Novell NetWare¤ 5.1 CSP 7

5.1

www.nove

NETWARE FTP SERVER ADMINISTRATION GUIDE

No

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

U.S. Patent No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903;5,633,931; 5,652,859; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,850,565; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,878,434; 5,884,304; 5,893,116; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,950,198; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,771; 5,991,810; 6,002,398; 6,014,667; 6,015,132; 6,016,499; 6,029,247; 6,047,289; 6,052,724; 6,061,743; 6,065,017; 6,094,672; 6,098,090; 6,105,062; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,192,365; 6,216,123; 6,219,652; 6,229,809. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

NetWare FTP Server Administration Guide
May 2002
103-000172-001

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Cluster Services is a trademark of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Novell NetWare Core Protocol and NCP are trademarks of Novell, Inc.

Novell Directory Services and NDS are registered trademarks of Novell, Inc., in the United States and other countries.

Novell eDirectory is a trademark of Novell, Inc.

Novell Storage Services is a trademark of Novell, Inc.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

Preface

Welcome to the NetWare FTP Server Administration Guide. NetWare® FTP Server software provides FTP service for transferring files to and from NetWare volumes. You can perform file transfers from any FTP client by using the FTP server to log in to a Novell® NDS tree. After logging in, you can navigate to other NetWare servers (in the same NDS tree) even if they are not be running FTP service.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

Also, a trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

1 Overview

NetWare® FTP Server software is based on the standard ARPANET File Transfer Protocol that runs over TCP/IP and conforms to RFC 959. You can perform file transfers from any FTP client by using the FTP Server to log in to the Novell® NDS tree.

Features of the NetWare FTP Server

The main features of NetWare FTP Server software include the following:

- MP enabled

  The NetWare FTP Server is fully multiprocessor (MP) enabled, preemptive and can run on any processor.

- Multiple instances of NetWare FTP Server software

  Multiple instances of NetWare FTP Server software can be loaded on the same NetWare server, providing different FTP services to different sets of users.

  See "Multiple Instances of the FTP Server" on page 37.

- FTP access restrictions

  FTP access can be restricted at various levels through various types of access rights.

  See "Access Restrictions" on page 39.

- Intruder detection

  An intruder host or user who tries to log in using an invalid password can be detected and restricted.

  See "Intruder Detection" on page 38.

- Remote server access

  FTP users can navigate and access files from other NetWare NDS servers in the same NDS tree and from remote IBM* servers, whether or not the remote servers are running NetWare FTP Server software.

  The Search list is a new feature of the FTP Server, using which you can specify the list of fully distinguished names of containers in which FTP users are to be looked for. For more details, see "SEARCH_LIST" on page 17.

  See "Accessing a Remote Server" on page 32 and Table 5, "Login Parameters," on page 16.

- Anonymous user access

  An Anonymous user account can be set up to provide users with basic access to public files.

  See "Anonymous User Access" on page 42.

- Special Quote Site commands

  These NetWare-specific commands can be used to change or view some of the NetWare server-specific parameters.

  See "Quote Site Commands" on page 35.

- Firewall support

  When the FTP client is behind a firewall and the FTP server cannot connect to the FTP client, NetWare FTP Server software supports passive mode data transfer and the configuration of a range of passive data ports.

  See Table 7, "Firewall Support Parameters," on page 19.

- Active Sessions display

  Details of all the active FTP instances at a particular time such as a list of all instances, details of each instance, all sessions in an instance, and all details of each session can be viewed.

  See "Viewing the Active Sessions Display" on page 30.

- Name space support

  NetWare FTP Server software can operate in both DOS and long name spaces. The FTP user can dynamically change the default name space by using one of the Quote Site commands.

  See "Name Space and Filenames" on page 36.

- Simple Network Management Protocol error reporting service

  Simple Network Management Protocol (SNMP) traps are issued when an FTP login request comes from an intruder host or from a node address restricted through Novell NDS. The traps can be viewed on the management console.

- FTP logs

  The FTP service maintains a log of various activities: FTP sessions, unsuccessful login attempts, active sessions details, and system error and FTP server-related messages.

  See "FTP Log Files" on page 43

- Welcome banner and message file support

  NetWare FTP Server software displays a welcome banner when an FTP client establishes a connection as well as a message file when a user changes the directory in which the file exists.

  See Table 8, "Welcome Banner and Message Files Parameters," on page 19.

- NetWare Web Manager based management

  NetWare Web Manager is a browser-based management tool used to configure and manage NetWare Web Services (such as NetWare Enterprise Web Server and NetWare Web Search Server) using a local database, LDAP, or Novell NDS.

  The NetWare Web Manager interface can also be used to administer (start and stop) the FTP server as well as to configure the server, security, user, and log settings. These settings can then be modified from a client workstation using an Internet browser.

  You can also get information such as the current server status by viewing different logs through the Web Manager interface.

  The Web Manager URL is https://*servername*: *port_number* (default port number = 2200).

  See "Configuring FTP Server from NetWare Web Manager" on page 21.

- Cluster Services Support

  NetWare FTP Server can be configured with Novell Cluster Services™ to achieve high availability. Running FTP Server on Novell Cluster Services provides benefits such as automatic restart without user intervention in case of a node failure in cluster.

See “Configuring with Cluster Services” on page 49.

2 Setting Up

This chapter discusses the following sections:

- "Configuring FTP Server" on page 13
- "Configuring FTP Server from NetWare Web Manager" on page 21

Configuring FTP Server

Before starting the NetWare FTP Server software, configure it by setting the configuration parameters in the configuration file. The default configuration file is SYS:/ETC/FTPSERV.CFG. The parameters in this configuration files are commented with their default values.

When the NetWare FTP Server is started, the IP address of the host (HOST_IP_ADDR) and the port number of the NetWare FTP Server (FTP_PORT), as defined in the configuration file, are used to bind to and listen for FTP client connection requests. If these parameters are not defined in the configuration file, the FTP Server binds to all configured network interfaces and the standard FTP ports.

Multiple instances of the NetWare FTP Server can run on a single machine with different IP addresses, or port numbers. The various parameters in the configuration file along with the default values are described in the following tables:

NOTE: The configuration, restriction, welcome banner and the message files must follow the 8.3 file naming format as long name is currently not supported for these files.

Table 1 **Multiple Instances Parameters**

Parameter	Default Value	Description
HOST_IP_ADDR	IP address of the host	The IP address of the host that the FTP Server software is being loaded on.
FTP_PORT	21 (Standard FTP port)	The port number that the FTP server should bind to and listen for connection requests from. The maximum port number is 65534.

Table 2 **FTP Session Parameters**

Parameter	Default Value	Description
MAX_FTP_SESSIONS	30	Maximum number of FTP sessions that can be active at a given point of time. Minimum value is 1. If this parameter value is set to zero, the FTP Server takes the default value.
IDLE_SESSION_TIMEOUT	600 (seconds)	Duration in seconds that any session can remain idle. The session will never time out if the value is set as negative, for example -1. The maximum value is 2^{32} (4294967296) seconds.

Table 3 **Anonymous User Access Parameters**

Parameter	Default Value	Description
ANONYMOUS_ACCESS	No	Specifies whether anonymous user access is allowed. Valid values are Yes and No.

Parameter	Default Value	Description
ANONYMOUS_HOME	SYS:/PUBLIC	The Anonymous user's home directory. This path can contain up to 512 bytes.
ANONYMOUS_PASSWORD_REQUIRED	Yes	Specifies whether to ask for an Email ID as the password for Anonymous user to log in. Valid values are Yes and No.

Table 4 Access Restrictions Parameters

Parameter	Default Value	Description
RESTRICT_FILE	SYS:/ETC/FTPREST.TXT	FTP Server can define access restrictions to various levels of users, hosts, etc. These restrictions are defined in a file, which can be specified here. The path with the filename can contain up to 512 bytes. The minimum value of the IP address allowed is is 0.0.0.0 and the maximum value is 255.255.255.254. The value 255.255.255.255 is invalid since 255.255.255.255 is a broadcast address and not supported for ADDRESS_RANGE.

Table 5 Login Parameters

Parameter	Default Value	Description
DEFAULT_USER_HOME_SERVER	Server where FTP is running	The name of the server that the default home directory is on. The path can contain up to 97 bytes.
DEFAULT_USER_HOME	SYS:\PUBLIC	The default home directory of the user. The path with the filename can contain up to 512 bytes.
IGNORE_REMOTE_HOME	No	Specifies whether to ignore the home directory, if it is on a remote server, and go to the default directory. Valid values are Yes and No.
IGNORE_HOME_DIR	No	Specifies whether to ignore the home directory and go to the default directory. Valid values are Yes and No.
FTP_CATALOG_NAME	FTPCAT	This is used for contextless login. This path with the name of the object can contain up to 512 bytes.

Parameter	Default Value	Description
SEARCH_LIST		A list of fully distinguished names of containers in which FTP users are to be looked for, separated by commas (without any spaces). The length of this string including the commas should not exceed 2048 bytes. Spaces refer to the spaces in between the commas and contexts specified, not the spaces in the context. Each context specified by fully distinguished name must begin with a leading dot (.). You can specify a maximum of 25 containers.

NOTE: When logging in for the first time without specifying the context, the search criteria used by NWFTPD to find them will be in the following order:

1. The first bindery context of the server, if it is set.
2. The NetWare server object's context, if bindery context is not set.
3. The NDS Catalog Services catalog specified by the FTP_CATALOG_NAME parameter in FTPSERV.CFG.
4. The contexts listed in the SEARCH_LIST parameter of FTPSERV.CFG, in the order listed.

On successful login, the FTP server context gets set to the user's context. Therefore, for next login in the same session where context is not specified, the context will be searched for under this FTP Server context set to the context of the user previously logged in successfully.

