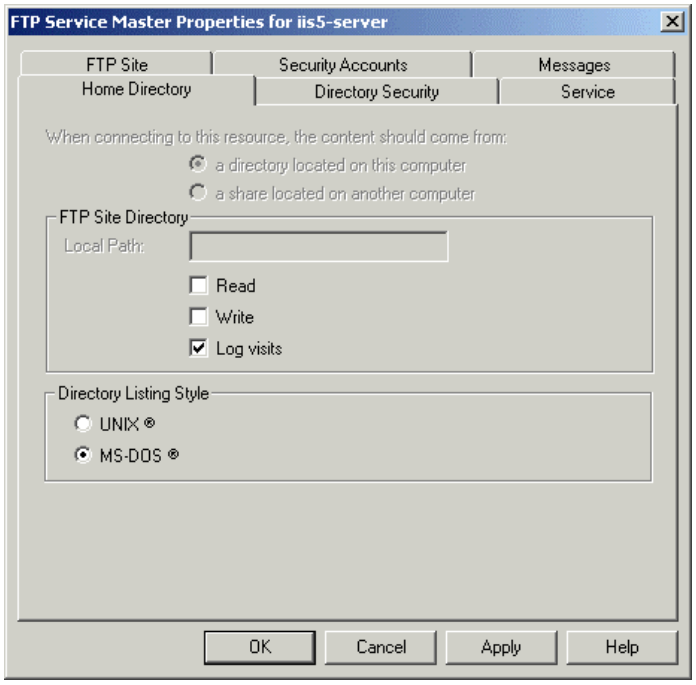



**Figure 13 Choosing *Log Visits* on Home Directory Tab for FTP Master Properties**

**Directory Security Tab –** See **Figure 14**.

**TCP/IP Access Restrictions –** This can be used to grant or deny access to all computer systems, except those included in the list identified. Again, depending on the use of the server, different options will be required. If the FTP server is intended to be accessible by the Internet, or the entire intranet, then administrator will want to grant access to all computers by default. If the server will have a specific user base and the user base does not have dynamically assigned addresses, deny all access and specifically identify allowed computers or groups of computers. Again, this is for mass coverage, and the individual site administrators can modify this to satisfy their own site security requirements.

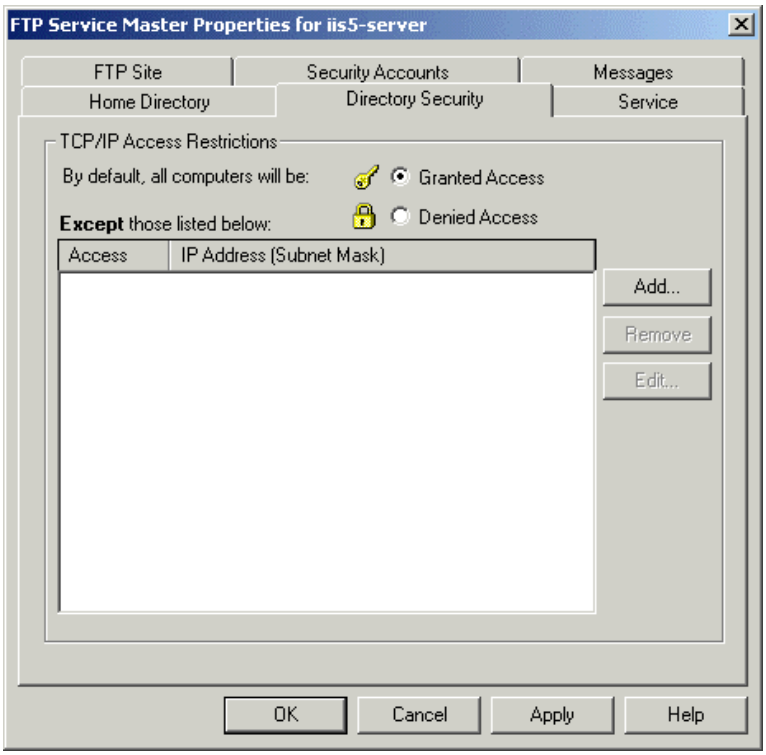



**Figure 14 Directory Security for FTP Master Properties**

## Server Property Server Extensions

The second section of the server's master properties is the **Server Extensions** tab (See **Figure 15**). IIS 5.0 allows remote authoring. These features are for the FrontPage product. Remote authoring allows an author to make changes to a web page and upload it to the server remotely. This poses a critical security issue. This tab allows high level defaults to be set for the remote authoring capabilities of the IIS 5.0 web sites. The options of concern on this property sheet are in the "Permissions" section at the bottom. The default permission is NOT to log authoring actions and NOT to require SSL. It is strongly recommended to select **Log authoring actions**, **Require SSL for authoring** and **Manage permissions manually**.

- Log authoring actions - generates audit trails when someone uploads new pages for a web site. The audit information includes the time an author's action was performed, the author's user name, the web name, the remote host, and per-operation data.
- Manage permissions manually – disables the security-setting functions of FrontPage Server Extensions administrative tools (such as the FrontPage MMC snap-in), so that those tools cannot be used to modify the security settings of the selected web. To make sure that neither the administrator nor anyone else accidentally overwrites custom permissions, disable permissions in front page by checking this box.
- Require SSL for authoring - will force authoring to be done over the SSL protocol, thus the communications will be encrypted. The ability to turn off authoring will be discussed in Chapter 3, individual site properties.

- Allow authors to upload executables - allows the administrator or possibly the intruder to upload scripts or executables to the web server for execution. This option should be left disabled.

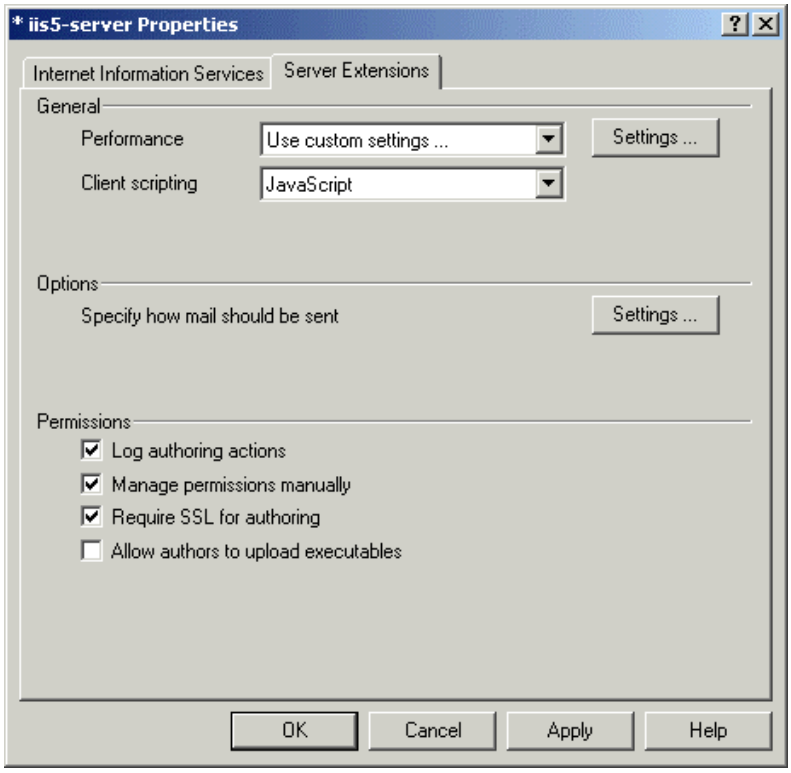



**Figure 15 Server Extensions for Web Server**

## Recommendation Checklist for Chapter 2:



### WWW Master Properties

**Web Site Tab**

- ❑ Ensure Enable logging is selected

**Home Directory Tab**

- ❑ Disable (uncheck) Read, Write, Directory browsing options
- ❑ Ensure Log visits is selected
- ❑ Ensure None is selected for the Execute Permissions drop down box

**Directory Security Tab**

- ❑ If any site hosted by this server will NOT allow Anonymous access, Disable (uncheck) Anonymous access, under Authentication methods and select appropriate authentication method

### FTP Master Properties

**FTP Site Tab**

- ❑ Set appropriate number of connections for max users on FTP server
- ❑ Set maximum seconds for timeout (inactivity), 600 seconds is reasonable
- ❑ Ensure Enable logging is selected

**Security Accounts Tab**

- ❑ Ensure Allow Anonymous Connections is selected
- ❑ Select Allow only anonymous connections

**Home Directory Tab**

- ❑ Ensure Log visits is selected

### Server Extensions Master Properties

- ❑ Ensure Log authoring actions is selected
- ❑ Ensure Require SSL for authoring is selected
- ❑ Ensure manage permissions manually is selected
- ❑ Ensure Allow authors to upload executable is **DISABLED** (**UNCHECKED**)

This Page Intentionally Left Blank

Chapter

3



# Services Installation and Administration

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

## Access Control Methods

### IP address grant/deny restrictions

The first line of defense in the IIS security model is the ability to grant or deny access to the web server based on IP address or Internet domain name of the requesting client. An Internet domain or IP address of certain machines can be specified and either granted or denied access to the web server. When any packet of data is received, its source IP address or domain name is checked against those defined in the “IP Address and Domain Name Restrictions” area of the **Directory Security** tab of the WWW Service property dalog box, and the predefined actions for access are applied to it. When using IP address access control, note that some web clients may be accessing your server through a proxy server or firewall. When this happens, the IP address of the incoming packets will be that of the proxy server or firewall itself, not of the actual user’s client machine. Steps to configure this option for each service are described later in this chapter.

#### Secure Sockets Layer (SSL)

SSL provides privacy, integrity, and authentication in a private point-to-point communications channel. Chapter 4 provides a description for the use of certificates in this environment.

#### Client and Server Digital Signatures

Digital signatures are used both to verify the identity of a user or server and for web servers and browsers to provide mutual authentication, confidentiality of the pages transferred, and integrity of the information in them. More detail can be found in Chapter 4.

### Identification and Authentication

Four options are available in IIS to identify and authenticate users. See **Figure 16**:

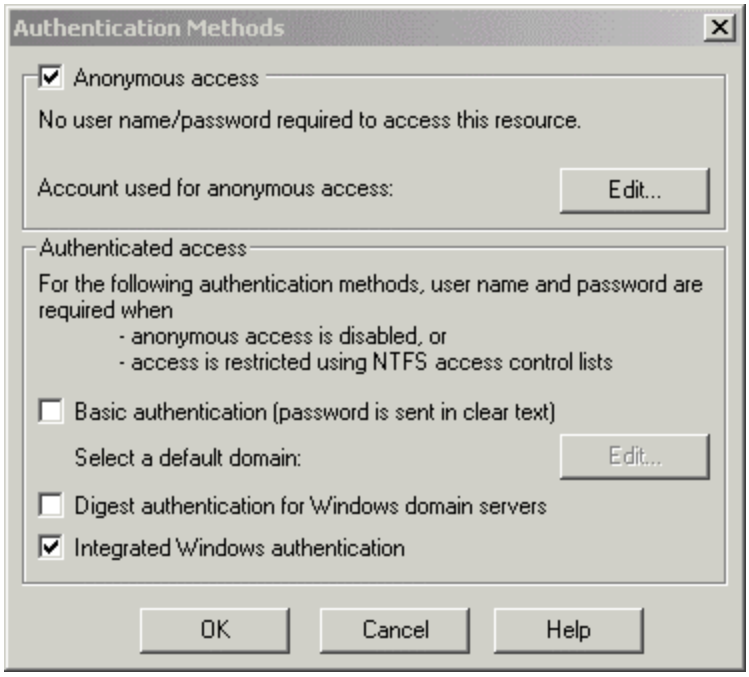



**Figure 16 Authentication Methods Dialog Box**

## Anonymous Access

This is the method most often used when accessing a web server. By default, IIS creates the account IUSR_*computername and* IWAM_*computername,* which is granted local logon (**log on locally**), **access this computer from the network**, and **log on as a batch job** user rights. Whenever an attempt to access server resources over the web is made, the user is automatically logged on using this account. The user can then only access resources based on the privileges granted to this anonymous account. The account name used for this purpose can be changed using the **Edit** button. It is also recommended that the **log on as a batch job** and **access this computer from the network** rights be removed if the site will not require them.

**Note: Whenever the IIS service is stopped and restarted or the system is rebooted, the log on as a batch job and access this computer from the network rights are restored for the IUSR_*computername and* IWAM_*computername* account.**

**Workaround: If it is insisted that the IUSR_*computername* account does not have the log on as a batch job and access this computer from the network rights the following can be done to prevent this. Create a new local user account and change the IIS 5.0 default anonymous account under Anonymous access and authentication control section of the Directory Security Tab of the WWW service or the Security Accounts Tab of the FTP Service. After that is assigned, delete the IUSR_*computername* account.**

**Note: The OS guide makes changes to remove user accounts from log on as a batch job and access this computer from the network user rights. However as the note above states, it is added back after a restart.**

### Basic Authentication

Almost every web browser on the market supports this. Basic authentication sends the user name and password in clear text, which can be stolen by any person with the ability to monitor the traffic. If the site requires the use of Basic authentication, it is recommended SSL be implemented as well. The combination will help maintain access control to sensitive data without risking logon information being intercepted.

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

- Obtain a Server Certificate (Details in Chapter 4)
- Require secure channel when accessing this resource (Details in Chapter 4)
- Enable Basic authentication and disable Anonymous and Integrated Windows authentication for this site (details on configuring these options can be found later in this chapter)

### Digest Authentication For Windows Domain Servers

This offers the same features as Basic authentication but involves a different way of transmitting the authentication credentials. The server will send some information to the client, which will combine that with the username and password, add some other information, and compute a hash. That hash is sent to the server, along with the additional information in cleartext. The server will then take the data, combine it with the username and password and obtain a hash. If the hashes match, the user is authenticated.

When enabling Digest authentication and disabling all other methods, a pop up box will appear stating that user account passwords are required to be stored using reversible encryption. It does not however, tell the administrator that they must explicitly enable a password policy to allow this to occur. Until the password policy is enabled, in effect *and* invoked, Digest authentication does not work. To enable this, use the Windows 2000 group policy editor snap-in. Under Computer Configuration->Windows Settings->Security Settings->Account Policies->Password Policy, there is a Policy of “Store Passwords using reversible encryption for all users in the domain”, which is disabled by default. Enable this setting and the next time the user changes their password, or a new account is created, the password will be stored using reversible encryption.

The Digest Authentication RFC readily admits that it is not a strong authentication mechanism and suffers from many known weaknesses. It is intended only as a replacement for much weaker and even more dangerous authentication mechanisms: Basic Authentication. The RFC has an entire section on security considerations, which does a pretty good job describing the protocol’s major weaknesses, so they are not repeated here. Security considerations addressed in the RFC include:

- Replay Attacks
- Man in the Middle Attacks
- Spoofing
- Password Storage
- Passive Dictionary Attacks
- Active Dictionary Attacks

Most of these security weaknesses are inherent in the protocol, consequently, Microsoft is not able to implement countermeasures and remain compliant.

**Note: digest authentication is only supported in HTTP 1.1 compatible browsers but has the advantage of working through firewalls and proxy servers (unlike NTLM authentication as discussed below). The IIS 5.0 server must belong to a Windows 2000 domain for this option to function.**

### Integrated Windows Authentication

**(formerly called NTLM or Windows NT Challenge/Response)**

This is a method for authenticating users that avoids placing a clear text password on the network. A cryptographic technique using hashing 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. This authentication can use both the Kerberos v5 authentication protocol and its own challenge/response authentication protocol. Only clients with the MS IE 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 non-secure 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 due to the account having insufficient access rights to a resource, 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 Anonymous access is not selected as an option, one of the other two options must be selected.

## Directory Management

In addition to the file and directory permissions established at the operating system level, described in Chapter 1, IIS 5.0 introduces application level permissions. "Read", "Write", "Directory Browsing", "Scripts only" and "Scripts and executables" are available access permissions for directories containing WWW and FTP content.

- Read permission - allows the contents to be viewed and passed to the client browser for rendering.
- Write permission - enables clients with browsers that support the "PUT" feature of the HTTP 1.1 protocol standard to upload files to the server or to change the content in a write-enabled file. This is generally not granted unless the administrator has a very specific need to make this type of access available.
- Directory browsing - allows a client to view all the files in a directory. Unless this is a public FTP server this option should be disabled.

- Scripts - restricts execution to scripts only, which is necessary if you are using ASP or CGI type programs. The file extensions for these scripts must be previously mapped to scripting applications (such as Perl and ASP).
- Scripts and Executables - allows the execution of not only ASP, CGI and other scripting languages, but it also allows EXE and DLL programs to run. This is a very dangerous feature and is NOT recommended unless absolutely required and appropriate permissions set. This in combination with the write privilege can lead to a compromised server very quickly.

These permissions are set through the WWW and FTP site properties dialog boxes. Images of the web site properties and FTP site properties are shown under the Figure 19 Web Site Home Directory Default Properties

and Figure 30 FTP - Home Directory Tab headings.

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

## Ability to Implement Restrictions on Virtual Servers and Directories

Virtual servers allows configuration of one computer running IIS to support several domain names (or web sites). When setting up a virtual server, either Host Header Names (HHN) or IP addresses are needed for the primary server and for each virtual server to be created. This makes the installation look like several web servers when viewed from the Internet, when only one copy of IIS is actually running, with possibly only one network card (using HHN's).

IIS allows the administrator to supply an alias for directory paths that contain information to be published. This alias is commonly referred to as a virtual directory and is used in URLs. As far as visitors to the site are concerned, virtual directories are subdirectories branching from the main /wwwroot directory. Security is enhanced with virtual directories because it adds another level of abstraction to the site, altering the way in which Internet users access the information. Read, Write, Directory Browsing, Scripts only, and Scripts and executables are IIS 5.0 permissions, which can be applied to a virtual directory and all of the files and folders contained within it. Read permission allows a client to download files stored in a virtual directory or subdirectory. Only directories that contain information to be published or downloaded should have Read permission set. To prevent clients from downloading executable files or scripts, it is recommended that they be located in separate directories without Read permission. Instead, these virtual directories should have Scripts only or Scripts and executables permission so web clients can run them.

**Note**: **If Read permission is also enabled, users may be able to look at the information contained within your scripts, some of which may be sensitive (i.e., passwords).**

## Summary of Web Server Configuration Issues

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

- Decide how access is to be controlled on your web site and set restrictions based on IP address/groups or Internet domains.
- Determine if SSL and Certificates are required in your environment.
- Select an authentication method. Anonymous access is the most common method. Do not use Basic authentication unless your site implements SSL.
- Create directories with Read only NTFS permission for the WebUsers group. These directories will also be assigned IIS 5.0 Read only permission during the WWW/FTP site setups. These directories will store the data that is to be made available to client browsers for viewing or downloading only.
- Create a directory with Read & Execute NTFS permission only for the WebUsers group. This directory will be assigned Scripts only permission during the WWW site setup. This directory will store executables, such as scripts.

## World Wide Web (WWW) Services



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

### Web Site Tab

See **Figure 17.** Highlight the web site to be configured in the ISM, then right-click and select properties to access this dialog box.

**Web Site Identification** – Specify a Description - the name that will be used in the ISM tree view to identify this web site; select the IP address of the network interface card (NIC) to serve the site to; a TCP Port and SSL Port (if these are changed from their defaults, the administrator must notify users or they will not be able to connect); and Advanced options, where multiple domain names or host header names can be mapped to a single IP address using the Host Header Name box. More information on this topic can be found in the IIS online documentation (Naming Web Sites).

