
WS_FTP Server

User's Guide

Software Version 3

Ipswitch, Inc.

Ipswitch, Inc.
81 Hartwell Ave
Lexington, MA 02421-3127

Phone: 781-676-5700
Web: <http://www.ipswitch.com>

The information in this document is subject to change without notice and should not be construed as a commitment by Ipswitch, Inc. While every effort has been made to assure the accuracy of the information contained herein, Ipswitch, Inc. assumes no responsibility for errors or omissions. Ipswitch, Inc. assumes no liability for damages resulting from the use of the information contained in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of that license.

Copyright © 2001 by Ipswitch, Inc. All rights reserved. WS_FTP, the WS_FTP logos, Ipswitch, and the Ipswitch logo are trademarks of Ipswitch, Inc. Other products or company names are or may be trademarks or registered trademarks and are the property of their respective companies.

No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transferred without the expressed prior written consent of Ipswitch, Inc.

Printing History

September 2000	First Edition
November 2001	Second Edition

Contents

Chapter 1: Introduction	1
What is WS_FTP Server?	1
How FTP Works	2
How WS_FTP Server Works	2
Major Features	3
WS_FTP Pro Client	4
WS_FTP Server Security	5
The WS_FTP Server Manager	5
Remote Management	6
System Requirements	7
Installing WS_FTP Server	7
Removing WS_FTP Server	7
Files Installed	7
Release Notes	8
Getting Updates and Giving Feedback	9
Chapter 2: Setting Up an FTP Site	11
Configuring the FTP Server	11
Setting WS_FTP Server Directories	12
Setting the FTP Server Port	12
Logging FTP Server Events	12
Starting and Stopping the FTP Server	13
Setting Up FTP Hosts	13
Adding the First FTP Host	14
Configuring an External User Database	17
Configuring an NT User Database	19
Setting Options for the FTP Host	20
Setting Timeouts for FTP Connections	20
Setting Maximum Users	21
Allowing Anonymous Access	22
Hiding Files and Folders	23
Setting Directory Listings to Use Local Time	23
Using Banner, Welcome, and Exit Messages	23
Creating Message Files for Folders and Directories	25
Setting Access by IP Address	25
Setting an Alias for the FTP Host	28
Other Options	28
Adding Additional FTP Hosts	28
Deleting an FTP Host	31
Renaming an FTP Host	31

Event Commands	32
Enabling event commands	32
Configuring Event Commands	33
Disabling Event Commands	34
Site Commands	34
Adding a Site Command:	34
Modifying Site Command Properties	37
Modifying Site Command Permissions.	38
Chapter 3: Managing FTP User Accounts and Permissions	41
How User Accounts Work	41
How Permissions Work	41
Adding an FTP User Account	42
Setting User Logon Options.	44
Setting User Options	44
User Directories and User Password.	45
Setting Logon, Public Directory, and Change Password Options.	45
Setting File and Disk Space Quotas	46
Setting Administrator Permissions	47
Deleting a User.	48
Renaming a User	48
Adding Users with the Command Line Utility	48
Basic Command Syntax	49
Adding a User	50
Modifying a User	50
Deleting a User	50
How Users Can Change Their Password.	50
Creating User Groups.	51
Adding Users to the Group	52
Deleting a User Group	53
Using Virtual Folders (to Grant Permissions)	53
Adding a Virtual Folder	54
Granting Permissions for FTP Folders	55
NT Permissions on Windows 2000.	56
Changing Folder Properties.	57
Deleting a Virtual Folder	58
Renaming a Virtual Folder.	58
Chapter 4: Managing FTP Hosts	59
Copying the Server Manager to a Remote Host	59
Connecting to the WS_FTP Server	59

Monitoring Active FTP Sessions	61
Server Statistics	61
Active Sessions	62
Monitoring FTP Server Statistics.	62
Reading the Log Files	63
Chapter 5: SSL Configuration	65
What is SSL?	65
How To Get Started	66
Generating a Certificate	68
Selecting a Certificate	69
Signing Requirement Option.	70
Signing a Certificate.	71
Trusted Authorities	72
Adding a Certificate	73
Exporting a Certificate	74
Removing a Certificate	74
Appendix A: Highlights of RFC 959.	75
Basics	75
FTP Commands	76
FTP Replies	83
Positive Preliminary Replies	83
Positive Completion Replies	83
Positive Intermediate Replies	84
Transient Negative Completion Replies	84
Permanent Negative Completion Replies	84
Index	87

Chapter 1: Introduction

This chapter begins with a basic introduction to WS_FTP Server, a brief description of File Transfer Protocol (FTP) and how an FTP server works (for newcomers), how the WS_FTP Server works, and a description of the product's main features.

In addition, you'll find an introduction to the FTP server's interface (the WS_FTP Server Manager), system requirements, and the installation procedure.

What is WS_FTP Server?

WS_FTP Server is a full-featured FTP server for Windows NT and Windows 2000 systems. WS_FTP Server lets you create an FTP site that makes files and folders on your PC available to other users and customers. Users can connect (via the Internet) to your site, list folders and files, and (depending on permissions) download and upload folders and files. You can control user access to the site itself and to its individual folders and files. You can create multiple FTP sites on the WS_FTP Server — each will function as a completely separate site.

WS_FTP Server complies with the current Internet standards for the FTP protocol (documented in RFC 959 and 1123). Users can connect to the server and transfer files by using an FTP client that complies with this protocol, such as WS_FTP Pro. The FTP server runs as a Windows NT service.

Note

The Internet Engineering Task Force (IETF) publishes Requests for Comments (RFCs) for all Internet Standards. Each RFC defines a standard. You can view RFCs online by connecting to: <http://rs.internic.net>.

How FTP Works

FTP is based on the client–server model of communication between computers: one computer runs a server program “serving up” information to other computers. The other computers, or systems, run client programs that request information and receive replies from the server. The system running the server program is an FTP server.

To access an FTP server, users must be able to connect to the Internet, Intranet, or local area network (via a modem or local area network) and an FTP client program.

An FTP client–server session establishes two connections: a control connection that stays open for the entire session and a data connection that opens and closes to transfer data such as folder listings and files to or from the client as requested by the client. Normally, the control connection occurs on port 21.

The FTP server runs continuously in the background and listens to port 21 for a connection request from an FTP client. When an FTP client requests a connection, the FTP server verifies the logon user ID and password and, if valid, it opens a control connection.

After a user logs on, their access to the FTP hosts’s file system is determined by permissions assigned to directories and folders.

How WS_FTP Server Works

WS_FTP Server is installed as a Windows NT service that runs continuously. WS_FTP Server lets you set up one or more FTP hosts, each with its own users, directories, and folders. Each FTP host functions as a separate FTP site. To set up an FTP host, you use the following components:

- **User accounts** — WS_FTP Server can use user accounts from an existing Windows NT, IMail Server (Ipswitch’s mail server product), or other ODBC external user database. You can also use the WS_FTP Server Manager to create accounts in an ODBC database, or its own user database. To log on from an FTP client, users enter their user ID and password.
- **Anonymous logon** — if enabled, a user can log on to your FTP site without having a user account. You can use “anonymous FTP” to make folders and files on your PC publicly available, without having to create and maintain individual user accounts.

To log on from an FTP client, users enter **anonymous** or **ftp** as their user ID. For the password, they should enter their e-mail address or no password.

- **Default public folders** — All users on an FTP host have a folder (with the same name as their User ID) under the FTP host's top directory. Users can transfer files to and from their own folders. If a folder named *public* is created in a user's folder, all other users (including anonymous users) can view and download files in this public folder.
- **Logon directory** — for each FTP host, you can set whether you want users to start in their own folder, or start in the top directory when they log on.
- **FTP folders and permissions** — If you want to grant FTP permissions for a folder on your computer, you can create an FTP folder and have it reference (point to) an existing folder. You can then grant permissions for any of the FTP users, including anonymous users.
- **User groups** — You can create a user group and add users to it so you can grant appropriate permissions on a group basis.

Major Features

WS_FTP Server provides the following major features:

- Supports all FTP clients and Web browsers that comply with the standards in RFC 959 and 1123.
- Supports multiple FTP hosts (sites/domains) on a single PC.
- Supports secure (SSL) connections so that all data transferred to and from the server can be encrypted.
- Uses an existing user database for user authorization (Windows NT, IMail Server, or another ODBC external database), or lets you create your own user database.
- Provides an unlimited number of user accounts on each FTP host.
- Supports anonymous logons.
- Supports "regets" — if the client connection is lost before a file transfer is complete, when the client logs on again, the client can resume the transfer where it was interrupted. (This feature must also be supported by the FTP client.)

- Lets you grant FTP permissions per folder.
- Lets you set maximum file counts and maximum disk space per user (or set a default value to be used by each user account).
- Lets you set maximum number of users logged on to an FTP host.
- Logs FTP server events.
- Lets you add or import users from the MS-DOS command line with the Add User utility.
- Lets you create customized commands that your users can use on your server.
- Runs as a Windows NT service.
- Ability to remotely manage your server.

WS_FTP Pro Client

If you need an FTP client, we recommend our own WS_FTP Pro. WS_FTP Pro lets you communicate with virtually all types of FTP servers.

WS_FTP Pro provides two user interfaces for 32-bit environments: the “classic” user interface, which runs as a stand-alone Windows application, and the “Explorer” interface, which looks and acts like Windows Explorer.

If you use WS_FTP Pro with WS_FTP Server, you will get premium performance and advanced functionality, such as:

- Encryption of user IDs and passwords sent over the network (when used with WS_FTP Pro Version 6.0 or later).
- The ability to resume a failed transfer.
- The ability to transfer from one remote FTP server to another (remote-to-remote transfer).
- The ability to make secure (SSL) connections to the server with WS_FTP Pro.

