Controlling Security by IP Address

To deny access to a specific computer or group of computers

1. In the Advanced property sheet of Internet Service Manager, choose the Granted Access button.
2. Click Add.
3. In the IP Address box, type the IP address of the computer to be denied access to your site or click the button next to the IP Address box to use a DNS name, such as www.company.com.

   To deny access to a group of computers, select Group of Computers. In the IP Address and Subnet Mask boxes, type the IP address and the subnet mask for a group to be denied access.
4. Click OK.

   Access will be granted to all computers except the ones in the window with an Access status of Denied.
5. In the Advanced property sheet, click OK.

To grant access to only a specific computer or group of computers

1. In the Advanced property sheet of the Internet Service Manager, choose the Denied Access button.

   This step denies access to all computers except those you specifically grant access to.
2. Click Add.
3. In the IP Address field, type the IP address of the computer to be granted access, or click the button next to the IP Address box to use a DNS name, such as www.company.com.

   To grant access to a specific group of computers, select Group of Computers. In the IP Address and Subnet Mask boxes, type the IP address and the subnet mask for the group to be granted access to.
4. Click OK.

   Access will be denied to all computers except those in the window with an Access status of Granted.
5. In the Advanced property sheet, click OK.

Controlling Security by ACL on NTFS Drives

To secure your files on a Windows NT NTFS drive

1 Put your files on your NTFS drive and add them to your Internet information service by using the Directories property sheet in Internet Service Manager.

2 In the Windows NT File Manager, select the directory you want to secure (select your site root to secure the entire site).

3 From the Security menu, choose Permissions.

4 In the Directory Permissions dialog box, click Add to add users and groups.

5 In the Add Users and Groups dialog box, add the users that you want to grant access to.

6 Click OK.

7 In the Directory Permissions dialog box, select the users and groups that you want to assign permission to.

8 From the Type of Access list box, choose the permission level you want for the selected user or group.

9 Click OK.

Logging to a File

To log to a file

1 In Internet Service Manager, double-cliick a service to display its property sheets, then click the Logging tab.

2 Select the Enable Logging check box.

3 Select Log to File.

4 To create a new log file when certain conditions are met, select the Automatically open new log check box.

The service will close the log file and create a new one with a different name in the same directory when the appropriate interval or file size is reached. Log filenames are as follows:

*SLOG if Automatically open new log is not enabled.

*S*nnn*.LOG (where *nnn* is a sequentially increasing number) if When file size reaches is enabled.

**mmddyy*.LOG (where *mmddyy* is the month, day, and year when the log file is created) if one of the Daily, Weekly, or Monthly options is enabled.

For the Daily, Weekly, or Monthly option, the log file is closed the first time a log record is generated after midnight on the last day of the current log file. The new log filename will include the date of the first day in the log file.

For the When file size reaches option, every time the log file is closed and a new one is created, the sequential number in the filename is incremented.

When logging to a file, the maximum total log line is 1200 bytes. Each field is limited to 150 bytes.

Logging to a Database

When you install Microsoft Internet Information Server, logging to a file is the default method of logging. If you prefer to collect logs in a database, you must install ODBC version 2.5. You should then use the sample HTML pages installed with Internet Information Server to set up logging to a database. To access the pages, ensure that the WWW service is running, then in the Internet Explorer Address box, type the local computer name. Alternatively, you can follow the manual procedure in this Help topic.

For best results, log to a Microsoft SQL Server version 6.0 database. If you do not want to log to a database or use the Internet Database Connector on a Web server, do not install any ODBC drivers.

When using ODBC for logging, each field is limited to 200 bytes.

To manually prepare for logging to a database

1 Create a table that conforms to the sizes of the fields for your database programs, such as Microsoft SQL Server.

   In SQL Server, the sizes of the fields for a table are as follows:

   ClientHost char(50), username char(50), LogDate char(12),
   LogTime char(15), service char(20), machine char(20),
   serverip char(50), processingtime int, bytesrecvd int,
   bytessent int, servicestatus int, win32status int,
   operation char(200), target char(200), parameters char(200))

2 Set up a database on your server and create a system Data Source Name (DSN).

   Note: For Microsoft Access, the system DSN is the filename of your database.

To log to a database

1 In Internet Service Manager, double-click the service for which you want to set up the database.

2 Click the Logging tab.

3 Select the Enable Logging check box.

4 Select Log to SQL/ODBC database.

5 In the ODBC Data Source Name (DSN) box, type the DSN that you added in step 2 of the previous procedure.

6 In the Table field, type the name of the table (not the filename of the table).

7 In the User Name and Password fields, type a username and password that is valid for the computer on which the database resides.

8 Click Apply and then click OK.

Often, the SQL Server database is kept on a separate computer. If you want to log activity to a SQL Server database located on another computer, Internet Information Server uses an anonymous user account (as set in the Sessions dialog box). The username must be a valid user account on the other computer. Even if the database is the same computer as the Internet Information Server (called "local" by Internet Information Server), the anonymous user must have permission to access the database.

How to Read Log Files

Following are three entries in a log from a server running the WWW, Gopher, and FTP services; the entries are in two tables only because of width limitations. Note that you can use the **convlog** utility to convert to other log formats.

Client's IP address	Client's username	Date	Time	Service	Computer name	IP address of server
10.75.176.21	-	12/11/95	7:55:20	W3SVC	TREY1	10.107.1.121
10.16.7.165	anonymous	12/11/95	23:58:11	MSFTPSVC	TREY1	10.107.1.121
10.55.82.244	-	12/11/95	0:00:34	GopherSvc	TREY1	10.107.1.121

Processing time	Bytes received	Bytes sent	Service status code	Windows NT status code	Name of the operation	Target of the operation
29282	277	3223	200	0	GET	small.gif
60	14	0	0	0	[376] PASS	intro
27069	21	62184	0	0	file	form1.bmp

Parameters for the operation, if applicable, will be listed in the final fields.

Note: All fields are terminated with a comma (,). A hyphen acts as a placeholder if there is no valid value for a certain field.

Converting Log File Formats

The Microsoft Internet Log Converter converts Microsoft Internet Information Server log files to either European Microsoft Windows NT Academic Centre (EMWAC) log file format or the Common Log File format. Convlog.exe is located in the \Inetsrv\Admin directory.

To convert logs to other formats

1 Add convlog.exe (in the \Inetsrv\Admin directory) to your path.

2 In a command prompt window, type the **convlog** command. See the syntax and examples below.

Syntax

convlog -s[f|g|w] -t [emwac | ncsa[:*GMTOffset*] | none]
-o [*output directory*] -f [*temp file directory*] -h *LogFilename*

Parameters

-s[f|g|w]

Specifies the service for which to convert log entries.

f = Process FTP log entries
g = Process Gopher log entries
w = Process WWW log entries

The default for the -s switch is to convert logs for all services.

-t [emwac | ncsa[:*GMTOffset*] | none]

Specifies the target conversion format . The default is to create output files in EMWAC format.

-o [*output directory*]

Specifies the directory for the converted files. The default is the current directory

-f [*temp file directory*]

Specifies a temporary directory to hold temporary files created by **convlog**. The default is C:\Temp or the directory specified by the "tmp" environment variable.

-n[m[*cachesize*]|i]

Specifies whether to convert IP addresses to computer or domain names. The default is to not convert IP addresses to computer names.

m[*cachesize*] = Specifies to convert IP addresses to computer names. The default *cachesize* is 5000 bytes.

i = Specifies to not convert IP addresses to computer names.

-h

Displays Help.

LogFilename

Specifies the name of the log to be converted. **Convlog** will display the filename for the converted file.

Examples

convlog -sf -t ncsa -o c:\logs in*.log
convlog -t ncsa:-0300 in*.log
convlog -o \\stats\logs c:\logs\in*.log
convlog -sfg in*.log
convlog -nm *.log
convlog -t none -nm:20000 *.log

Specifying Your Home Directory

To change your home directory

1 In Internet Service Manager, double-click the service for which you want to change the home directory.
2 Click the Directories tab.
3 In the Directory list, select the directory with the <home> alias.
4 Click Edit Properties.
5 In the Directory box type the name of the new directory or select a new directory by using the Browse button.
6 In the Access box select the access that you want to give users who connect to that directory.
7 Click OK.
8 Click Apply and then click OK.

To add a directory

1 In Internet Service Manager, double-click the service for which you want to add a directory.
2 Click the Directories tab.
3 Click Add.
4 In the Directory box, type the name of the new directory or select a new directory by using the Browse button.
5 In the Access box (if applicable), select the access you want to give users who connect to that directory.
6 Click OK.
7 Click Apply and then click OK.

To delete a directory

1 In Internet Service Manager, double-click the service for which you want to delete a directory.
2 Click the Directories tab.
3 In the Directory list select the directory you want to delete.
4 Click Remove.
5 Click Apply and then click OK.

Creating Virtual Directories

To create a virtual directory

1 In Internet Service Manager, double-click the service for which you want to add a virtual directory.

2 Click the Directories tab.

3 Click Add.

4 Click the Virtual Directory button, and type the name of the virtual directory in the Alias box.

5 Set the Access permissions.

6 Click OK.

7 Click Apply and then click OK.

Note: Virtual directories will not appear in directory listings (also called "directory browsing" for the WWW service). To access virtual directories users must know a virtual directory's alias and type in the URL address. For the WWW service, you can also create links in HTML pages. For the Gopher service, you can create explict links in tag files for users to access virtual directories.