Table 6 Intruder Detection Parameters

Parameter	Default Value	Description
DEFAULT_NAMESPACE	Long	The default name space. The valid values are DOS and LONG.

Parameter	Default Value	Description
INTRUDER_HOST_ ATTEMPTS	20	The number of unsuccessful log in attempts for intruder host detection. The maximum value is 2 ^{32} (4294967296) attempts.
INTRUDER_USER_ATTEMPTS	5	The number of unsuccessful log in attempts for intruder host detection. The maximum value is 2^{32} (4294967296) attempts.
HOST_RESET_TIME	5	Time interval in minutes during which the intruder host is not allowed to log in. The maximum value is 2^{32} (4294967296) minutes.
USER_RESET_TIME	10	Time interval in minutes during which the intruder user is not allowed to log in. The maximum value is 2 ^{32} (4294967296) minutes.

NOTE: To disable intruder detection, set both intruder detection parameters, INTRUDER_HOST_ ATTEMPTS and INTRUDER_USER_ATTEMPTS to 0.

To enable intruder detection, set both intruder detection parameters, INTRUDER_HOST_ ATTEMPTS and INTRUDER_USER_ATTEMPTS to a value greater than zero 0. Also, set the value of the INTRUDER_HOST_ ATTEMPTS parameter to a value greater than the value set for the INTRUDER_USER_ATTEMPTS parameter.

Table 7 Firewall Support Parameters

Parameter	Default Value	Description
PASSIVE_PORT_MIN	1	Minimum port number used for establishing passive data connection. The port value range is 1 to 65534. The minimum port number must always be greater than zero, and less than 65534.
PASSIVE_PORT_MAX	65534	Maximum port number used for establishing passive data connection. The port value range is 1 to 65534. The maximum value should always be greater than zero and less than 65534.

Table 8 Welcome Banner and Message Files Parameters

Parameter	Default Value	Description
WELCOME_BANNER	SYS:/ETC/WELCOME.TXT	When the FTP client establishes a connection, the content of this file is displayed. The path with the filename can contain up to 256 characters.
MESSAGE_FILE	MESSAGE.TXT	When the user changes the directory, the contents of this file are displayed. For this, the file with that name should exist in the directory. The path withe the filename can contain up to 256 characters.

Table 9 FTP Logs Parameters

Parameter	Default Value	Description
FTP_LOG_DIR	SYS:/ETC	The directory where log files will be stored. This path could contain up to 256 characters.
NUM_LOG_MSG	32000	Maximum number of messages that will be logged in each log file. The range is 2^{31} messages. However, the maximum messages allowed is based on the memory available.
FTP_LOG_LEVEL	7	Indicates the level of messages logged. These are: 1= ERROR 2= WARNING 4= INFORMATION The following combinations can be given. 3= ERROR, WARNING 5=ERROR, INFORMATION 6= INFORMATION, WARNING 7=ERROR, WARNING, and INFORMATION
FTPD_LOG	FTPD	FTPD.LOG file is automatically created. This file contains all the internal system related information encountered by the FTP server. The path with the filename could contain up to 256 characters.

Parameter	Default Value	Description
AUDIT_LOG	FTPAUDIT	FTPAUDIT.LOG file is automatically created. This file contains details about the login activities of the user. The path with the filename could contain up to 256 characters.
INTRUDER_LOG	FTPINTR	FTPINTR.LOG file is automatically created. This file contains information about unsuccessful login attempts. The path with the filename could contain up to 256 characters.
STAT_LOG	FTPSTAT	FTPSTAT.LOG file is automatically created. This file contains details about all active sessions. The path with the filename could contain up to 256 characters.

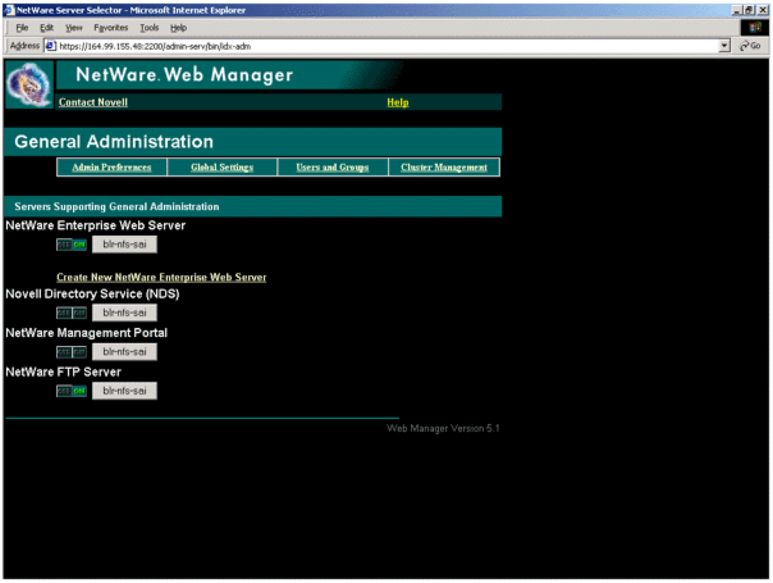
Configuring FTP Server from NetWare Web Manager

You can use the NetWare Web Manager for administering FTP Service from client- side.

To do this, enter the following URL to display the Service Selector panel (the default port number is 2200):

https://*remote_server_name* : *port_number*

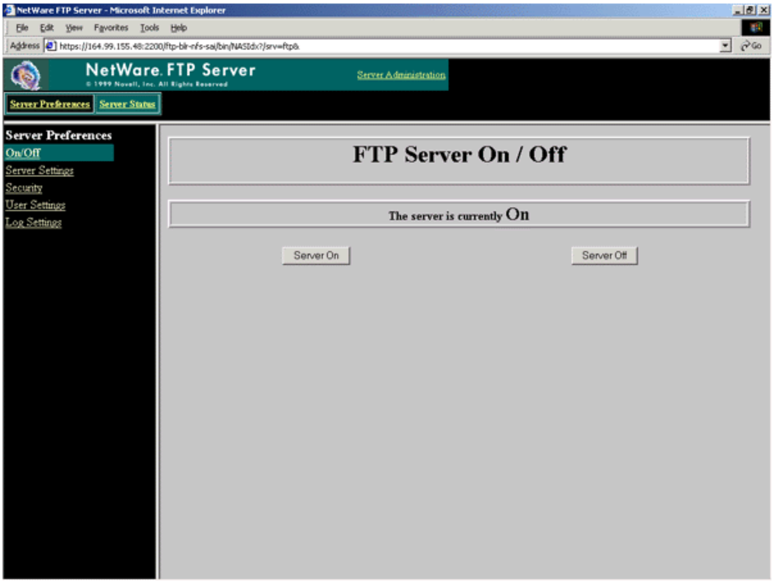
Figure 1 Service Selector Panel


NetWare Server Selector - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://164.99.155.48:2200/admin-serv/bin/idx-adm
Go
NetWare. Web Manager
Contact Novell
Help
General Administration
Admin Preferences
Global Settings
Users and Groups
Cluster Management
Servers Supporting General Administration
NetWare Enterprise Web Server
ON
blr-nfs-sai
Create New NetWare Enterprise Web Server
Novell Directory Service (NDS)
blr-nfs-sai
NetWare Management Portal
blr-nfs-sai
NetWare FTP Server
ON
blr-nfs-sai
Web Manager Version 5.1

In the Service Selector panel, select NetWare FTP Server to display the Service Manager panel.

NOTE: From the Service Manager panel, do not click the Back icon in the navigation toolbar of the browser to return to the Service Selector panel of NetWare Web Manager. Instead, click the Home icon in the Service Manager panel to return to the Service Selector panel.

Figure 2 Service Manger Panel



The server is currently On

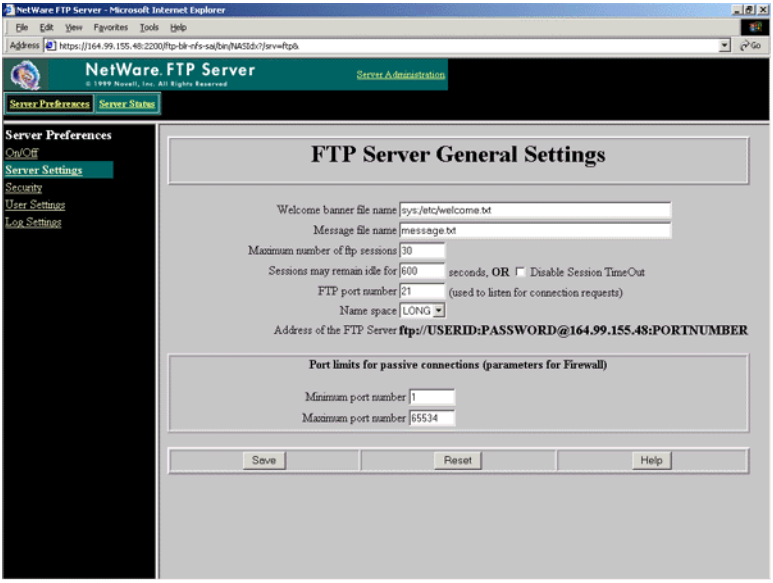
In the Service Manager panel you can view the Server Preferences menu, which provides links to the configuration pages of FTP Server by clicking the Server Preferences icon at the top of the panel.

When you click this icon, the initial main panel displays FTP Server On/off Panel. You can start or stop NetWare FTP Service from the client side by clicking either of the buttons.