For more information about WS_FTP Pro, visit our web site at:
<http://www.ipswitch.com>

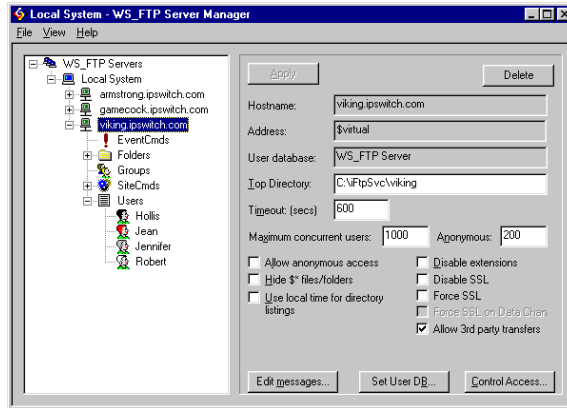
WS_FTP Server Security

WS_FTP Server provides the following security features:

- Complete SSL capabilities with multiple levels of security that can be configured at the server level.
- When used with the WS_FTP Pro Version 6.0 client or higher, logon connections send the user ID and password in an encrypted form, rather than sending them across the network in clear text.
- Users on an FTP client get three chances to send the correct user ID and password, after which the connection fails.
- User IDs and passwords are stored in the Windows NT registry when using WS_FTP Server database.
- Ability to control access to an FTP host by setting an IP address or range of addresses for which the FTP host either grants or denies access.
- Ability to set permissions on virtual folders.
- Ability to deny anonymous logins.
- Ability to lock users to their home folder.

The WS_FTP Server Manager

The WS_FTP Server Manager lets you manage your FTP server configuration, and any FTP sites you create.



The WS_FTP Server Manager presents a two panel window. In the left panel, click the plus sign (+) next to an item to display sub-items. When you click an item, its properties appear in the right panel.

You can have multiple FTP hosts (each functioning as a separate FTP server) on the WS_FTP Server. In the left panel, under Local System, there is an entry for each FTP host that you create. Under each FTP host, there are user accounts, groups of users, and folders (FTP directories) for that host.

You can manage all FTP server functions from the WS_FTP Server Manager.

Remote Management

Before you can remotely manage WS_FTP Server, you need to install WS_FTP Server Manager on the computer that will be used to do the remote management (Any Windows 2000, or Windows NT computer that the server is not running on.)

Installing from the WS_FTP Server CD-Rom:

Run the install program on that computer and select the option to install the Remote Server Manager.

Installing from the e-commerce download:

After installing WS_FTP Server on the host computer, transfer the mgr_inst.exe file to the computer you want to use to remotely manage your server (found in the WS_FTP Manager Install folder in the directory you installed WS_FTP Server 3.0). Double-click the file and follow the directions to install the WS_FTP Server Manager.

System Requirements

WS_FTP Server requires the following system resources:

- Windows NT 4.0 or later or Windows 2000.
 - A 32-bit TCP/IP protocol stack (such as the stack bundled with Windows NT)
-

Installing WS_FTP Server

You must log on to the Windows NT system as a system administrator in order to install the WS_FTP Server software.

If you purchased WS_FTP Server online, install it by double-clicking the file you downloaded and following the prompts on your screen.

To install the software from the CD:

Insert the WS_FTP Server disk into a disk drive. If the welcome screen does not appear:

- 1 Click the Start button and select **Run**.
- 2 Enter the drive letter followed by *autorun.exe*. For example, `d:autorun.exe`
- 3 Follow the instructions on your screen.

Removing WS_FTP Server

The uninstall function removes all files associated with WS_FTP Server from your PC.

To remove WS_FTP Server:

Go to the Add/Remove Programs section of your Windows NT Control Panel and select Ipswitch WS_FTP Server Manager.

Files Installed

When you install WS_FTP Server, the following files are placed on your hard disk:

ftpsec.dll, program that provides an interface between WS_FTP Server and the Windows NT security system

iFTPAddU.exe, the command line utility for adding and modifying users

iFtpMgr.cnt, the Help table of contents

iftpmgr.exe, the Server Manager application

iFtpMgr.hlp, the Help file

iftpsvc.exe, the FTP server

iFtpSvcP.dll, program that generates FTP server statistics in the Windows NT Performance Manager

release.txt, the release notes

remove.exe, the uninstall utility

sslsvc.dll, program that provides the SSL functionality

sslsvc.chm, the Help file for the SSL Utility

ipswitch.crt, the Ipswitch SSL certificate.

server.crt, the default SSL certificate.

server.key, the default SSL private key.

odbuser.dll, program that provides support for external user databases.

server_0.cdb, a database that contains several commonly used trusted certificates.

rand.dat, a program that generates random numbers.

mgr_inst.exe, the program that allows you to install the Server Manager remotely.

Release Notes

Please refer to the file named *release.txt* for information regarding enhancements or changes that may have been made to the software since this manual was printed.

Getting Updates and Giving Feedback

If a software patch is created to update the currently shipping version of WS_FTP Server, Ipswitch will make it available on our FTP and Web sites. You can check our download FTP directory or the download directory on our web site for current software patches. Note that to download most product upgrades, you must have a valid service agreement.

To download software from the Ipswitch FTP Site:

- 1 From your FTP client, connect to the Ipswitch FTP server by entering:
Hostname: `ftp.ipswitch.com`
User ID: `anonymous`
Password: *your e-mail address*
- 2 Open the `Product_Support` folder. Open the `WS_FTP_Server` folder.
- 3 Transfer the patch file and place it in your `WS_FTP_Server` directory. Run the patch file to update WS_FTP Server.

To download software from the Ipswitch web site:

- 1 In your web browser, go to: <http://www.ipswitch.com>
- 2 Click the **Services & Support** link.
- 3 Click **Patches and Upgrades**.
- 4 Save the patch file in your `WS_FTP_Server` directory. Run the patch file to update WS_FTP Server.

We welcome your feedback on WS_FTP Server. Please e-mail any comments and suggestions to feedback@ipswitch.com.

Chapter 2: Setting Up an FTP Site

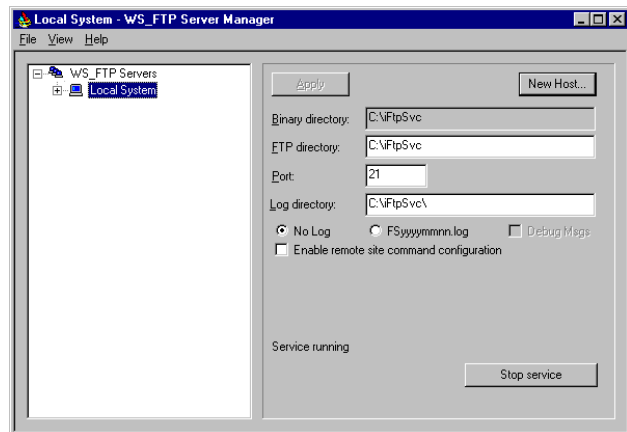
This chapter describes how to configure the WS_FTP server and how to set up one or more FTP sites on the server. You need to create an FTP host for each FTP site that you will have.

Configuring the FTP Server

On installation, WS_FTP Server is ready to work. You can use the default configuration for FTP connections (port 21, no logging, no access restrictions) or you can set the options described in this section.

To view and set options for the WS_FTP Server configuration:

- 1 In the left panel, select Local System. The Local System properties appear in the right panel.



- 2 Set or change any of the properties described in the following sections. These properties apply to all FTP hosts that you add to the FTP server.

Setting WS_FTP Server Directories

The Local System properties display the main directories for the WS_FTP Server.

Binary directory. The directory in which the FTP service (*iftpsvc.exe*) is installed. This directory can only be changed by uninstalling WS_FTP Server and re-installing in a new directory.

FTP directory. The top directory under which directories for each FTP host will appear.

Log directory. If logging is enabled, log files are placed in this directory.

Setting the FTP Server Port

Any FTP hosts that you create on the WS_FTP Server will use the same FTP port number. The default port number is 21, which is the standard port for FTP service on an Internet host.

FTP clients assume that the FTP server uses port 21. You can change this to any unused port number, but you must notify users to set the port in their FTP client.

To change the server's port number:

- 1 In the left panel, select Local System. The Local System properties appear in the right panel.
- 2 In the **Port** box, enter a new port number.

Logging FTP Server Events

You can set WS_FTP Server to write FTP events (such as connect, change directory, get file, put file) to a log file. If you make a change to the logging options, you must restart the FTP server.

To set the logging options:

- 1 In the left panel, select Local System. The Local System properties appear in the right panel.
- 2 Select one of the following options:
 - No log.** Server events will not be logged.

FSyyyymmnn.log. Server events for all FTP hosts are logged to a file named *FSyyyymmnn.log* where *yyyy* is the year, *mm* is the month, and *nn* is the day. This log is created daily in the **Log directory**. See “Reading the Log Files” on page 63 for information on using the log files to manage your server.

If this option is selected, you will be able to select the **Debug Msgs** option, which adds more detailed information to the log.

- 3 Optionally, change the **Log directory** to which log files are written. By default, this is set to the WS_FTP Server top directory. You can enter any valid path on your computer.

Starting and Stopping the FTP Server

The FTP server starts automatically and runs continuously as a Windows NT service. If you need to stop the server:

- 1 Start the WS_FTP Server Manager.
- 2 In the left panel, select Local System.
- 3 Click **Stop Service**.

To restart the service, click **Start Service**.

You can also start and stop the service by using the Services applet in the Control Panel. In the Services applet, look for the Ipswitch FTP Service.

Setting Up FTP Hosts

To use the WS_FTP Server with a single FTP host, the process is simple — the FTP host uses the Internet hostname and IP address of the host on which you are installing. To add additional FTP hosts to the same system, you can use the virtual host function.

For each FTP host you add, you need to consider the following:

- To create FTP user accounts, choose whether you will create your own user database, create users in an existing external (ODBC) database, or let the Server Manager use user accounts from an existing Windows NT, IMail Server user database on your PC, or external (ODBC) database.