Setting Bandwidth

Limiting the amount of bandwidth dedicated to users of Microsoft Internet Information Server is a handy feature if your Internet line has multiple purposes. Limiting bandwidth will then allow other operations (such as e-mail and remote logons) to use the same line with without being slowed down by too much activity on the Internet server.

To change bandwidth

1 In Internet Service Manager, double-click the service for which you want to change the bandwidth usage.

2 Click the Advanced tab.

3 Select Limit Network Use by all Internet Services on this computer.

4 Select the number of kilobytes per second you want to allow for Internet services.

5 Click Apply and then click OK.

As long as the actual bandwidth being used remains below the level you set, the read, write, and transfer functions are enabled. If actual bandwidth approximates the value you set, reads are blocked. If actual bandwidth exceeds the level you set, reads are rejected and file transfers are blocked until bandwidth equals or falls below the set value.

Registry Overview

The configuration Registry stores values that define the working environment for the Windows NT operating system and any services installed on the Windows NT Server computer. Usually, to change these values, you use graphical tools, such as Control Panel, Windows NT Setup, or Internet Service Manager. Windows NT Server also includes a utility, the Registry Editor (Regedt32.exe), which you can use to inspect and modify the configuration Registry directly.

Microsoft Internet Information Server services are configured by using Internet Service Manager. The services also use several additional configuration parameters in the Registry not configured by using Internet Service Manager. Parameters are either specific to a service or are global to Internet Information Server and all services.

Wherever possible, you should use Microsoft Internet Information Server to make changes to your Internet Server settings. For a Registry change to take effect, you must restart the service affected by the change. For global entries you must restart all services.

The entries listed in this Help file are the values used by Internet Information Server.

- Global Entries
- Service-Specific Entries with Common Names
- WWW Service Entries
- FTP Entries
- Gopher Entries
- Setup Entries

The following topics help you configure the Registry for specific needs.

- Server MIME Mapping
- Configuring More than Five Virtual Servers
- Associating Interpreters with Applications (Script Mapping)
- Adding Virtual Directories

Before you modify the Registry, it is strongly recommended that you read Part IV of the *Windows NT Resource Guide* (found in the Microsoft Windows NT Resource Kit). This part of the book describes in detail how to use and change parameters in the Registry.

CAUTION Using Registry Editor incorrectly can cause serious problems, including corruption that may make it necessary to reinstall Windows NT or Microsoft Internet Information Server. Using the Registry Editor to edit entries in the Registry is equivalent to editing raw sectors on a hard disk. If you make mistakes, your computer's configuration could be damaged. You should edit Registry entries only for settings that you cannot adjust through the user interface, and be very careful whenever you edit the Registry directly.

Global Registry Entries

These parameters are used for global control of the Microsoft Internet Information services.

Registry Path:

HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet
\Services
\InetInfo
\Parameters

BandwidthLevel REG_DWORD

Range: 0 - 0xFFFFFFFF

Default: 0xFFFFFFFF

Specifies the maximum network bandwidth used for Internet Information Server. This helps to prevent overloading the network with Internet Information Server activity. For example, for administrators of small corporate servers, where a single server is used for multiple sites, this will help to reduce network usage for Internet Information Server servers. It is recommended that this parameter be set from Internet Service Manager. Otherwise, the server must be stopped and restarted for this value to take effect. The value 0xFFFFFFFF means "do not restrict bandwidth".

MemoryCacheSize REG_DWORD

Range: 0 - 0xFFFFFFFF

Default: 3072000 (3MB)

Internet Information Server caches system handles, directory listings, and other values of frequently used data to improve performance of the system. This parameter specifies the amount of memory in bytes to allocate for that cache. When this value is changed, the server must be stopped and restarted for this to take effect. A value of 0 means "do not do any caching". The performance may be low when caching is off. Sites with heavy traffic can increase this size, provided there is sufficient RAM on the computer.

LogFileBatchSize REG_DWORD

Range: 0 - 0xFFFFFFFF

Default: 64*1024 (64 KB)

Specifies the batch size for writing a log file. The server caches the last LogFileBatchSize bytes of data in memory buffers before it dumps the current buffer to disk. Such batch processing reduces the amount of disk traffic created by log files. In some instances, you may need to reduce the time between writing the buffer to disk. To change the default setting you must add this value to the key using the new setting.

ListenBackLog REG_DWORD

Range: 1-unlimited

Default: 15

Specifies the maximum number of active connections to hold in the queue waiting for server attention. Enhanced Internet Information Server functionality generally makes it unnecessary to use or modify this entry, although extremely heavy use might benefit by increasing this value up to 50.

Service-Specific Registry Entries with Common Names

These parameters are stored in the Registry by service, for service-specific behavior, but have the same name.

Registry Path:

HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet
\Services
ServiceName
\Parameters

where *ServiceName* is

MSFTPSVC FTP Service

GOPHERSVC Gopher Service

W3SVC WWW Service

AdminName REG_SZ

Range: String

Default: Administrator

Specifies the user-friendly administrator name. Gopher service uses this name to send back responses for Gopher+ queries. This parameter also serves as a way of identifying who administers a service.

AdminEmail REG_SZ

Range: String

Default: Admin@corp.com

Specifies the e-mail address for the administrator of a particular service. Gopher service uses this name to send back responses for Gopher+ queries.

ServerComment REG_SZ

Range: String

Default: “”

Specifies a user-friendly comment for a service. This information is used to add a configurable comment in Internet Service Manager.

EnableSvcLoc REG_DWORD

Range: 0, 1

Default: 1

The Internet Information Server services register themselves with a service locator so that the service can be discovered by Internet Service Manager. This parameter controls such registration. If set to 0, the service will forgo registration. Set to 1, it registers the service for service location. To change the default setting, you must add this value to the key using the new setting.

AllowAnonymous REG_DWORD

Range: 0, 1

Default: 1

Specifies if an anonymous user should be allowed to connect and make a request to the server. By convention, most Internet services allow anonymous connections to gain access to files.

AnonymousOnly REG_DWORD

Range: 0, 1

Default: 0

Specifies if only anonymous connections are permitted. If set to 1, only anonymous connections are permitted (especially true of FTP service). To change the default setting, you must add this value to the key using the new setting.

AnonymousUserName REG_SZ

Range: String

Default: Guest

Specifies the name of the local user account to use for anonymous users. All server actions associate a username and password with the action. This parameter should not be changed in the Registry. You must change this parameter by using Internet Service Manager so that the appropriate password can also be set. The password is stored in protected area in the Registry.

ConnectionTimeOut REG_DWORD

Range: 0-0xFFFFFFFF

Default: 600 seconds

Specifies the time the server should maintain a connection when there is no activity.

LogAnonymous REG_DWORD

Range: 0, 1

Default: 1

Controls whether a log record should be written for anonymous connections. If set to 0, no log records are written for anonymous connections.

LogNonAnonymous REG_DWORD

Range: 0, 1

Default: 1

Controls whether a log record should be written for non-anonymous connections. If set to 0, no log records are written for non-anonymous connections. Only the FTP and WWW services have non-anonymous user support.

LogFileDirectory REG_EXPAND_SZ

Range: String

Default: %systemroot%\system32\logfiles

Specifies the directory in which log files are to be stored. Each service generates a log record for each request processed.

LogFilePeriod REG_DWORD

Range: 0,1,2,3

Default: 1

Specifies the type of log files to be produced where

0=No period. Each log file is limited by size specified in LogFileTruncateSize.

1=Open a new log file each day

2=Open a new log file every week

3=Open a new log file every month

LogFileTruncateSize REG_DWORD

Range: 0-0xFFFFFFFF

Default: 4,000,000,000 bytes

Specifies the maximum size of each log file generated. Once the specified size is reached, the logging module automatically opens a new log file. A value of 0 means "do not truncate".

LogSqlDataSources REG_SZ

Range: String

Default: “”

This string specifies the name of the ODBC data source to use for sending the request logs for the service to a SQL-compatible database system. This data source should be a system DSN in the ODBC installation on the server.

LogSqlTableName REG_SZ

Range: String

Default: “”

Specifies the name of the ODBC table name used for sending the request logs for the service to a SQL-compatible database system. The table should be created by the administrator as per the specification provided with the services. The user should also have proper access permissions to insert data into the table.

LogSqlUserName REG_SZ

Range: String

Default: “”

Specifies the username to use when accessing the ODBC data source specified for ODBC-based logging. This user must be a valid user on the server to which the LogSqlDataSource Registry parameter is pointing.

LogSqlPassword REG_SZ

Range: String

Default: “”

Specifies the password to establishing an ODBC connection for a particular user account on the ODBC data source. The password is stored as a clear text.

LogType REG_DWORD

Range: 0, 1, 2

Default: 1

Specifies the type of logging. The type specifies the destination of log files where

0=No logging

1=Log to files

2=Log to ODBC data source

MaxConnections REG_DWORD

Range: 0 - 0xFFFFFFFF

Default: 1000

Specifies maximum number of simultaneous connections that server allows at any given time. When the number of current connections exceeds this value, the service rejects the request. A friendly message can be sent to the client refused access.

WWW Service Registry Entries

In addition to the parameters listed in Service-specific Registry Entries with Common Names, the WWW service maintains the following parameters.

