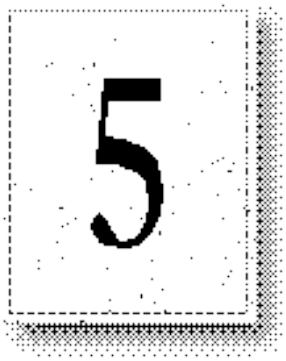
CHAPTER 1



Connecting computers to the Internet provides for some very powerful and useful scenarios. Within hours it becomes possible to communicate with millions of people and computers worldwide using Transfer Control Protocol/Internet Protocol (TCP/IP). This broad flexibility imposes a degree of risk — not only can you communicate with people and other systems, it is also possible for users to attempt to initiate communication with your system. Although connecting to servers on the Internet is generally done with good intentions, there are malicious individuals who attempt to infiltrate internal networks. The Windows NT operating system was designed with security in mind.

Your security configuration is crucial for safe operation of your server on the Internet. Although it is unlikely that your site will be maliciously tampered with, Internet servers are available to the general public and there may be some degree of public intrusion. This chapter will help you effectively use Windows NT security and Internet Information Server security at your site. You should understand all of the information in this chapter before connecting your computer to a public network. If you do not understand the information, you should consult Windows NT documentation, an authorized Microsoft Solution Provider, or other source before installing your site on the Internet.

This chapter explains:

- General Windows NT security and how to apply it to your site.
- How Internet Information Server security works.
- How to securely configure the WWW service.

Note

Securely Configuring Windows NT Server

Windows NT provides user-account security and Windows NT File System (NTFS) file-system security. You can use the topics below as a checklist to ensure you have effectively used User Accounts and NTFS to secure Windows NT Server. Additionally, you can prevent security breaches by properly configuring the services running on your computer.

Preventing Intrusion by Setting Up User Accounts

Windows NT security helps you protect your computer and its resources by requiring assigned user accounts. You can control access to all computer resources by limiting the user rights of these accounts.

Every operation on a computer running Windows NT identifies who is doing the operation. For example, the username and password that you use to log on to Windows NT identifies who you are and defines what you are authorized to do on that computer.

What a user is authorized to do on a computer is configured in User Manager by setting User Rights in the Policies menu. User rights authorize a user to perform certain actions on the system, including the right to “Log on locally,” which is required for users to use Internet Information Server services.

Allowing Anonymous Access with the IUSR_*computername* Account

The IUSR_*computername* account is created during Microsoft Internet Information Server setup. For example, if the computer name is marketing1, then the anonymous access account name is IUSR_marketing1.

By default, all Microsoft Internet Information Server client requests use this account. In other words, information server clients are logged on to the computer using the IUSR_*computername* account. The IUSR_*computername* account is permitted only to log on locally. No network rights are granted that could allow an unauthorized user to damage your server or its files.

The IUSR_*computername* account is also added to the group Guests. If you have changed the settings for the Guests group, those changes also apply to the IUSR_*computername* account. You should review the settings for the Guests group to ensure that they are appropriate for the IUSR_*computername* account.

If you allow remote access only by the IUSR_*computername* account, remote users do not provide a username and password, and have only the permissions assigned to that account. This prevents hackers from attempting to gain access to sensitive information with fradulent or illegally obtained passwords. For some situations this can provide the best security.

Requiring a Username and Password

Conversely, if you require "authenticated" clients, users must supply a valid Windows NT username and password.

Basic authentication does not encrypt your username and password before transmission. Basic authentication is encoded only by using UUencode, and can be decoded easily by anyone with access to your network, or to a segment of the Internet that transfers your packets.

Using basic authentication means you that will send your Windows NT username and password unencrypted over public networks. Intruders could easily learn usernames and passwords.

The WWW service also supports the Windows NT Challenge/Response encrypted password transmission. Microsoft recommends only the Windows NT Challenge/Response method of password authentication.

Windows NT authentication, currently supported only by Microsoft Internet Explorer for Windows 95, encrypts the username and password, providing secure transmission of usernames and passwords over the Internet.

With both basic authentication and Windows NT authentication, no access is permitted unless a valid username and password is supplied. Password authentication is useful if you want only authorized individuals to use your server or specific portions controlled by NTFS. You can have both IUSR_*computername* access and authenticated access enabled at the same time.