Configuring Server Settings

1 In the Server Preferences menu, click Server Settings.

Figure 3 Server Settings Panel



NetWare FTP Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://164.99.155.48:2200/ftp-blr-nfs-sai/bin/NASIdx?/srv=ftp&
Go
NetWare. FTP Server
© 1999 Novell, Inc. All Rights Reserved
Server Administration
Server Preferences
Server Status
Server Preferences
On/Off
Server Settings
Security
User Settings
Log Settings
Save
Reset
Help

FTP Server General Settings

Welcome banner file name: sys:/etc/welcome.txt

Message file name: message.txt

Maximum number of ftp sessions: 30

Sessions may remain idle for: 600 seconds, OR □ Disable Session TimeOut

FTP port number: 21 (used to listen for connection requests)

Name space: LONG

Address of the FTP Server: **ftp://USERID:PASSWORD@164.99.155.48:PORTNUMBER**

Port limits for passive connections (parameters for Firewall)

Minimum port number: 1

Maximum port number: 65534

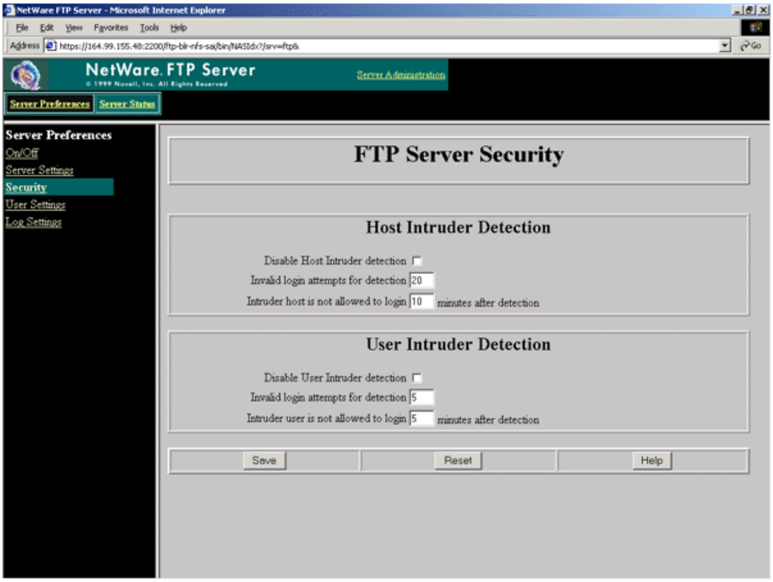
2 Specify the FTP Server settings. For specific information about each parameter, refer the online help.

3 Click Save to save your settings or click Reset to retain the previous settings.

Configuring Security Settings

1 In the Server Preferences menu, click Security.

Figure 4 Security Panel



NetWare FTP Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://164.99.155.48:2200/ftp-blr-nfs-sai/bin/NASIdx?/srv=ftp&
Go
NetWare. FTP Server
© 1999 Novell, Inc. All Rights Reserved
Server Administration
Server Preferences
Server Status
Server Preferences
On/Off
Server Settings
Security
User Settings
Log Settings
Save
Reset
Help

FTP Server Security

Host Intruder Detection

Disable Host Intruder detection ☐

Invalid login attempts for detection 20

Intruder host is not allowed to login 10 minutes after detection

User Intruder Detection

Disable User Intruder detection ☐

Invalid login attempts for detection 5

Intruder user is not allowed to login 5 minutes after detection

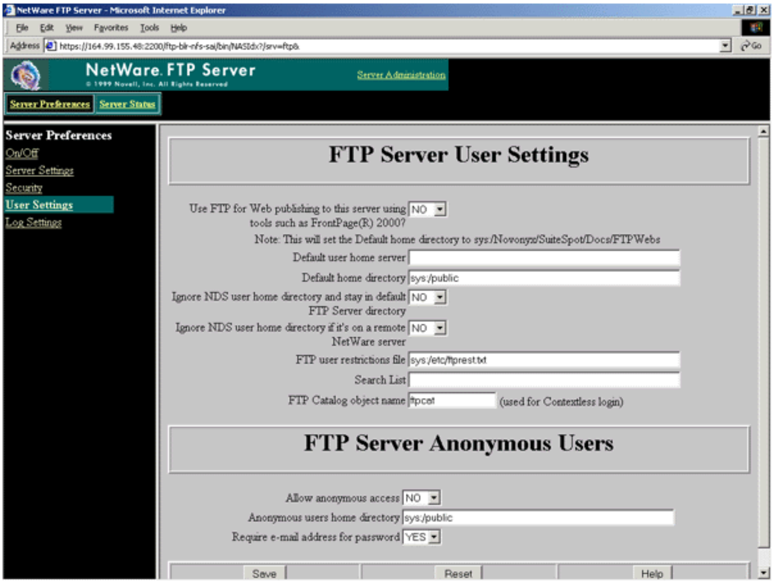
2 Specify the FTP Server Security settings. For specific information about each parameter, refer the online help.

3 Click Save to save your settings or click Reset to clear your settings.

Configuring User Settings

1 In the Server Preferences menu, click User Settings.

Figure 5 User Settings Panel



NetWare FTP Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://164.99.155.48:2200/ftp-blr-nfs-sai/bin/NASIdx?/srv=ftp&
Go
NetWare. FTP Server
© 1999 Novell, Inc. All Rights Reserved
Server Administration
Server Preferences
Server Status
Server Preferences
On/Off
Server Settings
Security
User Settings
Log Settings
Save
Reset
Help

FTP Server User Settings

Use FTP for Web publishing to this server using tools such as FrontPage(R) 2000? NO

Note: This will set the Default home directory to sys:/Novonyx/SuiteSpot/Docs/FTPWebs

Default user home server

Default home directory sys:/public

Ignore NDS user home directory and stay in default FTP Server directory NO

Ignore NDS user home directory if it's on a remote NetWare server NO

FTP user restrictions file sys:/etc/ftprest.txt

Search List

FTP Catalog object name ftpcat (used for Contextless login)

FTP Server Anonymous Users

Allow anonymous access NO

Anonymous users home directory sys:/public

Require e-mail address for password YES

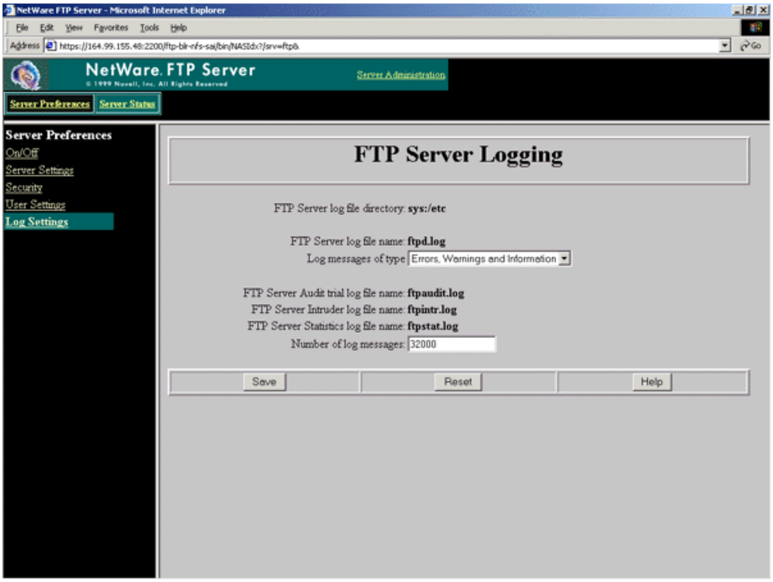
2 Specify the FTP Server User Settings. For specific information about each parameter, refer the online help.

3 Click Save to save your settings or click Reset to clear your settings.

Configuring Log Settings

1 In the Server Preferences menu, click Log Settings.

Figure 6 Log Settings Panel


NetWare FTP Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://164.99.155.48:2200/ftp-blr-nfs-sai/bin/NASIdx?/srv=ftp&
Go
NetWare. FTP Server
© 1999 Novell, Inc. All Rights Reserved
Server Administration
Server Preferences
Server Status
Server Preferences
On/Off
Server Settings
Security
User Settings
Log Settings
FTP Server Logging
Save
Reset
Help

FTP Server log file directory: **sys:/etc**

FTP Server log file name: **ftpd.log**

Log messages of type: Errors, Warnings and Information

FTP Server Audit trial log file name: **ftpaudit.log**

FTP Server Intruder log file name: **ftpintr.log**

FTP Server Statistics log file name: **ftpstat.log**

Number of log messages: 32000

2 Select the type of log messages from the Log Messages of Type drop down list, and enter the Number of Log messages. For specific information about each parameter, refer the online help.

3 Click Save to save your settings or click Reset to retain previous settings.

IMPORTANT: You might not receive an error even if the changes to the configuration file are not successfuly saved. To save the changes, make sure that the configuration file is not open when you are configuring the server using NetWare Web Manager.

3 Managing

This chapter discusses the following topics:

- "FTP Server Startup" on page 29
- "Using the FTP Server from an FTP Client" on page 30
- "Administering the NetWare FTP Server" on page 37

FTP Server Startup

Load the FTP Server software on the NetWare® server by giving the following command:

```
nwftpd
```

The server takes the default configuration file SYS:/ETC/FTPSERV.CFG. On installation, this configuration file has all the parameters, commented, with their default values.

To start the NetWare FTP Server software with a different configuration file, for example, MYCONFIG.CFG, place the file in the SYS:/ETC directory and enter the following at the command line:

```
nwftpd -c myconfig.cfg
```

NOTE: Reload nwftpd if there is any change in the configuration file.

Creating an Anonymous User

To create an anonymous user, enter

```
nwftpd -a [-c Configfile]
```

The server takes the anonymous user home directory from the configuration file and displays it on the screen with the option to modify the directory.

NOTE: The -a option modifies the configuration file for anonymous user access. For this change to take place, reload **nwftpd**.