Registry Path:

HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet
\Services
\W3SVC
\Parameters

CacheExtensions REG_DWORD

Range: 0-1

Default: 0x1

Specifies whether ISAPI extensions are cached in memory. If set to 0, ISAPI extensions are not cached. See the ISAPI documentation for more information.

CheckForWAISDB REG_DWORD

Range: 0, 1

Default: 0

The WWW Service uses the WAIS Toolkit to support Web based searches. Microsoft does not provide the WAIS Toolkit. This flag is used to specify if search is supported and if the service should check for WAIS Toolkit. If set to 0, the service does not support searches and does not look for WAIS Toolkit. If set to 1, then the service supports searches if Waislook.exe is installed in the system.

CreateProcessAsUser REG_DWORD

Range: 0-1

Default: 1

For CGI scripts, by default the server runs the script in the context of the user making the request by using the Win32 CreateProcessAsUser API. If you set this flag to 0, CGI scripts will be started with the CreateProcess API and the scripts will run in the system context. This has serious security implications because CGI scripts will have much greater access to the system then they normally would have.

Default Load File REG_SZ

Range: String

Default: Default.htm

Specifies the file to return to a client if no file is included in a client's request.

Dir Browse Control REG_DWORD

Range: see the explanation paragraph

Default: 0x4000001e

Specifies both the display attributes of directory browsing and whether the **Default Load File** is used. the value used here is arrived at by "Oring" (adding) the hexidecimal values of the attributes listed below. The first four digits of the specified value controls whether directory browsing is enabled and whether the default file is enabled. For example, the default setting 0x4000001e has directory browsing disabled but the default file is loaded. To enable directory browsing, you would add the value 0x80000000 to the default setting 0x4000001e, resulting in the value 0xc000001e. To control browsing attributes, you would modify the last four digits. For example, to

show only the date of files you could use the value 0xc0000002.

Behavior	**Value**
Load Default File	0x40000000
Directory browsing enabled	0x80000000
Browsing Attributes	
Show Date	0x00000002
Show Time	0x00000004
Show Size	0x00000008
Show Extension	0x00000010
Display long date	0x00000020

Filter DLLs REG_SZ

Range: String

Default: sspifilt.dll

Comma-separated list of ISAPI filter DLLs.

GlobalExpire REG_DWORD

Range: 0x0-unlimited (seconds)

Default: 0xffffffff

Specifies the time in seconds that files will be considered valid. This value is used by the server in the expires header [using Greenwich Mean Time (GMT) time] to indicate to clients how long a static file is valid. This is typically set to 0x0, to prevent the files on the server from being cached by proxies or clients.

NTAuthenticationProviders REG_SZ

Range: String

Default: NTLM

Lists possible Windows NT authentication schemes returned to clients. Internet Information Server provides the default NTLM scheme enabled in the WWW Service property sheet. Third parties may provide alternate Windows NT authentication schemes in the future.

ScriptTimeout REG_DWORD

Range: 0x1-0x80000000

Default: 0x384

Specifies the maximum time the WWW service will wait for a response from CGI scripts.

SecurePort REG_DWORD

Range: 0x0-0xfa00

Default: 0x1bb

Specifies the TCP port to use for SSL.

ServerSideIncludesEnabled REG_DWORD

Range: 0x0-0x1

Default: 0x1

Set to 0x1, this value enables the use of Include files to permit including repetitive information in files.

ServerSideIncludesExtension REG_SZ

Range: String

Default: .stm

Specifies the file extension for files that will use Include statements.

FTP Service Registry Entries

In addition to the parameters listed in Service-specific Registry Entries with Common Names, the FTP service maintains the following parameters.

Registry Path:

HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet
\Services
\FTPSVC
\Parameters

EnablePortAttack REG_DWORD

Range: 0, 1

Default: 0

This parameter is set by default to prevent a security problem in the FTP protocol specification. The FTP service specification allows passive connections to be established based on the port address given by client. This can allow hackers to execute destructive commands in the FTP service. The problem occurs when the FTP service connects using a port other than FTP Data port (20) and port number is less than IP_PORT_RESERVED (1024). **EnablePortAttack** controls if such an attack should be allowed. By default, the service does not make any connections to port numbers lower than IP_PORT_RESERVED (other than 20). If you want to users to connect using other ports as specified in the FTP RFC, this flag should be enabled.

ExitMessage REG_SZ

Range: String

Default: “”

FTP Service sends back an exit message when a client sends a **quit** command. This string specifies the exit message sent.

GreetingMessage REG_MULTI_SZ

Range: String

Default: “”

When a new user connects to the FTP Server, the server can send a friendly welcome message detailing contents and administrative information. This string (multiple lines) specifies the message to use for greeting the new client connections.

MaxClientsMessage REG_SZ

Range: String

Default: “”

When the current connection exceeds the MaxConnections specified for the service, the service can send a friendly message to clients. This message is a single-line message.

AccessCheck REG_DWORD

Range: any

Default: any

Used for access check of incoming user connection. The server impersonates the logged-on user and attempts to open the Registry key for read and write. If the key does not exist, then read and write permissions are granted. If the key exists, then based on the access permission on the Registry key, read and write permissions are

granted to the user. This feature is useful for servers that publish content on a FAT volume and hence do not have the rich security features of NTFS. This is not a recommended approach to provide security because of poor manageability and performance. To enable this feature, you must add this value to the key using the appropriate access settings.

AllowGuestAccess REG_DWORD

Range: 0, 1

Default 1

Specifies if guest logons are permitted for FTP service. When a new user logs on, the server checks to see if the user is logged on as WIndows NT user with guest permissions. For a guest connection, based on the value of this entry, the FTP service either rejects or accepts the new connection. Permitting Guest access has been known to create problems in poorly managed sites. Under default installation of Windows NT systems, Guest is granted permissions for many types of access on the system. It is recommended that administrators do not permit access by using the Guest account. To change the default setting to "no access using the Guest account" you must add this value to the key using the new setting.

AnnotateDirectories REG_DWORD

Range: 0, 1

Default: 0 (FALSE)

FTP service supports annotating a directory with custom messages. The annotation text is stored in a special file named ~ftpsvc~.ckm in the directory to be annotated. If this file exists in the target directory of a Change Directory (CWD) FTP operation, then the service responds with the contents of this file for the operation. This provides a way for administrators to add custom messages for directories under consideration. By default the service is configured to not send annotation text. If you choose to add a custom message, the annotation file should be created as well as setting this value to 1. Also, it is recommended you make the annotation file a hidden file so that the file does not show up on a directory listing.

MsdosDirOutput REG_DWORD

Range: 0, 1

Default: 1 (TRUE)

Specifies the style of directory output for a LIST operation from an FTP client. If the value is set to 1, the service generates a MS-DOS-style directory listing. If the value is set to 0, the service generates an UNIX-style listing. Some clients will not display MS-DOS-style listings. For this reason you should consider setting this value to 0. UNIX style listings consume more CPU time.

LowercaseFiles REG_DWORD

Range: 0, 1

Default: 0 (FALSE)

The FTP service uses the native case for filenames (how the filenames are stored in file system). However, in order for exact comparisons with case-sensitive file systems to work, it may be necessary to ensure that proper filenames are used. Administrators can add this value to ensure that the service uses lowercase for such comparisons.

Gopher Service Registry Entries

In addition to the parameters listed in Service-specific Registry Entries with Common Names, the Gopher service maintains the following parameters.

Registry Path:

HKEY_LOCAL_MACHINE\SYSTEM
\CurrentControlSet
\Services
\GOPHERSVC
\Parameters

CheckForWAISDB REG_DWORD

Range: 0, 1

Default: 0

The Gopher Service uses the WAIS Toolkit to support Gopher-based searches. Microsoft does not provide the WAIS Toolkit. This flag is used to specify if search is supported and if the service should check for WAIS Toolkit. If set to 0, the service does not support searches and does not look for WAIS Toolkit. If set to 1, then the service supports searches if Waislook.exe is installed in the system.

Setup Registry Entries

The Internet Information Server creates the following parameters during setup. These values are used by the Setup program after initial setup to determine the current configuration of your Internet Information Server. Note that multiple Registry paths are included in this Help topic.

HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft
INetMgr

InstalledBy REG_SZ

Range: INetStp

Default: INetStp

The presence of this entry indicates that Internet Information Server is installed.

HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft
INetMgr
\Parameters

MajorVersion REG_DWORD

Range: 1

Default: 1

Indicates the major version number, for example, the 1 in version 1.0.

MinorVersion REG_DWORD

Range: 1-9

Default: 0

Indicates the minor version number, for example, the 0 in version 1.0.

HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft
INetMgr
\Parameters
\AddOnServices

FTP REG_SZ

Range: string

Default: fscfg.dll

Defines the configuration DLL used by the FTP service.

Gopher REG_SZ

Range: string

Default: gscfg.dll

Defines the configuration DLL used by the Gopher service.

WWW REG_SZ

Range: string

Default: w3scfg.dll

Defines the configuration DLL used by the WWW service.

HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft
INetStp

AnonymousUser REG_SZ

Range: String

Default: IUSR_*computername*

Specifies the anonymous user account created during setup.

InstallPath EG_SZ

Range: String

Default: c:\inetsrv

Specifies the installation location for Internet Information Server.