Choose Difficult Passwords

The easiest way for someone to gain unauthorized access to your system is with a stolen or easily guessed password. Make sure that all passwords used on the system, especially those with administrative rights, have difficult-to-guess passwords. In particular make sure to select a good administrator password (a long, mixed-case, alphanumeric password is best) and set the appropriate account policies. Passwords can be set by using the User Manager utility, or at the system logon prompt.

Maintain Strict Account Policies

The User Manager utility provides a way for the system administrator to specify how quickly account passwords expire (which forces users to regularly change passwords), and other policies such as how many bad logon attempts will be tolerated before locking a user out. Use these policies to manage your accounts, particularly those with administrative access, to prevent exhaustive or random password attacks.

Limit the Membership of the Administrator Group

By limiting the members of the Administrator group, you limit the number of users who might choose bad passwords and expose your system.

NTFS File Security

In addition to user accounts, you should place your data files on an NTFS partition. NTFS provides security and access control for your data files. You can limit access to portions of your file system for specific users and services by using NTFS. In particular, it is a good idea to apply Access Control Lists (ACLs) to your data files for any Internet publishing service.

The NTFS file system gives you very granular control on files by specifying users and groups that are permitted access and what type of access they may have for specific files and directories. For example, some users may have Read-only access, while others may have Read, Change, and Write access. You should ensure that the IUSR_*computername* or authenticated accounts are granted or denied appropriate access to specific resources.

You should note that the group Everyone contains all users and groups, including the IUSR_*computername* account and the Guests group. By default the group Everyone has full control of all files created on an NTFS drive.

If there are conflicts between your NTFS settings and Microsoft Internet Information Server settings, the strictest setttings will be used.

You should review the security settings for all Microsoft Internet Information Server directories and adjust them appropriately. Generally you should use the settings in the following table:

Directory Type	Suggested Access
content	Read access
programs	Read and Execute access
databases	Read and Write access

Enable Auditing

You can enable auditing of NTFS files and directories on Windows NT Server through the File Manager. You can review the audit records periodically to ensure that no one has gained unauthorized access to sensitive files.

Running Other Network Services

You should review all of the network services that you are using on any computer connected to the Internet.

Run Only the Services that You Need

The fewer services you are running on your system, the less likely a mistake will be made in administration that could be exploited. Use the Services applet in the Windows NT Control Panel to disable any services not absolutely necessary on your Internet server.

Unbind Unnecessary Services from Your Internet Adapter Cards

Use the Bindings feature in the Network applet in the Windows NT Control Panel to unbind any unnecessary services from any network adapter cards connected to the Internet. For example, you might use the Server service to copy new images and documents from computers in your internal network, but you might not want remote users to have direct access to the Server service from the Internet. If you need to use the Server service on your private network, the Server service binding to any network adapter cards connected to the Internet should be disabled. You can use the Windows NT Server service over the Internet; however, you should fully understand the security implications and licensing issues.

The FTP Server service included with Windows NT should also be disabled (this is required if the Microsoft Internet Information Server FTP service will be installed) or configured to ensure adequate security.

Check Permissions on Network Shares

If you *are* running the Server service on your Internet adapter cards, be sure to double-check the permissions set on the shares you have created on the system. It is also wise to double-check the permissions set on the files contained in the shares' directories to ensure that you have set them correctly.

How Internet Information Server Security Works

Internet Information Server integrates Windows NT authentication (username and password) security and NTFS file system security. Additional security is implemented by the Internet Information Server by using IP address security and directory access settings.

A simple overview of the security process used on each request is presented in the following illustration.

IP Address Security

The source IP address of every packet received is checked against the Internet Information Server settings in the Advanced property sheet. If Internet Information Server is configured to allow access by all computers except those listed as exceptions to that rule, access is denied to any computer with an IP address included in that list. Conversely, if Internet Information Server is configured to deny all IP addresses, access is denied to all remote users except those whose IP addresses have been specifically granted access.

IP address security is probably most useful on the Internet to exclude everyone except known users. IP address security can also be used to exclude individuals or entire networks that you do not want to grant access to.