Viewing the Active Sessions Display

To load the Active Sessions Display utility, enter

```
ftpstat [-p port number]
```

The server takes a port number that the HTTP browser should connect to in order to view the NetWare FTP active sessions. The default port is 2500.

Using the FTP Server from an FTP Client

This section discusses the following:

- "Starting an FTP Session" on page 30
- "Paths Formats" on page 35
- "Accessing a Remote Server" on page 32
- "Quote Site Commands" on page 35
- "Name Space and Filenames" on page 36

Starting an FTP Session

Users can start an FTP session from a workstation running the FTP client software using the following command:

```
ftp hostname | IP Address
```

where *hostname* is the name of the server in the DNS or IP address of the NetWare server running the FTP service. The FTP client then prompts the user for a username and password.

The following are the session-based details and are not tied to individual user logins: bytes sent, bytes received, session duration, files sent, files received, and current Novell® eDirectory™ context.

For more details, see Table 2, “FTP Session Parameters,” on page 14.

Logging In to the eDirectory Tree

A user can login to the FTP server either by specifying the username with full context or with a context relative to the default context (which is the context of the NetWare server where FTP is running). If the context is not specified, the FTP server searches for the user only in the current session context.

If a user with an expired password attempts to log in to the FTP server, a message stating that the password has expired is returned after the user logs in. Logging in with an expired password uses the grace logins. If all the grace logins of the user expire, the user cannot log in and receives an error message.

After the user logs in, the FTP server places the user in the user's eDirectory home directory (if defined) and attaches the user to the server where the home directory resides.

If the home directory is not defined or cannot be located, the FTP server places the user in the default user home directory specified in the configuration file.

The DEFAULT_USER_HOME_SERVER parameter can be used to specify the name of the server where the default user home directory is located. If the parameter is not specified, by default the FTP server considers the default user home directory to be on the server where the FTP server is running.

A user is placed in the default user home directory under the following conditions:

- If IGNORE_DIR_HOME = Yes.
- If IGNORE_REMOTE_HOME = Yes, and the user’s home directory is on a remote server.

Logging In to an IBM Server

To log in to a remote IBM server, the user needs to have a user account in that server.

To log in to the IBM server from FTP client, start an FTP session using FTPHost and give the username in the following format:

```
@IBMservername.username
```

To log in to an IBM server from a browser, use the following format:

```
ftp //+IBMserver+username:password@FTPHost
```

For logging in as anonymous user, the user name and password need not be specified:

```
ftp //+IBMservername@FtpHost
```

On logging in to an IBM server, the user is placed in the home directory in that IBM server.

While logging in to an IBM server, the user is not authenticated to the eDirectory tree. So, navigation between IBM servers and eDirectory servers is not possible.

Accessing a Remote Server

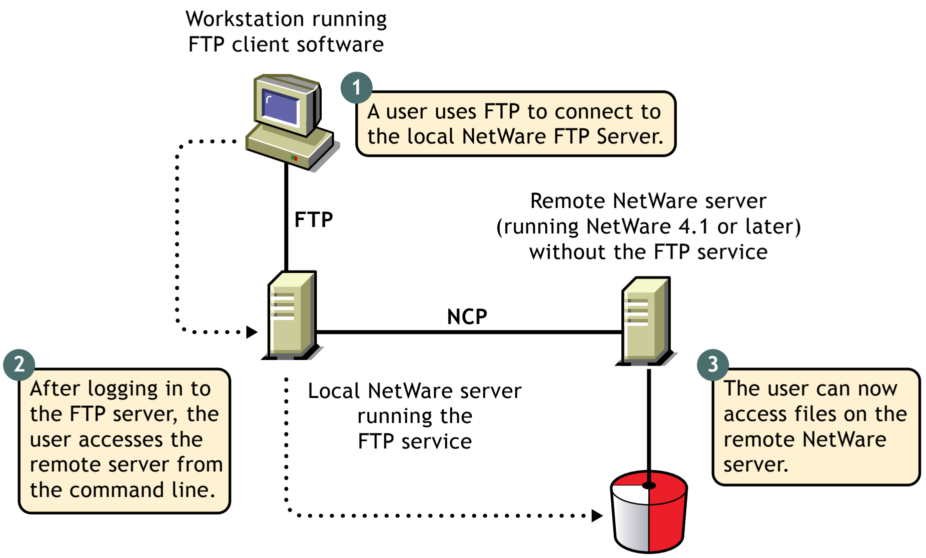
The double slash (//) indicates that the user wants to access a remote server. The name of the remote server must be the first entry after the double slash.

Navigating to eDirectory Servers

After logging in to the eDirectory tree, users can access files and directories on a remote NetWare server whether or not the server is running NetWare FTP Server software.

The NCP™ protocol lets you transfer files and navigate to and from remote eDirectory servers.

Figure 7 How a NetWare FTP Server Accesses Remote NetWare Servers


Workstation running FTP client software
1
A user uses FTP to connect to the local NetWare FTP Server.
FTP
Remote NetWare server (running NetWare 4.1 or later) without the FTP service
NCP
2
After logging in to the FTP server, the user accesses the remote server from the command line.
Local NetWare server running the FTP service
3
The user can now access files on the remote NetWare server.

To navigate to remote servers, enter

```
cd //remote server name/volume/directory pathname
```

Use the file operations such as **get**, **put**, and **delete** on the remote server, even without changing directory path to that server. For example:

```
get //remote_server_name/volume/directory path/filename
```

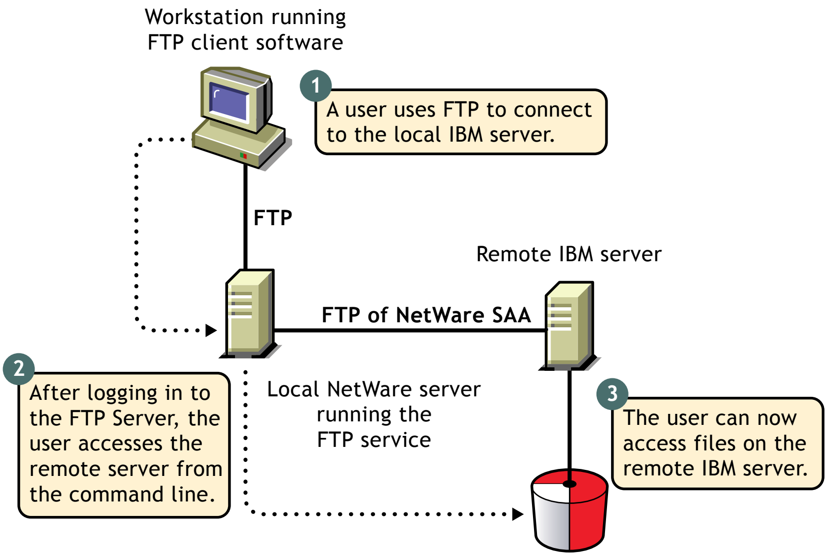
If the current directory is on a remote server and the remote server goes down, the user is placed in the home directory in the home server. If the home server is not available, the user is placed in the default user home directory.

Navigating to IBM Servers

After logging in to the eDirectory tree, users can access files and directories on a remote NetWare server whether or not the server is running Novell FTP Server software.

The NetWare FTP Server uses the AFTP Gateway component of NetWare SAA to access remote IBM servers.

Figure 8 How a NetWare FTP Server Accesses Remote IBM Servers


Workstation running FTP client software
1
A user uses FTP to connect to the local IBM server.
FTP
Remote IBM server
FTP of NetWare SAA
2
After logging in to the FTP Server, the user accesses the remote server from the command line.
Local NetWare server running the FTP service
3
The user can now access files on the remote IBM server.

The IBM server that the user logs in to first will be considered the home server. Once logged in to an IBM server, the user can navigate to other remote IBM servers which identify the user with the same username and password. To navigate to remote servers the following format should be used:

```
cd //IBM server name/path
```

File operations such as get, put, and delete can be done only when the user is currently in that server.

If the current directory is on a remote server and the server goes down, the user is placed in the home directory in the home server. If the home server is not available, the remote server is made the home server. If the current directory is in the home server and the server goes down, the user is logged out.

Paths Formats

The volume and directory path name must be specified in following format:.

```
//server_name/volume_name/directory_path
```

To navigate to different volumes, enter:

```
cd /volume_name
```

To switch back to home directory, enter:

```
cd ~
```

To switch to home directory of any user, enter:

```
cd ~user_name
```

Quote Site Commands

The SITE command enables FTP clients to access features specific to the NetWare FTP Server.

The SITE command has the following syntax:

```
QUOTE SITE [SLIST | SERVER | HELP | CX {CONTEXT} | LONG |
  DOS | OU]
```

When the file structure is set, the command `quote stat` displays the current transfer structure that the FTP Server supports for the files with different structures such as record or file.

NOTE: The settings done through Quote Site comments is valid only for current session.

These commands are unique to the NetWare FTP service and are not standard FTP commands.

A list of quote site commands and their descriptions are given below:

Command	Description
SLIST	Lists all the NetWare servers within the eDirectory tree
SERVER	Lists all NetWare servers in the current eDirectory context and its sub-OUs. For example, SITE SERVER displays all NetWare servers in the current context.

Command	Description
HELP	Displays the help file related to the Quote Site commands. It gives the syntax, and description of all site commands.
CX	CX without a context displays the current context of the FTP Server CX with a context as an argument sets the current eDirectory context to a given value. For example: cx ou=test sets the context to the OU test using the relative context cx.ou=test.o=acme sets the context to the OU test using the absolute context CX with the argument ~ ,resets the context back to user's context
OU	Displays all the organizational units relative to the current context OU enables users to display the eDirectory organizations (containers) below the current eDirectory context.
LONG	Changes the configured namespace to the LONG name space.
DOS	Changes to the configured name space to the DOS name space. DOS changes the configured name space to the DOS name space. This change takes place only for the current session. All NetWare volumes support the DOS name space.