MajorVersion REG_DWORD

Range: 1

Default: 1

Indicates the major version number, for example, the 1 in version 1.0.

MinorVersion REG_DWORD

Range: 1-9

Default: 0

Indicates the minor version number, for example, the 0 in version 1.0.

HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft
INetStp
Help

The presence of this entry indicates that Help is installed.

HKEY_LOCAL_MACHINE\SOFTWARE
\Microsoft
\INetExplore

InstalledBy REG_SZ

Range: INetStp

Default: INetStp

The presence of this entry indicates that Internet Explorer version 1.5 is installed.

Server MIME Mapping

If your server provides files that are in multiple formats, you must configure your server's Multiple Internet Mail Extensions (MIME) mapping to ensure your server maps the file type correctly when returning the file to remote browsers. If MIME mapping on the server is not setup for a specific file type, browsers may not be able to retrieve the file. Over 100 MIME-mappings are installed by default.

To configure additional MIME mappings

1 Start Regedt32 and open

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\InetInfo\Parameters\MimeMap

2 Add the value for the MIME mapping needed on your server using the following syntax.

Syntax:

<mime type>,<filename extension>,,<gopher type>

Note the double comma before the gopher type parameter.

Example:

```
text/html,htm,,1

image/jpeg,jpeg,,5
```

The default entry with the filename extension specified as an asterisk (*) is the default MIME type used when a MIME mapping does not exist. For example, to handle a request for the file Current.vgr when the the filename extension .vgr is not mapped to a MIME type, the server will use the MIME type specified for the asterisk extension, which is the type used for binary data.Usually, this will cause browsers to save the file to disk.

Configuring More than Five Virtual Servers

The Windows NT user interface allows only five IP addresses to be assigned to a network adapter card. You must use Regedt32.exe to assign more than five IP addresses to a network adapter card. You must know the network adapter card name and card number used in the Registry. You can get the name from the manufacturer of your network adapter card. For example, the first Intel EtherExpress PRO card installed in a computer running Windows NT uses the name **EPRO1**.

To configure more that five IP addresses on a network card

1 Start Regedt32.exe and open

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<*net card name*><*card number*>\Parameters\Tcpip

2 Double-click the IPAddress value.

3 Type every IP address you want assigned to the network adapter card. Each address must separated by a space or carriage return.

4 If applicable, double-click the SubnetMask value.

5 Type subnet masks for the IP addresses added in step 3. Pair the subnet masks to an IP address by entering the subnet masks in the same order as the IP addresses.

Associating Interpreters with Applications (Script Mapping)

With filename-extension mapping, you can map filename extensions to the proper program to run files with those extensions. The file extensions shown below are preinstalled.

.bat or .cmd=C:\WINNT35\System32\cmd.exe /c %s %s

.idc=c:\Inetsrv\Server\Httpodbc.dll

For other filename extensions, you must edit the information in the the Windows NT Registry.

In the .bat example above, the first %s is the mapped URL (that is, E:\Webroot\Scripts\Test.bat). The second %s represents the parameters to the URL (in other words, the query string; the second %s is used only if an equals sign is not found).

Thus you can reference URLs like: /scripts/test.bat?This+is+a+search

or /scripts/bugs.idc?Assign=Johnl

To configure additional script mappings

1 Start Regedt32.exe and open
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ScriptMap
2 From the Edit menu, choose Add Value. The Data type is REG_SZ.
3 Type the filename extension used for your scripts.
4 In the String editor, type the full path to the interpreter used with that script.
5 Restart the WWW service.

Adding Virtual Directories by Using the Registry

You should use Internet Service Manager to manage your virtual directories. You can, however, add or modify virtual directories by using Regedt32.exe.

To add virtual directories using the Registry:

1 Start Regedt32.exe and open
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<*service*>\Parameters\Virtual Roots
where <*service*> is W3SVC, GOPHERSVC, or MSFTPSVC

2 From the Edit menu, choose Add Value. The Data type is REG_SZ.

3 Type the alias name for your directory and click the OK button.

4 In the String editor, type the full path to the virtual directory.

Note Virtual directories will not appear in directory listings (also called directory browsing for the WWW service). To access a virtual directory users must know the virtual directory's alias, and type the URL address in their browser. For the WWW service, you can also create links in HTML pages. For the Gopher, service you can create explicit links in tag files for users to access virtual directories. For the FTP service, you can list virtual directories using directory annotations.

Directories Overview

Each of the Internet services publishes information stored in one or more directories. The administrator specifies these publishing directories on the Directories property sheet of Internet Service Manager. Adding a directory on this property sheet allows the respective service to make available to clients information stored in the specified directory, and all of its subdirectories. Directories not listed on this property page are not available to clients.

Home Directories

One of the directories listed on the Directories property sheet is marked as a home directory (sometimes referred to as a *root* directory). The path used in a client request to refer to the home directory is a forward slash (/). When a client request contains a path of /, or does not specify the path to a resource, the Internet server looks in the defined home directory for the resource. For example, all of the following URLs refer to the Web server's home directory.

http://inetsrvr.microsoft.com

http://inetsrvr.microsoft.com/

http://inetsrvr.microsoft.com/content.htm

The action taken by the Web server for the first two URLs above depends on the settings of the Default Document and Directory Browsing options, specified on the Service property sheet of Internet Service Manager. For the third example, the HTML file content.htm, located in the home directory, is sent to the client. If a file by that name does not exist in the home directory, the server returns an error to the client. Other directories are not searched for such a file.

When a client logs on to the FTP service, the service looks for a subdirectory under the specified home directory with the name of the user logging on. For anonymous FTP logons, the service looks for a directory called 'anonymous' under the home directory. If such a directory exists, the user will start the session with it as the current directory. If such a directory is not found, the current directory will be the home directory.

Subdirectories of the home directory are accessible to clients. For example, if a Web server is configured with a home directory of C:\Wwwroot, then the following URL:

http://inetsrvr.microsoft.com/data/content.htm

looks for a file by the name content.htm in the directory C:\Wwwroot\data. If the 'data' subdirectory doesn't exist, or the file is not found in that directory, the server will return an error. The FTP service allows changing the current directory to subdirectories of the home directory (by using the **cd** command), and Gopher selectors can refer to objects in subdirectories of the home directory.

Virtual Directories

Each of the Internet services can publish from multiple directories. Each directory can be located on a local drive, or across the network, by specifying the directory with a Universal Naming Convention (UNC) name, and a username and password to use for access permission. Virtual directories on network drives must be on computers in the same Windows NT domain as the Internet Information Server. An Internet service can have one home directory and any number of other publishing directories. These other publishing directories are referred to as virtual directories.

To simplify client URL addresses, the services present the entire set of publishing directories to clients as a single directory tree. The home directory is the root of this "virtual" directory tree, and each virtual directory is addressed as if it were a subdirectory of the home directory. Actual subdirectories of the virtual directories are available to clients as well.

Note Virtual directories will not appear in directory listings (also called directory browsing for the WWW service). To access a virtual directory users must know the virtual directory's alias, and type the URL address in their browser. For the WWW service, you can also create links in HTML pages. For the Gopher, service you can create explicit links in tag files for users to access virtual directories. For the FTP service, you can list virtual directories using directory annotations.

When a virtual directory is defined in Internet Service Manager, an alias is associated with the virtual directory. The alias is the subdirectory name that will be used by clients to access information in the virtual directory. If

alias names for virtual directories are not specified by the administrator, an alias name is generated automatically by Internet Service Manager.

For example, suppose an administrator defines two directories for the Web service as follows:

C:\Inetsrv\Wwwroot	<home directory>
D:\Webdata	Alias = data

If C:\Wwwroot contains the subdirectory C:\Wwwroot\scripts\, and D:\Webdata contains the subdirectory D:\Webdata\images\, the following Uniform Resource Locators (URLs) can be requested by a Web client:

http://inetsrvr.microsoft.com/schedule.htm

http://inetsrvr.microsoft.com/scripts/query1.htm

http://inetsrvr.microsoft.com/data/stocks.htm

http://inetsrvr.microsoft.com/data/images/graph1.htm

Troubleshooting an IP Network

To troubleshoot an IP network

- Always begin at the network interface layer and work up to the application layer.
- Make sure protocols at each layer of the Internet protocol suite can communicate with the layer above and below it.

There are two steps in troubleshooting. Make sure you can

1 Ping successfully.

   If you can ping successfully, you have verified IP communications between the network interface layer and the internet layer. The **Ping** command uses the Address Resolution Protocol (ARP) to resolve the IP address to a hardware address for each echo request and echo reply.

2 Establish a session with a host.

   If you can establish a session, you have verified TCP/IP session communications from the network interface layer through the application layer.

Note: If you are unable to resolve a problem, you may need to use an IP analyzer (such as Microsoft Network Monitor) to view network activity at each layer.

The first goal in troubleshooting is to make sure you can successfully ping an IP address. Ping a host with its host name only after you can successfully ping the host with its IP address.

To troubleshoot the network interface and internet layers by using the Ping command

1 Ping the loopback address to verify that TCP/IP was installed and loaded correctly.

   If this step is unsuccessful, verify that the system was restarted after TCP/IP was installed and configured.

2 Ping your IP address to verify that it was configured correctly.

   If this step is unsuccessful, view the configuration by using the Network applet in the Windows NT Control Panel to verify that the address was entered correctly, and verify that the IP address is valid and that it follows addressing guidelines.