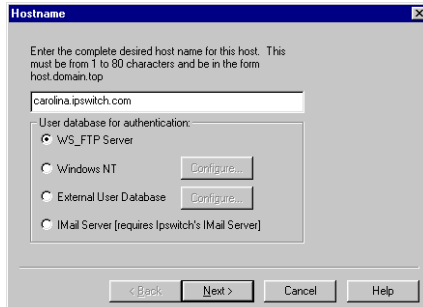
- By default, each user on the FTP host will have a folder (with the same name as their User ID) for uploading and downloading files and folders. If you want users to have access to other folders on the host, you need to create a virtual folder that references (points to) the local or networked folder. You can then grant user permissions for each virtual folder. You cannot change permissions on the user folders.
- You can set an option to determine where the user is placed in the file system when they log on: either in their own folder or in the top directory of the FTP host.
- Whether you want to provide anonymous access to the FTP host. If you provide anonymous access, any user can log on to the FTP host with a username of **anonymous** or **ftp** and a password that specifies their e-mail address (or no password). When a user logs on anonymously, they are placed in the top directory of the FTP host. Anonymous users can access any folders for which you have granted permissions to **anonymous**.

The following sections describe how to add the first FTP host, how to set options for a host (such as allowing anonymous access and setting maximum concurrent users), and how to add additional FTP hosts.

Adding the First FTP Host

To add the first (or only) FTP host:

- 1 Make sure your host has a valid Internet hostname and IP address and make sure the host has an entry on your Domain Name Server (DNS). If you use an Internet Service Provider (ISP) for connection to the Internet, your host must have an entry in the ISP's DNS.
- 2 Start the WS_FTP Server Manager. In the left panel, select Local System. The directory, port, logging, and FTP service information for this server appears in the right panel.
- 3 In the right panel, select **New Host**. The first screen of the New Host wizard appears.



- 4 Enter the Internet hostname of the host you are installing on. This can be from 1 to 80 characters and must be in the form `host.domain.top`.

Select the database to use for user authorization:

WS_FTP Server. If you want to create your own FTP user accounts (through the Server Manager or the Add User utility), select this option.

If you want WS_FTP Server to use user accounts from an existing user database, select one of these options:

Windows NT. All users in the Windows NT user database on your computer have access (using their Windows NT username and password) to the FTP host. Each user appears in the *users* folder in the top directory of the FTP host.

You may also use WS_FTP Server Manager to authenticate users on an NT domain, even if the computer WS_FTP Server is installed on is not the domain controller. For more information, see “Configuring an NT User Database” on page 19.

External User Database. All users in the correctly configured external ODBC database stored on your computer have access to the FTP host. Each user appears in the *users* folder in the top directory of the FTP host.

For more information on configuring external user databases, refer to the directions that appear in “Configuring an External User Database” on page 17.

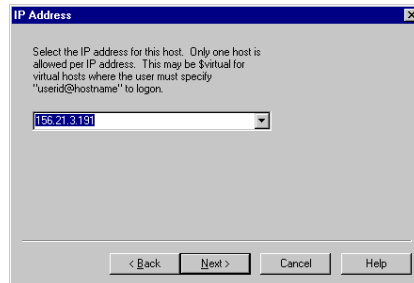
IMail Server. All users in the IMail Server user database on your local system have access (using their IMail Server username and password) to the FTP host. Each user appears in the *users* folder in the top directory of the FTP host.

Important: To use this option, the IMail Server for Windows NT software must be installed on your computer. Also, note the following:

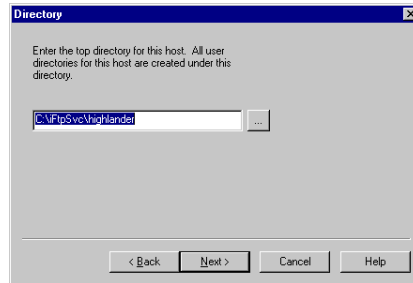
- The hostname you enter for the FTP host must be the exact name of the official hostname used by the IMail Server.
- You cannot use this option if the IMail Server is using the Windows NT user database for user authorization.
- The FTP host does not use the IMail Server top directories by default, but you can set the top directories to be the same, thus allowing FTP users to access their mail folders.

If you use the Windows NT or IMail Server user databases, you can display each user account and modify FTP settings for an account, but you cannot add or delete user accounts. You must add or delete user accounts through the user database. You can disable an account — see the section “Setting Options for the FTP Host.”

- 5 Click **Next**. The IP Address screen appears.



- 6 Enter or select the actual IP Address for this host. (The **\$virtual** IP address is for use with virtual hosts. Do not select it for the first FTP server that you add to a host.)
- 7 Click **Next**. The Directory screen appears.



- 8 Enter the top directory for this FTP host. All user folders for this FTP host are created under this directory. We recommend that you create a directory just for this host (this is the default). If you later add other FTP hosts (using the virtual hosts feature), you can have separate directories for each FTP host.
- 9 Click **Next**. The Summary screen appears and shows the Host-name, IP Address, and Directory for the FTP server. Click **Finish** to create the new FTP host. In the left panel, an entry for the host appears under Local System.

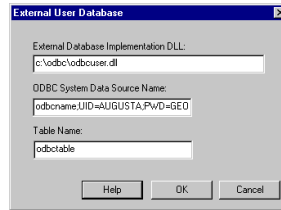
The host properties appear in the right panel — you can set additional host properties as described in the following section.

Configuring an External User Database

When you configure an external user database using these directions, WS_FTP Server creates an ODBC database that holds tables configured with the correct fields. Those fields are identified in the Table Name section of this chapter. After the database is created and the ODBC system data source name is established in the ODBC Source Administration tool (Found in your Windows Control Panel) you can use that database to store your user authentication information and user properties. This information can still be managed through the WS_FTP Server Manager, including adding and deleting users.

Follow the directions for creating a new host found in “Setting Up FTP Hosts” on page 13. While in the New Host wizard, select the **External User Database** option and click **Configure**. You can also click the **Set User DB** button in the host properties pane after the host has been created.

The External User Database dialog box appears.



- 1 Enter the correct information in all of the boxes.

External Database Implementation DLL. Enter the full path to the odbcuser.dll installed on your local server.

ODBC System Data Source Name. Enter the source name created using the ODBC Source Administration tool described above.

If the database requires you to log in using a username and password, place the following after the data source name.

;UID=<username>;PWD=<password>

Example: If you were using the source name `WS_FTP` and the username and password of `AUGUSTA` and `GEORGIA`, the correct format of the ODBC System Data Source Name box would be:

`WS_FTP;UID=AUGUSTA;PWD=GEORGIA`

Table Name. Enter the name of the database table that was created with the correct standard fields.

In order for `WS_FTP` server to use an external database, the information tables will be created with the following fields in the following format. The names are case sensitive.

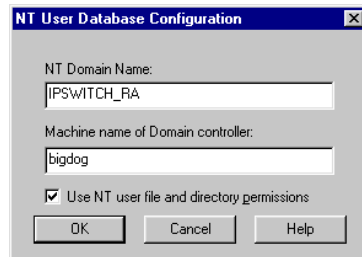
<u>Name</u>	<u>Type</u>
USERID	VARCHAR
PASSWORD	VARCHAR
FULLNAME	VARCHAR
FTPSPACE	INTEGER
FTPFILES	INTEGER
FTPFLAGS	INTEGER

- 2 Click **OK** to continue creating the host.

Configuring an NT User Database

You may use WS_FTP Server Manager to authenticate users on an NT domain, even if the computer WS_FTP Server is installed on is not the domain controller.

If the user database is located on the domain, identify the following fields on the NT User Database Configuration dialog after selecting the **Windows NT** option on the Hostname dialog. If the database is local, leave these fields blank.



NT Domain Name. Enter the name of the NT domain.

Machine name of Domain controller. Enter the name of the computer that controls the domain.

If you want to use the permissions you have set up in the NT User database, you must select the **Use NT user file and directory permissions** option.

Once you complete the Configuring an NT User Database dialog, click **OK** to continue creating the host, making sure you set the top level directory to the directory you want your users to have access to.

(example: C:\wsftp

Once the host is completely established, you must do the following to use the NT user permissions:

- 1 Create a virtual folder for each folder that is listed in the top directory of the host using the same name. For example, if you use the C:\wsftp directory and that directory contains a folder called *upload*, you must create a virtual folder called *upload* in the WS_FTP Server Manager.
- 2 Set permissions for all of the virtual folders you just created to Everyone - All Permissions.

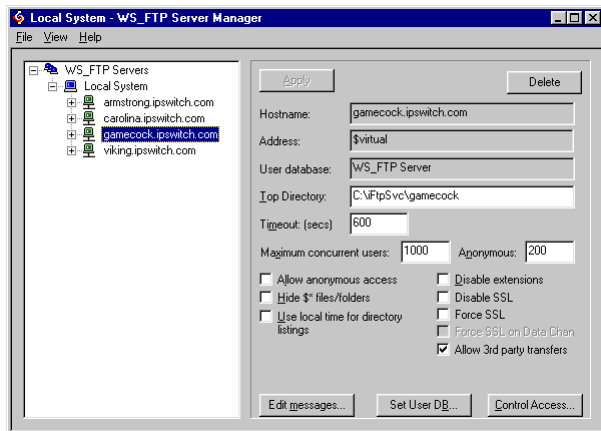
- 3 Select the **Do not include in top level folder listing** option for each folder.
- 4 In Windows Explorer, set your desired permissions for each of these directories.

Note

When using Active Directory on Windows 2000 Active directory must be installed with backward compatibility.

Setting Options for the FTP Host

After creating an FTP host, you can set additional options or change the existing setup for the host. In the left panel, select the FTP host. The host's properties appear in the right panel.



The **Hostname**, **Address**, **User Database**, and **Top Directory** are selected when you create a new FTP host.

The following sections describe the options.

Setting Timeouts for FTP Connections

You can set a timeout for FTP client connections to the FTP host. After this number of seconds, if the FTP server has not received a command from the FTP client, the client is disconnected.

- 1 In the left panel, select the FTP host. The host's properties appear in the right panel.
- 2 In the **Timeout (secs)** box, enter a timeout value.
- 3 Click **Apply**.

Setting Maximum Users

You can use the default settings for maximum number of users logged on to the FTP host, or you can change the settings as described here.