**Connections** – Allows the administrator to limit the number of simultaneous accesses to the web site and to set a connection timeout. Timeout settings are recommended to assist in preventing a possible denial of service attack.

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

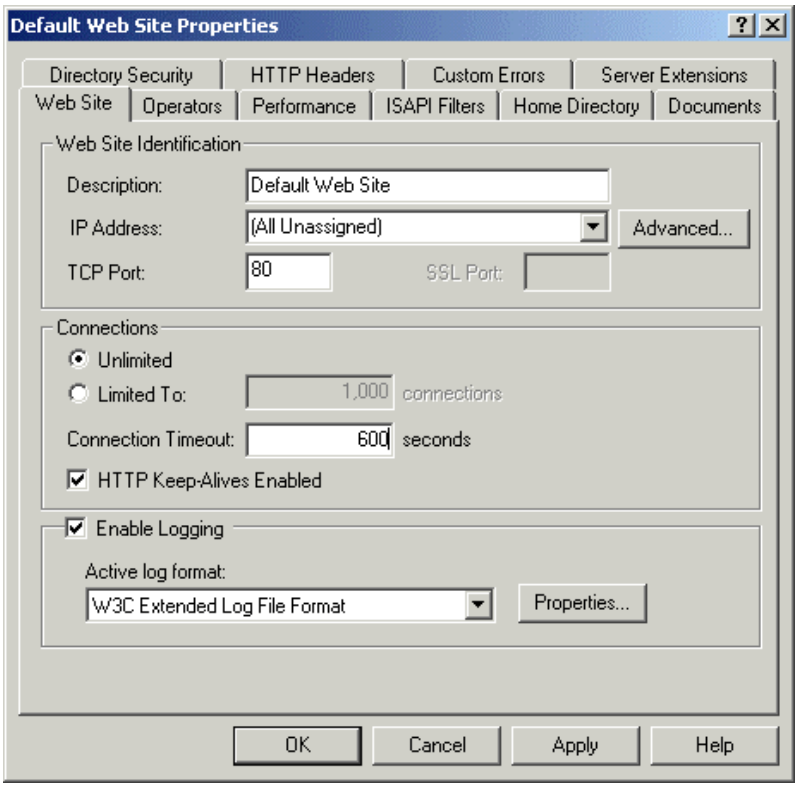



**Figure 17 Web Site Identification Property Sheet**

## Operators Tab

**Web Site Operators** – See **Figure 18**

This is where the administrator designates which Windows 2000 Server group/user accounts to administer the web site. This should be a group (if server is in a domain) and the accounts within the group should not necessarily require Windows 2000 Administrative permissions. Operators can work only with the properties that affect the web site for which they were created. They cannot access the properties that control overall IIS setup, the Windows 2000 server operating system that hosts IIS, or the network on which the system runs. The following are some functions that can be performed by Web Operators.

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

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

Only members of the Windows 2000 Administrators group can perform the following tasks related to IIS:

- Change application isolation
- Create virtual directories or alter their paths
- Change the Anonymous Username and Password
- Alter the identification or configuration of a web site

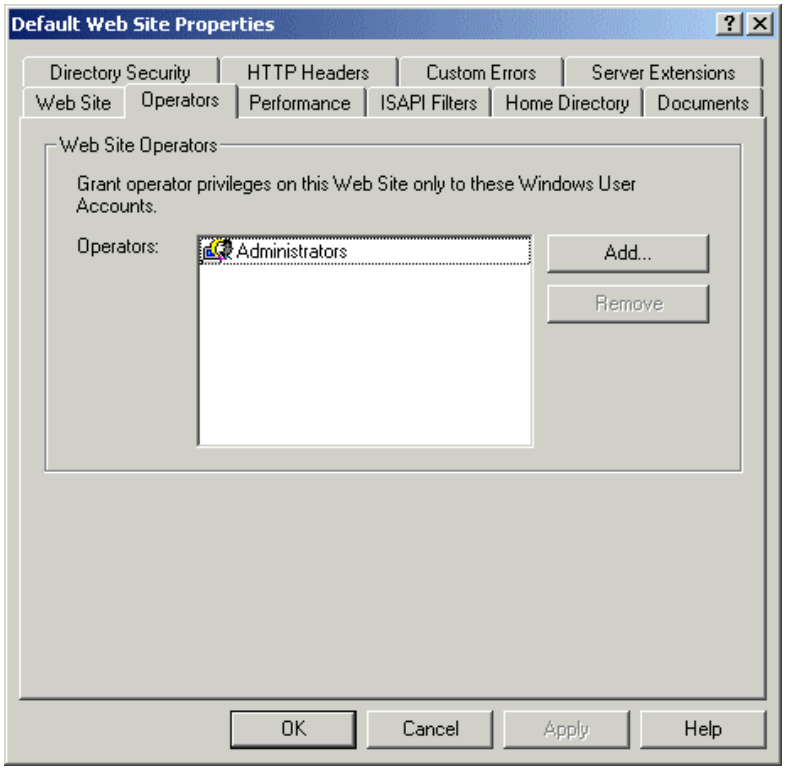



**Figure 18 Operators Tab for Default Web Site Properties**

## Home Directory Tab

See **Figure 19**

The Home Directory property dialog box allows the administrator to look at and change settings that control web content delivery, access permissions, and Active Server Page configuration and debugging. Options that are available 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.

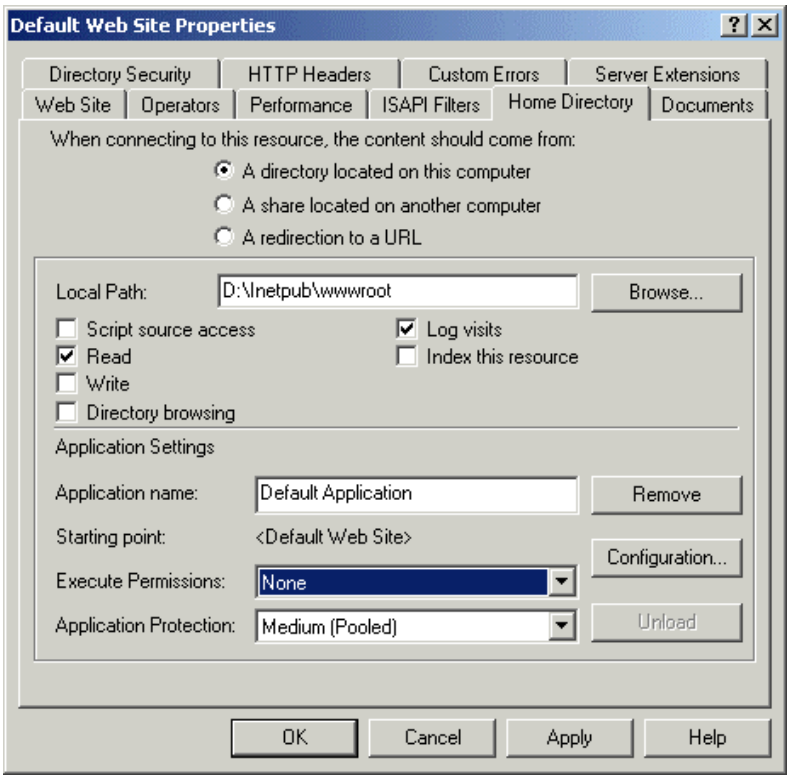



**Figure 19 Web Site Home Directory Default Properties**

**Access Permissions**

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

**Content Control**

**Script source access** – Users can access source files. If Read is selected, then source can be read, if Write is selected, then source can be written to. Script source access includes the source code for scripts, such as the scripts in an ASP application. This option is recommended to remain unchecked. This option is not available if neither Read nor Write is selected. This feature is only applicable and necessary when utilizing remote authoring, (i.e. WebDAV).

**Directory browsing**– 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. Make sure this option is NOT selected.

**Log visits** – It is recommended to enable logging, which is the default. This ensures that all visits to this directory are logged into the log file.

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

**Application protection** – This option enables the administrator to isolate a web-based application by having it run in a memory area that is separate from the web server software and/or other applications. It is recommended that this be set to medium or high. If set to medium, protection is provided to help preclude applications from inadvertently causing problems with the web server software. If set to high, the application will be run in a completely separate memory space that will not affect other applications either.

**NOTE: Server-side include (SSI) and Internet Database Connector applications cannot be run in a separate memory space from the web server's memory space.**

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

- **None** - prevents programs or scripts from executing.

- **Scripts** – 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).

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

## Application Configuration

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 High application protection is selected); and App Debugging. Information regarding the security of App Mappings is covered in the Script Mappings section of Chapter 4. The Script Mapping section also plays a critical role in protecting the IIS server from potential compromise.

## App Options Tab

These options can be configured at the web site, virtual directory, and directory level. See **Figure 20**:

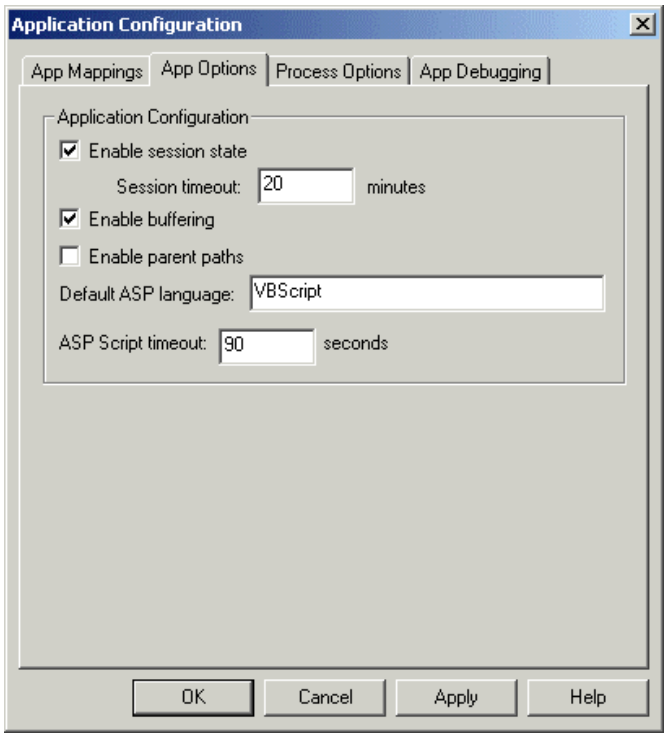



**Figure 20 Application Configuration App Options Tab**

**Enable session state** and **Session timeout** – Check this option so that Active Server Pages (ASPs) create a new session for each user who accesses an ASP application. This lets you identify the user across several ASP pages in your application. When the user does not request a page or refresh within the session timeout period, the session will be terminated. Set an “ASP Script timeout” value so that if a script does not complete execution within the allotted time, an entry will be made into the Windows 2000 Server Event Log and execution of the script will stop. Setting timeout values will help prevent a denial of service attack.

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

## Process Options Tab

Enable **Write unsuccessful client requests to event log (only available when using high isolation).** See **Figure 21**:

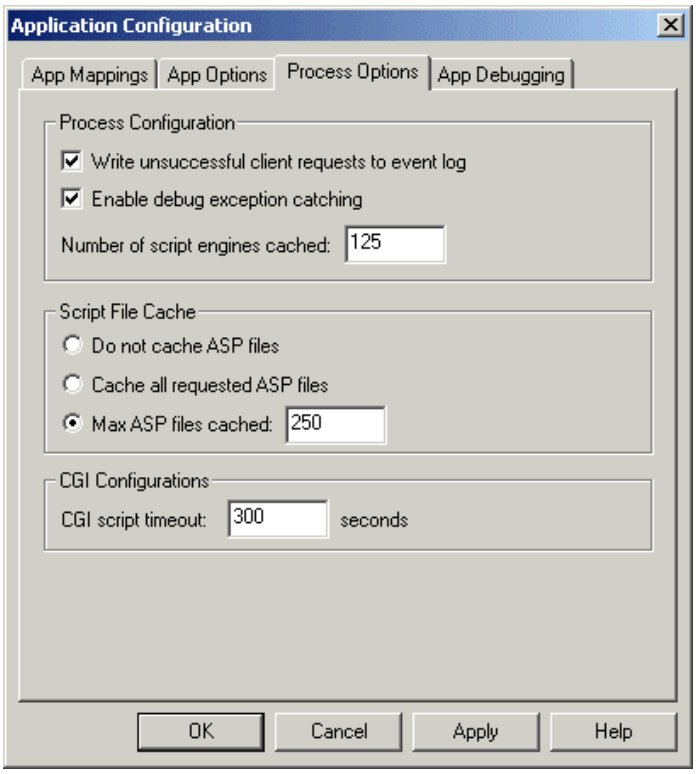



**Figure 21 Application Configuration Process Options Tab**

## Documents Tab

It is recommended that the administrator always provide a default document that all users will see when accessing the site(s). This helps prevent displaying the directory structure of the site to a user unintentionally. This happens when the Directory browsing option is left enabled. See **Figure 22**:

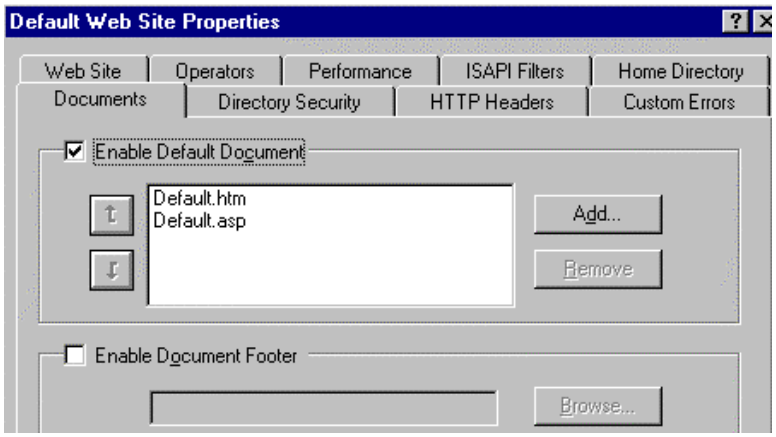



**Figure 22 Documents Tab**

## Directory Security Tab

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. See **Figure 23**:

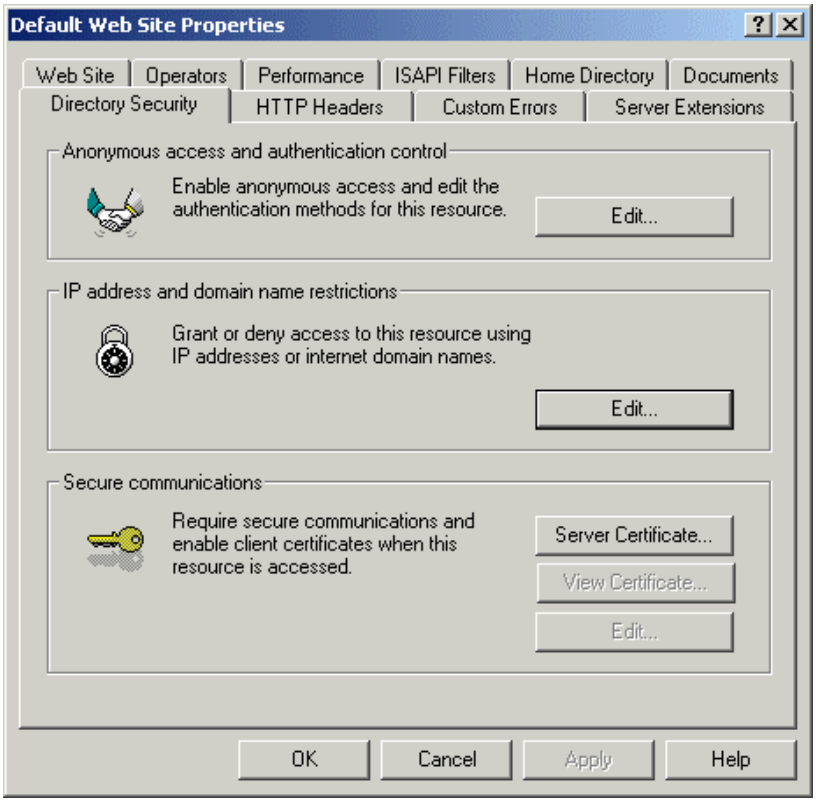



**Figure 23 Directory Security Tab**

**Anonymous access and Authenticated access** – The options presented on this property dialog box are described at the beginning of this chapter. See **Figure 24**:

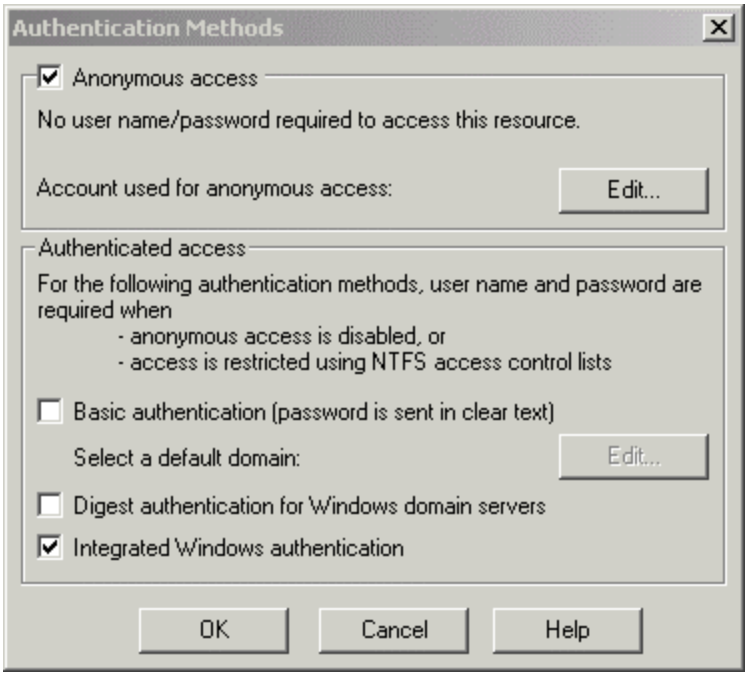



**Figure 24 Authentication Methods Dialog Box**

**IP Address and Domain Name Restrictions** - This option allows the administrator to specify who can access your WWW site based on IP address. There are two options on this property dialog box, **Granted Access** and **Denied Access**. **Granted Access** allows all computers access to your resources except those specifically identified by IP address. **Denied Access** restricts access to resources to ONLY computers with IP addresses specifically listed, requests from any other computers are denied. Three options are available when specifying computer IP addresses: **single computer**, where administrator specifies a single IP address; **Group of computers**, where administrator specifies the network ID and subnet mask; or **Domain name** (a warning message appears stating this option will cause a significant degradation in performance, due to the need to perform a DNS reverse lookup on each connection request). See **Figure 25**:

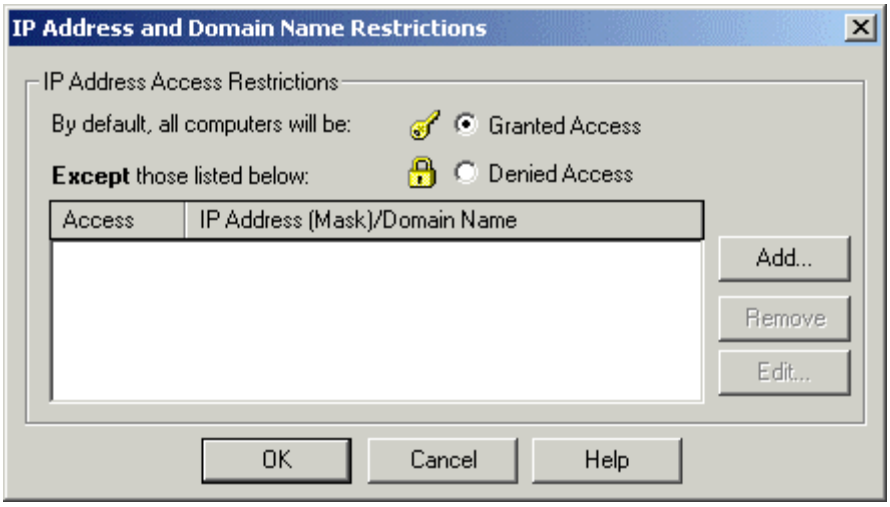



**Figure 25 IP Address and Domain Name Restrictions**

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

## Server Extensions Tab

IIS 5.0 allows remote authoring. For every applicable web site on the IIS server, it is our strong recommendation that the **enable authoring** option be disabled. This feature would allow the FrontPage product to make changes to a web page and upload the new page to the server. See **Figure 26:**

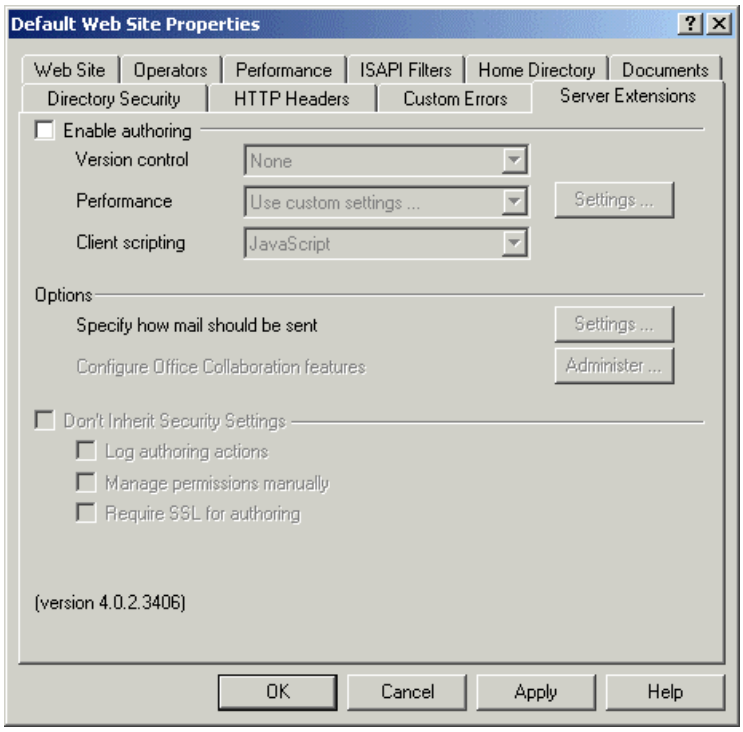



**Figure 26 Server Extensions Tab**

**Version control** – Allows the administrator to keep track of who is modifying web content, identifying any changes, and prevent one author's changes from erasing another's. If authoring is enabled, version control should be enabled as well.