3 Ping the IP address of the default gateway to verify that the gateway is functioning and configured correctly.

   If this step is unsuccessful, verify that you are using the correct IP address and subnet mask.

4 Ping the IP address of a remote host to verify the connection to the wide area network.

   If this step is unsuccessful:

- Make sure that IP routing is enabled.
- Verify that the IP address of the default gateway is correct.
- Make sure that the remote host is functional.
- Verify that the link between routers is operational.

After you can successfully ping the IP address, ping the host name to verify that the name is configured correctly in the HOSTS file.

Verifying TCP/IP Session Communications

The next goal in troubleshooting is to successfully establish a session. Use one of the following methods to verify communications between the network interface layer and the application layer.

To establish a session with a Windows NT–based computer or other RFC-compliant NetBIOS-based host, make a connect with the **Net use** or **Net view** command. If this step is unsuccessful:

- Verify that the target host is NetBIOS-based.
- Confirm that the scope ID on the target host matches that of the source host.
- Verify that you used the correct NetBIOS name.
- If the target host is on a remote network, check the LMHOSTS file for the correct entry.

To establish a session with a non-RFC-compliant NetBIOS-based host, use the Telnet or FTP utility to make a connection. If this step is unsuccessful:

- Verify that the target host is configured with the Telnet daemon or FTP daemon.
- Confirm that you have the correct permissions on the target host.
- Check the HOSTS file for a valid entry if you are connecting using a host name.

Error Messages

A home directory already exists for this service. Creating a new home directory will cause the existing directory to no longer be a home directory. An alias will be created for the existing home directory.

This message is a warning only. It appears when the new home directory you are trying to add already exists. The maximum number of home directories allowed is one per virtual root.

Invalid Server Name

While trying to connect to a server, you typed an invalid server name. Try to connect again and make sure you type the name correctly.

More than 1 home directory was found. An automatic alias will be generated instead.

When getting the directory entries from the server, Internet Information Manager had determines that a duplicate exists. This duplicate may have been added through Registry editor or someother way.

No administerable services found.

While trying to connect to a server, you typed the name of a server that has no installed services that Internet Information Manager can administer. That is, WWW, FTP, or Gopher have not been installed on the computer you connected to.

The alias you have given is invalid for a non-home directory.

You're trying to assign the alias '/' to a non-home directory. This alias automatically means *home*.

The connection attempt failed because there's a version conflict between the server and client software.

This message is an RPC error message. The RPC interface doesn't match what is expected. This should happen only if you're running a beta admin or server. The official error is RPC_S_UNKNOWN_IF.

The service configuration DLL '*filename*' failed to load correctly.

The named service configuration dll (for example, W3scfg.dll) failed to load. The dll or one if its dependencies could be missing or corrupt. Generally this is a setup problem. Run the Setup program and Remove All and reinstall Microsoft Internet Information Server.

Unable to connect to target machine.

This message is an RPC error message that appears while executing an API. The computer could be down. The system error was EPT_S_NOT_REGISTERED or RPC_S_SERVER_UNAVAILABLE.

Unable to create directory.

The directory name and/or path you typed in in the New Directory Name box cannot be created. It could be an invalid path or a file may already exist that has this name.

Authentication and Security Integration with Windows NT

The WWW, Gopher, and FTP services included with the Microsoft Internet Information Server are fully integrated with Windows NT Server user accounts and file access permissions.

Every access to a resource (file, html page, Internet Server API (ISAPI) application, and so on.) is done by the services on behalf of a Windows NT user. The service uses that user's username and password in the attempt to read or execute the resource for the client.

The NTFS file system allows Access Control Lists (ACLs) to be assigned to files and directories. ACLs grant or deny access to the associated file or directory by specific Windows NT user accounts, or groups of users. When an Internet service attempts to read or execute a file on behalf of a client request, the user account offered by the service must have permission, as determined by the ACL associated with the file, to read or execute the file, as appropriate. If the user account does not have permission to access the file, the request fails, and a response is returned, informing the client that access has been denied.

File and directory ACLs are configured by using the Windows NT File Manager.

Anonymous Connections

An anonymous connection is processed when a client request does not contain a username and password. This occurs in the following cases:

- An FTP client logs on with the username "anonymous".
- All Gopher requests.
- A Web (HTTP) request's headers do not contain a username and password (this is the default on new Web connections with most browsers).

Each Internet service maintains a Windows NT username and password to be used for the processing of anonymous requests. When an anonymous request is received, the service "impersonates" the user configured as the "anonymous logon" user. The request will succeed if the "anonymous logon" user has permission to access the requested resource, as determined by the resource's ACL. For WWW only, if the user does not have permission to access the resource, the response returned to the client contains a list of supported authentication schemes for gaining access to the resource, based on server configuration. See the following paragraphs for more information.

The "anonymous logon" user account can be viewed and modified on the Service property sheet of Internet Service Manager. Multiple Internet Information Server services running on the same computer can use the same, or different, "anonymous logon" user accounts. Including the "anonymous logon" user account in file or directory ACLs allows for precise control of the resources available to "anonymous" clients.

The "anonymous logon" user account specified must be a valid Windows NT user account on the server computer, and the password specified must match the password for this user in that computer's user database. User accounts and passwords are configured using the Windows NT User Manager. The "anonymous logon" user account must have the user right (in the User Manager Policies Menu) to "Log on Locally."

When Internet Information Server is installed, Setup creates a user account on the server computer to be used for anonymous connections. The username of this account has the form "IUSR_*computername* where *computername* is the name of the computer running Windows NT Server. For example, the server's computer name is WEB1, the username created will be "IUSR_WEB1". The same "anonymous logon" user account is set up for all Internet Information Server services installed on the computer. The account is made a member of the computer's Guest group. This will, in most cases, give anonymous client requests access to public content published on the server. Run the Network applet in Control Panel to see the computer name configured for the Windows NT Server computer.

A randomly generated password is created for the "IUSR_*computername*" account. For maximum convenience and security, it is suggested that you change the password associated with this account to a password that you will remember, but is not easily guessed. To do this, you must specify the new password for the account in User Manager, and on the Service sheet of the Internet Service Manager, for each Internet Information Server service installed.

When Internet Information Server is installed on a primary or secondary domain controller, the "anonymous logon" user account is created in the user account database of the domain. When Internet Information Server is installed on a domain member-server, or a stand-alone server, the account is created on the local computer.

If Internet Information Server is installed on multiple domain controllers of the same domain, a separate user account is created in the domain user database for each Internet server computer. This does not cause any conflicts because each username is unique, containing the name of the associated computer. However, you may find it more convenient to create a single "anonymous logon" user account in the domain to use for all Internet Information Server domain controllers in the domain. This can simplify administration of ACLs. To do this, follow these steps:

- In User Manager, create a new "anonymous logon" user account in the domain. Be sure that this account is made a member of appropriate groups, given a secure password, and is given the User Right (in the Policies menu) to "Log on Locally".
- On the Service property sheet of Internet Service Manager, specify the new "anonymous logon" username and password. You must do this for each Internet Information Server service running on all primary and secondary domain controllers in the domain.
- When later installing Internet Information Server on other domain controllers in the domain, be sure to use Internet Service Manager to modify the "anonymous logon" username and password to match those created with User Manager. Do this for each Internet Information Server service installed.

Client Requests Containing Credentials

A request containing credentials is one of the following:

- An FTP client logs on with a valid Windows NT username and password. This requires that the FTP service's "Allow only anonymous connections" check box be cleared.

WARNING: FTP sends passwords across the network in clear text.

- A WWW (HTTP) request's headers contain a username and password (this is generally in response to an "access denied" response from a server). This is HTTP basic authentication.

WARNING: HTTP basic authentication sends passwords across the network in clear text.

- A WWW browser supports Windows NT Challenge/Response authentication protocol, and an anonymous client request is denied access to a resource. In this case, the browser automatically sends the Windows client's username and password to the Internet Information Server Web server using the Windows NT Challenge/Response authentication protocol. In this release, the only browser that supports Windows NT Challenge/Response authentication protocol is the Internet Explorer 2.0 for Windows 95.

When an Internet Information Server service receives a client request that contains credentials (a username and password), the "anonymous logon" user account is not used in processing the request. Instead, the username and password received by the client are used by the service. If the service is not granted permission to access the requested resource while using the specified username and password, the request fails, and an error notification is returned to the client.

For WWW (HTTP) only, when an anonymous request fails because the "anonymous logon" user account does not have permission to access the desired resource, the response to the client indicates which authentication schemes the service supports. This is determined by the configuration of the WWW service's authentication features. If the response indicates to the client that the service is configured to support HTTP basic authentication, most Web browsers will display a username and password dialog box, and reissue the anonymous request as a request with credentials, including the username and password entered by the user.

If a Web browser supports Windows NT Challenge/Response authentication protocol, and the WWW service is configured to support this protocol, an anonymous WWW request that fails due to inadequate permissions will result in automatic use of the Windows NT Challenge/Response authentication protocol. The browser will then send a username and encrypted password from the client to the service. The client request will then be reprocessed, using the client's user information. The user account obtained from the client is that with which the user is logged on to the client computer. Because this account, including its Windows NT domain, must be a valid account on the Web server computer, Windows NT Challenge/Response authentication is very useful in an intranet environment, where the client and server computers are in the same, or trusted, domains. In this release, Internet Explorer version 2.0 for Windows 95 is the only browser that supports Windows NT Challenge/Response authentication protocol.