Name Space and Filenames

FTP Server software supports DOS and LONG name space. The default name space is configured in the configuration file. FTP users can also change it dynamically using the QUOTE SITE DOS command or the QUOTE SITE LONG command.

NOTE: The namespace changed using Quote Site command is in effect only in the current status.

The default configured name space is LONG.

When the user changes the name space, the change affects only those volumes that support the specified name space. If the LONG name space is not supported on a specific volume, users must follow the DOS file naming conventions of using no more than eight characters for the name plus no more than three additional characters for the extension.

In both name spaces, the user views the response to the ls or Dir in the NetWare format only. Format of the directory listing is as follows:

type rights owner size time name

where the above variables stand for:

- *Type*: Type of file, where {-} indicates a file and {d} indicates a directory
- *Rights*: Effective NetWare rights of the user to this file or directory.
- *Owner*: NetWare user who created this file or directory. In case the mapping of objects and the owner's name is not found, the object ID is displayed.
- *Size*: The size, in bytes, of the file or directory. In case of a directory, it is always 512.
- *Time*: The modification date and time of the file or directory.
- *Name*: The name of the file or directory in the current name space.

Administering the NetWare FTP Server

This section discusses the administering the following:

- "Multiple Instances of the FTP Server" on page 37
- "Intruder Detection" on page 38
- "Access Restrictions" on page 39
- "Anonymous User Access" on page 42
- "FTP Log Files" on page 43
- "Active Sessions Display" on page 47

Multiple Instances of the FTP Server

Multiple instances of the FTP server can be initialized if the NetWare server has multiple Network Interface Cards. Each FTP server should have a unique

IP address and port number combination. Each FTP server instance can have its own configuration file and access restrictions file, and can listen on different IP addresses and port numbers.

The IP address of the host (HOST_IP_ADDR) and the port number (FTP_PORT) as defined in the configuration file are used to bind to and listen for FTP client connection requests. The configuration file can be specified while starting the FTP server. If these parameters are not defined in the configuration file, the default IP address and the standard FTP port number are used.

For more details, see Table 1, "Multiple Instances Parameters," on page 14.

Intruder Detection

A user is considered an intruder when the number of unsuccessful log in attempts is greater than those specified by the parameter INTRUDER_USER_ATTEMPTS in the configuration file. Similarly, a host/client machine is considered an intruder when the number of consecutive login failures for any user from that host is greater than the configured limit specified by the parameter INTRUDER_HOST_ATTEMPTS.

- If a successful login is encountered before the attempts limit is reached, the login failures count is reset to zero.
- When the user becomes an intruder, the user's account is locked out for an interval of time specified by the parameter USER_RESET_TIME in the configuration file.
- When a host becomes an intruder, access to the FTP Server is denied for that host machine for an interval of time specified by the parameter HOST_RESET_TIME in the configuration file.
- To disable intruder detection, both intruder detection parameters, INTRUDER_HOST_ ATTEMPTS and INTRUDER_USER_ATTEMPTS, must be set to 0.
- To enable intruder detection, both intruder detection parameters, INTRUDER_HOST_ ATTEMPTS and INTRUDER_USER_ATTEMPTS, must be set to a value greater than 0.
- Enables the setting of user attempts to 0 or 1 while host attempts are 0 or 1 and viceversa.

- The users and hosts that are not detected as intruder but fail to login less than number of maximum attempts allowed are removed from the corresponding list after refresh time, of 24 hours.
- All failed attempts from a user from different hosts are considered for intruder detection as same user. When the accumulated attempts for the same user from different hosts exceeds the maximum attempts, then that user is detected as intruder.
- The user that has been identified as an intruder, will not be allowed to log in from a different host until the reset time is over.
- When the user is detected as an intruder, the user does not receive the password prompt from any host.
- When the user is detected as an intruder, the server closes the session.
- The intruder host, and the intruder user list are refreshed every 72 hours.

Access Restrictions

The FTP service enables you to specify access restrictions for a user, a client host, and the IP address of a client host. The access restrictions are specified in the restrictions file, which can be configured (RESTRICT_FILE). Access restrictions can be specified at various levels and multiple access rights are allowed.

Restriction Levels

The following table describes the supported levels of access restrictions.

Restriction Level	Description
Container	Restriction can be specified for any eDirectory container. This will control all the users in that container and its sub-OUs. Container level: Restriction can be specified for any eDirectory container. This will control all the users in that container and its sub-OUs. *.*container name* The asterik (*) indicates the container level restriction. The container should be a fully distinguished name.
User	Restriction can be specified for a particular user. *.user name* The period (.) indicates user level restriction. The user name should be a fully distinguished name.
Domain	Restriction can be specified at the domain level. This will control all the hosts in that domain and its sub domains. The following is the RESTRICT file format: DOMAIN= *domain name* The DOMAIN= key word indicates the domain level restriction. The domain restrictions will not work if the host does not have a DNS entry.
Host	Restriction can be specified for a particular host machine. ADDRESS= *host name/IP address* The ADDRESS= key word indicates the host level restriction. The host name or IP address of the host can be specified. The DNS configuration should be proper for address and domain name restrictions.

Access Rights

The following table describes the permitted access rights.

Access Right	Description
DENY	Denies access to the FTP Server for that client.
READONLY	Gives read-only access to the client.
NOREMOTE	Restricts access to remote server navigation.
GUEST	Gives only Guest access to the user. guest users are those users who cannot navigate to remote servers. A guest user has access only within the guest user's home directory and subdirectories.
ALLOW	Gives normal FTP access without restriction.

Keywords

The following table describes the possible keywords.

Keyword	Description
ADDRESS=	Restricts a particular node. The IP address or machine name can be used.
DOMAIN=	Restricts a particular Domain. The asterisk (*) should be used for container level restrictions.
ACCESS=	Is mandatory for each line. It should be followed by access rights.

Restrict File

The format and organization of the restrict file is as follows:

- Each line should have one entity name and corresponding access rights.
- The rights of the entities will be assigned according to the order of the RESTRICT file. If different rights apply to the same entity, the latest entities that appear in the RESTRICT file will be taken.

- All rights specified in the same line will be applied to that entity.
- If the RESTRICT file does not exist or is empty, the access is given to all users without any restrictions.

Example 1

```
*.novell                                     ACCESS=ALLOW
*.testou.novell                              ACCESS=DENY
.user1.testou.novell                      ACCESS=READONLY
```

User1 at testou will be allowed read-only rights. The other users at testou.novell will be denied the right. However, all other OUs at .novell will be allowed.

Example 2

```
*.testou.novell                              ACCESS=DENY
*.novell                                     ACCESS=ALLOW
```

All OUs at .novell will be allowed because both rights apply to testou and the later would be taken.

Example 3

```
ADDRESS=Clientmachine1.blr.novell.com ACCESS=NOREMOTE
.user1.novell ACCESS=READONLY
```

The user1 logging from clientmachine1 will have read-only and no remote access.

For more details, see Table 4, “Access Restrictions Parameters,” on page 15

Anonymous User Access

NetWare FTP Server software supports an anonymous user account. This account provides people with access to public files. Access to the Anonymous user account can be enabled or disabled by setting the ANONYMOUS_ACCESS parameter in the configuration file. By default, the parameter is set to No. The path of the Anonymous user's home directory can be specified in the configuration file, in the ANONYMOUS_HOME directory parameter.

An Anonymous user account can be created by loading the FTP server with the `-a` option. This creates the Anonymous user, creates the home directory (if it is not available), and assigns access rights to the Anonymous user. The administrator name and password are then taken from the screen and the Anonymous user is created in the eDirectory tree at the default context. Also, the configured anonymous home directory is displayed on the screen with an option to modify it.

If the administrator does not specify a home directory, then the default directory is taken. The Anonymous user will have only Read and File Scan rights to the default directory. If the administrator specifies the anonymous home directory, then the directory is created and the Anonymous user will have Read, File Scan, Create, Delete, and Modify rights to that directory.

For more details, see Table 3, "Anonymous User Access Parameters," on page 14.

FTP Log Files

The FTP server has four log files for recording different activity information. All the log files are created in the FTP_LOG_DIR directory specified in the configuration file. The amount and type of information logged is controlled by the LOG_LEVEL parameter defined in the configuration file.

The log levels indicate bits for which any combination can be give

- 1= ERROR
- 2= WARNING
- 4= INFO

If the LOG_LEVEL = 3, then error messages and warning messages will be logged. If LOG_LEVEL = 4, then error messages and warning messages will be logged.At default value of LOG_LEVEL = 7, all messages will be logged.

The parameter NUM_LOG_MSG is used to specify the maximum number of messages that can be logged into each of the log files. Once this limit is exceeded the log files are overwritten and the old messages are lost.

All these log files can be viewed from NetWare Web Manager.

Audit Log File

The Audit log contains details about the login and activities of the user. The default path is SYS:/ETC/FTPAUDIT.LOG. The file has entries for login, logout and other file system related operations like mkdir, rmdir, put, set, and delete.