- 1 In the left panel, select the FTP host. The host's properties appear in the right panel.
- 2 In the **Maximum concurrent users** box, enter the maximum number of users (including anonymous users) that can connect to the FTP host at the same time. The default is 1000 users.
- 3 In the **Anonymous** box, enter the maximum number of anonymous users that can connect to the FTP host at the same time. The default is 200 users.

Note

If either limit is exceeded, a System Administrator or Host Administrator can still log on using the Server Manager. Also, a System Administrator can always log on using an FTP client.

Entering zero for either option disables new connections. This provides a way to temporarily "stop" the FTP server, so you can update files. New connections are not allowed, but current connections will continue until the user logs off or the connection exceeds the timeout value. Setting **Maximum concurrent users** to zero disables any new connections, setting **Anonymous** disables only new anonymous connections.

Allowing Anonymous Access

You can allow anonymous access to an FTP host so that users can access specified folders on the host without needing a user account. Users can then log on using **anonymous** or **ftp** as the username and their e-mail address for the password (or no password), for example:

Username: anonymous

Password: rhyne@ipswitch.com

To enable anonymous access to the FTP host:

- 1 In the left panel, select the FTP host. The host's properties appear in the right panel.
- 2 Select **Allow anonymous access** to this host.

When an anonymous user logs on, they are placed in the host's top directory.

- 3 Optionally, set permissions for **anonymous** on any virtual FTP folders. For example, you can use virtual folders to create a download or an upload folder for anonymous users.
- 4 Click **Apply**.

When an anonymous user logs on to the FTP host, they will see the following files and folders:

- Any files in the top directory. Anonymous users can list and download these files. You can put a *readme* file that describes the contents of any public directories here.
- Any virtual folders for which you have granted permissions to **anonymous**. Virtual folders appear in the host's top directory and reference a directory on the host or network.
- The *users* folder. If a user on the FTP host has a folder named public in their own folder, it appears under the *users* folder. For example, if the users fred and homer have public folders, an anonymous user will see a listing like the following when they list the users folder contents:

```
/fred  
/homer
```

Anonymous users can list and download files in these public folders. We recommend that you hide a user's public folder by selecting **Disable Public Access Directory** in the user's properties or by selecting the **Do not list user folders** on the Users Properties page.

Hiding Files and Folders

You can hide a file or folder in any directory by prepending a \$ character to the file or folder name and doing the following:

- 1 In the left panel, select the FTP host. The host's properties appear in the right panel.
- 2 Select **Hide Files and Folders that start with '\$'** to hide all files and folders whose name begins with a dollar sign (\$) character, for example *\$banner.txt* or *\$Marketing*.

Setting Directory Listings to Use Local Time

By default, WS_FTP Server displays directory listings in GMT (Greenwich Mean Time). You can set the directory listings on the FTP host to use the host's local time.

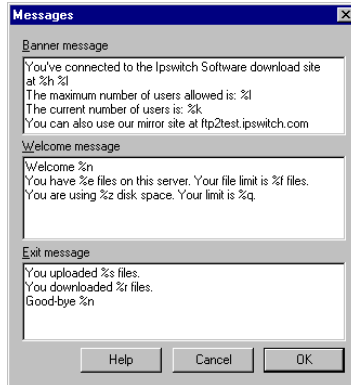
- 1 In the left panel, select the FTP host. The host's properties appear in the right panel.
- 2 Select **Use local time for directory listings**.

Using Banner, Welcome, and Exit Messages

You can create messages to send to an FTP client on successful connection, logon, and logoff. The FTP client usually displays these messages in the message log.

To create the messages for an FTP host:

- 1 In the left panel, select the FTP host. The host's properties appear in the right panel.
- 2 Click **Edit messages**. The Edit Messages screen appears.



- 3 In the edit boxes, enter text for the messages.
- 4 Click **OK**.

Banner Message. The FTP server sends this message to a user upon successful connection, before the user logs on. You can use this message to tell users about the organization of your FTP site, any rules, times of operation, mirror sites, or contact information. You can use the message variables to provide information, for example, that the FTP host has reached the maximum number of concurrent users.

Welcome Message. The FTP server sends this message to a user upon successful logon. You can use the message variables to report information, such as the current number of files and the maximum for this user.

Exit Message. The FTP server sends this message to the user on logoff. You can use the message variables to provide statistics for the FTP session, for example, the number of files received and sent by the user.

The messages can also contain the following variables:

- %a = Current number of anonymous users for this host
- %b = Maximum number of anonymous users for this host
- %d = Number of files deleted by user
- %f = Maximum number of files the user can have (or unlimited)
- %e = Number of files the user currently has
- %h = Hostname

%I = IP address of remote user
%k = Current number of users logged on
%l = Maximum number of users that can log on
%n = Fullname
%q = Maximum disk space the user can have (or unlimited)
%r = Number of files received by user
%s = Number of files sent by user
%u = User ID
%z = Current disk space used by the user

When these messages are created they are placed in the specified Top Directory of the Host. If this directory does not exist the Messages will not save. You can either manually create this directory, or it will be automatically created when a user logs in. (You need write permission for that directory.)

Please note that a Virtual host without an IP will not display a banner message. The Banner Message is displayed when a connection is first established. An IP-less virtual host is not connected to until a user logs in.

Creating Message Files for Folders and Directories

You can create a message named *\$message.txt* in any directory or folder and when a user changes to that directory or folder, WS_FTP Server displays the message. WS_FTP Server sends the *\$message.txt* in response to the CWD (change working directory) or CDUP (change directory to up one level) command from the FTP client.

For example, when a user opens a directory or folder, you can display a message that refers them to a *readme* file for a description of the folder's contents.

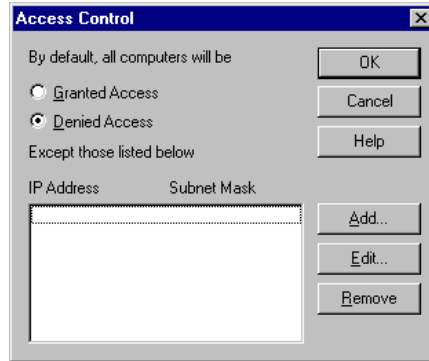
The message can also contain any of the variables described in the previous section, "Using Banner, Welcome, and Exit Messages."

Setting Access by IP Address

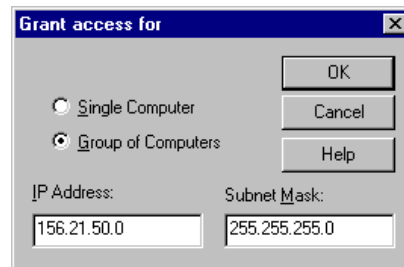
You can control access to an FTP host by setting an IP address or range of addresses for which the FTP host either grants or denies access.

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

- 1 In the left panel, select the FTP host. The host's properties appear in the right panel.
- 2 Click **Control Access**. The Access Control properties appear.



- 3 Select **Denied Access**.
- 4 Click **Add**. The Grant Access For dialog box is displayed.

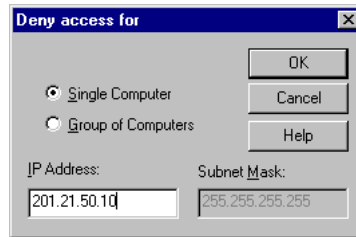


- 5 In the **IP Address** box, enter the IP address of the computer to be granted access to the server.
- 6 To grant access to a group of computers, select **Group of Computers**. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be granted access. For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This will grant access to those 254 systems.

- 7 Click **OK** to add the IP address(es) to the list. Access will be denied to all computers except those listed.
- 8 Click **OK** to save the changes. Note that you must stop and restart the FTP server for the changes to take affect.

To deny access to a specific computer or group of computers:

- 1 In the left panel, select the FTP host. The host's properties appear in the right panel.
- 2 Click **Control Access**. The Access Control properties appear.
- 3 Select **Granted Access**.



- 4 Click **Add**. The Deny Access On dialog box is displayed.
- 5 In the **IP Address** box, enter the IP address of the computer to be denied access to the server.
- 6 To deny access to a group of computers, select **Group of Computers**. In the **IP Address** and **Subnet Mask** boxes, enter the IP address and subnet mask for the group to be denied access. For example, if you have a class C address space of 156.21.50.0, enter a group address of 156.21.50.0 and a subnet mask of 255.255.255.0. This will deny access to those 254 systems.
- 7 Click **OK** to add the IP address(es) to the list. Access will be granted to all computers except those listed.
- 8 Click **OK** to save the changes. Note that you must stop and restart the FTP server for the changes to take affect.

Setting an Alias for the FTP Host

Many FTP sites use an alias in their Domain Name Server (DNS) system so they can assign a familiar name to the site. Rather than connecting to an FTP host using its actual hostname (for example, gyro.ipswitch.com), it may be easier for users to remember or guess a name like ftp.ipswitch.com. You can add a record to your DNS system to create such an alias, for example:

```
ftp IN CNAME gyro.ipswitch.com
```

Users could then log on to ftp.ipswitch.com. The alias also allows you to move your FTP site to another host without changing the hostname.

Other Options

Disable extensions. When this option is selected, the server will no longer support FTP server extensions. Those extensions include XAUT and FEAT, as well as any customized SITE commands. Selecting this option will also disable SSL capabilities.

Disable SSL. Selecting this option keeps users from connecting to the server through a secure connection. Once this option is set, you must clear it before users can use SSL connections.

Force SSL. Select this option to force users to make an SSL connection. While this does not change the way they are connecting automatically, it will refuse any connection not using SSL negotiations, and send an error message stating why the connection was refused.

Force SSL on Data Chan. Select this option to force users to make an SSL connection, and to refuse any data that is not SSL encrypted.

Allow 3rd party transfers. Selecting this option will allow users to transfer files from one server to another if both servers allow it.