Internet Service Manager Authentication Options

In addition to the "anonymous logon" username and password fields, the Service property sheet of Internet Service Manager contains the following authentication options:

WWW

- **Allow Anonymous** When this check box is selected, anonymous connections are processed, and the "anonymous logon" username and password are used for these connections. When this checkbox is unchecked, all anonymous connections are rejected, and basic or Windows NT Challenge/Response authentication protocol is required to access content.
- **Basic** When this check box is selected, the WWW service will process requests using basic authentication. **WARNING:** Basic authentication sends Windows NT usernames and passwords across the network without encryption. This check box is cleared by default for security reasons.
- **Windows NT Challenge/Response** When this check box is selected, the service will honor requests by clients to send user account information using the Windows NT Challenge/Response authentication protocol. This protocol uses a one-way hash to prevent passwords from being transmitted across the network. The Windows NT Challenge/Response authentication process is initiated automatically as a result of an "access denied" error on an anonymous client request. Currently, Windows NT Challenge/Response authentication protocol works only with Internet Explorer 2.0 for Windows 95.

Note: If the "Basic" and "Windows NT Challenge/Response" check boxes are both cleared (and the "Allow Anonymous" check box is selected), all client requests are processed as anonymous requests. In this case, if the client supplies a username and password in the request, this username and password are ignored by the WWW service. The "anonymous logon" user account will be used to process the request.

FTP

- **Allow Anonymous Connections** When this check box is selected, FTP logons in which the user enters a username of "anonymous" will be processed. These anonymous connections will be processed on behalf of the Windows NT user account specified on the Service property sheet. When this check box is cleared, users will be required to enter valid Windows NT usernames and passwords to log onto the FTP service.
- **Allow only anonymous connections** When this checkbox is selected, user logons with a username other than "anonymous" will be rejected.

Warning: FTP usernames and passwords are sent across the network in clear text. When this check box is cleared, Windows NT passwords will be sent to the server without encryption. This check box is checked by default for security reasons.

Other Authentication Issues

Secure Sockets Layer (SSL)

SSL is a WWW feature that supports data encryption and server authentication. All data sent to and from the client using SSL is encrypted. If HTTP basic authentication is used in conjunction with SSL, the username and password are transmitted after they are encrypted by the client's SSL support. In this release, the only browser that supports SSL is Internet Explorer 2.0. See the *Installation and Planning Guide*, online tour, and Help files for more information on SSL.

"INTERACTIVE" and "NETWORK" Users

If you use the predefined Windows NT user accounts "INTERACTIVE" and "NETWORK" for access control, your use of these accounts may affect client access to some resources. In order for a file to be accessed by anonymous client requests or client requests using basic authentication, the requested file must be accessible by the INTERACTIVE user. In order for a file to be accessible by a client request using Windows NT Challenge/Response authentication protocol, the file must be accessible by the NETWORK user.

Log on Locally

In User Manager, when configuring a Windows NT user account to be used either as the Internet Information Server "anonymous logon" account, or as a user account specified by client requests using HTTP basic authentication, be sure that the user account is granted the "Log on locally" User Right. This is specified in User Manager's Policies menu.

Customized Authentication

If you need a WWW request authentication scheme not supported by the service directly, obtain a copy of the Internet Server API (ISAPI) Software Developer's Kit (SDK), and read the ISAPI Filters specification on how to develop user-written ISAPI Filter DLLs that handle request authentication. The ISAPI SDK can be found at http://www.microsoft.com/intdev.

Networking for the Internet or an Intranet

The Internet is a network of networks. Every Internet Information Server must be configured to operate in a network, whether it is the global Internet or your local intranet.

This topic explains the basic Transport Control Protocol/Internet Protocol (TCP/IP) networking requirements for nearly all Internet Information Server sites, especially those with more than one information server.

Routers and Security Devices

TCP/IP is a routeable protocol, meaning each piece of information (packet) has a specific address that it is routed to. Dedicated routers connect two networks, routing packets between the networks. The routers check the destination for each packet on one network, and if the destination is on the router's other network, it routes the packet to its destination.

Routers can be configured to allow only certain packets between networks, a process called packet filtering. Packet filtering can be used to prevent users from seeing or connecting to internal computers and resources.

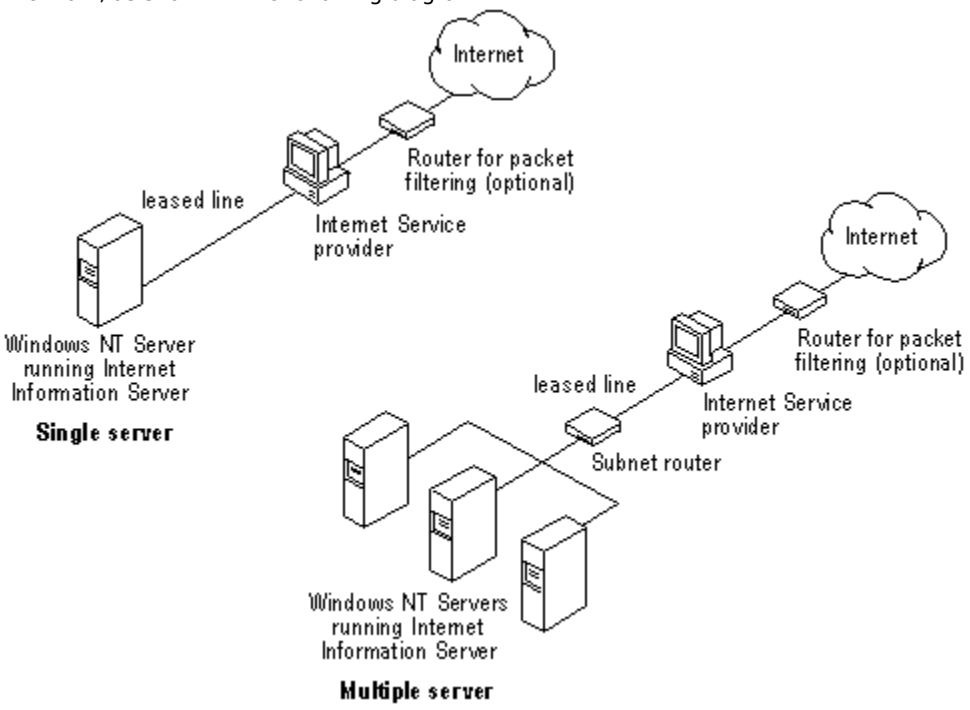
If you have a TCP/IP network you probably have routers in your network already. Often an Internet Service Provider (ISP) will install a router between the Internet and your information server. This will enable you to filter the incoming and outgoing packets. See your ISP or router documentation for more information about configuring routers or similar security devices.

Internet Sites

If you will have only one computer running Internet Information Server at your site, your Internet Service Provider (ISP) can help you with many details, such as router configuration and the IP address of the default gateway that your server will use.

If you have multiple computers running Internet Information Server on your network, you must configure their TCP/IP settings to operate correctly through your Internet connection configuration, including any routers used between your servers and the default gateway

Typically, sites with more than one computer running Internet Information Server will add another router. With the addition of another router, the servers can be grouped into a single subnet isolated from your private network, as shown in the following diagram.



To create a subnet you will need:

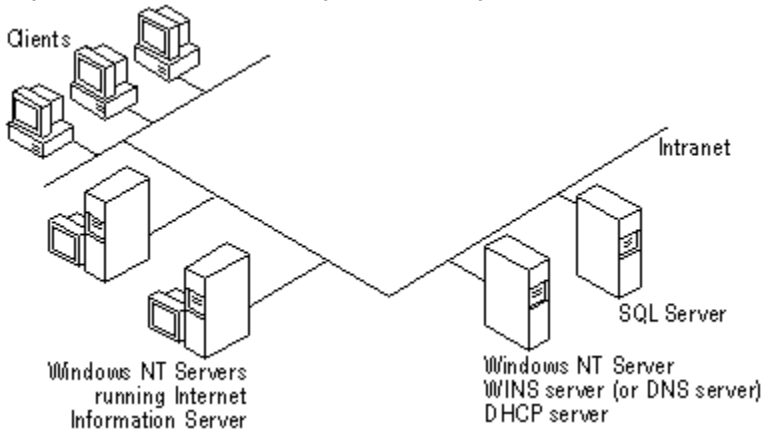
- One computer with two network adapter cards and Windows NT TCP/IP routing enabled, or a dedicated router for your subnet.

  See Help in Windows NT for the procedure to create a simple router on a computer running Windows NT and for the procedure to set routing tables by using the **route** command.
- Valid IP addresses for every network adapter card in your subnet and the correct Subnet Mask.
- Correct Default Gateway IP address configurations.

  Your ISP will provide you with the Internet IP addresses, subnet mask (if any), and your default gateway configuration.

Intranet Sites

If you are publishing only to your own intranet, Internet Information Server can be integrated into any TCP/IP network. If Dynamic Host Configuration Protocol (DHCP) and Windows Internet Name Service (WINS) are enabled on your network, clients can use the server's computer name to connect with the server. If Domain Name System (DNS) is enabled on your network, you will use host names.