Username Authentication

By default, all requests use anonymous access through the IUSR_*computername* user account created during Internet Information Server setup. This account is a user account and it granted the right to log on locally.

Username authentication is probably most useful if you want to control access to your server by individual user or group.

Internet Server Permissions

When you assign home and virtual directories for use by Internet Server services, you also specify the type of access that users have for the files in that directory. The WWW service allows you to assign these permissions to a directory:

Read
: Allows users to view files contained in a directory.

Execute
: Allows users to start applications or scripts. All Internet Server API (ISAPI) applications and Common Gateway (CGI) scripts must be placed into the default \Scripts directory or into a directory configured with Execute permission.

  Execute pemission must be set in both Internet Service Manager and File Manager when you install applications and scripts on an NTFS drive.

  Install server applications into a directory that is configured for Execute in Internet Service Manager and is *not* configured for Write permission on an NTFS drive. This will prevent malicious users from copying programs to your computer that could damage it when run.

Require Secure SSL Channel
: Allows users to send information to the server in encrypted format, ensuring data privacy.

Note that the FTP service supports Read and Write only; the Gopher service supports Read only.

NTFS Permissions

On NTFS drives you must also ensure that similar permissions are set on directories.

Securely Configuring the WWW Service

In addition to implementing the previous suggestions on securing Windows NT Server, you can further enhance your security by using Internet Service Manager to configure the WWW service.

Controlling Access by Username

To gain access to files, users must be identified with a valid username and password.

If you are allowing anonymous logon using the IUSR_*computername* account, you should first ensure that computer-wide User Rights (in the User Manager Policies menu) do not allow the IUSR_*computername* account, the Guests group, or the Everyone group any right other than to "Log on Locally." Next, ensure that the file permissions set in the Windows NT File Manager are appropriate for all content directories used by Microsoft Internet Information Server.

If you allow basic or Windows NT Challenge/Response password authentication, users can supply a username and password to gain access to areas that require specific authorization. The usernames must be valid usernames on the computer running Internet Information Server, or in a Windows NT domain accessible from that computer.

Controlling Access by IP Address

Microsoft Internet Information Server can be configured to grant or deny access to specific IP addresses. For example, you can exclude a harassing individual by denying access to your server from a particular IP address, or prevent entire networks from accessing your server. Conversely, you can choose to enable only specific sites to have access to your service.

Use the Advanced property sheet for the appropriate information service to limit access by IP address.

Choose the Granted Access button or the Denied Access button, and then list the exceptions by using the Add button.

Grant or Deny Access

Choose Single Computer and provide the IP address to exclude a single computer. Choose Group of Computers and provide an IP address and subnet mask to exclude a group of computers.

You are specifying (by IP address) which computer or group of computers will be granted or denied access. If you choose to grant access to all computers by default, you can then specify the computers to be denied access. Conversely, if

you choose to deny access to all users by default, you can then specify which computers are allowed access.

Disable Directory Browsing

Unless it is part of your strategy, you should disable directory browsing on the Directories property sheet. Directory browsing exposes the entire file structure; if it is not configured correctly, you run the risk of exposing program files or other files to unauthorized access.

Securing Data Transmissions with Secure Sockets Layer (SSL)

Previous sections of this chapter have dealt with securing your Microsoft Information Internet Server from unauthorized access. This section discusses protocols that use cryptography to secure data transmissions to and from your server.

Microsoft Internet Information Server provides users with a secure communication channel through support for Secure Sockets Layer (SSL) and RSA encryption.

Important

The SSL protocol provides secure data communication through data encryption and decryption. An SSL-enabled server can send and receive private communication across the Internet to SSL-enabled clients (browsers), such as Microsoft Internet Explorer version 2.0 for Windows 95 (included on the Microsoft Internet Information Server compact disc in the \Clients directory).

SSL is a protocol layer between the TCP/IP layer and the application layer (HTTP). SSL provides server authentication, encryption, and data integrity. Authentication assures the client that data is being sent to the correct server and that the server is secure. Encryption assures that the data cannot be read by anyone other than the secure target server. Data integrity assures that the data being transferred has not been altered.