Adding Additional FTP Hosts

You can have multiple FTP hosts on a single system, with each host functioning as a separate FTP site. The first FTP host you add should use the primary hostname and IP address of the local host. Subsequent FTP hosts that you add can be "virtual hosts." There are two kinds of virtual FTP hosts:

- Virtual host with an IP address — We strongly recommend that each FTP host you create have its own IP address, which requires your computer to have multiple IP addresses available. Using separate IP addresses ensures that an FTP client (or a browser) can connect to the FTP host. Make sure your host has a valid Internet hostname and IP address and make sure the host has an entry on your Domain Name Server (DNS). If you use an Internet Service Provider (ISP) for connection to the Internet, your host must have an entry on the ISP's DNS.
- Virtual host without an IP address — If no other IP addresses are available on the host, you can create an FTP host and assign it a virtual IP address (\$virtual). However, to log on to the host, FTP users must include the hostname in their userid; for example, *userid@hostname* or *anonymous@hostname*. This may present a problem for some FTP clients and for browsers.

To add a virtual FTP host:

- 1 In the left panel, select Local System. The directory, port, log options, and FTP service information for this host appear in the right panel.
- 2 In the right panel, select **New Host**. The first screen of the New Host wizard appears.
- 3 Enter the desired hostname for the FTP host. This can be from 1 to 80 characters and must be in the form host.domain.top.
- 4 Select the database to use for user authorization:

WS_FTP Server. To create your own FTP user accounts (using the Server Manager or the Add User utility), select this option.

If you want WS_FTP Server to automatically use user accounts from an existing user database, select one of these options:

Windows NT. All users in the Windows NT user database on your computer will have access (using their Windows NT username and password) to the FTP host. Each user appears in the *users* folder in the top directory of the FTP host.

External User Database. All users in the correctly configured external ODBC database stored on your computer have access to the FTP host. Each user appears in the *users* folder in the top directory of the FTP host. (You may also use WS_FTP Server Manager to create users in this database.)

IMail Server. All users in the IMail Server user database on your local system will have access (using their IMail Server username and password) to the FTP host. Each user appears in the *users* folder in the top directory of the FTP host.

Important: To use this option, the IMail Server for Windows NT software must be installed on your computer. Also, note that:

- The hostname you enter for the FTP host must be the exact name of the official hostname used by the IMail Server.
- You cannot use this option if the IMail Server is using the Windows NT user database for user authorization.
- The FTP host does not use the IMail Server top directories by default, but you can set the top directories to be the same, thus allowing FTP users to access their mail folders.

If you use the Windows NT or IMail Server user databases, you can display each user account and modify FTP settings for an account, but you cannot add or delete user accounts. You must add or delete user accounts through the specific user database.

- 5 Click **Next**. The IP Address screen appears.
- 6 If the virtual host has an IP address, select the IP Address. If the virtual host does not have an IP address, select \$virtual.
If an IP address is marked with an x, it is already used by another FTP host; if you select it, the other FTP host will be disabled.
- 7 Click **Next**. The Directory screen appears.
- 8 Enter the top directory for this FTP host. All user folders for this FTP host are created under this directory. We recommend that you create a directory just for this host. If you later add other FTP hosts, you can have separate directories for each FTP host.

- 9 Click **Next**. The Summary screen appears and shows the Host-name, IP Address, and Directory for the FTP server. Click **Finish** to create the new FTP host. In the left panel, an entry for the host appears under Local System.

The host properties appear in the right panel — you can set additional host properties. See “Setting Options for the FTP Host” on page 20.

Deleting an FTP Host

To delete an FTP host from the WS_FTP Server:

- 1 In the left panel, select the FTP Host, and then select **Delete** from the right mouse menu.

A message box appears, verifying the deletion. If you select **Yes** from this box, the host will be deleted. A dialog box appears and asks if you would like to delete the top level directory (and all folders in it) for this host.

- 2 Click **No** if you want to save files and folders to move to another directory (the host is deleted but the directory structure remains). Click **Yes** to delete all files and folders associated with the FTP host. Click **Cancel** if you do not want to delete the FTP host.

Renaming an FTP Host

To rename an FTP host on the WS_FTP Server:

- 1 In the left panel, select the FTP Host, and then select **Rename** from the right mouse menu.
- 2 Enter a new name for the host. This should be a valid Internet hostname in the form host.domain.top.

Note that the FTP host’s top directory does not change.

Event Commands

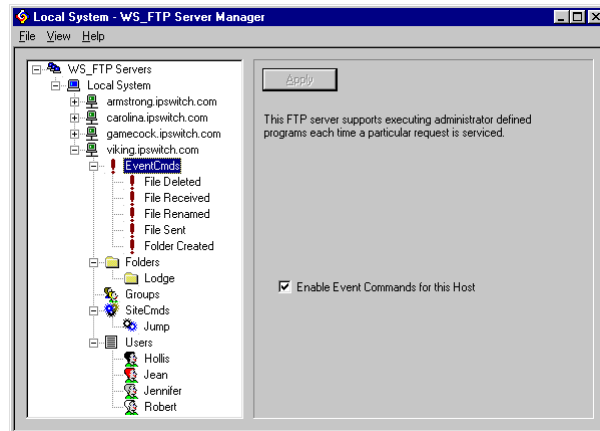
With the Event Command feature, server administrators can set up WS_FTP Server to execute a program each time a specific event is performed on the host. The following is a list of these events:

- File Deleted
- File Received
- File Renamed
- File Sent
- Folder Created

Enabling event commands

To enable an event command.

- 1 In the left panel of the WS_FTP Server Manager, select the FTP host and then select EventCmds. The Event Command window appears.



- 2 In the Event Commands pane, select **Enable Event Commands for this Host**.
- 3 Click **Apply**.

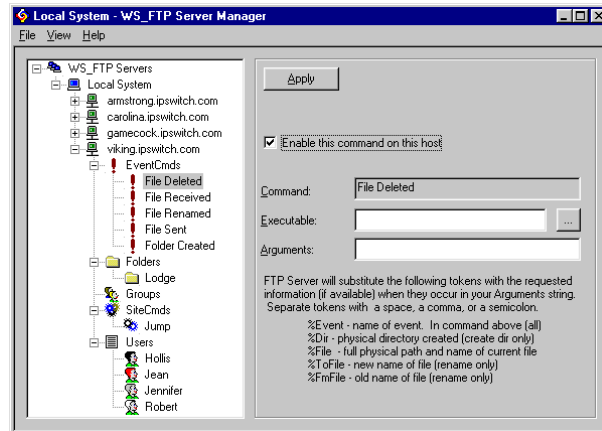
The **EventCmds** section under the Host will expand, displaying the events that can be set up.

Configuring Event Commands

The first step in configuring the use of Event Commands, is to enable the specific event you want to configure.

To do this:

- 1 Select the event in the left pane. The right pane will display the Configure Event Commands window.



- 2 Select **Enable this command on this host**.
- 3 Click **Apply**.

You will now be able to configure WS_FTP Server to invoke the program or batch file identified in the **Executable** box, whenever the event occurs on the server.

Note

If you want to use a batch file, enter `CMD.EXE /C` in the **Executable** box, and in **Arguments** specify the full path to the batch file in quotes. Example: `"c:\iftpsvc\run.bat"`

Command. The command or event name. This field can not be edited.

Executable. Enter the path and name of the program or batch file to be run when the event happens on the host. You can also click the **Browse (...)** button to select it from your local system.

Arguments. Enter any arguments that will be sent when the program is called. See the description of arguments on the screen for more information.

Disabling Event Commands

To disable ALL event commands for a host:

- 1 In the left panel of the WS_FTP Server Manager, select the FTP host and then select **EventCmds**. The Event Command window appears.
- 2 In the Event Commands pane, clear the **Enable Event Commands for this Host** option.
- 3 Click **Apply**.

To disable event commands for a single event:

- 1 In the left panel of the WS_FTP Server Manager, select the FTP host and then select **EventCmds**. The Event Command window appears.
- 2 From the **EventCmds** list, select the event you want to edit.
- 3 Clear the **Enable this command on this host** option.
- 4 Click **Apply**.

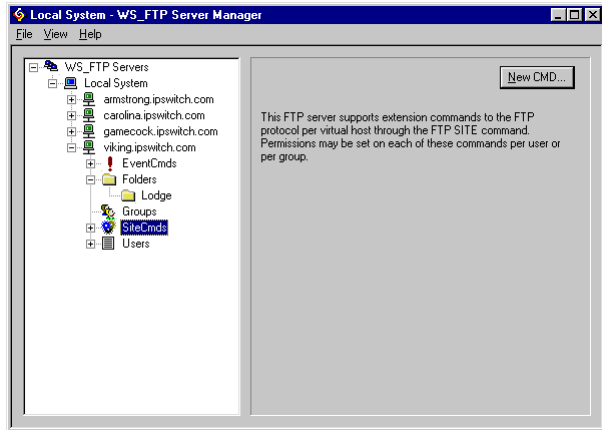
Site Commands

With the Site Command feature, server administrators can use WS_FTP Server to create customized FTP commands that users can use to execute applications on the FTP server.

Adding a Site Command:

To add a new Site command

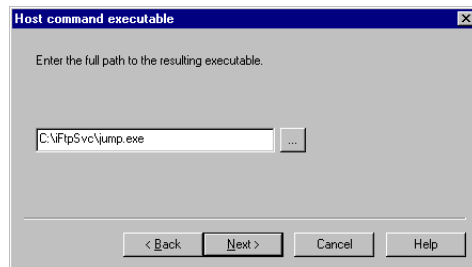
- 1 In the left panel of the WS_FTP Server Manager, select the FTP host and then select SiteCmds. The Site Command properties appear.



- 2 In the Site Command pane, select the **New CMD** button. The first window of the Custom Site Command wizard appears.



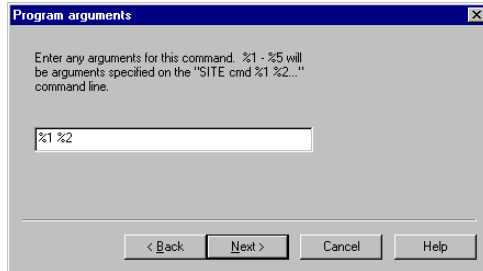
- 3 Enter the name of the site command in the text box. Click **Next**. The Host Command Executable screen appears.