Integrating Your Intranet with the Internet

It is possible to just connect your entire intranet to the Internet, rather than connecting a subnet containing only your Information Servers to the Internet. However, there are many security implications to connecting an intranet to the Internet. You should thoroughly understand the security implications and understand TCP/IP networking before you decide to integrate your entire network with the Internet. Integrating a network with the Internet requires information that is outside the scope of this manual. See Chapter 5, "Securing Your Site Against Intruders," for more information about security, and consult the Internet or other sources for additional information about Internet security, firewalls, and TCP/IP networking.

Publishing on the Internet

For the world to reach your site, you must have an Internet connection. Connections to the Internet are usually leased from ISPs. In addition to providing your physical Internet connection and IP address (and subnet mask if appropriate), your ISP can provide many of the Internet services, such as domain name registration, routers, and DNS service. To plan for publishing on the Internet you must consider:

- How to choose the right internet connection
- Internet connection types
- IP addresses and DNS

How to Choose the Right Internet Connection

Your connection to the Internet will be through a network adapter card or other network device, such as a modem or Integrated Services Digital Network (ISDN) card. Internet bandwidth is measured in bits per second (bps).

Your server configuration and Internet bandwidth determine how fast data gets to your computer and how many requests can be serviced simultaneously. As the number of computers getting data through your Internet connection increases, delays or failures will occur unless you have enough bandwidth.

When you lease an Internet connection a network cable is installed by your ISP to your site. Leased connection speeds range from 56,000 bps (with Frame Relay) to 45,000,000 bps (with a T3 connection). A dial-up ISDN line can offer speeds up to 128,000 bps.

Internet Connection Types

The connection types described in the following table represent typical levels of service for full Internet connections in North America and Japan. The Internet services offered through Internet service providers in your country may differ significantly.

Connection Types

Connection	Maximum BPS	Simultaneous Users Supported
Frame Relay	56,000	10-20
ISDN	128,000	10–50
T1	1,500,000	100–500
Fractional T1	varies as needed	
T3	45,000,000	5000+

A light-duty server can use Frame Relay or ISDN. A server with medium traffic might have a T1 line or some fraction of a T1 line installed. Large businesses that expect heavy Internet traffic may need fractional or multiple T1 lines or even T3 service in order to handle thousands of users.

Modem connections to the Internet are available, but are typically used for individual client browsing, and are not recommended for servers. A connection to the Internet using a phone line and modem can service only two or three simultaneous users. (Modem connections might be used for text-only Internet servers with only a small number of potential users.) Modem connections are often called “slow links” because data is transmitted at the speed of the modem, typically from 9,600 to 28,800 bps, far too slow for efficient operation of a WWW server.

IP Addresses and DNS

The Internet is a world-wide collection of individual Transmission Control Protocol/Internet Protocol (TCP/IP) networks. Each computer on the Internet has a unique address (IP address). Information is transmitted on the Internet in data packets. Each packet is addressed to a specific computer's IP address, such as 10.212.57.189.

Because IP addresses are difficult to use and remember, the Domain Name System (DNS) was created to pair a specific IP address, such as 10.189.54.1, with a friendly domain name, such as microsoft.com. When a user browses the Internet by using a domain name, the browser first must contact a DNS server to resolve the domain name to an IP address, then contact the computer with that address.

This has two implications for your Internet Information Server:

- You must have a permanent IP address assigned to a server on the Internet.
- You must register a domain name in the DNS for your permanent IP address.

Your ISP will generally provide your IP addresses and may also register your domain names. Contact the Internet Network Information Center (InterNIC) or your ISP for more information about DNS registration.

Publishing on an Intranet

Microsoft Internet Information Server can also be used on any private TCP/IP network to provide files and applications to network users. To plan for publishing on a private intranet you must consider:

- Distributing Internet Explorer to Clients.
- Name Resolution Systems.
- Using DHCP.
- Using Computer Names in URLs.
- SNMP Monitoring (if used at your site).

Internet Explorer

Internet Explorer makes it easy for users to browse your information services. Users point and click on links to move from page to page. If links to non-HTML files are encountered, Internet Explorer automatically displays the file with the proper viewer, or downloads the file to the local hard drive.

Internet Explorer versions are included for your intranet users running any of the following operating systems:

- Windows NT Server version 3.51 or later
- Windows NT Workstation version 3.51 or later
- Windows 95
- Windows for Workgroups version 3.11
- Windows version 3.1

What are the Differences Between Versions?

All Internet Explorer versions perform the same basic functions and have very similar operation. Internet Explorer takes advantage of the features of the operating system it is running. Setup.exe in the \Clients directory on the compact disc automatically installs the correct version.

Windows NT Server and Windows NT Workstation

Internet Explorer version 1.5 runs on versions 3.51 and later. It is a 32-bit application.

Windows 95

Internet Explorer version 2.0 runs on Windows 95. It is a 32-bit application that takes advantage of the Windows 95 interface.

The Windows 95 version of Internet Explorer also supports many advanced features, such as:

- Inline video (.avi files)
- Background sound and bitmaps
- Scrolling banners
- Context-sensitive menus

Windows for Workgroups and Windows version 3.1

Internet Explorer version 1.5 runs on Windows for Workgroups version 3.11 and Window version 3.1. It is a Win32s application.

How Do I Distribute Internet Explorer to Users?

You can use File Manager to share the contents \Clients directory on your compact disc, and then instruct users to run the Setup program from the network share. Setup automatically installs the appropriate version.

You can also copy the \Clients directory to a network share on a hard disk and allow clients to run Setup from the network share.

To fully automate installation for clients and control the installation configuration, you can use the file Unattend.txt. Unattend.txt is in each directory containing Setup.exe. First modify Unattend.txt to reflect the default configuration for users, then instruct users to install Internet Explorer from a batch file that starts unattended-mode Setup. See Chapter 1, “Installing Internet Information Server,” for more information about unattended-mode setup.

Name Resolution Systems

If you want intranet clients to be able to use friendly names with Internet Explorer when browsing information servers, you must provide a name resolution system for clients.

Windows NT Server offers you the advantage of automatic IP address administration with the DHCP server and WINS server methods for name resolution offered by WINS servers.

Using Computer Names with WINS Servers

A WINS server is a Windows NT Server–based computer running Microsoft TCP/IP and WINS server software. A WINS server maintains a database that maps TCP/IP addresses to Windows Networking computer names.

Microsoft Internet Information Server uses WINS server software to map TCP/IP addresses to computer names on the network. WINS uses Microsoft Networking computer names, which makes it much more flexible than DNS for name resolution. WINS also provides a dramatic reduction of IP broadcast traffic in Microsoft internetworks, while allowing client computers to easily locate remote systems across local or wide area networks. If you use WINS servers on the Internet, your computers must be using valid Internet IP addresses.

Using Computer Names and LMHOSTS

An LMHOSTS file is a simple text file resolving Windows computer names to IP addresses. If you have a small or infrequently changing network you can distribute an LMHOSTS file to each computer in the network. Each time a host changes you will have to manually change the LMHOSTS files.

Using Domain Names with DNS Servers

You can maintain a DNS server and Internet-assigned TCP/IP domain names as used on the Internet. If you plan to connect your network to the Internet, your IP addresses and DNS server routing configuration must be valid for the Internet.

Using Domain Names and HOSTS

A HOSTS file is a simple text file resolving DNS domain names to IP addresses. If you have a small or infrequently changing network, you can distribute a HOSTS file to each computer. Each time a host changes you will have to manually change the HOSTS files.

Using DHCP in Your Intranet

You can take advantage of DHCP server automatic IP address administration.

A DHCP server is a Windows NT Server–based computer running Microsoft TCP/IP and the DHCP server software.

If you use DHCP servers, you must use WINS Servers for clients to have automatic IP address name resolution. DHCP is defined in Requests for Comments (RFCs) 1533, 1534, and 1541. See Tcpip.hlp in Windows NT Server for more information about DHCP servers.

Using URLs and Creating HTML Links for Intranets

When you connect to a server or create HTML files and links on an intranet, you must name computers in accordance with the name resolution system implemented on your network. For example, if you use WINS servers on your network, your links will use Windows computer names, such as http://sales1/homepage.htm, where sales1 is the name of the computer running Internet Information Server.

SNMP Monitoring

If you monitor your network by using Simple Network Management Protocol (SNMP), you can use the SNMP Management Information Bases (MIBs) provided by Microsoft Internet Information Server to monitor your Web server.

The MIB files included in the \Sdk directory of the Microsoft Internet Information Server compact disc can be used by third-party SNMP monitors to enable SNMP monitoring of the WWW, Gopher, and FTP services of Microsoft Internet Information Server.

Internet Information Server supports SNMP monitoring only. SNMP configuration is not supported.

You will need to compile the MIB files using the MIB compiler that comes with your SNMP software before using them with the Windows NT SNMP service. You must start the services to be monitored before configuring and starting the SNMP service on your Internet Information Server–based computer. Once the SNMP service has been started on both the remote and local computers, you can use SNMP tools to monitor the running services.

Overview

This glossary documents terms found in the documentation for Internet Information Server and Internet Explorer. It does not document terms specific to Microsoft Windows NT. For those terms, see the Windows NT online help.