Enabling SSL security on a Microsoft Internet Information Server involves the following steps:

1. Generate a key pair file and a request file.
2. Request a certificate from a Certification Authority.
3. Install the certificate on your server.
4. Activate SSL security on a WWW service directory.

Keep in mind the following points when enabling SSL security:

- You can enable SSL security on the root of your Web home directory (\Wwwroot by default) or on one or more virtual directories.
- Once enabled and properly configured, only SSL-enabled clients will be able to communicate with the SSL-enabled WWW directories.
- URLs that point to documents on a SSL-enabled WWW directory must use “https://” instead of “http://” in the URL. Any links using “http://” in the URL will not work on a secure directory.
- SSL security is enabled and disabled by using Internet Service Manager.

How to Acquire an SSL Digital Certificate

The following procedure details the entire SSL configuration process, including how to obtain an SSL digital certificate. You must consult your certificate authority before performing the following steps.

1. Change directories to C:\Inetsrv\Server (or the directory in which you installed Internet Information Server). This is the directory where the key and certificate utilities (Keygen.exe and Setkey.exe) are contained.

2. Use Keygen.exe to create two files. The first file is a key file containing the key pair; the second file is a certificate request file. (Type **keygen** with no arguments to see command syntax and an example).

Note

The following example creates the key file named Keypair.key and the certificate request file named Request.req for a server named www.mycompany.com: The files are generated in the current directory, C:\Inetsrv\Server.

```
C:\inetsrv\server>keygen MyPassword1 keypair.key request.req "C=US,
S=Washington, L=Redmond, O=Example, OU=Marketing,
CN=www.mycompany.com"

PCT/SSL Key generation utility, Version 1.0
Copyright (c) 1995 Microsoft Corporation

Generating key pair of length 1024 bits...
Completed.

Send the generated request file, Request.req, to your Certificate Authority for
signing.
```

By default Keygen.exe generates a key pair 1024 bits long. You can use the **-bits** parameter to specify keys that are 512 or 768 bits in length.

The argument in quotation marks in the Keygen.exe command line ("C=US, S=Washington, L=Redmond, O=Example, OU=Marketing, CN=www.mycompany.com") specifies several fields for the certificate request related to your organization and server.

Do not use commas in any field. Commas are interpreted as the end of that field and will generate a bad request without warning.

The valid field types follow:

C= 2 Letter ISO Country designations (for example, US, FR, AU, UK, DE)

S= State or Province (for example, Washington, Alberta, or California — do not abbreviate)

L= Locality (for example, Redmond, Calgary, or Redwood City)

O= Organization (Preferably ISO-registered top-level organization or company name)

OU= Organizational Unit

CN= Common Name (Domain Name of server, for example, www.mycompany.com).

If you run Keygen.exe more than once, note that it does not overwrite existing files; instead, it returns an error 80, meaning that the file already exists. Be sure to delete any existing files created by Keygen.exe if you need to run it more than once.

3. E-mail your request to your certificate authority for signing. It is best to include the Keygen.exe command line used, followed by the text from your request file (Request.req). Be sure to remove your password from the command line sent to your certificate authority. For example:

   From: webmaster@mycompany.com
   To: certificates@authority.com
   Subject: Certificate Request

   C:\inetsrv\server>keygen **<be sure to remove your password>** keypair.key request.req "C=US, S=Washington, L=Redmond, O=Example, OU=Marketing, CN=www.mycompany.com"

   -----BEGIN NEW CERTIFICATE REQUEST-----
   MIIBSzCBEQIBADAOMQwwCgYDVQQGEwNVU0EwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
   MIGJAoGBAI7nOitueTDEChjJTy0pKPSlDbtRDRouhCei5SWw2t5fxc7Vs46kPTF9
   lJ9UuwpM5TtzqDbBDn7PkpqfV5Cea6LYaAp5U10d8s+IAAqOlRivVf8az3M8cDUB
   eEBbdcWS7Oa2X9/
   R44p1oXODwUnuOnGVW3rh00QgpFOi85bAVvMRAgMBAAEwDQYJ
   KoZIhvcNAQEEBQADgYEAicID2qfNkttpx3zagtEEoDgDi5VQfA7bSIjXQ0RNtKKr
   MBa3tsqqNOUdA8KY4Abb7Yr9nFrjf3emSgJ2QcE2NxnEX59NS+JEbLkBTVRt/Twr
   3xjU8wq3sBMuy/9ReozxGWTWQB0RXyhDpJyOncwuSo/
   N8GUWAB2ddUm6+d+LraA=
   -----END NEW CERTIFICATE REQUEST-----