The general Audit log format is

```
Log Level:Thread ID:Date Time:IPaddress:Username:message
```

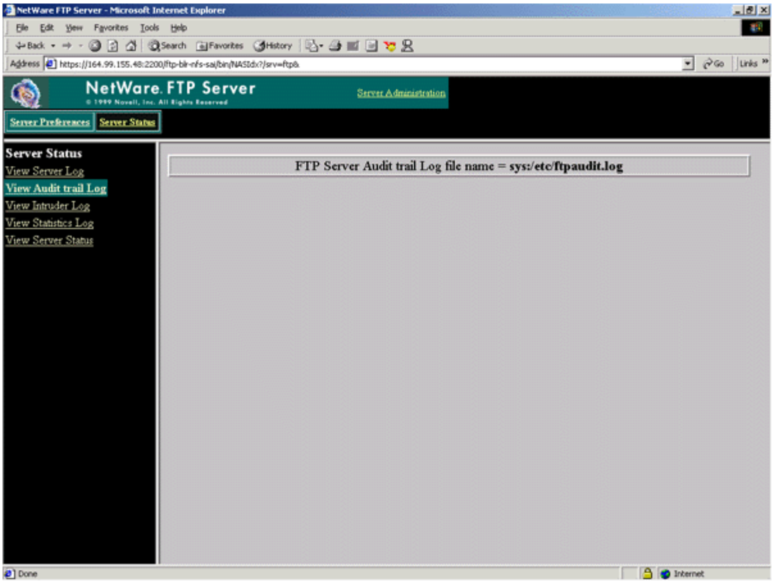
Viewing Audit Log File from NetWare Web Manager

NOTE: FTP administration from the Web Manager will not work if Enterprise Web Server is not installed, even though Web Manager is installed.

You need to install the Enterprise Web Server along with the FTP Web Manager to administer the FTP Server from Web Manager.

1. In the NetWare Web Manager Service Selector panel, click NetWare FTP Server.
2. In the Service Manager panel, click the Server Status icon.
3. In the Server Log panel, click View Auditor Trail Log to display the following panel.

Figure 9 Audit Trail Log Panel


NetWare FTP Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address https://164.99.155.48:2200/ftp-bin-nfs-sai/bin/NASIdx?/srv=ftp&
Go Links
NetWare. FTP Server
© 1999 Novell, Inc. All Rights Reserved
Server Administration
Server Preferences
Server Status
Server Status
View Server Log
View Audit trail Log
View Intruder Log
View Statistics Log
View Server Status
Done
Internet

FTP Server Audit trail Log file name = sys:/etc/ftpaudit.log

Statistics Log File

The Statistics log file contains details of all active sessions in the log file. The default path is SYS:/ETC/FTPSTAT.LOG.

The Statistics log file maintains three record types, each of which is separated by a comma.

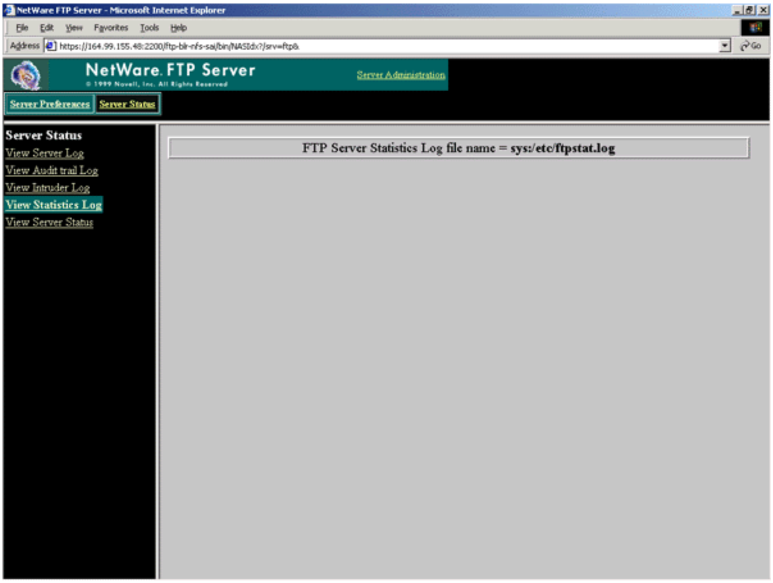
- TRANSFER: Contains information related to the data transfer

- USER: Contains information related to users logged in/out
- FAILURE: Contains information about the number of failures during data transfer

Viewing Statistics Log file from Web Manager

1. In the NetWare Web Manager Service Selector panel, click the NetWare FTP Server.
2. In the Service Manager panel, click the Server Status icon.
3. In the Server Log menu, click View Statistics Log link to display a panel similar to the following:

Figure 10 Statistics Log Panel



https://164.99.155.48:2200/ftp-blr-nfs-sai/bin/NASIdx?/srv=ftp&

FTP Server Statistics Log file name = **sys:/etc/ftpstat.log**

Intruder Log File

The Intruder log file contains information about unsuccessful login attempts. The default path is SYS:/ETC/FTPINTR.LOG. The following information is recorded in the file:

- The address of the machine where the login originated
- The time of the attempted access

- The login name of the user

The general Intruder log format is:

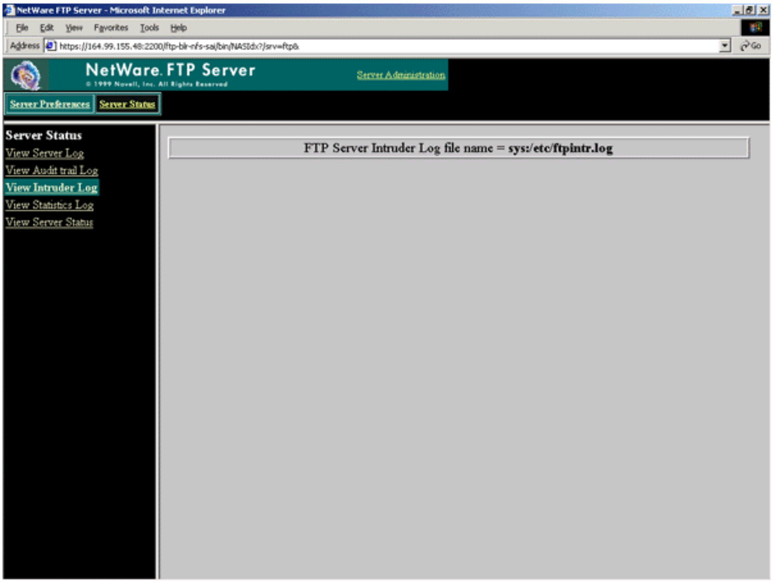
```
ErrorLevel: Date Time : Client IPaddress : UserName :
  message
```

If the parameter INTRUDER_HOST_ATTEMPTS = 0 then intruder detection is disabled.

Viewing Intruder Detection from Web Manager

1. In the NetWare Web Manager Service Selector panel, click the NetWare FTP Server.
2. In the Service Manager panel, click the Server Status icon.
3. In the Server log panel, click View Intruder Log to display a panel similar to the following:

Figure 11   Intruder Log Panel


NetWare FTP Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://164.99.155.48:2200/ftp-blr-nfs-sai/bin/NASIdx?/srv=ftp&
Go
NetWare. FTP Server
© 1999 Novell, Inc. All Rights Reserved
Server Administration
Server Preferences
Server Status
Server Status
View Server Log
View Audit trail Log
View Intruder Log
View Statistics Log
View Server Status

FTP Server Intruder Log file name = **sys:/etc/ftpintr.log**

System Log File

The System log file contains all the internal system-related information encountered by the FTP Server.

The general System log file format is

```
Error: Thread ID: Date Time: Message
```

For more details, see Table 9, "FTP Logs Parameters," on page 20

Active Sessions Display

To load the Active Sessions Display utility, enter

```
ftpstat [-p port number]
```

Enter the port number that the HTTP browser should connect to in order to view the NetWare FTP Active Sessions:

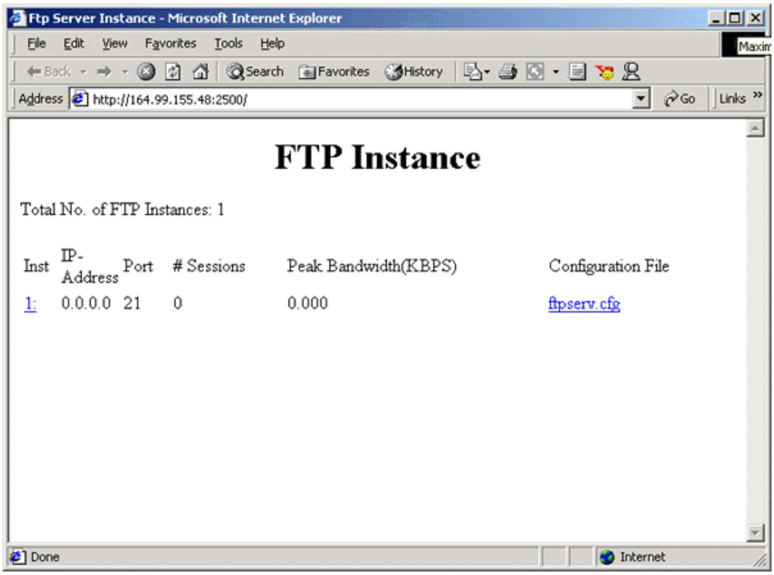
```
http://servername:port/
```

The default port is 2500.

You can directly view the active sessions information using NetWare Web Manager.

1. In the NetWare Web Manager Service Selector panel, click the NetWare FTP Server.
2. In the Service Manager panel, click the Server Status icon.
3. In the Server Status menu, click View Server Status to display the View Server Status panel.
4. Click the View Server Status button in the panel to view the FTP Instance Panel.

Figure 12 FTP Instance Panel



Ftp Server Instance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://164.99.155.48:2500/
Go Links
Done
Internet

FTP Instance

Total No. of FTP Instances: 1

Inst	IP-Address	Port	# Sessions	Peak Bandwidth(KBPS)	Configuration File
1:	0.0.0.0	21	0	0.000	ftpserv.cfg

The FTP Instance panel appears displaying active sessions of the FTP server. You can view details such as the total number of active session, IP address, port number, number of sessions, peak bandwidth, and configuration.