A

annotation file

anonymous logons

associating

authentication

B

bandwidth control

Basic clear-text authentication

BIND

bits per second (bps)

bps

browser

C

cache

CGI

challenge/response

client-server architecture

Common Gateway Interface (CGI)

connected user

cryptography

D

data integrity

Data Source Name (DSN)

DHCP

dial-up

discovery mechanism

DNS

DNS spoofing

domain

domain controller

Domain Name System (DNS)

DSN

Dynamic Host Configuration Protocol (DHCP)

E-F

encryption

file-extension mapping

File Transfer Protocol (FTP)

filter

firewall

friendly name

FTP (File Transfer Protocol)

G

gateway

Gopher

Gopher Plus

Gopherspace

H

home directory

HTML

HTTP

hyperlink

hypertext

HyperText Markup Language (HTML)

HyperText Transfer Protocol (HTTP)

I

Integrated Services Digital Network (ISDN)

interactive applications

Internet

Internet Log Converter

Internet Network Information Center (InterNIC)

Internet Protocol (IP)

Internet Protocol (IP) address

Internet Service Providers (ISPs)

InterNIC

intranet

IP

IP address

ISDN

ISPs

L

leased line

link

log file

logging

M

Management Information Databases (MIBs)

MIBs

MIME mapping

Multipurpose Internet Mail Extension (MIME) mapping

N

name resolution

Network News Transfer Protocol (NNTP)

NNTP

W

Web

Web browser

Web page

Windows Internet Name Service (WINS) server

WINS server

World Wide Web

WWW

For the FTP service, a summary of the information in a given directory. This summary appears automatically to remote browsers.

This feature allows remote access only by the IUSR_*computername* account. Remote users can connect to that computer only without a username and password, and they have only the permissions assigned to that account.

Connecting all files with a certain filename extension to a program. For example, through the Windows NT File Manager, all .txt files are associated by default with Notepad. In Internet Explorer, you can associate file extensions with applications through the Helpers dialog box. To display this dialog box, from the View Menu, choose Helpers. *Also called* Filename-extension mapping.

Determining if a user has permission to access a resource or perform an operation.

Setting the maximum capacity that a service is allowed to use. Deliberately limiting a server's Internet workload by not allowing it to receive requests at full capacity, to save resources for other programs such as e-mail.

The only authentication protocol supported by Internet Explorer. There is no encryption with this protocol.

The measure of speed at which data is transferred over a network.

A tool for navigating and accessing information on the Internet.

A store of files from an Internet server copied locally for quicker access. To configure your cache on the Internet Explorer browser, from the View menu choose Cache Settings.

A method of authentication in which a server uses Windows NT security to allow access to its resources.

The structure of services that run over the Internet. The client computer accesses the server, which supplies the client with resources or information not found on the client's own host. Also, CGI and ISAPI applications do processing on the server and return results to the client.

An interface used by an application that runs on a WWW server when a client requests it.

A user who is currently accessing one of the Microsoft Internet Information Server services.

A method of securing data transmissions to and from your server.

A way of preventing data from being altered in transit.

The name that allows a connection to an ODBC data source, such as a SQL Server database. You set this name through the ODBC icon in the Control Panel.

An industry-standard protocol that assigns Internet Protocol (IP) configurations to computers.

A connection to a computer by telephone, through a modem.

A way of finding other servers on the network. In Internet Server Manager, choose Find All Servers from the Properties menu.

Assuming the DNS name of another system by either corrupting a name-service cache, or by compromising a domain-name server for a valid domain.

For Windows NT Server, a collection of computers that share a common domain database and security policy. Each domain has a unique name.

For a Windows NT Server domain, the server that authenticates domain logons and maintains the security policy and the master database for a domain.

A protocol and system used throughout the Internet to map Internet Protocol (IP) addresses to user-friendly names. DNS is sometimes referred to as the BIND service.

A way of making data indecipherable while it is being sent from computer to computer.

A feature of ISAPI that allows pre-processing of requests and post-processing of responses, permitting site-specific handling of HyperText Transport Protocol (HTTP) requests and responses.

A system or combination of systems that enforces a boundary between two or more networks and keeps hackers out of private networks.

A name that substitutes for an IP address, for example, www.microsoft.com instead of an IP address such as 157.45.60.81.

An industry standard for sharing files between computers.

A hierarchical system for finding and retrieving information from the Internet.

An enhanced version of Gopher, including a way of getting more information about an item (such as file size, last date of modification, and the administrator's name), the ability to display a single file in multiple formats (such as regular text, rich text, and PostScript), a way to add a short description of the item, and the ability to ask a user to fill out a form to obtain an item.

All files available on a server for display through the Gopher protocol.

The root directory for a service, where the content files are stored. By default, the home directory and all its subdirectories are available to users.

A way of jumping to another place on the Internet. Hyperlinks usually appear in a different format from regular text. You initiate the jump by clicking the link.

Documents with links to other documents. Click a link to display the other document.

The language in which documents on the World Wide Web are written.

The underlying protocol through which WWW clients and servers communicate.

A connection to the Internet installed by your internet service provider (ISP). A dial-up ISDN line can offer speeds up to 128,000 bps.

A program written in C, Perl, or as a Windows NT batch file. The user initiates the program by clicking a hyperlink.

The global network of computers that communicate through a common protocol (TCP/IP).

A program that turns Microsoft Internet Server log files into either European Microsoft Windows Academic Centre (EMWAC) log file format or the Common Log File format. Convlog.exe is in the \Inetsrv\Admin directory.

The coordinator for DNS registration.

The part of TCP/IP that routes messages from one Internet location to another.

A unique address that identifies a host on a network. It identifies a computer as a 32-bit address that is unique across a TCP/IP network. An IP address is usually represented in dotted-decimal notation, which depicts each octet (eight bits, or one byte) of an IP address as its decimal value and separates each octet with a period, for example: 102.54.94.97

Public providers of remote connections to the Internet.

A TCP/IP network that can be connected to the Internet but is usually protected by a firewall or other device. For example, a corporate network.

A high-capacity line (most often a telephone line) dedicated to network connections.

The file in which logging records are stored. This file can be either a text file or a database file.

Storing information about events that occurred on a firewall or network.

Software that describes manageable aspects of your network using the Simple Network Management Protocol (SMNP). The MIB files included in the \Sdk directory of the Microsoft Internet Information Server compact disc can be used by third-party SNMP monitors to enable SNMP monitoring of the WWW, Gopher, and FTP services of Microsoft Internet Information Server.

A way of configuring browsers to view files that are in multiple formats.

A configuration that maps friendly names to IP addresses.

A protocol for reading messages posted in thousands of news groups on the Internet.

A piece of information sent over a network.

Conditions set by the system administrator such as how quickly account passwords expire and how many unsuccessful logon attempts are allowed before a user is locked out. These policies manage accounts to prevent exhaustive or random password attacks.

A number identifying a certain Internet application. For example, the default port number for Gopher is 70, and for WWW it is 80.

A file that starts an application or program. A program file has an .exe, .pif, .com, .cmd, or .bat filename extension.

Software that allows computers to communicate over a network. The Internet protocol is TCP/IP.

A software program that connects a user to a remote destination through an intermediary gateway.

A service that allows remote clients running Microsoft Windows or Windows NT to dial in to a network.

Administering a computer from another computer over the network.

A message-passing facility that allows a distributed application to call services available on various computers in a network.

Hardware or software device that directs network traffic.

A CGI application. *See also* Common Gateway Interface

A protocol that supplies secure data communication through data encryption and decryption.

One of the three services offered by the Internet Information Server: WWW, Gopher, or FTP.

A protocol used for exchanging mail on the Internet.

A protocol for monitoring your network. *See also* MIBs.

A modem connection, usually 9,600 bps through 28,800 bps.

Logging to a SQL Server database instead of to a text file. *See also* Logging.

HTML pages prepared in advance of the request and sent to the client upon request. This page takes no special action.

A TCP/IP configuration parameter that extracts network and host configuration from an IP address.

A name that can be used by any process on the computer. Internet Informatiion Server uses system DSNs to access ODBC data sources. *See also* Data Source Name.

Information about files on a Gopher server. This information is sent to clients and it typically contains the file name, host name, and port number.

Controlling the maximum amount of bandwidth dedicated to Internet traffic on your server. This feature is useful if you have other services (such as e-mail) sharing the server over a busy link.

A networking protocol that allows computers to communicate across interconnected networks and the Internet. Every computer on the Internet supports TCP/IP.

A naming convention that uniquely identifies the location of a computer, directory, or file on the Internet. The URL also specifies the appropriate Internet protocol, such as Gopher, HTTP, and so on.

The most popular news group hierarchy on the Internet.

A directory outside the home directory that appears to browsers as a subdirectory of the home directory. For any of the three services (WWW, Gopher or FTP), you can configure a virtual directory through the Directories property sheet in the Internet Server Manager.

A computer with several IP addresses assigned to the network adapter card. To a browser, this configuration makes the computer look like several servers.

A software program, such as Internet Explorer, that retrieves a document from an Internet server, interprets the HTML codes, and displays the document to the user with as much graphics as the software can supply.

A World Wide Web document. Pages can contain almost anything, such as news, images, movies, and sounds.

A protocol for mapping Internet Protocol (IP) addresses to user-friendly names. *See also* Domain Name System.

The most graphical service on the Internet. The Web also has the most sophisticated linking abilities.