4. After completing all documentation requirements from your certificate authority and sending the e-mail in the previous step, you will probably receive an e-mail response containing a signed certificate from your certificate authority. For example:

   From: certificate@authority.com
   To: webmaster@mycompany.com
   Subject: Certificate Response

   -----BEGIN CERTIFICATE-----
   ZIICUjCCAb8CBQJyAAL3MA0GCSqGSIb3DQEBAgUAMF8xCzAJBgNVBAYTAlVTMSAw
   HsYDVQQKExdSU0EgRGF0YSBTZWN1cml0eSwgSW5jLjEuMCwGA1UECxMlU2VjdXJl
   IFNlcnZlciBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw05NTA5MTkwMDAwMDBa
   FwZaNjAzMjAyMzU5NTlaMIGFMQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGlu
   Z3RvbjEQMA4GA1UEBxMHUmVkbW9uZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBv
   cmF0aW9uMQ8wDQYDVQQLEwZibGRnMjYxHjAcBgNVBAMUFUtleU5ldCoubWljcm9z
   b2Z0XCVvbTCBnTANBgkqhkiG9w0BAQEFAAOBiwAwgYcCgYEAvp3bjApkrNNBtj4q
   3ngFdfVMF+Jonem6zwsyBM0WmxVbE0larmFAK1MAaRro9qvqH2LFRdWHHdgb8dhp
   h5mzYMtEoRiLnY/saoUDu1VMBloUpVh1ErbkNtdVDXoQvwq+Ij5df7y2rQTezf55
   uVDNQ8kmcJYDBkAXNSZQbEknpOUCAQMwDQYJKoZIhvcNAQECBQADfgAdT6fQntzx
   YXzMsL78qaOheMk+Mb6CKclzLBCYQwKSOGZBWFuhpLbOkMoBCV3u37UcK/RxLSzp
   XIMU5aDWP6gv8XUraDXlWhEAB3fBPdHKQE81nKpcVjiR53UkLGTljLATYnoCdx9a
   HQyCVVSmbsyFKMX4Q5PXoOAYd1fOUA==

-----END CERTIFICATE-----

5. Copy the text to a file by using Notepad or other text editor and save it (for example, as Certif.txt).

6. Use Setkey.exe to install your signed certificate on the server, for example:

   ```
   setkey MyPassword1 keypair.key certif.txt
   ```

If you do not specify an IP address, the same certificate will be applied to all virtual servers on the system that are configured to use a secure SSL channel for communication. Specify the IP address of a virtual server if the certificate should apply only to that IP address or domain name. For example:

```
setkey MyPassword1 keypair.key certif.txt 10.191.28.45
```

---

7. Use Internet Service Manager to set the Require Secure SSL Channel option for directories that you want to protect by using SSL. For example:

   The configuration in the preceding graphic shows the SSL-protected directory C:\Www\Secure-content for the virtual server on IP address 10.191.28.45. To gain access to this content, a client would specify https://www.mycompany.com/storefront (note the “https” rather than “http”). Clients must then use the https:// syntax to access any content in the \Storefront directory. Links to content in the \Storefront directory should be changed to use “https” as well. Standard requests (for example, http://www.mycompany.com/storefront) will fail.

Suggestions for SSL Configuration and Operation

Microsoft recommends that you use separate content directories for secure and public content (for example, C:\Inetsrv\Wwwroot\Secure-Content and C:\InetsrvWwwroot\Public-Content). It is important to avoid having a server directory not protected by SSL as a parent for a secure directory.