4 Configuring with Cluster Services

Before configuring NetWare® FTP Server with Novell® Cluster Services™, NetWare FTP Server must be installed on each server in your cluster that will run it. NetWare FTP Server is selected by default during the NetWare 5.1 installation, and might already be installed.

Running FTP Server in Active/Active and Active/Passive Modes

Running NetWare FTP Server in the ACTIVE/ACTIVE mode is the recommended configuration because it provides faster recovery after a failure. In this mode, FTP Server runs simultaneously on multiple servers in the cluster. When a Web server fails, the FTP sites on that server fail over to other FTP servers in the cluster. Only FTP sites move in ACTIVE/ACTIVE mode.

NetWare FTP Server can also be run in ACTIVE/PASSIVE mode. In this mode, FTP Server runs on only one node in the cluster at a time. When a Web server fails, FTP Server starts on other specified nodes in the cluster, and the FTP sites that were on the failed server fail over to other nodes in the cluster. This makes ACTIVE/PASSIVE mode marginally slower because FTP Server has to load on other servers in the cluster before FTP sites can fail over.

Editing FTPSERV.CFG Configuration Files

The configuration file FTPSERV.CFG is created by default during the FTP Server installation and is placed in the SYS:\ETC directory. A separate FTPSERV.CFG file exists for each FTP Server that is installed on the cluster.

Each FTPSERV.CFG file contains a line that specifies the IP address assigned to the FTP server. By default, the IP address assigned to the FTP server is the same IP address that is assigned to the NetWare server where the FTP server resides.

A separate unique IP address must be assigned to the FTP server so that it can move with the FTP server during failover and failback. Edit the FTPSERV.CFG file and change the HOST_IP_ADDR line to specify the unique IP address you want to assign to the FTP server. For example, if the unique IP address you want to assign to the FTP server is 123.45.67.012, the line would read Host_IP_ADDR=123.45.67.012.

Assigning a unique IP address to the FTP server allows it to bind to the unique IP address instead of to the IP address of the local host.

FTPSERV.CFG also contains a line that specifies the default home directory for FTP users. This home directory must reside on a volume on the shared disk system. The volume where the home directory resides doesn't have to be cluster enabled.

Edit FTPSERV.CFG and change the DEFAULT_USER_HOME line to specify the user home directory and volume on the shared disk system. For example, if the user home directory on the shared volume is SHARE1:/HOME, the line would read DEFAULT_USER_HOME=SHARE1:HOME.

Editing AUTOEXEC.NCF Files

If you are running NetWare FTP Server in ACTIVE/PASSIVE mode, it should be launched from the FTP Server Cluster Resource load script. For more details, see *Novell Cluster Services Overview and Installation* (http://www.novell.com/documentation/).

If you are running FTP Server in ACTIVE/ACTIVE mode, it should be launched from the AUTOEXEC.NCF file of each NetWare server in the cluster that will run FTP Server.

Add the following lines in the order specified to the AUTOEXEC.NCF file of each NetWare server in the cluster that will run FTP Server in ACTIVE/ACTIVE mode:

```
ADD SECONDARY IPADDRESS A.B.C.D NOARP
NWFTPD
LOAD DELAY.NLM
DELAY 5
DEL SECONDARY IPADDRESS A.B.C.D
```

Replace *A.B.C.D* with the unique IP address you assigned the FTP server.

If you are running multiple FTP servers on your cluster, repeat the ADD and DEL SECONDARY IPADDRESS lines for each FTP server, because each FTP server requires its own IP address. Also, each FTP server must have its own uniquely named configuration file which specifies the FTP server's IP address and shared volume directory. Running FTP Server in ACTIVE/ ACTIVE mode is required if you plan to run more than one FTP Server on the same NetWare server.

For example, if you have three FTP servers on your cluster, you can create three configuration files named FTPSERV1.CFG, FTPSERV2.CFG, and FTPSERV3.CFG and then copy them to the SYS:\ETC directory of each NetWare server in the cluster that will run the FTP servers. Each configuration file contains the IP address and shared volume directory for its corresponding FTP server. In this example, you would add the following lines to the AUTOEXEC.NCF file of each server in the cluster that will run the three FTP servers in ACTIVE/ACTIVE mode:

```
ADD SECONDARY IPADDRESS A1.B1.C1.D1 NOARP
ADD SECONDARY IPADDRESS A2.B2.C2.D2 NOARP
ADD SECONDARY IPADDRESS A3.B3.C3.D3 NOARP
NWFTPD -C FTPSERV1.CFG
NWFTPD -C FTPSERV2.CFG
NWFTPD -C FTPSERV3.CFG
LOAD DELAY.NLM
DELAY 5
DEL SECONDARY IPADDRESS A1.B1.C1.D1
DEL SECONDARY IPADDRESS A2.B2.C2.D2
DEL SECONDARY IPADDRESS A3.B3.C3.D3
```

DELAY.NLM provides enough time for the FTP server to load before the secondary IP addresses are deleted. The delay time might need to be altered to ensure enough time is allotted.

IMPORTANT: If you are also running Netscape* Enterprise Server in ACTIVE/ ACTIVE mode on the same server, be sure to add the lines in the above example *before* the NSWEB command.

When FTP Server is configured to run in the Active/Passive mode, make sure to comment the `nwftpd` entry in AUTOEXEC.NCF. Also, before you bring the resource online, execute unload `nwftpd` to bring down the FTP service already running.

Novell Cluster Services Configuration and Setup

Once FTP Server is installed, you must create and configure an FTP server resource in Novell Cluster Services for each FTP server that will run in your cluster. This includes configuring load and unload scripts; setting Start, Failover, and Failback modes; and assigning the FTP server resource to specific nodes in your cluster.

Creating a Cluster Volume Object

Before you start using FTP Server with cluster support, create a shared volume and a Cluster Volume object.

1 Create a shared volume using NWCONFIG > NSS volumes.

2 Create a Cluster Volume object in ConsoleOne by completing the following:

2a Select the Cluster object.

2b Click File > New > Cluster > Cluster Volume.

2c Browse and select the shared volume.

2d Enter the secondary IP address or the virtual IP address associated with the cluster.

The address will be in the following format:

```
AAA.BBB.CCC.DDD
```

2e Check the Define Additional Properties check box and click Create.

2f Set the Start, Failover, and Failback Modes.

2g Verify the order of the servers in the nodes list.

2h To save the changes to the Cluster Volume object, click OK.

IMPORTANT: After the shared volume *servername_shared vol name* is cluster-enabled, ConsoleOne renames it to *cluster object name_shared vol name*.

ConsoleOne creates a virtual server associated with the shared volume called *cluster object name_shared vol name_SERVER*.

ConsoleOne also creates a Cluster Volume object called *shared vol name_SERVER* in the Cluster object container.

Configuring FTP Server Load and Unload Scripts

For ACTIVE/PASSIVE modes, select and right-click the Cluster Volume object and then click Properties to find the Cluster Resource Load Script and Cluster Resource Unload Script.Novell Cluster Services requires load and unload scripts to start and stop the FTP server.

- To the load script, add **`NWFTPD`** at the end of the existing script.
- To the unload script, add **`UNLOAD NWFTPD`** at the beginning of the existing script.

Setting FTP Server Start, Failover, and Failback Modes

The following table explains the different FTP Server resource modes.

Mode	Settings	Description
Start	AUTO, MANUAL	AUTO allows FTP Server to automatically start on a designated server when the cluster is first brought up. MANUAL lets you manually start the FTP Server on a specific server whenever you want. Default = AUTO
Failover	AUTO, MANUAL	AUTO allows FTP Server to automatically move to the next server in the Assigned Nodes list in the event of a hardware or software failure. MANUAL lets you intervene after a failure occurs and before FTP Server is moved to another node. Default = AUTO

Mode	Settings	Description
Failback	AUTO, MANUAL, DISABLE	AUTO allows FTP Server to automatically move back to its preferred node when the preferred node is brought back online. MANUAL prevents FTP Server from moving back to its preferred node when that node is brought back online until you are ready to allow it to happen. DISABLE causes FTP Server to continue running in an online state on the node it has failed to. Default = DISABLE

To set FTP Server Start, Failover, and Failback modes, do the following:

1. In ConsoleOne, double-click the cluster object container.
2. Right-click the cluster resource object *shared vol name*_SERVER and select Properties.
3. Click the Policies tab on the property page.
4. View or change the Start, Failover, or Failback mode.

5 NetWare FTP Server Architecture

This chapter describes the architecture and components of the NetWare FTP server.

The FTP Server is fully multiprocessor enabled, preemptive and can run on any processor. NetWare FTP Server architecture comprises two main modules, FTP Daemon and Protocol Engine.This chapter has the following sections:

- "FTP Daemon" on page 55
- "Protocol Engine" on page 56
- "Remote Server Navigation" on page 57
- "FTP Client Information: Data Access Routines" on page 59

FTP Daemon

When an FTP client initiates a connection request, the FTP Daemon accepts and opens a Control Connection, and then spawns a thread group which acts as the FTP Protocol Engine and processes further requests from the client. A data connection is established between the Protocol Engine and the FTP client whenever required for file transfer.

When the FTPServer.NLM is loaded, the FTP daemon is started. The FTP daemon initializes the Configuration Parameters, Access Restrictions, Catalog services, Logs and statistics. The FTP Daemon binds to the FTP port specified in the configuration file and listens for connection requests from the clients.