**Don't inherit security settings** – The ability is given to inherit or not inherit the security settings of the global master properties (identified in Chapter 2). Although these options are selected on the master property sheet, in the event that authoring is enabled, it is recommended to explicitly set them again.

## File Transfer Protocol (FTP)

FTP allows clients to transfer files to and/or from an FTP server. Although much of the FTP functionality on the Internet is being replaced by the WWW service, FTP is still in common use. It is recommended to configure the FTP server so that uploading of files to the server **is prohibited**. If uploads need to be allowed to come into the server, create a separate directory (a "drop box") called \INCOMING to receive these files. Also, monitor this directory regularly as part of your security policy.

### Organizing FTP Directories

It is recommended that FTP directories be organized for the users. For FTP downloads, the directory names should reflect directory contents. For example, device drivers could be organized within directories with operating system names. Make sure FTP download directories are configured for Read ONLY permission. Create a "drop box" directory for temporary storage of files written to the FTP server. Files written to this directory should be examined for suitability and security risk then placed in the directory for downloading by others. Access to the "drop box" is limited to the Write permission for the anonymous user's account. Conversely, the FTP directory configured for user downloads is set to

Read ONLY. This may be a little inconvenient because the anonymous users will not be able to look at files uploaded by others, but it will prevent them from altering or deleting those files. This will also prevent unauthorized users from using your site to store illegal software, pornography and hacking tools. A web site administrator should review files uploaded to the drop box and place them in the Read ONLY directory for downloading by others.

## FTP Site Tab

Contains the same properties as the **Web Site** tab, but apply specifically to your FTP service. The administrator can set the FTP site identification information, control the number of connections, and set a connection timeout. It is recommended that the **Enable Logging** option be selected and assigned a connection timeout value to allow better control potential of DoS attacks and server resource consumption. See **Figure 27**:

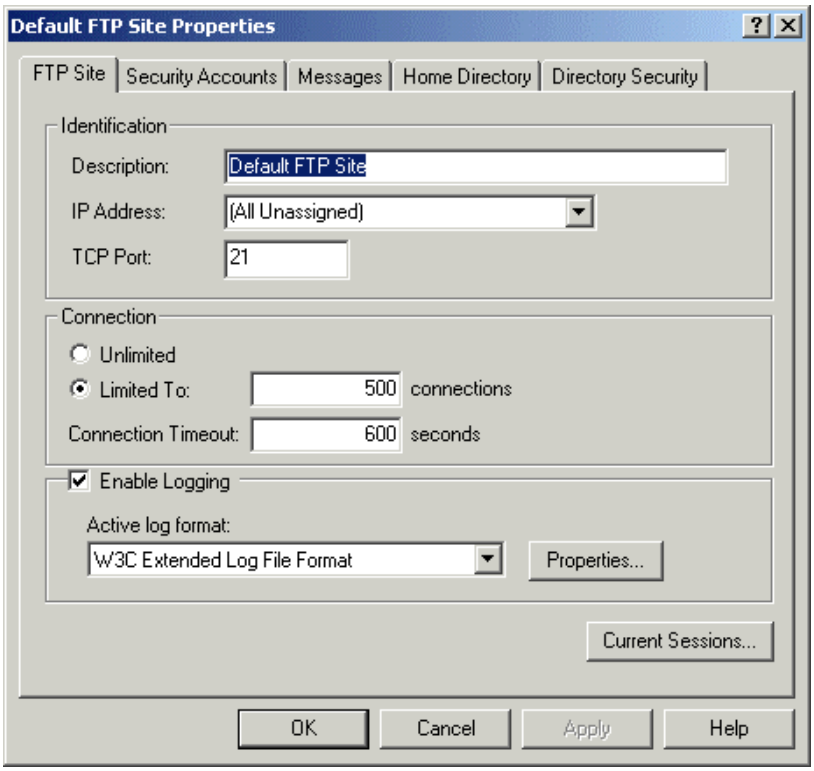



**Figure 27 FTP Site Tab**

## Security Accounts Tab

This tab is used to configure anonymous FTP access and FTP site operators. It is recommended that the **Allow only anonymous connections** box be checked 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. Please note that even with this option checked there is nothing to prevent a user from *attempting* to log on with user name/password – this needs to be carefully factored into a decision to stand up a FTP server. A user in the habit of entering a user name/password combination will probably do so at the FTP prompt. Even though the connection attempt will be rejected, the damage has already occurred as the password was sent in the clear. When users log on anonymously they typically use their e-mail address as their password. The FTP server then uses the IUSR_*computername* account as the logon account for permissions. Integrated windows authentication is not available for the FTP service. The lower portion of the property dialog box is used to designate which user accounts will be administered to the FTP site. It is recommended that user accounts be used, since IIS 5.0 does not allow the inclusion of created local groups (unless it belongs to a domain, then the administrator can include domain local/global/universal groups). See **Figure 28**:

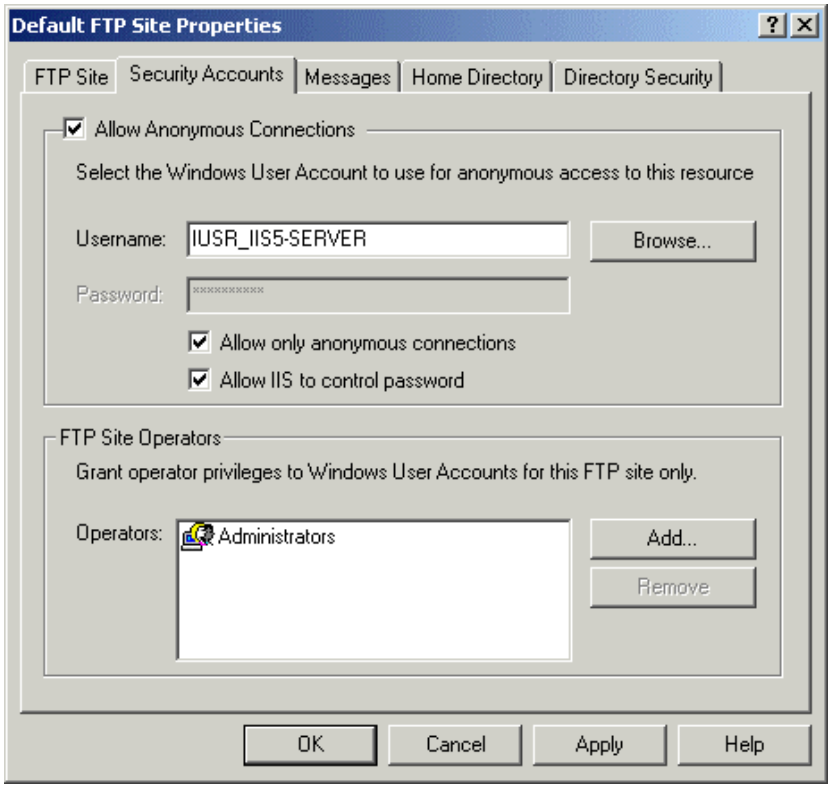



**Figure 28 FTP- Security Accounts Tab**

Select the **Allow IIS to control password** option to match the anonymous FTP logon user name and password (typically IUSR_*computername*) with the account created in the users section of the Computer Management Snap-in. If IUSR_*computername* is not the anonymous user account, make sure the anonymous user account defined is an account

on the local computer. This will help ensure that the web server is available if the domain controller is inaccessible and the anonymous account is a domain account.

## Messages Tab

There are three types of messages that can be displayed to the user; Welcome, Exit, and Maximum Connections. It is recommended that a Welcome message in the form of a Security Banner be displayed to any user connecting to your FTP server. Exit messages can be used to display notices to users upon connection termination. In the event the maximum number of connections has been reached, the Maximum Connections message can be used to notify the user of this event. See **Figure 29**:

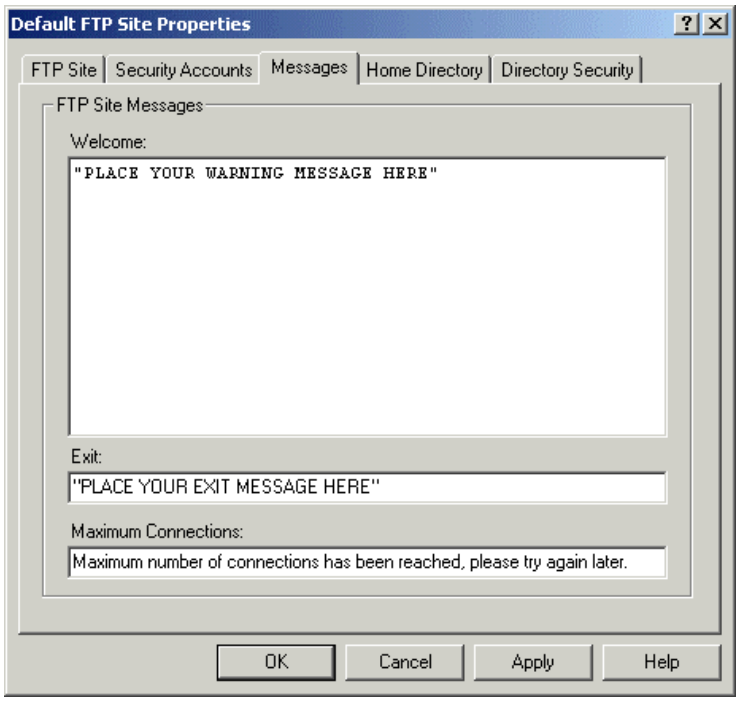



**Figure 29 FTP - Messages Tab**

## Home Directory Tab

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

It is recommended that this directory have Read access ONLY. If your site requires users to upload data, create two directories beneath the “ftproot” directory. One with Read ONLY access to store data made available to all users for download, and one with Write Only permission to be used as a “drop box” for users to upload data into. A web operator could then be responsible for reviewing the data in the “drop box” prior to making it available to all users in the Read ONLY directory. See **Figure 30**:

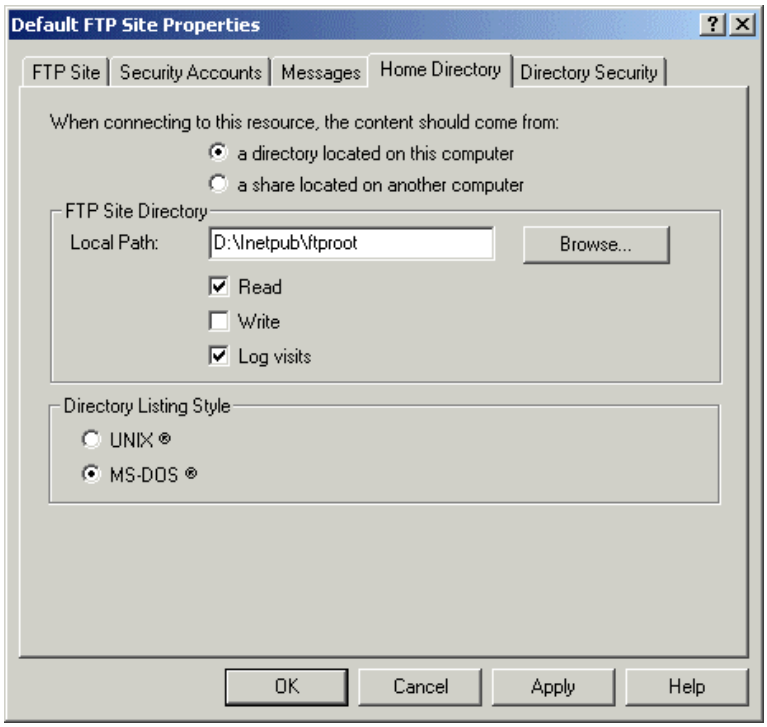



**Figure 30 FTP - Home Directory Tab**

## Directory Security Tab

This tab (See **Figure 31**) will allow specification of who can access your FTP site based on IP address. There are two options on this tab, **Granted Access** and **Denied Access**. **Granted Access** allows all computers access to your resources except those specifically identified by IP address. **Denied Access** allows ONLY those computers with listed IP addresses access to your resources and denies all other requests. Three options are available when specifying computer IP addresses: **single computer**; **group of computers** (where the network ID and subnet mask is specified); or **Domain Name** (be careful when choosing this option, a warning message appears stating this option will cause a significant degradation in performance, due to the need to perform a DNS reverse lookup on each connection request).

If there is a defined set of users that will be permitted to access the ftp directory, it is recommended to select **Denied Access**. This will permit only specified computers access to the data within the ftp directory and deny access to all others.

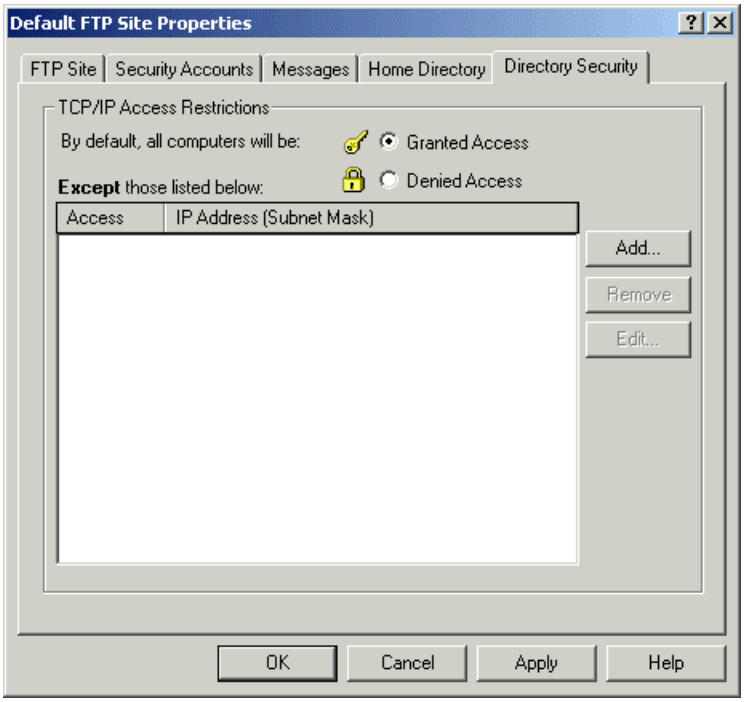



**Figure 31 FTP - Directory Security Tab**

## Simple Mail Transfer Protocol (SMTP)

IIS 5.0 includes an SMTP mail service used to transfer Internet messages between servers. 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 fully compatible with most SMTP servers and clients. This service is intended for use with building Internet applications that utilize SMTP. 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. Because of this, the web server listens on the standard SMTP port (tcp 25), which makes it vulnerable to attack. Shown below are dialog boxes available for configuring SMTP properties. Access the dialog boxes by highlighting the SMTP site on the Internet Service Manager and selecting **properties** on the **Action** pull down menu.

### General Tab

This tab (See **Figure 32**) gives the administrator the ability to control several options of the general SMTP server. Ensure **Enable Logging** is checked and configure the logging properties as you would the services discussed previously.

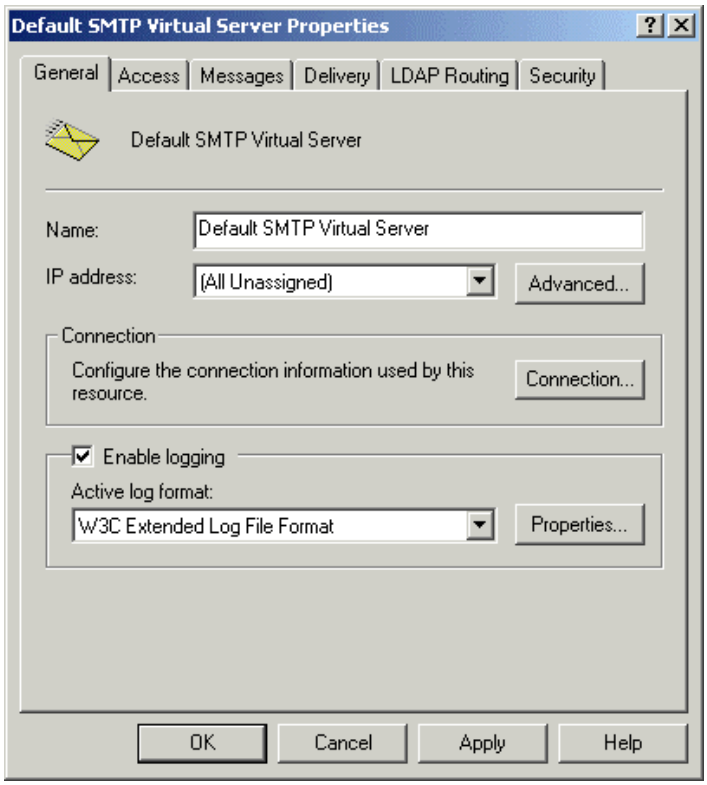



**Figure 32 SMTP - General Tab**

## Access Tab

To access the Authentication dialog box, simply click on the **Authentication** button. The authentication options are similar to those mentioned in the other services (See **Figure 33**). An explanation of each follows. Depending on the use of the server different recommendations would be necessary, thus a single recommendation is not presented.