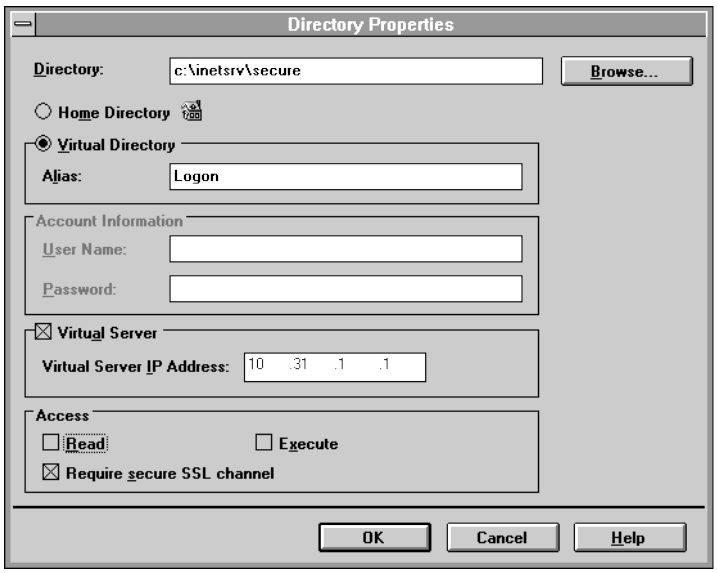
It is suggested that you save your key file (Keypair.key) in a safe place in case you need it in the future. It is a good idea to store Keypair.key on a floppy disk and remove it from the local system after completing all setup steps. Do not forget the password you assigned to the key pair file in step 2.

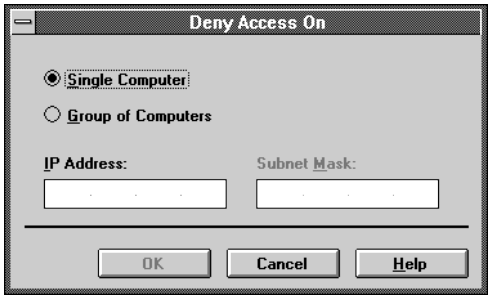
Setkey.exe Notes

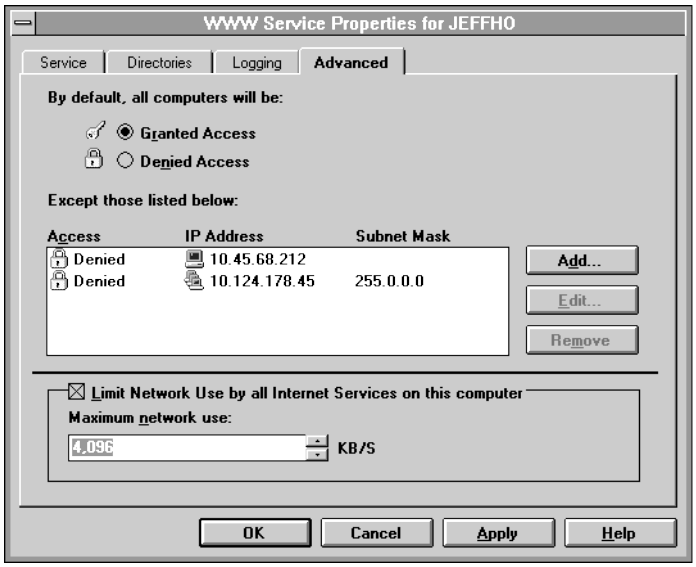
Do not specify a server name when running Setkey.exe on the local computer. After running Setkey.exe, restart the WWW service to enable SSL.