- 4 Enter the full path for the file that is to be executed when the site command is run, or select it by clicking the **Browse (...)** button. Click **Next**. The Program Arguments screen appears.

Note

Never use server side applications (such as Notepad or Wordpad) as the executed program in a site command. Using these will display nothing for the user, but each time the command is run, a new copy of the program is opened on the server.



- 5 Enter %1-%5 for the allowed number of user defined variables, as well as any command line arguments that are to be used when the command is executed. Click **Next**. The Summary window appears.

Note

If you allow user-defined variables, it is a good idea to select the **Send Output** option on the SITE Command Properties window after you set up the command. If this is not done, only a general success or failure message will be returned to the user on the server.

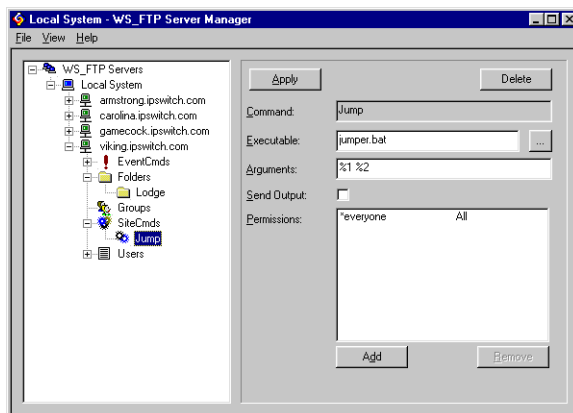
- 6 Review the information displayed to make sure it is correct. If the information is correct, click **Finish** to add the command. If the information needs to be changed, click **Back** to move to the window that needs to be changed.

After you set up the site command, you can add or change permissions for the command.

Modifying Site Command Properties

To view or change the properties for a SITE command:

- 1 In the left panel, under Local System, select the FTP host the command is associated with. Select SiteCmds and the specific command you want to view. The site command's properties appear in the right panel.



- 2 Make changes to any of the properties (defined below).
- 3 Click **Apply** to save the changes.

Command. The name of the SITE command. This is also the command that is used to execute the program. This property cannot be changed.

Executable. The path and file name of the application that is run when the correct command is given. This can be changed by typing the full path and file name of the application, or by clicking the **Browse (...)** button and selecting the application from a browse dialog box.

Arguments. Number of available user-defined variables that can be used with the command (up to 5), as well as command line arguments.

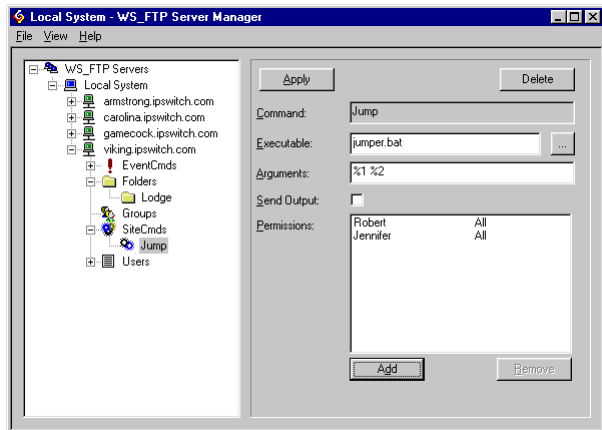
Send Output. When this option is selected, all output generated by the server will be shown to the user as the command is executed. If the option is cleared, no output will be returned other than a success or failure message. Command variable errors will not be returned unless this option is selected.

Permissions. A list that displays which users are able to use the site command. Click **Add** to add new permissions. To delete a user's permission, select it in the list and click **Remove**.

Modifying Site Command Permissions

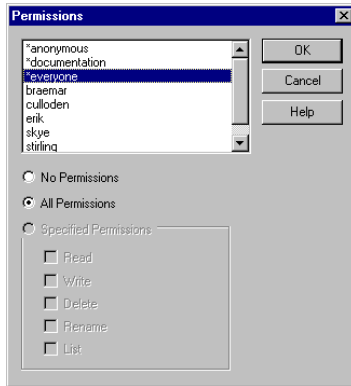
To control who can use a command:

- 1 Select the FTP host in the left pane of the WS_FTP Server Manager and select SiteCmds. Select the command from the list to view the Site Command Properties window.



When the command was set up on the WS_FTP Server Manager, it automatically added an entry to the Permissions box that allows all users to use the command.

- 2 If you want to change the permission, select the default permission value and click **Remove**. This will delete the permission.
- 3 Click **Add** to view the Permissions properties.



- 4 In the Permissions properties, associate the user or group of users with the appropriate access to the command. In the case of site commands, permission is either all or none.
- 5 Click **OK** to add the user.

Note

Permissions are used in the order in which they appear in the Permissions list. If a user appears at the top of the list, and that same user is below it in a group, the permissions set on the user will be used before the permissions for the group.

Chapter 3: Managing FTP User Accounts and Permissions

This chapter describes how to set up and manage FTP user accounts and how to set permissions for FTP folders.

How User Accounts Work

You can have an unlimited number of users for each FTP host. When you add an FTP host to the server, you select the user database for the host: Windows NT, IMail Server, WS_FTP Server, or external ODBC user database.

If you selected the Windows NT, IMail Server, or external (ODBC) user databases, you may already have a list of users for the FTP host. (In the Server Manager, in the left panel, expand the Users item to view the list of users.)

If you selected Windows NT or IMail Server, you cannot use the Server Manager to add or delete users, but you can set additional user options in the user properties.

If you selected the WS_FTP Server, or external user database, you can add users by using the New User wizard. See “Adding an FTP User Account” on page 42.

How Permissions Work

By default, users have the following permissions:

- User accounts — Each user has their own folder (with the same name as the User ID) where they can upload and download files and folders. They have full permissions to their folder (permissions for this folder cannot be changed.)
- Anonymous users — If you selected to allow anonymous access (in the FTP host’s properties), any user can log on to the FTP host with a username of **anonymous** or **ftp** and a password that specifies their e-mail address (or no password).

When a user logs on anonymously, they are placed in the top directory of the FTP host. Anonymous users can access any folders for which you have granted permissions to the special user group named **anonymous**.

- **Public folders** — If a user wants to make their folders or files available to other users, they can create a folder named *public* in their folder. When another user (or anonymous user) logs on to the FTP host, in the folder named *users*, they will see a folder for any user that has a *public* folder. For example, if the users fred and homer have public folders, another user will see a listing like the following:

```
/fred  
/homer
```

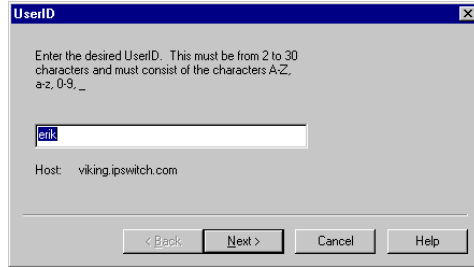
You can disable access to a **public** folder by selecting **Disable Public Access** in the user's properties.

- **Virtual folders** — To grant permissions to any other folders, you use a virtual folder. You can grant permissions for a virtual folder to any user or user group. You can also grant permissions to the special user groups named **anonymous** and **everyone** (which includes all users on the FTP host as well as anonymous users). When you create a virtual folder, by default, it grants List and Read permissions to **everyone**.

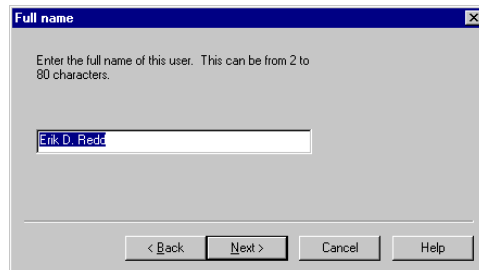
Adding an FTP User Account

To add a new user to an FTP host:

- 1 In the left panel, select the FTP host, and then select Users. The Users properties appear in the right panel.
- 2 Click the **New Users** button. The first screen of the New User wizard appears.



- 3 Enter a **User ID** for the user and click **Next** to continue. The User ID can be from 2 to 30 characters and must be from the character sets: A-Z, a-z, 0-9.
- 4 Enter the user's full name and click **Next** to continue. The full name can be from 2 to 80 characters.



- 5 Enter a password and click **Next** to continue. The password can be from 2 to 30 characters.



- 6 Click **Finish** to create the new user.

The user account appears in the list of users for the FTP host.

To set additional properties for the user account, in the left panel, select the user. The user properties appear in the right panel.

See "Setting User Options" on page 44.

Setting User Logon Options

For each FTP host, you can set whether you want users to start in their own folder, or start in the top directory when they log on.

To set the logon option:

- 1 In the left panel, select the FTP host, then select Users. The properties appear in the right panel.

- 2 Select one of the options:

Logon users to home folders. When a user logs on, they are placed in their own folder (which has the same name as their user ID).

Logon users to /. When a user logs on, they are placed in the top directory of the FTP host.

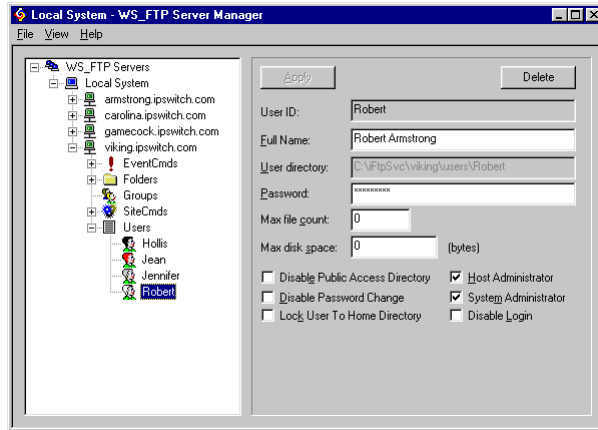
User folder under root. When a user account is created, the folder for that account is created under the top directory of the FTP host.

Do not list user folders. When this option is selected, users will not be able to see other user folders. Only their own user folder, non-user folders, and files will be listed.