**Anonymous access –** Defined earlier in this chapter.

**Basic authentication –** Defined earlier in this chapter.

**Requires TLS encryption –** Selecting this option will encrypt the incoming messages to the server using Transport Layer Security.

Default domain – To use Basic authentication a default domain will be appended to the username supplied. This section gives you the ability to assign the default domain.

**Windows security package –** When using a mail client that supports this authentication method, such as Microsoft Outlook Express (IE 5.0), the authentication is done in a more secure manner. The Windows security package uses a cryptographic technique that does not transmit the actual passwords across the network.

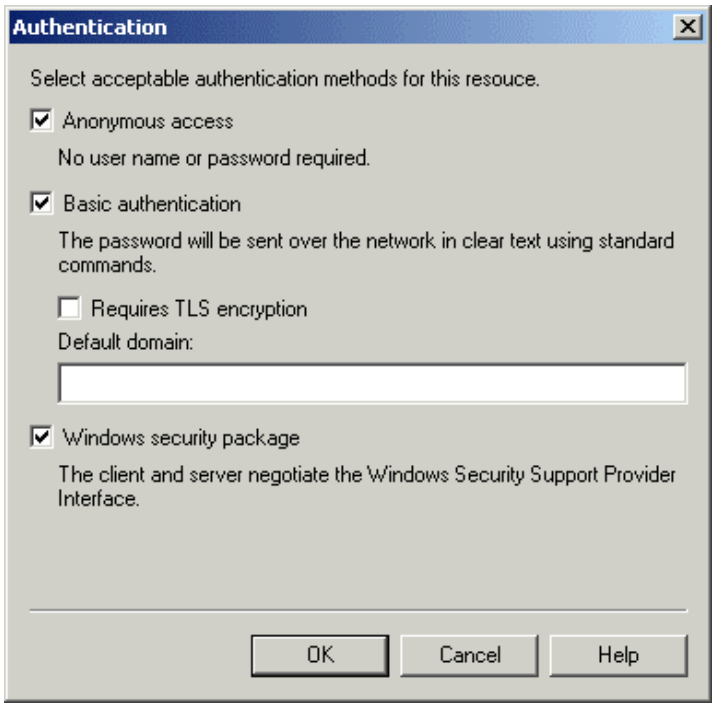



**Figure 33 SMTP - Authentication Dialog Box**

Microsoft SMTP Service supports the use of Transport Layer Security (TLS) for encrypting transmissions. The use of TLS can be required for all incoming connections through the Secure Communication section of the **Access Tab**. To use TLS for the server, key pairs must be created and key certificates must be configured. Select the **Certificate** button, which will allows the creation of a certificate request to send to a CA. Once the certificate is received, the administrator can require encryption by clicking on the **Communication** button of the Secure Communication section of the **Access Tab**. If the TLS encryption will be used select the **Require 128-bit encryption** option shown below (See **Figure 34)**. This will maximize the protection of the data between the web clients and the server from unauthorized view and modification.

**Figure 34 Security Dialog Box for SMTP**

The Connection dialog box can be accessed by clicking on the connection button on the Access Tab from the SMTP Virtual Server Properties sheet. The connection box works the same as the domain blocking from the WWW and FTP services. If this machine will be an Internet server, then select **All except the list below**. If the server will only be accessed from computers within your network domain, select **Only the list below** and add your network class domain to the allowed list. See **Figure 35**:

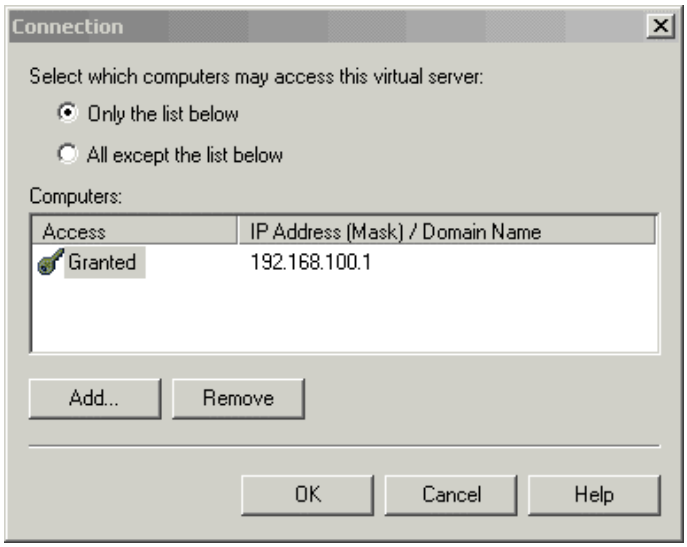



**Figure 35 Connection Dialog Box for SMTP**

The **Relay** button on the **Access Tab** for SMTP Virtual Server Properties provides the capability to restrict which computers can drop off messages for relay to other SMTP servers. Configuring this option is similar in concept to configuring the IP Address and Domain Name Restrictions property. Select either **Only the list below** to allow only specifically defined computers to relay through this service, or **All except the list below** to allow all computers to relay requests. Be careful when configuring this option. Accepting a request to relay could possibly allow spammers to forward mail through your server and have it appear as though that is where it originated. It is recommended that you select **Only the list below** and not allow any exceptions. If the administrator chooses to allow the server to become a Mail Relay, only allow authenticated computers by selecting the option **Allow all computers which successfully authenticates to relay, regardless of the list above**. Authentication is accomplished through Integrated Windows authentication or Basic authentication set on the SMTP mail directory. See Figure 36.

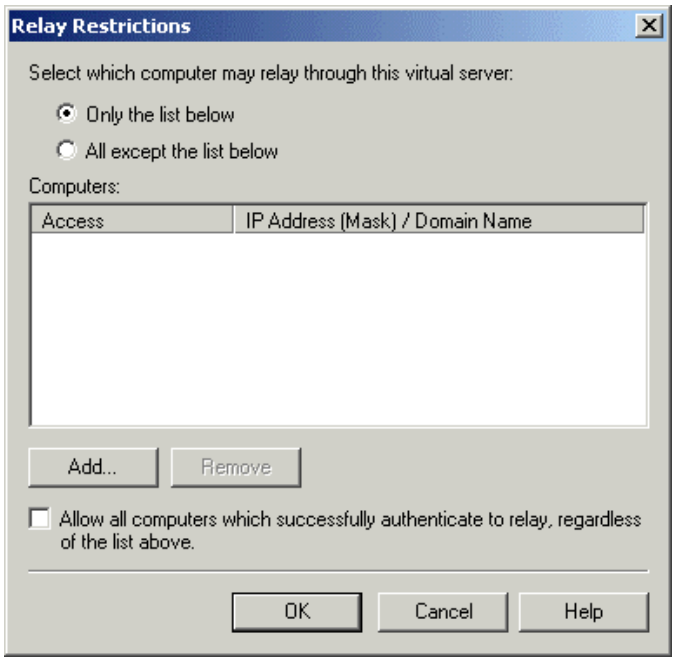



**Figure 36 Relay Restrictions for SMTP**

To set authentication for outgoing mail, click the **Outbound Security** button on the **Delivery Tab** located on the SMTP Virtual Server Property sheet. For outgoing mail, the administrator can specify what authentication method will be required by the receiving SMTP server and whether or not to use TLS encryption. Of course the authentication/encryption choices must be compatible with the server at the other end of the connection, which makes setting any security on outbound messages impractical if the server is sending messages to a heterogeneous environment such as the Internet. The specific options available on dialog box have been explained earlier in this chapter.

Particularly if operating over an Intranet and if your server is sending any type of sensitive information, it is recommended to use at least minimum security such as Basic authentication with TLS encryption. See **Figure 37**:

**Figure 37 Outbound Security Dialog Box for SMTP**

## Security Tab

The Security tab allows the definition of a user or group responsible for managing this service. Unlike the WWW and FTP services, there is the ability to create local groups to manage user accounts. This local group can be included as an operator for the SMTP server and is the recommended method. Note: If utilizing a domain and domain groups do not utilize local groups here for ease of administration. See **Figure 38**:

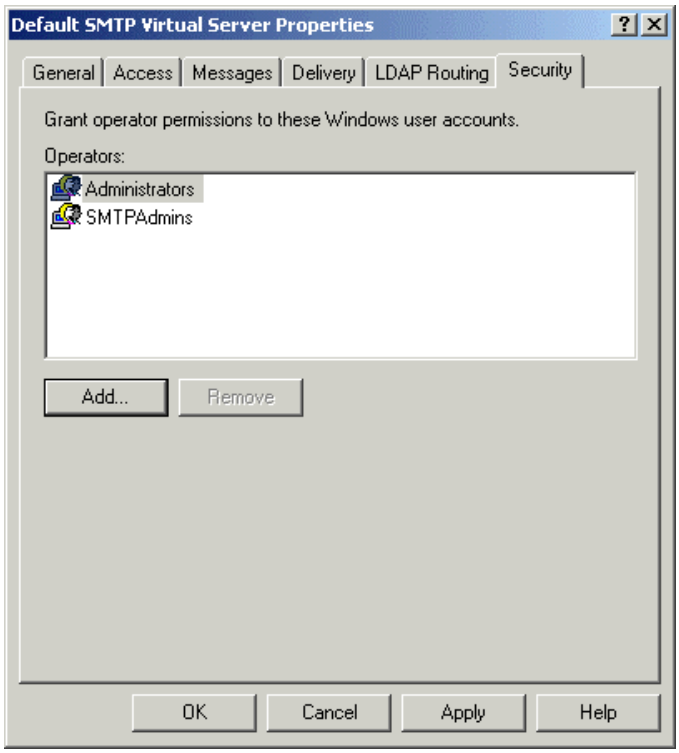



**Figure 38 SMTP - Security Tab**

## Network News Transfer Protocol (NNTP)

IIS 5.0 includes an NNTP news service used to host USENET-style discussion groups on an intranet/extranet. It supports multiple authentication methods, IP/domain blocking and news feed downloads. Shown below are dialog boxes available for configuring NNTP properties. Access the dialog boxes by highlighting the NNTP site on the Internet Service Manager and selecting **properties** on the **Action** pull down menu.

**General Tab -** Make sure **Enable logging** is selected. See **Figure 39**:

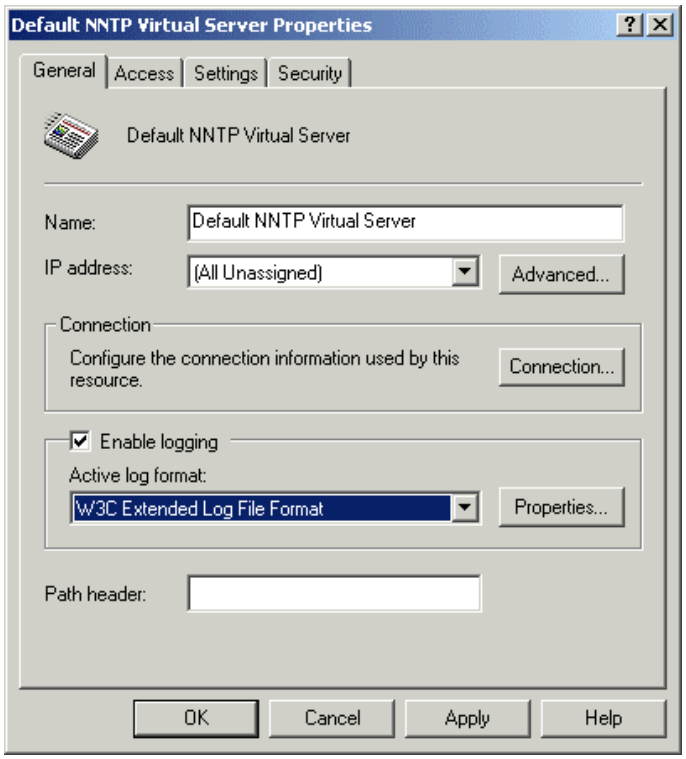



**Figure 39 NNTP - General Tab**

**Authentication Methods dialog box** – See **Figure 40**. This box can be reached by clicking the **Authentication** button on the **Access Tab** from the NNTP Virtual Server Property Sheet. This sheet gives the ability to choose the authentication method to use for clients connecting to your news server. Due to the nature of news messages and the ability to post messages using falsified information, it is highly recommended that the box for **Allow anonymous** be cleared if the news server is outside the security perimeter (i.e. firewall). This is often an overlooked feature and causes a company to allow the whole world to use their news server to post messages (including vulgar, explicit material and also pirated software). If the news service is being allowed for only internal users, put the server inside the security perimeter (i.e., firewall, border router) and then select the option for authentication that is compatible with all the clients that you use. If the administrator has the ability to obtain a server certificate, SSL would be an excellent choice, this way there is less dependence on the client platform.

By using authentication other than anonymous, there is better granularity over the material that different users or groups of users can see. This allows easier administration and the ability to customize discussion groups for specific departments and or special project groups.

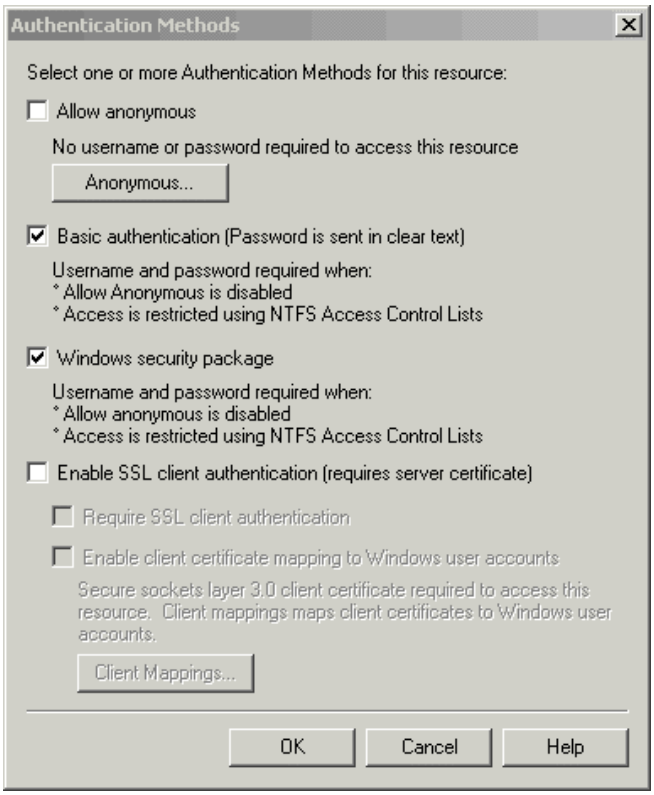



**Figure 40 NNTP Authentication Methods**

The Connection dialog box (See **Figure 41**) can be accessed by clicking on the **connection** button on the Access Tab from the NNTP Virtual Server Properties sheet. The connection box works the same as the domain blocking from the SMTP, WWW and FTP services. If this machine will be an Internet server, select **All except the list below**. If the machine will be used by computers within your network domain, select **Only the list below** and add your network class domain to the allowed list.

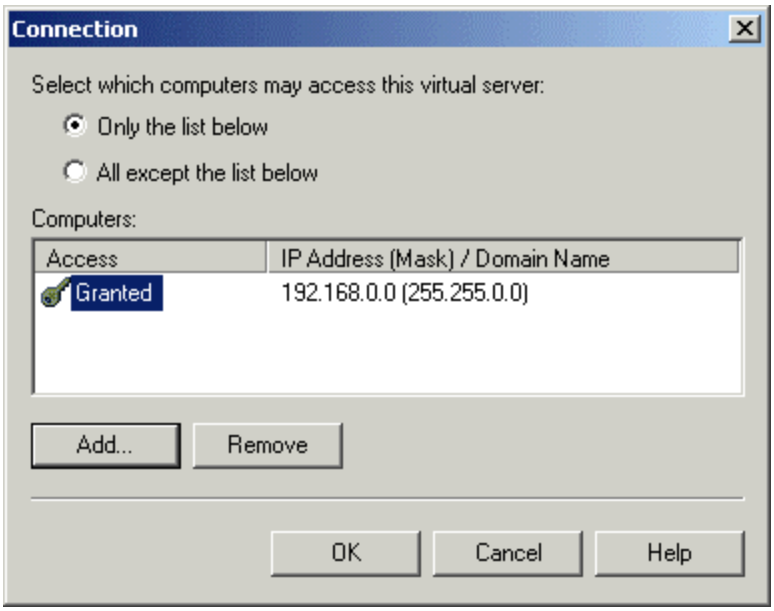



**Figure 41 NNTP - Connection (domain blocking)**

## Settings Tab

On the Settings tab (See **Figure 42**) there are several customizable features for size of messages, who is allowed to post, server pulling, and SMTP server and moderator information. There will be two aspects of this screen discussed.

The **Allow servers to pull news articles from this server** is an important option, especially if the machine will be located outside the security perimeter. It is recommended that this option be cleared. This will stop messages posted to the server from being propagated throughout the world's NNTP servers. This is especially true if it is used for internal messaging. If users and news feeders will not be allowed to delete news groups or messages, it is recommended to clear the **Allow control messages** check box. Malicious users have been known to use control messages to create problems with mis-configured or unpatched news servers.

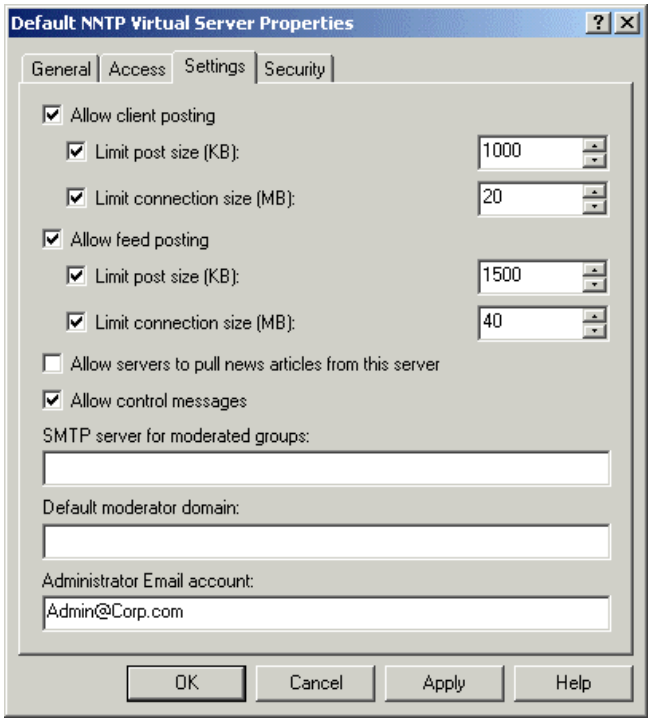



**Figure 42 NNTP - Settings Tab**

## Security Tab

The Security tab (See **Figure 43**) allows the definition of a user or group responsible for managing this service. Unlike the WWW and FTP services, there is the ability to create local groups to manage user accounts. This local group can be included as an operator for the NNTP server and is the recommended method. Note: If utilizing a domain and domain groups do not utilize local groups here for ease of administration.