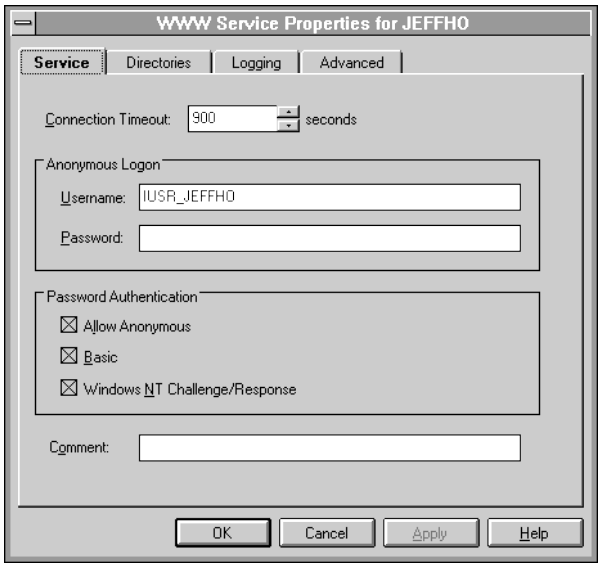
BLANK PAGE

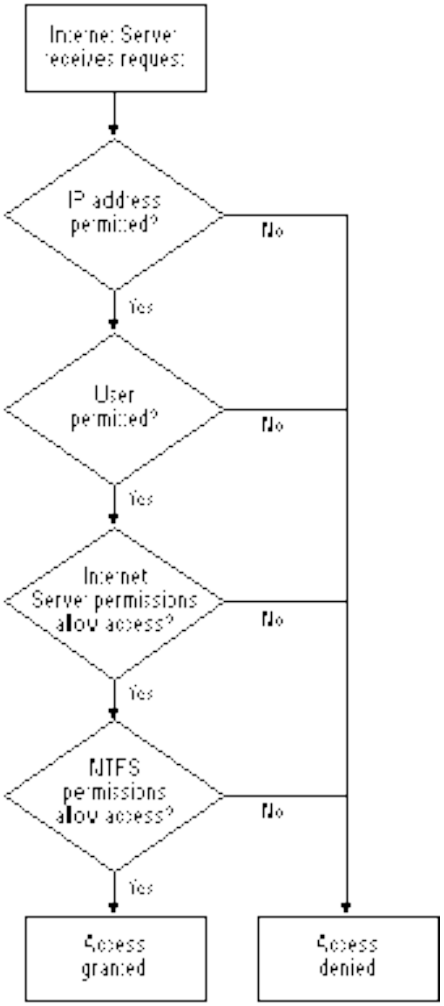
This page is intentionally left blank to preserve page numbering for the Table of Contents and Index. This text will appear on screen, but will not print on a PostScript printer.

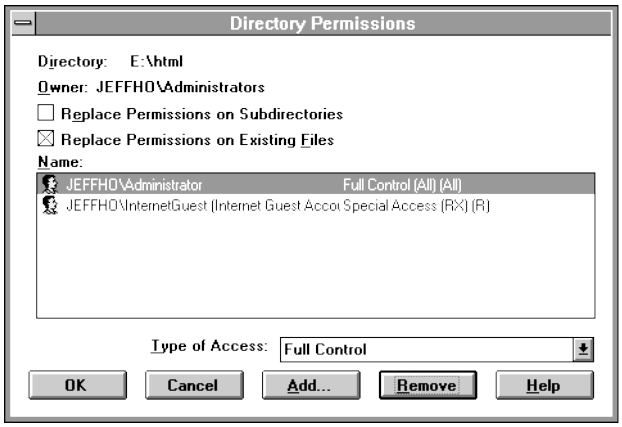





WWW Service Properties for JEFFHO
Service
Directories
Logging
Advanced
By default, all computers will be:
Granted Access
Denied Access
Except those listed below:
Access
IP Address
Subnet Mask
Denied
10.45.68.212
Denied
10.124.178.45
255.0.0.0
Add...
Edit...
Remove
Limit Network Use by all Internet Services on this computer
Maximum network use:
4,096
KB/S
OK
Cancel
Apply
Help


WWW Service Properties for JEFFHO
Service
Directories
Logging
Advanced
Connection Timeout:
900
seconds
Anonymous Logon
Username:
IUSR_JEFFHO
Password:
Password Authentication
Allow Anonymous
Basic
Windows NT Challenge/Response
Comment:
OK
Cancel
Apply
Help


Internet Server receives request
IP address permitted?
No
Yes
User permitted?
No
Yes
Internet Server permissions allow access?
No
Yes
NTFS permissions allow access?
No
Yes
Access granted
Access denied


Directory Permissions
Directory: E:\html
Owner: JEFFHO\Administrators
Replace Permissions on Subdirectories
Replace Permissions on Existing Files
Name:
JEFFHO\Administrator Full Control (All) (All)
JEFFHO\InternetGuest (Internet Guest Acco Special Access (RX) (R)
Type of Access:
Full Control
OK
Cancel
Add...
Remove
Help