- 3 Click **Apply** to save the changes.

Setting User Options

After creating user accounts, you can set additional options for each user or change the user setup. In the left panel, select the user. The user's properties appear in the right panel.



The following sections describe the options.

User Directories and User Password

In the user properties, the **User directory** box shows the full path name to the user's folder. This folder has the same name as the User ID and is created under the users folder of the FTP host. The user can transfer files to and from this directory. When the user logs on, they are placed in this folder. By default, this is the only folder for which the user has full permissions. You can grant the user permissions for other folders by using the virtual folders feature.

The Password box shows the user's password in an encrypted form. You edit this box to change the password. The password can be from 2 to 30 characters.

Setting Logon, Public Directory, and Change Password Options

You can use the following options to set whether the user can access the FTP host, whether other users can access this user's public directory, and whether the user can change password from an FTP client.

- 1 In the left panel, select the FTP host, then select a user. The user's properties appear in the right panel.

- 2 If you do not want this user to be able to log on to the FTP host, select **Disable Login**. You can use this option to disable a Windows NT or IMail Server user's account without having to delete the user account from the Windows NT or IMail Server user databases. (The WS_FTP Server Manager cannot delete user accounts from either of these user databases.)
- 3 If you do not want other users to have permissions to this user's public directory, select **Disable Public Access Directory**.

If the user has a folder named public in their folder, all users (including anonymous users) have List and Read permissions to the folder. This allows the user to maintain their own public directory for transferring files. When any other user logs on to the FTP host, this public folder appears in the *users* folder (in the host's top directory) and has the same name as the User ID.
- 4 If you do not want this user to be able to change their password from an FTP client, select **Disable Password Change**.
- 5 Click **Apply** to save changes.

Setting File and Disk Space Quotas

You can set user global quotas for files and disk space (the quotas apply to each user on the FTP host) or per individual user. A user quota setting overrides a global (or host) quota setting as long as the user quota setting is not zero.

To set the maximum number of files and maximum amount of disk space allowed for every user on an FTP host:

- 1 In the left panel, select the FTP host, then select Users. The properties appear in the right panel.
- 2 In the **Max file count** box, enter the maximum number of files a user can keep on the FTP host. This is the total number of files for each of the user's folders.
- 3 In the **Max disk space** box, enter the maximum number of bytes a user can consume on the FTP host's drives.
- 4 In the user properties, make sure quotas for each individual user is set to zero.
- 5 Click **Apply** to save the settings.

To set the maximum number of files and maximum amount of disk space on a per user basis:

- 1 In the left panel, select the FTP host, then select a user. The properties appear in the right panel.
- 2 In each user's properties, set the quotas for the user.

This setting overrides a global quota setting.

Setting Administrator Permissions

You can grant Host Administrator or System Administrator permissions to a user. These permissions determine what the user sees when they log on to the FTP host from an FTP client or when they log on to the FTP server from the Server Manager (for remote management). For information on remote management capabilities, see “Chapter 4: Managing FTP Hosts” on page 59.

In the user properties, set the following options:

- 1 In the left panel, select the FTP host, then select a user. The user's properties appear in the right panel.
- 2 Select **Host Administrator** to grant this user Host Administrator permissions. A Host Administrator has full permissions for all user folders on the FTP host, and has any permissions granted via virtual folders. In addition, the Host Administrator has remote management capabilities for the FTP host and all of its users, folders, and groups.
- 3 Select **System Administrator** to grant this user System Administrator permissions. A System Administrator has full permissions for their own folder, and has any permissions granted via virtual folders (just like a regular user). If you want the System Administrator to have access to all user folders, you need to also select Host Administrator. In addition, the System Administrator has remote management capabilities for all FTP hosts on the WS_FTP Server.
- 4 Click **Apply** to save changes.

Note

In the left panel, the user icon indicates the type of access the user has to the FTP Host's file system:

- Normal user — has full permissions to their own folder and any other permissions assigned by the Host Administrator. User icon has black hair.
 - Host Administrator — User icon has brown hair.
 - System Administrator — User icon has white hair.
-

Deleting a User

To delete a user from an FTP host:

- 1 In the left panel, select the user, and then click **Delete** from the right pane.

A dialog box appears and asks if you would like to delete all files and folders in the user's folder.
 - 2 Click **No** if you want to save files and folders to move to another directory (the user is deleted but the directory structure remains). Click **Yes** to delete all files and folders associated with the user. Click **Cancel** if you do not want to delete the user.
-

Renaming a User

To rename a user on an FTP host:

- 1 In the left panel, select the user, and then select **Rename** from the right mouse menu.
- 2 Enter a new name for the user.

The name of the user's top directory is changed. You can change the user's full name in the user's properties.

Adding Users with the Command Line Utility

The Add User program is a command line utility for WS_FTP Server; you can use it to add, modify, or delete users on an FTP host.

You cannot use this utility to add users to an FTP host that uses the Windows NT, the IMail Server, or an ODBC external user database.

The Add User utility accepts input from the MS-DOS prompt and returns messages to the MS_DOS display. You can type Add User commands at the MS-DOS prompt or run them in a batch file.

To start the Add User utility:

- 1 Open an MS-DOS window and change directories to the WS_FTP Server directory.
- 2 For a list of command options, enter: `iftpaddu /?`

If you invoke the utility with no command line options (by entering only `iftpaddu` at the MS-DOS prompt), you can then manually input commands, pressing Enter after each line. If you do this, press CTRL-Z to exit the utility when you are done.

Basic Command Syntax

```
iftpaddu -u userid [-h hostname] [-n "full name"] [-p password] [options]
```

```
iftpaddu -modify -u userid [-h hostname] [-n "full name"] [-p password] [options]
```

```
iftpaddu -kill -u userid [-h hostname]
```

Argument	When to use
<code>-u <i>userid</i></code>	Adds a user ID, where <i>userid</i> is the ID you want to add. This is the only required argument. Only one <i>userid</i> can be added in a single command.
<code>-h <i>hostname</i></code>	Specifies the user's FTP host, where <i>hostname</i> is the name of the FTP host. The primary FTP host is used if no host is specified.
<code>-n "<i>full name</i>"</code>	Specifies the <i>full name</i> of the user in double quotes.
<code>-p <i>password</i></code>	Specifies a <i>password</i> for the user. If you omit this argument, the user's password is "password."
<code>-modify</code>	Use before entering any other arguments when you want to modify an existing user.
<code>-kill</code>	Use to delete a user. You must enter <code>-u userid</code> . If the user is not on the primary FTP host, you must also enter <code>-h hostname</code> .

Argument	When to use
+active	Enables the user to log on. (This is the default setting when adding a new user.)
-active	Disables the user's ability to log on.
+chgpas	Enables the user to change password from an FTP client.
-chgpas	Disables the user's ability to change password from an FTP client.

Adding a User

The following examples add a user ID of test01.

```
iftpaddu -h myhost.com -u test01 -n "ms test"
-p yourpass

iftpaddu -u test01 -n "mr test" -p newpass

iftpaddu -u test01
```

Modifying a User

The following examples modify a user ID.

```
iftpaddu -modify -h myhost.com -u test01
-p newpass

iftpaddu -modify -h myhost.com -u test01
-chgpas

iftpaddu -modify -u test01 -active
```

Deleting a User

The following example deletes a user ID.

```
iftpaddu -kill -u test01 -h myhost.com
```

How Users Can Change Their Password

If the FTP client supports sending a SITE or QUOTE command, users can change their password from the client. If you do not want a user to be able to change their password, in the user properties, select **Disable Password Change**.

For example, using the WS_FTP Pro “classic” client, you change the password as follows:

- 1 Log on to the FTP host.
- 2 In the Remote Site (right-side) panel, select **FTP Commands ->Site** from the right mouse menu.
- 3 In the Input dialog box, enter the following command:
`CPWD password`
where *password* is the new password.
- 4 Check the Log Window (LogWnd) to see that the command was successful.
- 5 Log off and log back on with your new password.

Some FTP clients also support the Quote command. In the Quote command box, you can enter `SITE CPWD password` where *password* is your new password.

Creating User Groups

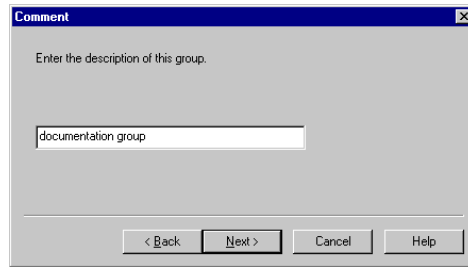
You can create a user group and add any users on the FTP host to the group. You can then grant permissions for FTP folders by user group, rather than for each individual user.

To add a user group to the FTP host:

- 1 In the left panel, select the FTP host, and then select **Groups**. The Groups properties appear in the right panel.
- 2 Click **New Group**. The first screen of the wizard appears.



- 3 Enter a name for the user group and click **Next** to continue. This can be from 2 to 20 alphanumeric characters.



- 4 Enter a description for the group and click **Next** to continue.
- 5 Click **Finish** to create the new group.

The user group appears in the list of groups for the FTP host.

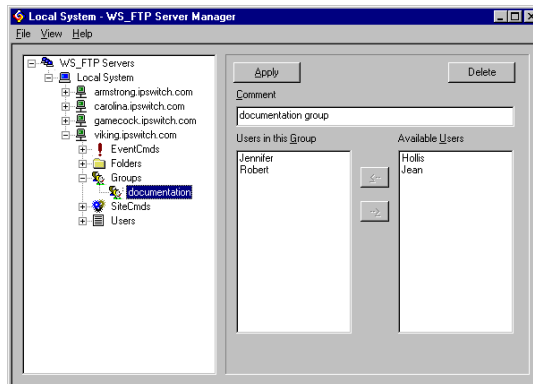
To add users to the user group, in the left panel, select the group. The group properties appear in the right panel. See Adding Users to the Group below.

Adding Users to the Group

You can add any users on the FTP host to a user group. You can then grant permissions for FTP folders by user group.