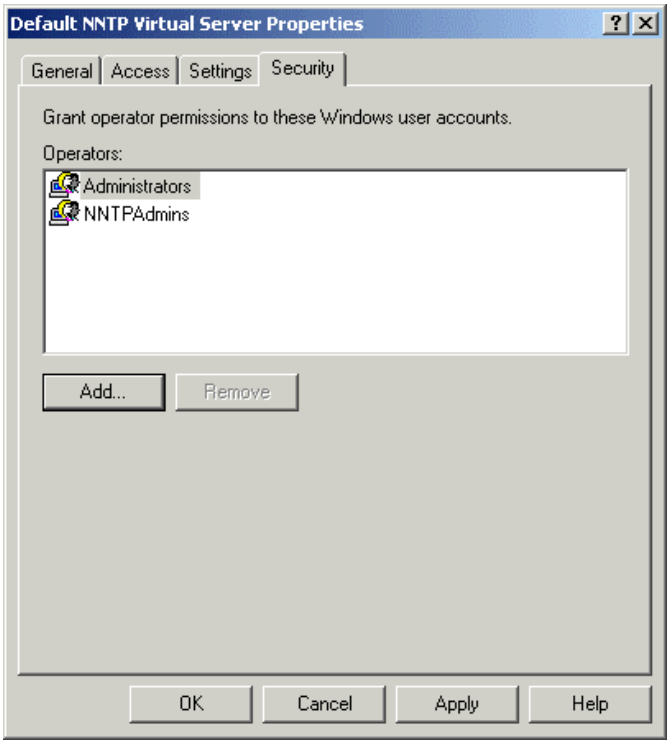



**Figure 43 NNTP - Security Tab**

[redacted]

## Recommendation Checklist for Chapter 3:



### WWW Properties

- ❑ Remove IUSR_*computername* **logon as a batch job** and **access this computer from the network** user rights, (if required, implement workaround)
- ❑ Identify need for SSL
- ❑ Identify IP address/groups or Internet domains for restrictions, if any
- ❑ Organize directory structure for file types (html, ASP, scripts, executables)
  - o Set NTFS permission for the WebUsers group. Use this group for all permissions with NTFS

**Web Site Tab**

- ❑ Ensure Enable logging is selected

**Operators Tab**

- ❑ Include local accounts of persons to administer site(s), or domain groups

**Home Directory Tab**

- ❑ Html, ASP have READ access
- ❑ Scripts, executables have Script or Scripts and executables access only, NOT READ
- ❑ Disable (uncheck) Directory browsing option
- ❑ Disable (uncheck) Script source access option
- ❑ Ensure Log visits is selected
- ❑ Ensure None is selected for the Execute Permissions drop down box

**App Options tab (from configuration button)**

- ❑ Enable session state and timeout
- ❑ Set session timeout period
- ❑ Disable (uncheck) Enable parent paths

**Process Options Tab (If using application protection in high {Isolated} mode)**

- ❑ Enable Write unsuccessful clients requests to event log

**Documents Tab**

- ❑ Provide a default document for all web sites

**Directory Security Tab**

- ❑ If using Basic authentication: Implement SSL
- ❑ If any site hosted by this server will NOT allow Anonymous access, Disable (uncheck) Anonymous access, under Authentication methods and select appropriate authentication method
- ❑ Set any IP/Domain name restrictions that will be utilized to protect the site(s)

**Server Extensions Tab**

- ❑ Disable (uncheck) enable authoring on web site(s)

**If authoring is permitted**

- o Select Don't inherit security settings
- o Enable Log authoring actions, Require SSL for authoring and Manage permission manually

## FTP Properties

- ❑ Configure so uploading is prohibited
- ❑ Organized directory structure for users
- ❑ Assign all NTFS permission for the FTPUsers group
- ❑ All download directories are read only

**If upload is necessary**

- o Create DROPBOX directory and give write permissions only

**FTP Site Tab**

- ❑ Set appropriate number of connections for max users on FTP server
- ❑ Set maximum seconds for timeout (inactivity), 600 seconds is reasonable
- ❑ Ensure Enable logging is selected

**Security Accounts Tab**

- ❑ Ensure Allow Anonymous Connections is selected
- ❑ Select Allow only anonymous connections

**Messages Tab**

- ❑ Put in Warning banner for welcome message

**Home Directory Tab**

- ❑ Ensure Log visits is selected
- ❑ Ensure read only permissions for the ftproot directory (IIS permissions)

**Directory Security Tab**

- ❑ Define the set of IP/domain name restrictions for the FTP site(s)

## SMTP Properties

**General Tab**

- ❑ Ensure enable logging is selected

**Access Tab**

**Authentication**

- o Enable the required authentication method

**If TLS is selected**

**Communications**

- o Select Require secure channel
- o Select Require 128-bit encryption

**Connection**

- o Define the set of IP/domain name restriction for the SMTP server if required

**Relay**

- o Select Only the list below
- o Deselect Allow all computers which successfully authenticate to relay, regardless of the list above

**Delivery Tab**

**Outbound Security**

- o Set appropriate authentication, use at least Basic authentication, include TLS encryption (requires certificates) if possible

**Security Tab**

- ❑ Add the SMTPAdmins group for Operator privileges

## NNTP Properties

**General Tab**

- ❑ Ensure Enable logging is selected

**Access Tab**

**Authentication**

**If being used outside of a security perimeter (i.e. firewall)**

- o Disable Allow Anonymous

- ❑ Use of SSL is recommended, especially with Basic authentication (requires certificates)

**Connection**

- o Select Only the list below and add your network domain

**Settings Tab**

- ❑ Disable (uncheck) Allow servers to pull news articles from this server
- ❑ Disable (uncheck) Allow control messages

**Security Tab**

- ❑ Add the NNTPAdmins group for Operator privileges

Chapter

4



# Additional Security Services

This chapter describes; how to configure auditing in IIS 5.0, a brief description of the installation, use of Certificates and touches on a couple of final security issues.

## Auditing

In addition to the audit settings described in the set of *NSA Windows 2000 Security Guides*, IIS logging should be enabled to enhance security auditing of the IIS environment. IIS logging tracks IIS-specific events related to HTTP/FTP/SMTP traffic in and out of the server. NNTP only offers general logging, not additional extended logging like the others. Included in the log is IP address information that is not available through Windows 2000 logging and auditing mechanisms. Actively reviewing and correlating IIS logs can identify the following suspicious activity:

- Multiple failed commands
- Attempts to upload files to directories configured for executable content
- Attempts to access non published .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 – See **Figure 44** (WWW, FTP, SMTP and NNTP) by selecting the **Properties** button.

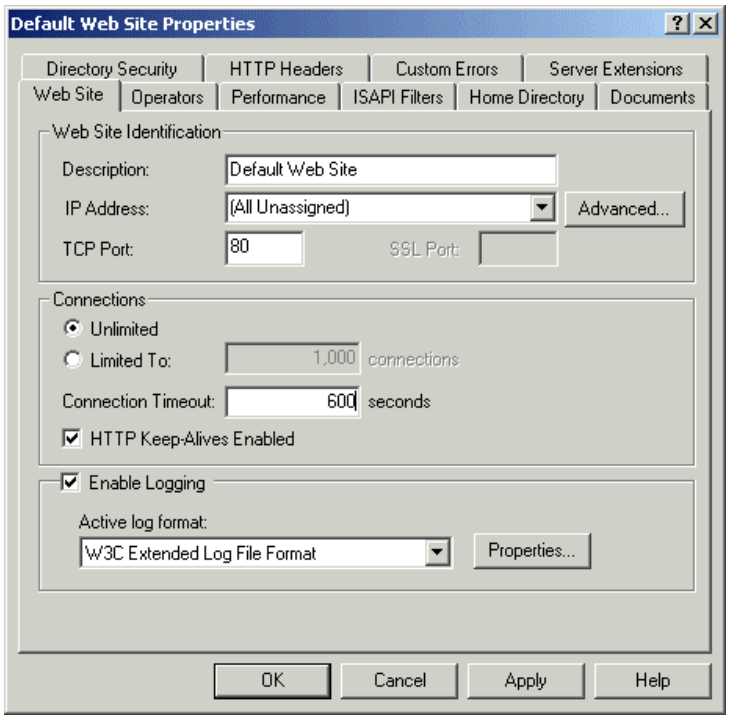
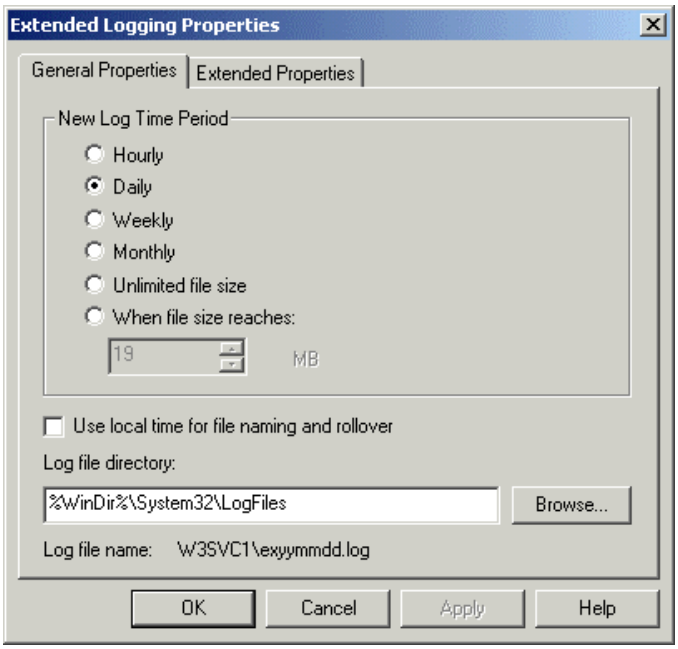



**Figure 44 IIS Logging Configuration Example**

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

- Move and rename the IIS Log Files directory. This can increase the difficulty unauthorized users experience while trying to cover their tracks.
- Full Control access to the IIS Log Files directory should be limited to SYSTEM and Administrators ONLY (or whichever group is created to manage auditing on your system). No other accounts should be given access.
- Create Files/Write Data, Create Folders/Append Data, Delete Subfolders and Files, Delete, Change Permissions, and Take Ownership are critical events for WWW content directories. They should be audited for success and failure in the Windows 2000 audit facility.

**Extended Logging Properties –** (See **Figure 45**) The following configuration is recommended including the items in your IIS 5 logs.



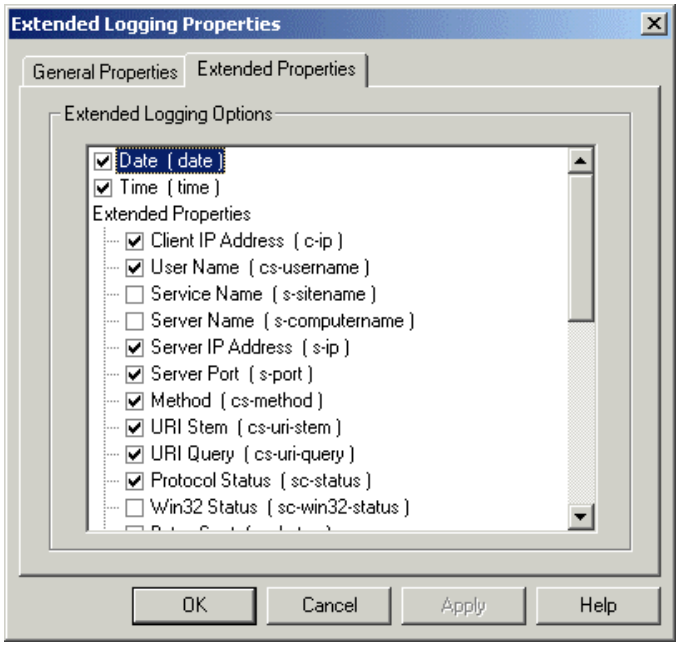




**Figure 45 General and Extended Properties**

- Date and Time event occurred
- IP Address of the client
- 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
- URL of the last site visited by the client

## Certificates

A more detailed description of how certificates and certificate authorities are implemented is available in a separate document entitled *Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services* and available via the same media in which this guide was delivered. The book entitled *Administering IIS 5.0* by Tulloch, M., Santry, P. gives a good description of how to implement the use of a certificate manager within your IIS environment. The following section provides a brief description.

If the system requires the use of SSL for secure communications between your clients and server, a server certificate must be installed and the client must have a browser that can support secure communications. Authentication, confidentiality, and data integrity can all be obtained with the use of digital certificates and SSL. A certificate is created by a certificate authority (CA). It is made up of a public key for cryptographic use, a validity interval, serial number, name, and certificate class.

The Certificate wizard is the tool used to manage certificates in the IIS 5.0 environment. The Certificate wizard can also be used to export and backup your IIS server certificate(s). It is used to configure background information that will be needed to apply for a digital certificate and create the required files. The Certificate wizard can be accessed through the Secure Communications **Server Certificate** button of the **Directory Security Tab** of the Server and Web Site Properties dialog boxes.

The following tasks are performed through the Certificate wizard, different options are available depending on if you have an existing certificate or not:

- Create a new certificate
- Assign an existing certificate
- Import a certificate from a Key Manager backup file
- Renew the current certificate
- Remove the current certificate

- Replace the current certificate

Once the site has been configured to use certificates, activate the SSL security on the server using the ISM for the site that requires secure access. See **Figure 46**:

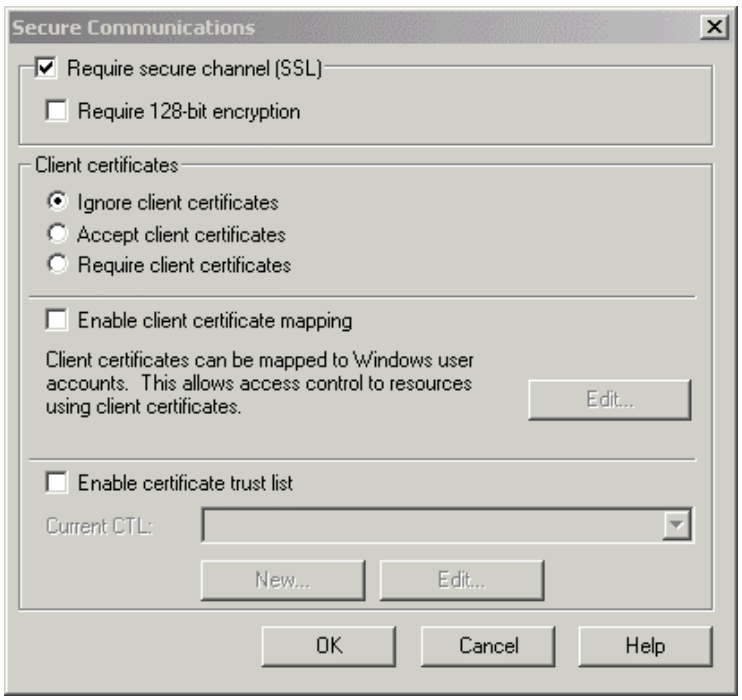



**Figure 46 Configuring Site to Require SSL**

Web site developers can use scripts and client side certificates to control access to the site. IIS supports the mapping of client certificates to specific Windows 2000 user accounts. This allows more control over published content on the web. Organizations can authenticate users who logon with a client certificate by creating mappings that relate information contained in the certificate to a Windows 2000 user account. Using the IIS certificate-mapping feature, administrators can either map a specific user's client certificate to an account (a one-to-one mapping – See **Figure 47**) or map multiple certificates to a single Windows 2000 user account (a one-to-many mapping – See **Figure 48**). IIS also supports wildcard mapping. To map multiple certificates to a single Windows 2000 user account, administrators define wildcard-matching rules that create a mapping by verifying whether a certificate contains certain items of information. For example, an administrator could define a matching rule that automatically maps any certificate issued by a particular organization to a user account, rather than creating a separate mapping for each client certificate.

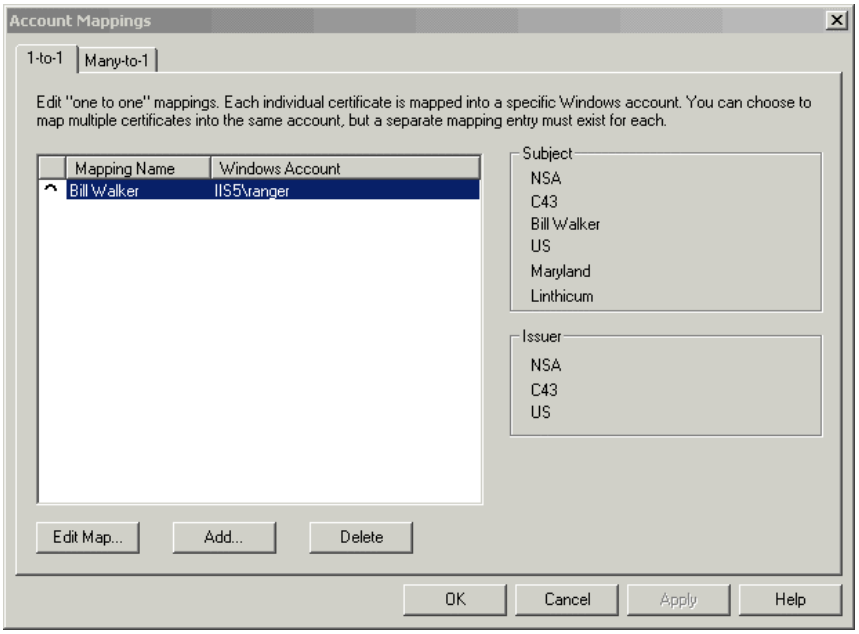



**Figure 47 1-to-1 Account Mapping Dialog Boxes**

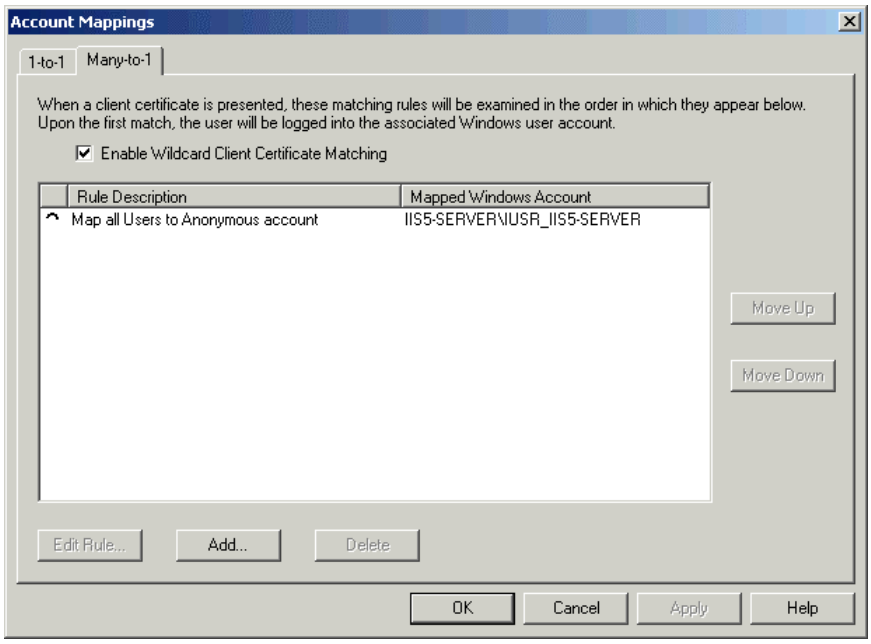



**Figure 48 Many-to-1 Account Mapping Dialog Box**

To utilize account mapping the following must occur:

- The web server must have a certificate and utilize SSL (see below for more information)
- The client must have a certificate (submit a request with the same procedure as the server)
- Both of these certificates must be installed properly (refer to the Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services)
- A copy of the clients certificate must be located on the web server (export clients `.cer` certificate and place on web server)
- Mapping must be added as necessary

To add a one-to-one mapping: Open the properties dialog box for the appropriate web site, click the **Directory Security Tab**, click **edit** under the Secure communications section, Enable client certificate mapping by selecting that option and click **edit** in that window. In the 1-to-1 dialog box (See Figure 47), click **Add**, **browse** to the clients certificate file that was brought over to the web server, create a Map Name, identify the account to associate with that user and identify the already existing password for that account, click **OK**. To create a many-to-1 mapping the steps are similar to those for a 1-to-1 mapping (See Figure 48).