On executing **`load ftpserv`** command, the FTP daemon is executed as the main thread. The FTP server can be unloaded at any time on executing the `unload ftpserv` command. While coming up, FTP Server initializes the following operations:

- Registers CleanupAndExitFTPServ() as function to be called while it is being unloaded
- Initializes UnloadFTPServ to zero
- Calls InitGlobalConfig() to initialize the configuration parameters global to FTP Server.
- Calls InitGlobalInfoAccess() to initialize the global data access locks.
- Gets the context of the FTP Server and stores in FTPContext.
- Initializes all functions related to Catalog Services for contextless login by calling InitializeCatalogFunctions()
- Imports all functions related to NetWare SAA for IBM-AFTP Support by calling ImportAFTPFunctions()
- Builds the user/host restrictions database by calling ReadAndBuildRestrictList()
- Initializes Intruder login detection by calling InitIntruderDetect()
- Initiates all logging by calling InitAllLogs()
- Initializes the facility of displaying the welcome banner / message file by calling InitWelcomeFile() and InitMsgFile()

After initialization, the FTP Daemon binds to the standard FTP port (21) or the port specified in the configuration file and listens for connection requests from FTP clients. On receiving a connection request, it establishes the Control Connection with the FTP client. It, then spawns a new thread in a separate thread group and hands over the socket information to Protocol Engine (ProtocolEngine) for processing the FTP commands that it receives on the connection.

Protocol Engine

On receiving the FTP connection request from the client, the Protocol Engine spawns a new thread in a new thread which can run on different processors group and hands over the Control Connection to the Protocol Engine. Protocol Engine checks, if the client is a intruder or a Restricted host. If it is a valid host, it creates a ConnectionInfo for this client and inserts into the linked list maintained.

The Protocol Engine maintains the CommandProcessTable Table, to map the FTP commands and the corresponding functions to be executed. Each FTP command is mapped to two functions; the NDS users, and for AFTP users. On receiving an FTP command from the client, the required function is executed based on the user type.

Access Restrictions

The Access Restrictions module enables access control and restrictions for the FTP user/host. This module maintains two levels of restrictions; User Level and Container Level.

The User Level specifies restrictions for a particular user while the Container Level specifies restrictions for all the users in that container. All the access restrictions are read from the restrictions file, FTPREST.TXT and are maintained in two static linked lists.

One list is the user level restrictions, when the restrictions have been specified in the file for the particular user. When a user logs in, this module determines the restrictions and access rights allowed for that user and stores them in UserInfo of the client. ConnectionInfo ReadAndBuildRestrictList() should be called first to initialize the restrictions.

Intruder Login Detection

The Intruder Detection module supports the intruder login detection. The configuration setup includes parameters needed for intruder checking and detection.

Whenever a login fails, the user name and password are stored in a list. A user is considered an intruder, when the number of consecutive failure attempts is more than that specified in the configuration.

Similarly, a host or a client machine is considered as intruder if the number of consecutive login failures for a user from that host is higher than the configured limit. If the user/host is considered as intruder, the access is denied to the FTPserver for a reset period of time specified in the configuration.

Remote Server Navigation

The Remote Server Navigation module enables navigation through the servers on a NDS tree or AFTP servers.

This enables connection with other servers, log out from a server and switching to default server if the remote working server goes down. The FTP Server could be running on any one of the servers on the NDS tree and the user can browse through all the servers on the NDS tree orAFTP servers and perform operations specified by FTP protocol on any of those File Servers.

Name Space Support Functions

The Name Space (NS) supported functions are used to set the NS required to operate. If the required NS is not supported by the current working volume then you need to work with the default NS, DOS.

File System Calls supporting NS functionality are used while interacting with the File System. These calls take NS as a parameter and this parameter specifies the NS in which the file name has been specified and the NS in which information related to that file is required.

Logging Support

The Logging Support module maintains various log files such as Audit/Trail log file, Statistics log file and Intruder log file. It initializes the log files to log messages at various stages. These log messages could be at any of three levels, L_ERROR, L_WARNING or L_INFO. InitAllLogs() should be called before starting to log into the log files.

Statistics Support

The Statistics Support enables generating various statistics:

All information related to an active session is updated in SessionInfo maintained in ConnectionInfo for every FTP session. This information is updated at various stages. For example, when the FTP client executes **CWD** command, it updates the Current Working Directory.

All history information related to Data Transfer (XferStat), Number of users logged in and out (UserStat), Number of failures during data transfer (FailureStat) is logged into a statistics log file. This module provides a utility to log into the statistics log file.

TCP Connection Handling Utilities

The TCP connection handling utilities module provides the utilities for all TCP socket related activities required for FTP server such as setting up Control/Data Connections, sending/receiving data/reply.

FTP Client Information: Data Access Routines

The FTP Client Information: Data Access Routines module maintains a static linked list containing information (stored in Connection Information structure) about all the active FTP clients and provides a set of utilities for allocating/adding a new Connection Information, deleting a Connection Information and traversing the linked list.

This module maintains a lock which it acquires while manipulating the linked list of client Connection Information and releases the same after the manipulation.

6 NetWare FTP Server FAQs

This section discusses the FAQs that users and system administrators might have while using NetWare® FTP Server.

NetWare FTP Server FAQs

When NWFTPD.NLM is loaded, why does the message "Unable to find default configuration file FTPSERV.CFG" display ?

Explanation: This message displays when you load the NWFTPD.NLM without the `-c` option and when FTPSERV.CFG, the default configuration file is not the configuration file in SYS:\ETC, the default directory.

Action: When loading NWFTPD.NLM, use the `-c` option to specify the configuration filename in use and include the complete path if this configuration file is not in the default directory SYS:\ETC.

When I load FTPServer, the message "FTPSERVER failed to bind to port " displays. What should I do?

Action: Ensure that the FTPServer is already loaded and is using the same port number. Also check if any other application is running on the same port which FTPServer is trying to use. For information on the valid port number range, refer to the FTP_PORT parameter in the FTPSERV.CFG file.

A newly created Anonymous user cannot login. What should I do?

Action: Reload the FTPSERVER after creating anonymous user for the changes to take effect.

The access restrictions specified in the restrictions file aren’t working. What should I do?

Possible Cause: The restrictions will not work if the restrictions file is not in the 8.3 format.

Action: Make sure that the restrictions file is in the 8.3 file format. Specify the DOS name assigned for the new restriction file in the FTPSERV.CFG.

Can I avoid clicking the Back button thrice to return to the Service Selector Page from the FTP Web Adminsitration?

Action: Click the home icon to return to the Service Selector page directly from Service Manager without clicking the Back button.

When using FTP Web Manager on some browsers, the newly modified fields aren’t displaying on saving to FTPSERV.CFG, and the message "Page not found" displays. What should I do?

Explanation: The browser has different caching settings.

Action: In the browser, set the caching off to display the newly modified fields.

A FTP Server Messages

NWFTPD Messages

Failed to bind to FTP port

Source: NWFTPD.NLM

Explanation: The port that the FTP Server is trying to bind to is busy.

Possible Cause: Another instance of the FTP Server or another application is bound to the port.

Action: Unload the application that is bound to the port, bind the FTP Server to a different port, or delete the busy port from TCPCON.

Failed to initialize Anonymous user

Source: NWFTPD.NLM

Explanation: The FTP Server failed to create an Anonymous user.

Possible Cause: Incorrect data was entered to create the user.

Action: Enter **`nwftpd -a [-c`** ***`Configfile`*** **`]`**.

Failed to add Anonymous User object to NDS

Source: NWFTPD.NLM

Possible Cause: The user entered has insufficient rights.

Action: Ensure that the user has sufficient rights.

Failed to generate an ObjectKeyPair

Source: NWFTPD.NLM

Possible Cause: The user entered has insufficient rights.

Action: Ensure that the user has sufficient rights.

Failed to open configuration file

Source: NWFTPD.NLM

Possible Cause: The configuration file is not available at specified location.

Action: Verify if the configuration file is available at the specified location.

Unable to find default configuration file

Source: NWFTPD.NLM

Possible Cause: Configuration file is not available at default location (SYS:/ETC).

Action: Verify if the configuration file is available at the default location.

Unable to locate Anonymous user in default context

Source: NWFTPD.NLM

Possible Cause: Anonymous user does not exist at the FTP Server's context.

Action: Run **`nwftpd -a`** to create anonymous user and reload **`nwftpd`**.

USAGE : nwftpd [-c <Config File>] [-a]

Source: NWFTPD.NLM

Possible Cause: The user might have tried to load nwftpd.nlm with wrong usage.

Action: Load NWFTPD.NLM by typing only the nlm name for default configuration file, or **ftpupgrd [-c *Config File*]** for specific configuration file name or nwftpd [-a] for creating anonymous user.

FTPUPGRD Messages

Could not create the .cfg file.

Source: FtpUpgrd.nlm

Possible Cause: Configuration file does not exist for ftp server upgrade, or existing configuration file has read only access.

Action: Modify the file access if it is read only or specify proper configuration file name with **`ftpupgrd [-c`** ***`Config File`*** **`]`** usage.

Could not create the FTP Server Restriction file.

Source: FtpUpgrd.nlm

Possible Cause: Restriction file does not exist for ftp server upgrade, or existing Restriction file has read only access.

Action: Modify the file access if it is read only or specify proper restriction file name.

Failed to upgrade.

Source: FtpUpgrd.nlm

Possible Cause: Configuration file does not exist for FTP server upgrade, or existing configuration file has read only access, or restriction file does not exist for ftp server upgrade, or existing Restriction file has read only access

Action: Modify the file access if it's read only or specify proper configuration file name with **`ftpupgrd [-c`** ***`Config File`*** **`]`** usage. Modify the file access if it is read only or specify proper restriction file name

Correct Usage: ftpupgrd [-c <Config File>]

Source: FtpUpgrd.nlm

Possible Cause: User might have tried to load FtpUpgrd.nlm with wrong usage.

Action: Use specified user ftpupgrd [-c *Config File*]