Server certificates will be obtained in accordance with your organization's security policies. For example, in the Department of Defense, the DoD Public Key Infrastructure will supply server certificates. Given the diverse nature of the audience for this document, the exact procedures for obtaining a server certificate cannot be specified. However, the following is an illustrative example of how IIS interacts with Microsoft Certificate Server 2000 to obtain a certificate.

EXAMPLE: The Certificate Services setup program available on the Windows 2000 Server and Advanced Server CDs installs the Certificate Server files and the web-based administration tools. Certificate Server runs as a Windows 2000 service and is configured by default to run automatically under the System account when the Windows 2000 Server system boots. A few steps need to be taken to allow your server to perform client authentication and for clients to perform server authentication.

- Certify the server – The process of becoming certified takes place between your server and a CA.
- Client certificate enrollment – A client submits a request to the server for a certificate and then installs it in the client application.

These steps are accomplished by using the Certificate Server Certificate Enrollment Tools dialog box. Open the Certificate Server Certificate Enrollment Tools dialog box by opening Internet Explorer on `C:\WINNT\System32\CertSrv\` (or the appropriate URL if accessing a certificate server over the network). It is a Web-based enrollment control used to perform the tasks listed. See **Figure 49**:

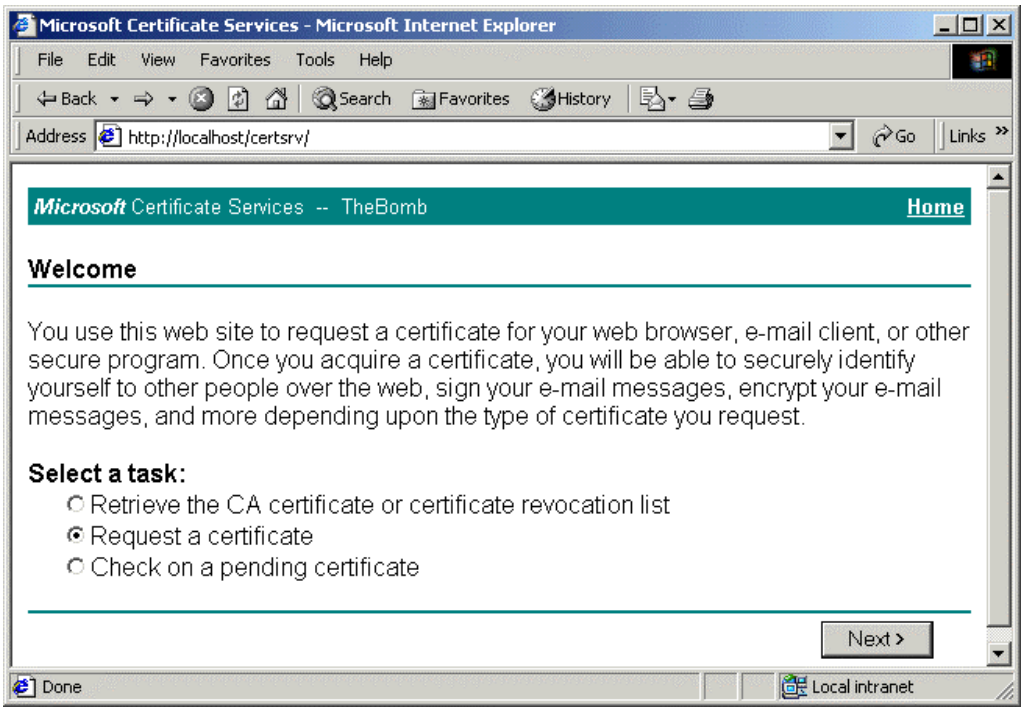



**Figure 49 Web Interface to Certificate Request**

**NOTE: Once SSL and the use of certificates are configured for your site, clients must access the secure content using HTTPS. Clients can communicate with both secure and non-secure HTTP servers. However, files and directories configured to require SSL would not be passed to clients that do not use HTTPS in their URL.**

## Many-to-One Certificate Mapping Weakness

Internet Information Services (IIS) 4.0 and 5.0 can allow the mapping of SSL client certificates to Windows NT (IIS 4.0) or Windows 2000 (IIS 5.0) user accounts. In order to do this, a certificate authority (CA) or CAs must be present in the physical store for Trusted Root Certification Authorities of the Local Computer. CA certificates are used to validate certificates used for certificate mappings. A possibility exists whereby a rogue CA can issue certificates that replicate client certificates of a peer or its peers and thus gain unauthorized access to restricted resources on a web site. The issue can be mitigated in IIS 4.0 without too much administrative over-ahead and minimal risk, i.e., limited to a CA's subordinate CAs if the CA does not apply name constraints. However, addressing the issue in IIS 5.0 requires significant administrative over-head. When reviewing this document, keep in mind that a CA's policies and practices may negate any need to address the issues raised. These documents should be reviewed before making any decision.

For full details please see Implementing IIS 4.0 and 5.0 Many-to-One Certificate Mappings.

## Script Mappings

The IIS web server is configured to support many different common filename extensions, which allows it to serve pages using a variety of different application `.dll` files (See **Table 2**). Some examples of this include `.html`, `.asp`, `.shtml` and `.shtm`. Many web servers are used only for static pages such as `.html`, so there is no need for including these other mappings. **The mappings that the server does not 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.**

A good example is the `.htr` entry. This entry is used to do web-based password resets and this is a default mapping. If this functionality is not being used, it should be removed, just like all other non-utilized features. If a need arises in the future to add some functionality, the mapping can always be added later.

Here are some references along with their uses:

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

**Table 2 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**.

**WARNING: To prevent the .printer mapping from returning after a system reboot: Disable web printing by modifying the Web Based Printing policy in the Group Policy snap-in. It is located under Computer Configuration-Administrative Templates-Printers. Also, be sure to check the domain policy, if the IIS server is accepting policies from a domain. To verify, the following key should exist if disabled: "HKLM\Software\Policies\Microsoft\windows\NT\printers\DisableWebPrinting REG_DWORD 0x1".**

## IPSEC Filtering

This feature is part of the operating system, but due to its importance it is felt that a brief description and recommendation is necessary. First and foremost, your organizational policy should dictate ports and services that are and are not allowed. For most DoD organizations the policy states all ports not specifically permitted and required for the mission are to be denied. Once the operating system is installed and the web server

configured, filtering out all the ports and allowing only those required is recommended. This will help to deter any potential vulnerability against ports and services that are not required for the web servers to operate.

Using the MMC, the IPSEC module can be loaded and configured to block all port access with one rule (See **Figure 50**). For each service or port required additional rules must be added to allow communication.

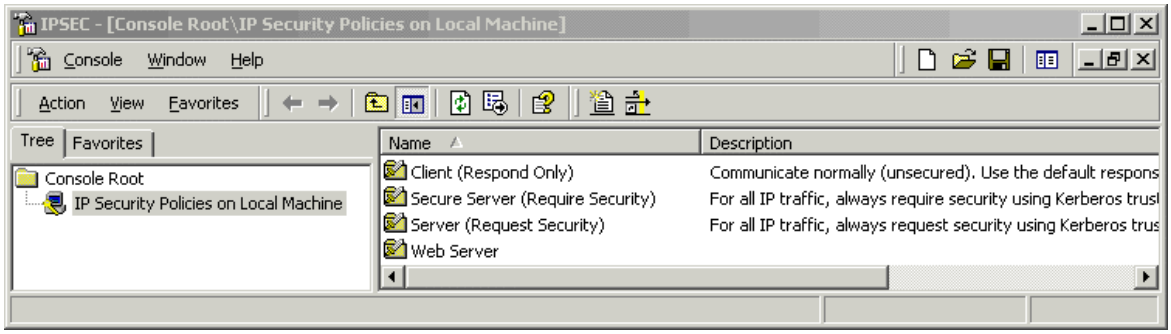



**Figure 50 IP Security Policies on Local Machine**

In **Figure 51**, all ICMP as well as all IP traffic has been blocked and that all the specific traffic that is allowed by the server has been permitted. It is important to note that the IPSEC traffic filters are not applied sequentially (as seen in the list), the most specific filters are applied first.

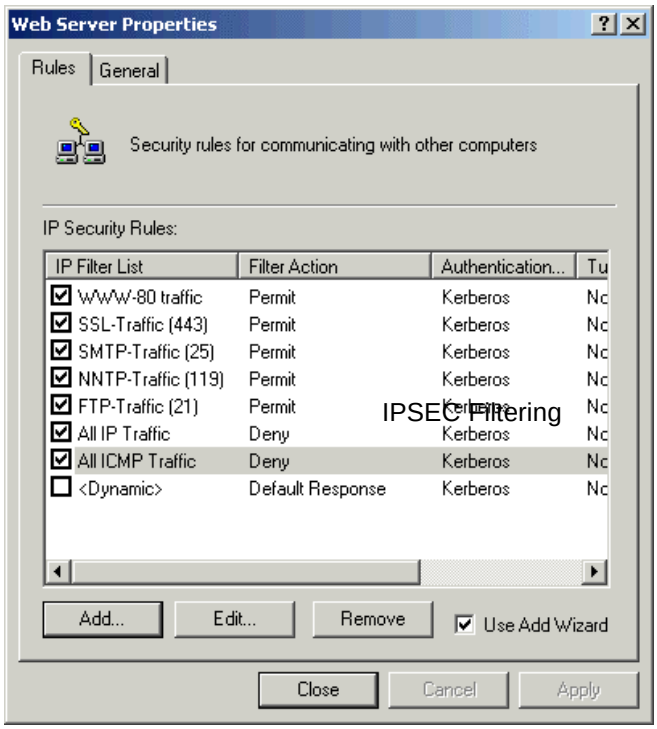



**Figure 51 IPSEC Filtering**

This sample configuration blocks all traffic to the web server, except, TCP ports 80 (WWW), 443 (SSL), 25 (SMTP), 119 (NNTP), and 20-21 (FTP).

Use caution when implementing IPSEC filtering. Make sure that every service that will be required is identified and a filter applied for it. If not, and these rules are implemented, those services will not be available to clients. This also includes ports required if the web server is participating in a domain.

Finally, note that use of a firewall or filtering router may also be prudent. For example, if the IIS server is a part of a domain it will be necessary to open additional ports on the IIS server but those ports should be blocked from access by untrusted networks (e.g., Internet).

The IISLOCK tool identified in Appendix A utilizes IPSEC filtering as part of its lock down. Please note the cautions identified in the tools section.

## IIS Default Samples and Printers

### Disable or Remove All Sample/Printer Applications

There are several directories and utilities in the default installation of IIS that are designed to highlight the capabilities of the server, see **Table 3**:

| Sample | Virtual Directory | Location |
|---|---|---|
| IIS Samples | \IISSamples | %systemdrive%\inetpub\iissamples |
| IIS documentation | \IISHelp | %windir%\help\iishelp |
| Data Access | \MSADC | %systemdrive%\program files\common files\system\msadc |
| Web Printing | \printers | %systemdrive%\WINNT\web\printers |

**Table 3 Directories and Utilities of Default Installation of IIS Samples**

During the installation of IIS, the administrator had the ability to not install the samples, but by default they are selected to be installed. The access to the samples is setup by default to only be accessible to the localhost (i.e., 127.0.0.1) via the web browser. Even though this is the case it is recommended to remove or disable the samples if and when they are no longer required.

To stop the \printers web page from restoring itself upon reboot, do the following: delete the virtual folder in the ISM, open windows explorer, go to %systemdrive%\winnt\web and right-click. Choose **properties** on that folder, remove all entries in the ACL except Administrators and SYSTEM. Add the “WebUsers” group, and select the box for “Deny” under “Full Control”. Now, whenever the system reboots, the printer web page will not automatically restore itself.

## Operating System Directories and Executables

### Remove or Set ACL's and Auditing on All Problematic Files and Directories

After the installation of IIS, and the user group memberships have been completed, there is a need to lock down access to certain files and directories. To accomplish this, add the "WebUsers" group to the ACL of the directory or file (in the windows explorer right-click the directory or file, click **properties**, click the **security tab**). Next, set that group's "Full Control" access to "Deny", this will put check marks in all the deny boxes for all the different types of access. As noted earlier, the IUSR account is also a member of the Users, Authenticated Users and Everyone group, so any directory or file that they have access to the IUSR account has potential access to. By using the Deny permission on the WebUsers group, the IUSR access is restricted and thus cannot access those files or directories because the deny permission always overrides the permit permission.

This type of access control will prevent unauthorized persons from gaining access to sensitive information or execute programs that allow further system exploitation. By hindering the ability to access these files you are extending the protection of the system and eluding potential compromise.

Besides setting ACL's, auditing of these files is also highly recommended. In the case that ACL's are bypassed (i.e. a buffer overflow causing SYSTEM level access), auditing will allow the administrator to identify the illegal file access and restore the system before further compromise is possible. Table 4 shows the recommended the files and directories to set ACL's and auditing for.

| Directories | Files | Notes |
|---|---|---|
| %systemdrive% (i.e. C:\) | | 1 |
| %systemroot% (i.e. C:\WINNT) | | 1 |
| %systemroot%\ | Explorer.exe, Regedit.exe, Poledit.exe, Taskman.exe | 2 |
| %systemroot%\system | | 1 |
| %systemroot%\debug | | 1 |
| %systemroot%\installer | | 1 |
| %systemroot%\repair | | 1 |
| %systemroot%\security | | 1 |
| %systemroot%\system32 | | 1 |
| %systemroot%\system32 | at.exe, cacls.exe, cmd.exe, command.com, cscript.exe, debug.exe, edlin.exe, finger.exe, ftp.exe, ipconfig.exe, krnl386.exe, nbstat.exe, net.exe, net1.exe, netsh.exe, posix.exe, rcp.exe, regedt32.exe, regini.exe, regsvr32.exe, rexec.exe, rsh.exe, runas.exe, runonce.exe, srvmgr.exe, sysedit.exe, syskey.exe, telnet.exe, tftp.exe, tracert.exe, usrmgr.exe, | 2 |

| | | |
|---|---|---|
| | wscript.exe, xcopy.exe | |
| %systemroot%\system32\dllcache | | [1] |
| %systemroot%\system32\drivers | | [1] |
| %systemroot%\system32\inetsrv | | [1] |
| %systemroot%\system32\inetsrv | iissync.exe | [2] |
| %systemroot%\system32\os2 | | [1] |
| %systemroot%\temp | | [1] |

**Table 4 Directories and Files for Auditing and ACL's**

[1] Apply to directory only, NOT ALL FILES and SUBDIRECTORIES.

[2] Apply to these files.

[redacted]

## Recommendation Checklist for Chapter 4:

- ❑ Move and rename the IIS Log Files directory
- ❑ Full Control access to the IIS Log Files directory should be limited to SYSTEM and Administrators.
- ❑ Write, Delete, Change Permissions, and Take Ownership audited for success and failure.

**Extended Properties**

- ❑ Date
- ❑ Time
- ❑ Client IP Address
- ❑ Username
- ❑ Server IP Address
- ❑ Server Port
- ❑ Method
- ❑ URI Stem
- ❑ URI Query
- ❑ Protocol Status
- ❑ Time Taken
- ❑ Referrer

- ❑ Remove unnecessary script mappings
- ❑ Implement IPSEC filters
- ❑ Remove all Sample pages/directories/sites
- ❑ Implement ACL's on operating system directories and files
- ❑ Implement Auditing on operating system directories and file

Chapter

5



# Backup Procedures and Antiviral Precautions

This final chapter of the *Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0* deals with backup procedures and antiviral precautions.

## Backup Procedures

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

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

## Antiviral Program

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

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

This Page Intentionally Left Blank

Appendix

A



# IIS 5.0 Security Configuration Tools

This section will identify some of the available IIS 5.0 security configuration tools. Microsoft offers these tools, which assist the user in configuring the security settings of their IIS 5.0 web server(s). If this guide has been implemented, then use of these tools is not necessary; however, some users may find the tools useful for automating certain aspects of IIS security. If using these tools, please note the associated warnings applicable to some of the tools and described below.

## IISperms (“What If” Tool)

Iisperms.exe is a downloadable tool from Microsoft that can assist in troubleshooting security issues with IIS. This tool is a small graphical web page that allows the choice of setup type (not all possibilities available). If the desired setup is not listed, the tool will make assumptions and display a small graphic to represent what resources your clients can access. See **Figure 52**:

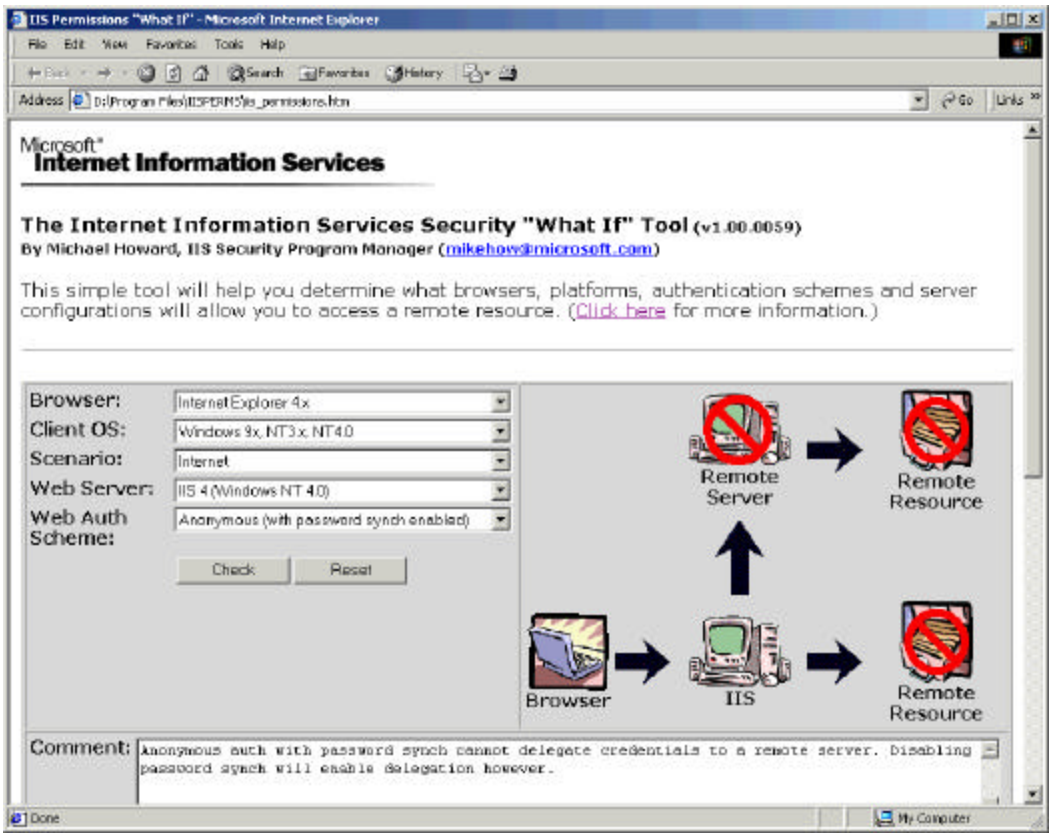



**Figure 52 IISPerms "What If" Tool Interface**

If interested in further information, go to the http://support.microsoft.com site, knowledge base article Q229694.

## HISECWEB.INF (Policy Template)

A self-extracting .exe file called hisecweb.exe can be downloaded from the Microsoft site that contains a policy template for securing an IIS 5.0 web server. After downloading and extracting the hisecweb.inf file into the %systemroot%\security\templates directory, launch the **Security Configuration and Analysis tool**. Load the hisecweb.inf template into the tool and review the default policy settings to see if they match your policy and needs. See **Figure 53**:

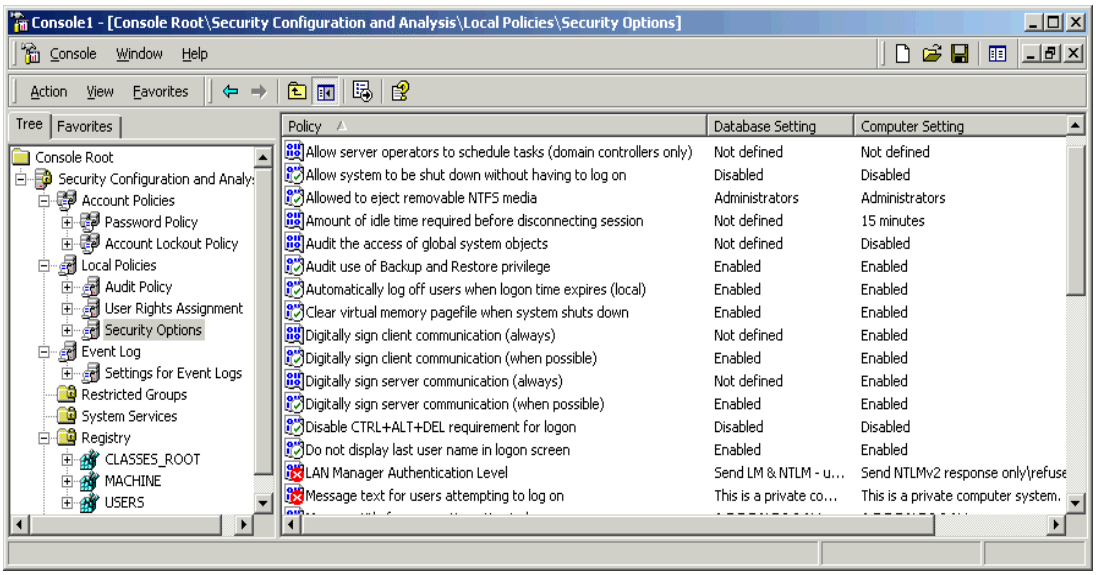



**Figure 53 HISECWEB.inf MMC Policy Snap-In**

Once policy changes are made, right-click the **Security Configuration and Analysis tool** and choose **Analyze Computer Now** from the context menu. The system will check the system configuration against the ones identified in the policy. When the configuration check is complete, a screen like **Figure 53** will appear. For each area, a list of current system settings and selected settings is generated. A red X identifies where the policies differ. A green check identifies where they are correct.

To apply the template, right-click the **Security Configuration and Analysis tool** and choose **Configure Computer Now** from the context menu. The system will go through and set the system according to the policy just identified. IPSEC policies will not be set using this tool and must be considered separately. It is recommended that all ports be blocked and only those necessary be added. There are many web security tasks that this tool will not do, some of them are: not set ACL's on your files or directories in NTFS, it will not set permissions on the files, directories or sites in IIS 5.0, it will not remove sample files (refer to chapter 4) and it will not move content directories from the default. All of these will still need to be done by the administrator as recommend in the prior sections of this guide.

Although this tool can be very valuable, if the set of *NSA Windows 2000 Security Guides* will be implemented, do NOT implement this policy without modification. The changes will override some of the settings the OS guide invoked. Compare the OS guide and your organization policy to this policy and make the necessary changes to possibly utilize a combination of both. If the OS guide will not be implemented, or a combination, the use of this policy configuration is recommended. If this tool is to be utilized it is recommended that this tool be used during the initial configuration of the web server. Please make sure that before use, web server installation and configuration plan is available and the administrator is knowledgeable of how to make policy changes and implement policy.

**WARNING: it is critical to have a backup of the system before implementing this policy. Also, utilizing another registry and system change software (i.e. configsafe) is recommended in case the user needs to quickly reverse the changes made. The policy cannot be automatically reversed.**

## IISLock (Windows 2000 Internet Server Security Configuration Tool)

The third tool is the IISLock utility. This is similar to the hisecweb utility, but it adds more features for configuration. In fact, this tool includes the use of the hisecweb.inf policy to implement some of the necessary changes. The documentation of this tool states, "The general philosophy of this tool is to lock down everything except that which is required by the Internet Server." The tool provides an HTML interface to obtain information about the intended use of the web server. Based upon the answers, a policy template will be built that can be implemented via a command line program. See **Figure 54**:

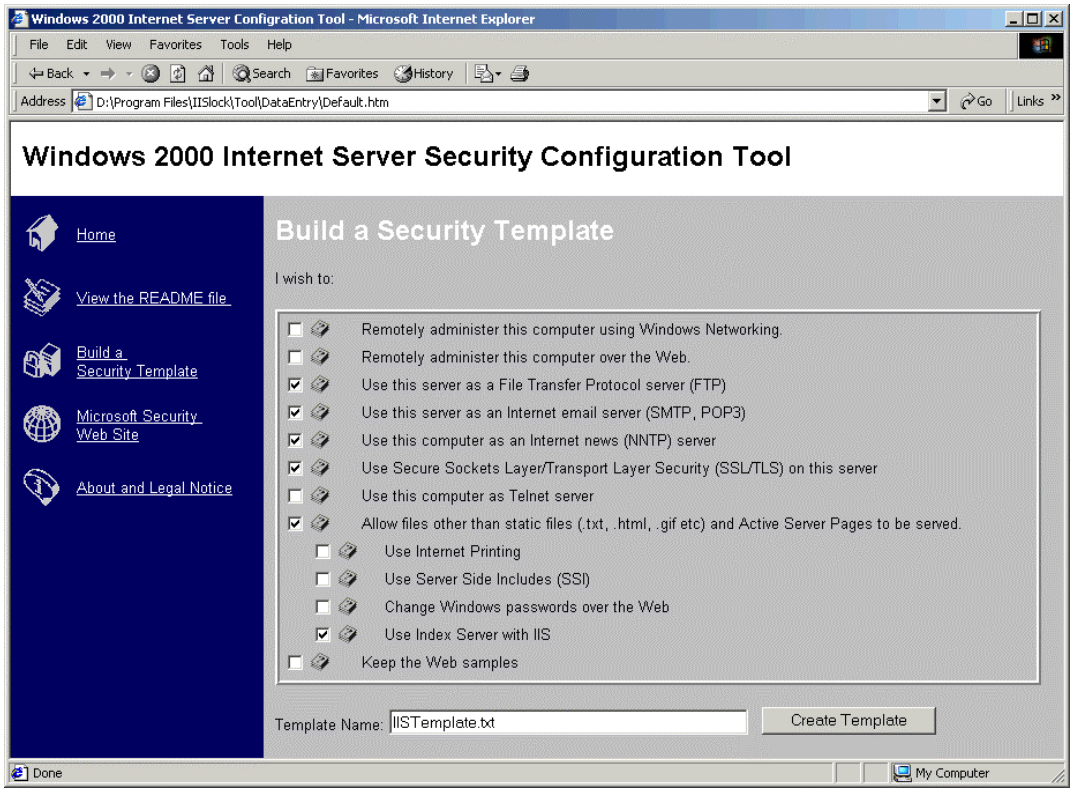



**Figure 54 IISLock Web Interface Tool**

This policy includes the IP Security Policy Management snap-in, which blocks all ports, except those identified for use, WHICH IS HIGHLY RECOMMENDED. It also modifies the script maps to avoid several other vulnerabilities. If your server participates in a domain, the ports need to be identified, which are required for IIS server communication to the domain controllers and other resources that are tied to the web server. Without permitting those communications using the IP Security Policy Management snap-in, all those communications will be blocked.

Once choices are selected, give the template a name and press the **Create Template** button. Next, from a command prompt, in the directory where the iissecuritywiz.dll file was installed, type "regsvr32 iissecuritywiz.dll" and press enter. This will register a COM+ component to allow service manipulation and administrative checks. Once completed, run the IISConfig command on the command line and use the necessary flags to properly set your site information (i.e. IISConfig –s myserver –f C:\temp\IISTemplate.txt –d)

**WARNING: It is critical to have a backup of the system before implementing this policy. Also, utilizing another registry and system change software (i.e., configsafe) is recommended in case the user needs to quickly reverse the changes made. The policy cannot be automatically reversed.**

A copy of the tool can be downloaded from either of the following URLs

http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19889

http://www.microsoft.com/WINDOWS2000/news/bulletins/iistool.asp

Although this tool can be very valuable, if the set of *NSA Windows 2000 Security Guides* will be implemented, do NOT implement this tool without modification of the policy it uses. The changes will override some of the settings that this and the OS guide have changed. Compare this IIS 5.0 guide, the OS guide and your organization policy to this policy and make the necessary changes to possibly utilize a combination of both. If the OS guide will not be implemented, or a combination, the use of this configuration tool is recommended. If this tool is to be utilized, it is recommended that this tool be used during the initial configuration of the web server due to the leniency toward the security of the server. Please make sure that before use, the web server installation and configuration plan are available and the administrator is knowledgeable of how to make policy changes, implement policy changes and block/unblock ports using the IP Security Policy Management snap-in.

This Page Intentionally Left Blank

Appendix

B



# IIS 5.0 Many-to-One Certificate Mapping Weakness

## Implementing IIS 4.0 and 5.0 Many-to-One Certificate Mappings

### Issue Preview

Internet Information Services (IIS) 4.0 and 5.0 can allow the mapping of SSL client certificates to Windows NT (IIS 4.0) or Windows 2000 (IIS 5.0) user accounts. In order to do this, a certificate authority (CA) or CAs must be present in the physical store for Trusted Root Certification Authorities of the Local Computer. CA certificates are used to validate certificates used for certificate mappings. A possibility exists whereby a rogue CA can issue certificates that replicate client certificates of a peer or its peers and thus gain unauthorized access to restricted resources on a web site. The issue can be mitigated in IIS 4.0 without too much administrative over-ahead and minimal risk, i.e., limited to a CA's subordinate CAs. However, addressing the issue in IIS 5.0 requires significant administrative over-ahead. When reviewing this document, keep in mind that a CA's policies and practices may negate any need to address the issues raised in this paper. These documents should be reviewed before making any decision to trust a CA.

### IIS 4.0 and 5.0 Certificate Mapping Types

The two certificate mapping types in IIS are one-to-one and many-to-one. One-to-one mappings are fairly straightforward and, therefore, no screen shots are shown. A one-to-one mapping involves getting copies of clients' certificates and mapping one certificate to one Windows NT (IIS 4.0) or Windows 2000 (IIS 5.0) user account. When a client certificate is presented to an IIS server through Secure Socket Layer (SSL) 3.0, IIS determines if a one-to-one mapping exists for the given certificate. If a client certificate matches a certificate that has been configured as part of a one-to-one mapping, the client will be authenticated to the associated Windows NT or 2000 account; otherwise, the authentication, if properly configured, will fail, i.e., Anonymous, Basic Authentication, etc. are all turned off. It is important to note that the comparisons between client certificates used during the SSL 3.0 session and the copies loaded into IIS are certificate-to-certificate comparisons. Many-to-one mappings are not based on comparisons of certificates, but rather comparisons between "subject" and/or "issuer" attributes that are contained in a client certificate, and "subject" and/or "issuer" attributes contained in a many-to-one mapping rule.

It is important to note that defining a many-to-one mapping rule in IIS 4.0 and IIS 5.0 differ significantly. Figure 55 shows the beginning of a definition for a many-to-one mapping in IIS 4.0. In IIS 5.0, the **Issuers** block has been removed. IIS 5.0 implements

a certificate trust list (CTL), but it does not have the same effect as choosing the *Match on selected certificate issuers* option that is in ISS 4.0.

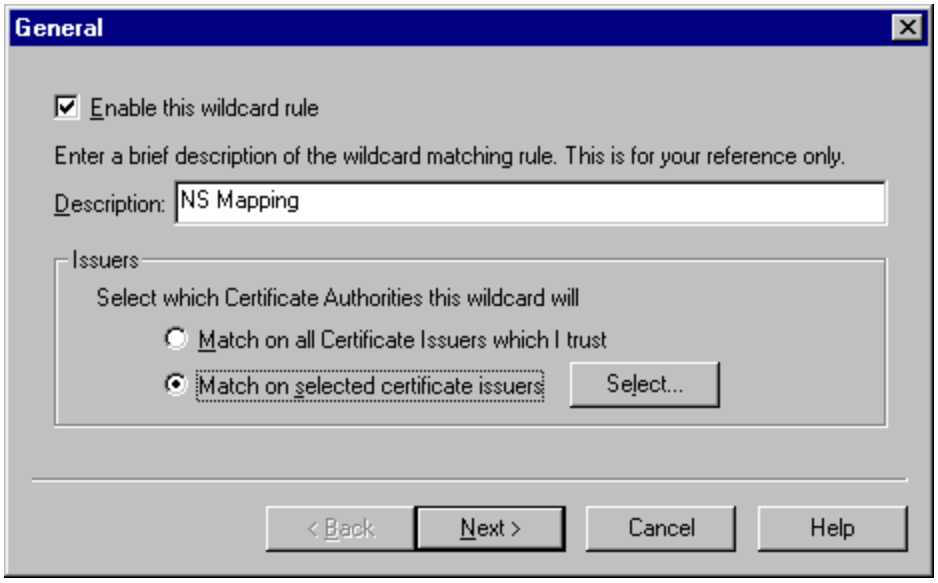



**Figure 55 IIS 4.0's option for specifying a many-to-one mapping's CAs**

A CTL in IIS 5.0 allows an administrator to define what CA(s) a particular web site will use to validate client certificates, whereas in IIS 4.0 the *Match on selected certificate issuers* option allows an administrator to define what CA(s) will be applied to a specific many-to-one mapping rule. Figure 56 shows an IIS 4.0 many-to-one mapping rule that will only be applied to client certificates issued by the NS CA and its subordinate CAs.

**Figure 56IIS 4.0 Trusted Root Certification Authorities**

The comparison of certificates in a many-to-one mapping is not binary and is performed irrespective of the length of the certificate chain. In this case, subject and/or issuer attributes from client certificates are extracted and compared to various attributes that are defined in a many-to-one mapping rule as shown in Figure 57.

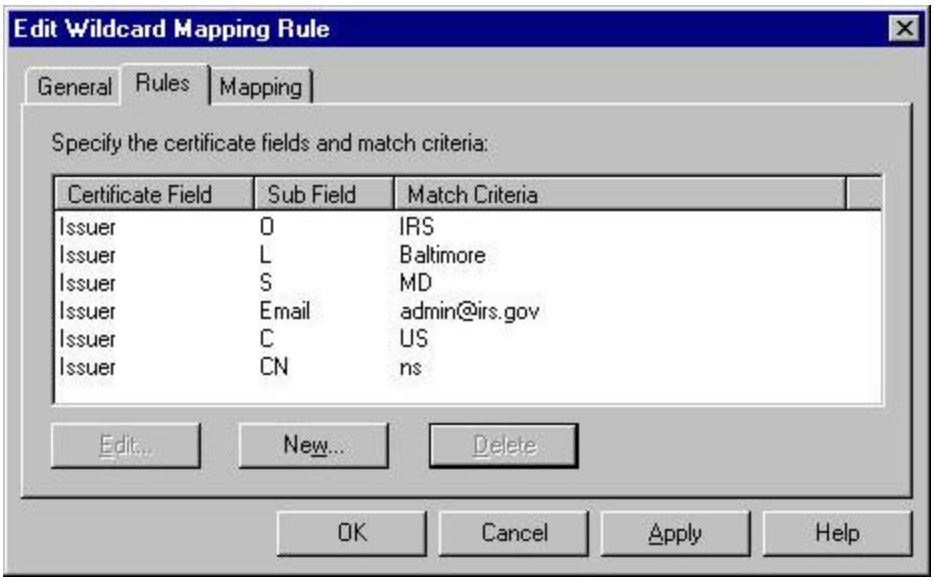



**Figure 57 Many-to-one mapping rule for issuer attributes**

Figure 57 illustrates a many-to-one mapping that compares attributes from the issuer's name of a client certificate to the rule and if valid, further maps the client certificate to a given NT or 2000 account as shown in Figure 58. The advantage of a many-to-one mapping is that it allows many different users with unique certificates to use the same account, thus relieving the burden of maintaining various NT or 2000 groups. However, in certain cases, this could lead to unintended authentication of client certificates.

**Figure 58 A many-to-one mapped account**

## IIS 4.0 Match on Selected Certificate Issuers Option vs. IIS 5.0 CTL Option

As previously stated, IIS 4.0 will allow an administrator to apply a specific CA or set of CAs to a many-to-one mapping whereas IIS 5.0 will not. IIS 5.0 implements CTLs to limit the set of CAs that can be used to validate a given web site. All CAs in the CTL can then be used to validate **all** many-to-one mappings for the site. The significance of this change is that in IIS 5.0, an administrator can define a many-to-one mapping that attempts to limit client certificates to a specific CA by specifying issuer attributes that must contain specific values, as in Figure 57. The issue of certificate masquerading could arise when more than one CA is contained in the CTL. Certificate masquerading is a well-known issue within the public key infrastructure community (PKI) and has been illustrated in published papers such as [Hay1] [Hay2] [Hay3]. "Certificate masquerading…allows a masquerader to substitute an unsuspecting certificate holder's valid certificate with the masquerader's valid certificate." [Hay3]

## Certificate Masquerading against IIS 5.0 Many-to-One Mappings

The best way to describe the issue of certificate masquerading in IIS 5.0 is to continue with the mapping that was defined in Figure 57 and the previous section's discussion. The Certificate Trust List Wizard is used to create a CTL. In the case of Figure 59, two CAs are included in the CTL and then given a CTL name as in Figure 60. Figure 61 shows the active CTL. Since IIS 5.0 does not have a binding feature between the mapping and a CA, an administrator can create a mapping similar to Figure 57 to limit what CA client certificates are authorized access to a web site resource. In this case, it will not work since the Trusted Hacker CA can in actuality create a subordinate CA that has a subject name that can be used to masquerade as the NS CA.

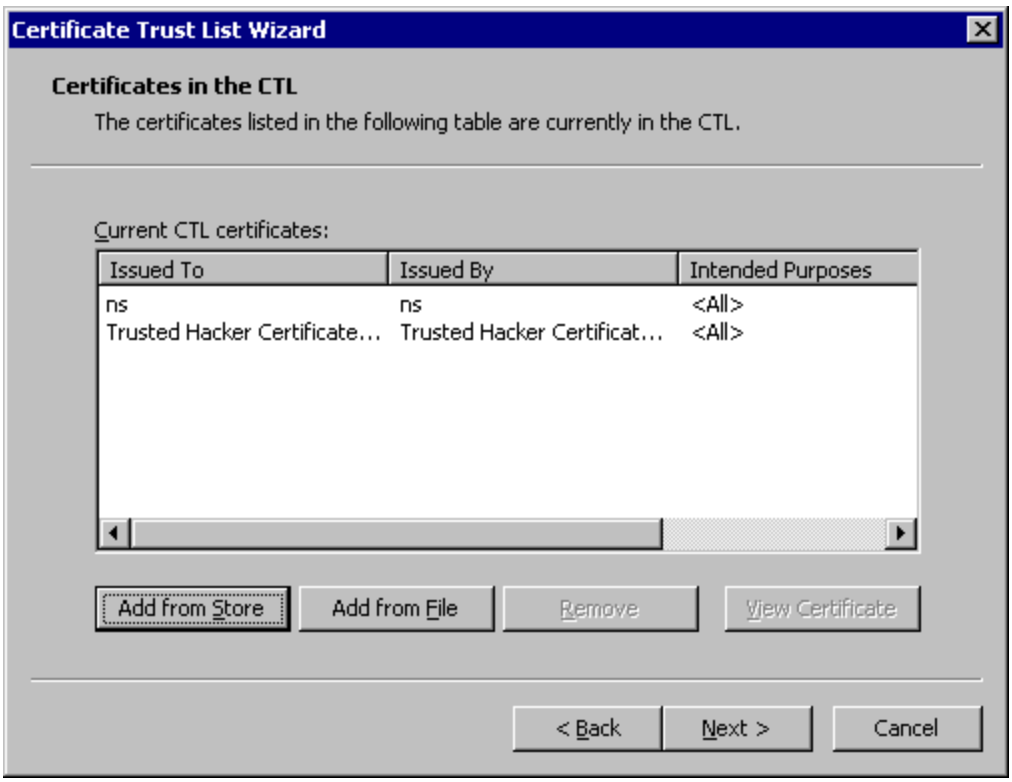



**Figure 59 Certificates added to a CTL**

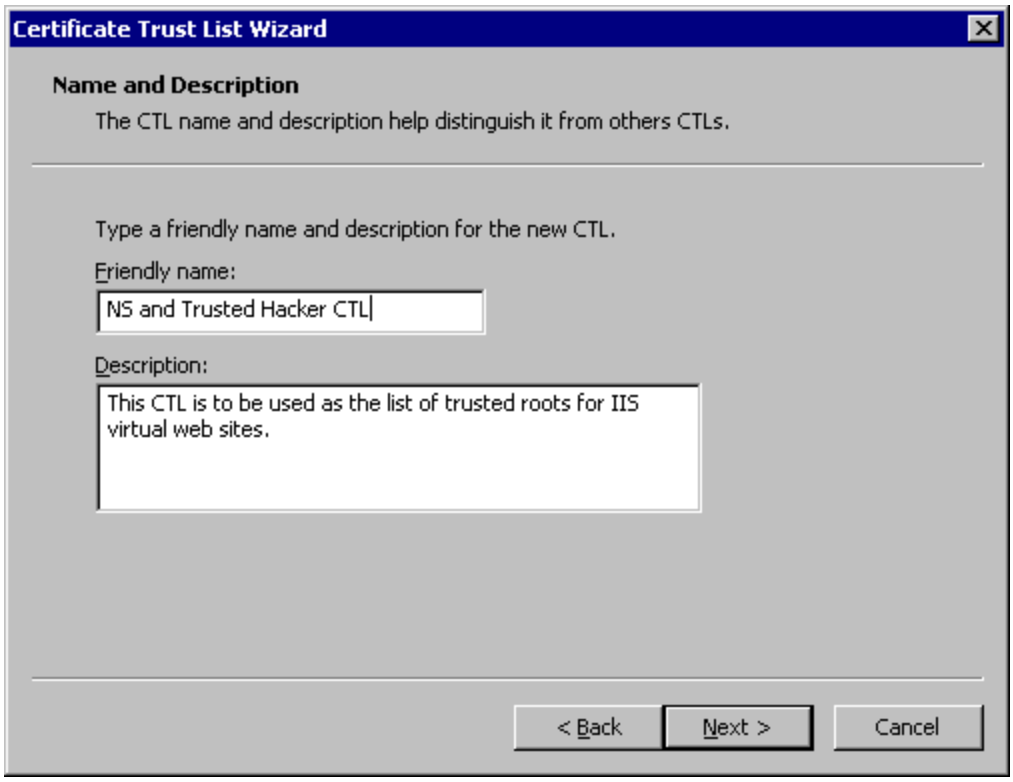



**Figure 60 Naming a CTL**

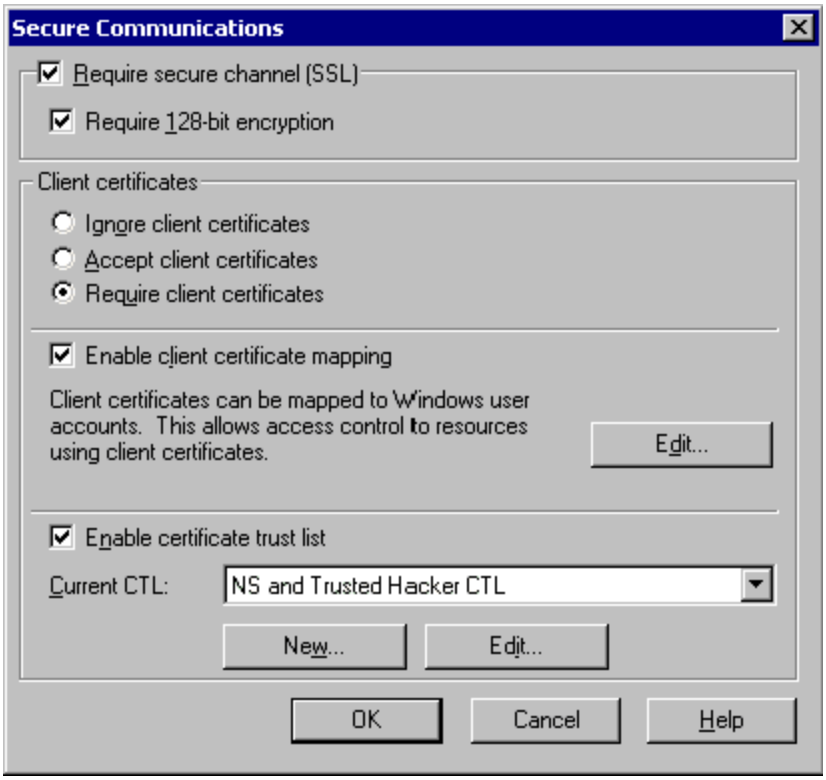



**Figure 61 An enabled CTL**

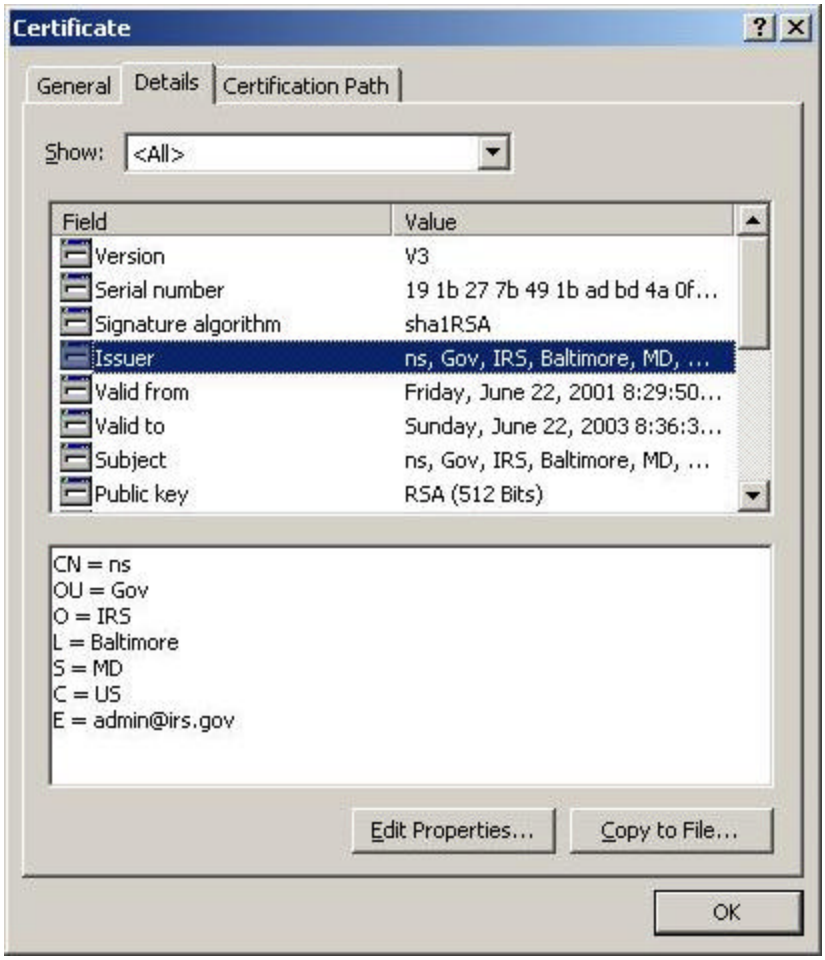



**Figure 62 Trusted ns root certificate**

Figure 62 shows the actual NS CA self-signed trusted root certificate. The issuer and subject names are identical. For each certificate that is issued by the NS CA, its subject name will be shown in the issuer field of those certificates. Figure 63 shows the Trusted Hacker CA's fake subordinate NS CA. This certificate's subject name is the same as the NS root CA and the issuer is the Trusted Hacker Certificate Authority. All certificates issued by this subordinate CA will have the same issuer name as the trusted NS CA. Since this is the case, a certificate chain, such as the one shown in Figure 64, can be created to get access through IIS 5.0 many-to-one mappings that are restricted to a client certificate that contains the NS CA issuer name. In the case just presented, Brian Snort would be able to get access to any resource restricted by the mapping in Figure 57.

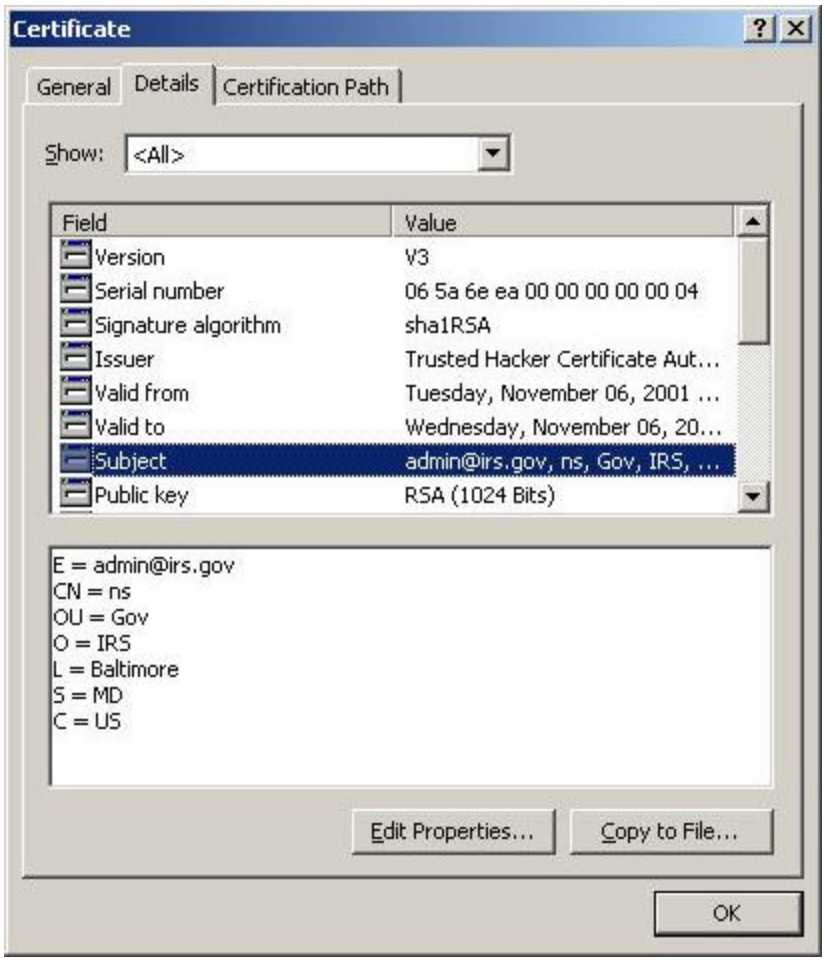



**Figure 63. Masquerading ns subordinate CA**

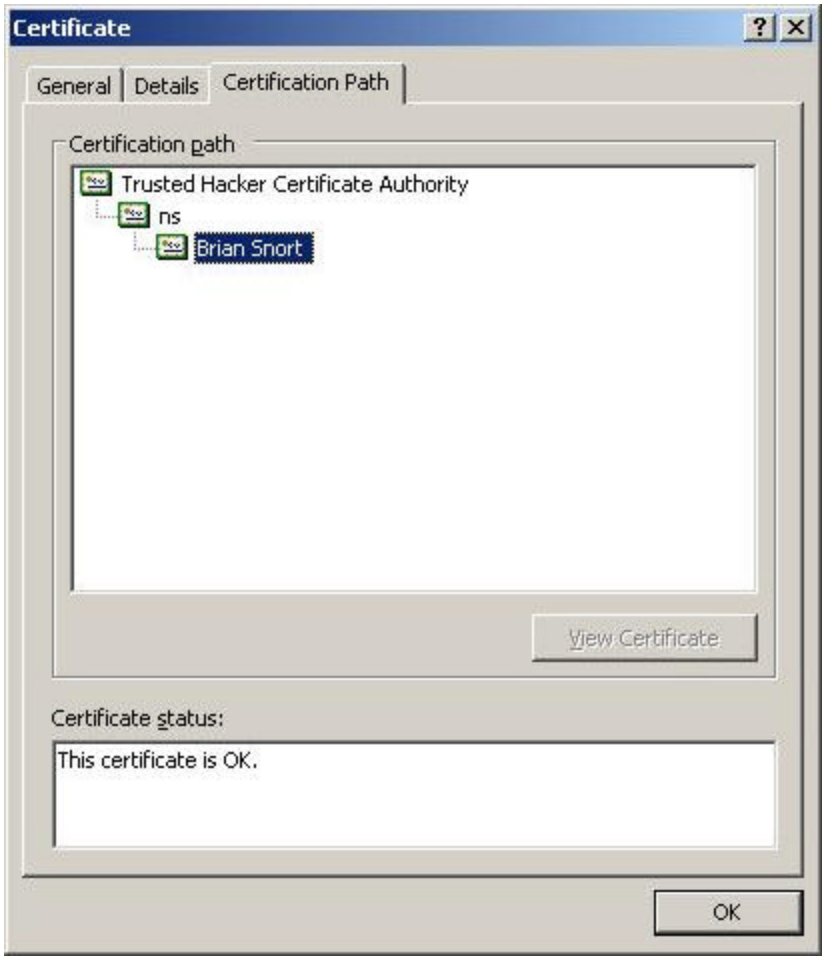



**Figure 64. Masquerading Brian Snort certificate and its chain**

## IIS 5.0 Many-to-one Work-Around

One solution to the many-to-one issue is one-to-one mappings and Windows 2000 groups. The "many", in this case, are the one-to-one certificate mappings and the "one" is the targeted group for the users. Using groups allows a resource to be limited to a specific set of users based on their Windows 2000 group membership and file permissions. One-to-one mappings enforce a one-to-one relationship between a certificate and a Windows 2000 user account. Client certificates cannot be masqueraded since each client certificate used during an SSL session must be compared to client certificates that have been bound to a Windows 2000 user account. Unfortunately, this solution can become an administrative burden for web sites with a large user base.

## IIS 4.0 and 5.0 Many-to-One Certificate Mapping Rules-of-Thumb

These rules provide guidelines for developing many-to-one mappings in IIS 4.0 and IIS 5.0. The IIS 5.0 guidelines should only be followed if all CAs that are to be trusted offer policies and practices that can assure its user community it has reasonable control over the creation of subordinate CAs.

| IIS 4.0 | IIS 5.0[1] |
|---|---|
| 1. Remove all untrusted CAs[2] | 1. Remove all untrusted CAs and ensure that only the appropriate certificate purposes are set for the remaining CA certificates.[3] |
| 2. When defining a rule, select the Match on certificate issuers radio button and then press Select to apply the appropriate CA or CAs to the rule. | 2. Define a CTL that only includes the required CAs for certificate mapping. |
| 3. If the rule definition requires issuer attributes or is intended to only use client certificates issued by a specific root CA or one of it's subordinates, then select only that root CA from the dialog box; otherwise, if it involves only subject attributes then select the CAs that apply to the rule. | 3. If the rule definition requires issuer attributes or is intended to only use client certificates issued by a specific root CA or one of it's subordinates, then apply all subject and issuer attributes for the issuing CA as required. |
| 4. When defining the actual rule, apply all subject attributes as required. Issuer attributes should only be required if the specific issuer attributes referred to are that of the root CA or one of its subordinate CAs.[4] | |



## Summary

The implementation of client certificates into a web site should not be taken lightly. Adding client certificates adds considerable overhead to the administration of the site, i.e., registration, initialization, certification, key pair recovery, key generation, key update, key expiry, key compromise, cross-certification, revocation, and certificate and revocation notice distribution and publication may all play a part in the underlying PKI that supports use of these certificates. Beyond the PKI aspects, one must clearly define the intended mapping of certificates and ensure that the appropriate mapping can be enforced. In terms of IIS 5.0, some solutions may be mitigated through a CA's policies and practices and others may require one-to-one mappings to accounts that are associated with a specific group in order to protect a resource.

[1] The suggestions for IIS 5.0 basically act as a filter of client certificates but will not protect against the masquerading that was previously discussed.
[2] The CA certificates for IIS 4.0 and 5.0 are stored in the Local Computer's certificate store. This may involve keeping other CAs that are to be trusted for other purposes other than client authentication.
[3] Use the Certificates snap-in for the Local Computer.
[4] Although beyond the scope of this paper, it is possible for a subordinate CA to masquerade as its root or one of its subordinates. Possible mitigation CAs policies and practices or name constraints; however, name constraint checking is not supported in Windows 2000, other than to determine if the extension is marked as critical.

Appendix

C



# References

Microsoft online help for FrontPage Server Extensions

Internet Information Services 5.0 Documentation, Microsoft Press

Administering IIS 5.0, Mitch Tulloch & Patrick Santry, McGraw-Hill, 2000

Guide to the Secure Configuration and Administration of Microsoft Internet Information Server 4.0, Sheila Christman, National Security Agency

Secure Internet Information Services 5.0 Checklist, Microsoft TechNet, Michael Howard, http://www.microsoft.com/technet/security/iis5chk.asp

Upgrading to IIS 5; Installing IIS 5 to a Custom Location. Hill, Brett. http://www.iisanswers.com/articles/Upgrading_to_IIS5/Changing_IIS5_install_location.htm, 2001

The .printer problem – Preventing Exploits of Default Application Mappings. Hill, Brett. http://www.iisanswers.com/articles/Application_Mappings.htm, 2001

[Hay1] James Hayes, "Guide to the Secure Configuration and Administration of iPlanet Web Server, Enterprise Edition 4.1," Systems and Network Attack Center, National Security Agency, http://www.nsa.gov, 2001.

[Hay2] James Hayes, "The Problem with Multiple Roots in Web Browsers – Certificate Masquerading," *Proceedings of the Seventh International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, IEEE, 1998.

[Hay3] James Hayes, "Restricting Access with Certificate Attributes in Multiple Root Environments – A Recipe for Certificate Masquerading", *Proceedings of the 17th Annual Computer Security Applications Conference*, ACSA, 2001.