To view or change user group properties:

- 1 In the left panel, select the FTP host, expand the **Groups** list and select the group. The group properties appear in the right panel.



- 2 In the **Comment** box, enter or modify the description for the user group (for example, documentation).
- 3 To add a user to the group, select a User ID in the **Available Users** list and click the left arrow (<-).
The user appears in the **Users in this Group** list.
- 4 To remove a user from the group, select a User ID in the **Users in this Group** list and click the right arrow (->).
The user no longer appears in the **Users in this Group** list.
- 5 Click **Apply** to save your changes.

Deleting a User Group

To delete a user group from an FTP host:

In the left panel, select the group, and then click **Delete** from the right pane. The group is deleted.

Using Virtual Folders (to Grant Permissions)

You can create "virtual folders" that reference, or "point to," any folder on the local host or on your network. You can then grant permissions to a user or a user group for each virtual folder. If a user has permissions to a virtual folder, when they log on to the FTP host, the folder appears in the top directory of the host.

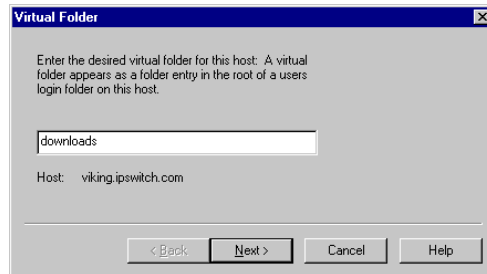
You can create a virtual folder that points to a folder that is already in the top directory (the only reason to do this is so you can grant permissions to the folder). Because virtual folders appear in the top directory, be sure to select the **Do not include in top-level directory listing** option — so the folder does not appear twice.

A virtual folder name is an alias for the real folder, thus it can have any name — it does not have to be the same name as the folder to which it references.

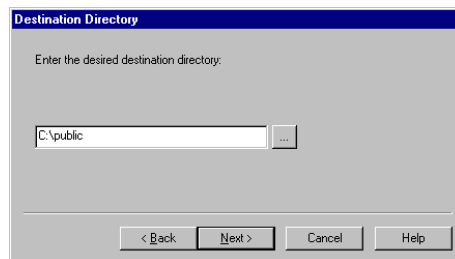
Adding a Virtual Folder

To add a new folder to an FTP host:

- 1 In the left panel, select the FTP host, and then select **Folders**. The Folder's properties appear in the right panel.
- 2 Click **New Folder**. The first screen of the New Folder wizard appears.



- 3 Enter a name for this "virtual" folder and click **Next** to continue.



- 4 Enter the path of the directory for which you are creating a virtual folder and click **Next** to continue. The path must contain the drive letter to be a valid path.

Example: E:\WS_FTP\Folder

- 5 Click **Finish** to create the new folder.

All new folders, by default, grant list and read permissions to a special user group called **everyone** (which includes all users and anonymous users). To view or change permissions for the folder, see [Granting Permissions for FTP Folders](#) below.

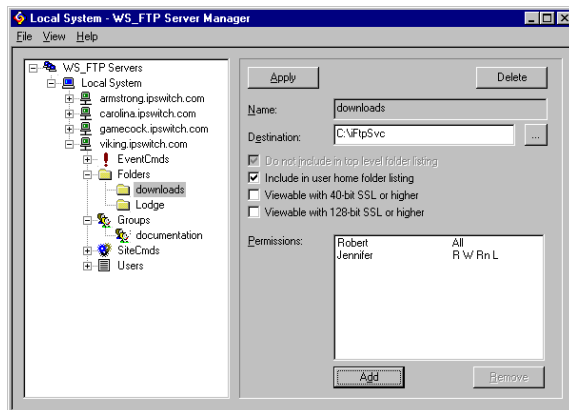
Granting Permissions for FTP Folders

You can grant permissions for any "virtual" folder shown in the Folders list (in the left panel). To grant permissions for other folders, you must create a virtual folder that references the real folder.

If you want all users on the FTP host to have permission for a folder, you can grant the permissions to **everyone** (this includes anonymous users). If you want users who log on anonymously to have permissions for a folder, you can grant the permissions to **anonymous**.

To grant permissions for a folder:

- 1 In the left panel, select an FTP host, expand the Folders list and select the folder. The folders properties appear.



- 2 In the Permissions list, select the user or user group for which you want to set permissions. (Names of user groups are marked with an x.)
- 3 Click **Add** to add the users to the folder.

4 Select the Permissions options:

No Permissions. No access to the folder. When logged on, the user or group will not see this folder.

All Permissions. Read, Write, Delete, Rename, and List access.

List. The user can display a listing of the folder contents.

Read. The user can download files from the folder.

Write. The user can upload files to the folder.

Delete. The user can delete files and folders in the folder.

Rename. The user can rename files and folders in the folder.

Specified Permissions. The user or user group has the selected permissions.

5 Optionally, select another user or user group and set their permissions.

6 Click **OK** to save your changes.

Notes on granting permissions

- To create an "upload" folder, you can grant Write permission only — this lets users upload a file or folder, but they cannot list the contents of the Upload folder and they cannot upload a file that has the same name as an existing file. You can add Delete permission if you want users to be able to overwrite an existing file.
- To create a "download" folder, you can grant List and Read permissions — this lets users list the contents of the folder and download a file or folder.

NT Permissions on Windows 2000

NT permissions will work on Windows 2000 computers.

To use this:

- 1 Set up a virtual folder to the top level folder you want to grant access to, and give rights to users and groups.
- 2 Using the NT permissions, set further restrictions on subfolders and files.

Note

Server will use the highest restriction level, so you can restrict users from areas that NT would grant permissions with the permissions on the virtual folder, or you can use NT to further restrict permissions for users that the server would give access to.

Changing Folder Properties

To view or change Folder properties:

- 1 In the left panel, select the FTP host, expand the Folders list and select the folder. The folder properties appear in the right panel.
- 2 The **Name** box shows the folder name. To change the folder name, in the left panel, right-click it the name, select **Rename** from the shortcut menu, and enter the new name.
- 3 In the **Destination** box, enter the path of the directory for which you are creating a virtual folder.

Use the **Browse** button to search your local and networked directories for the path.

Note that if you want to create a virtual folder that references a folder on the local network, you must run WS_FTP Server under a user account that has Windows NT permissions for that folder.

- 4 If you create a virtual folder that points to a folder in the top directory of the FTP host (the only reason to do this is so you can grant permissions to the folder), be sure to select the **Do not include in top-level directory listing** option — so the folder does not appear twice in the top directory.
- 5 To have virtual folders appear in user's home folders, select the **Include in user home folder listing** option. When this option is selected, **Do not include in top-level directory listing** will also be selected.
- 6 You can increase security by selecting either **Viewable only with 40-bit SSL or higher** or **Viewable only with 128-bit SSL or higher**. Clients that do not have SSL enabled will not be able to view the folder when this option is selected.

- 7 Click **Apply** to save your changes.
-

Deleting a Virtual Folder

To delete a virtual folder from an FTP host:

In the left panel, select the virtual folder, and then select **Delete** from the right mouse menu. The virtual folder is deleted, but the folder or directory to which it points remains.

Renaming a Virtual Folder

To rename a virtual folder:

- 1 In the left panel, select the folder, and then select **Rename** from the right mouse menu.
- 2 Enter a new name for the folder.

Chapter 4: Managing FTP Hosts

This chapter describes how you can use the WS_FTP Server Manager to manage FTP hosts from the local host or from a remote location.

Copying the Server Manager to a Remote Host

You can copy the WS_FTP Server Manager install program (*mgr-inst.exe*) to another Windows NT, or Windows 2000 system and run it to install the Server Manager which allows you to manage FTP hosts remotely.

If you installed WS_FTP Server 3.0 from a CD-Rom, you can use the CD-Rom to install the Server Manager on another Windows NT or Windows 2000 system to manage your server remotely.

Note

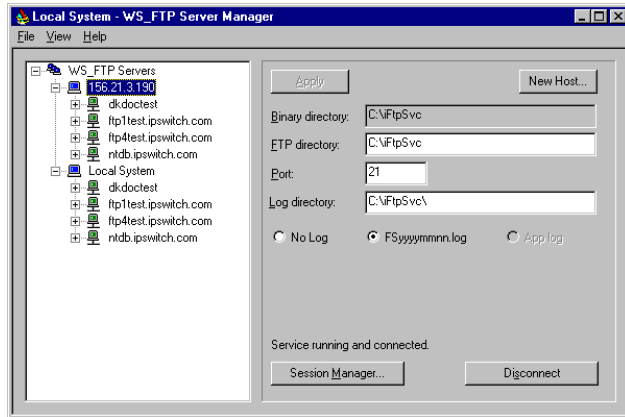
If using NT User database with Active Directory on Windows 2000, FTP Administrators must also be a member of an Admin group (or some other group to give them permission to write to the NT registry).

Connecting to the WS_FTP Server

To connect to the FTP server:

- 1 Start the WS_FTP Server Manager.
- 2 In the left panel, select WS_FTP Servers.
- 3 In the right panel, click **Connect**. The Logon dialog box appears.
- 4 In the **IP Address** box, enter the IP address of the host on which the FTP server is installed. (Note that you can connect to the server from the same host on which it is installed.)
- 5 In the **Server port** box, if your WS_FTP Server is not using port 21, change the port number to be assigned to the port.

- 6 Enter your **User ID** and **Password**. You must be a Host Administrator to access a particular FTP host, or a System Administrator to access all FTP hosts.
- 7 Click **OK**. The Server Manager connects to the FTP server.



In the left panel, you will see the IP Address of the FTP server. Select the IP Address and expand it to show the FTP hosts on the FTP server. You can make changes to FTP hosts, users, and folders (your access to FTP hosts and users depends on whether you are the System Administrator or the Host Administrator — see user properties for more information).

For the most part, you can use the same Server Manager functions that you can use if you were on the local system, but note the following differences:

- You cannot stop or start the server.
- Any changes you make remotely occur immediately, without stopping and restarting the server (except the server port).
- You can change the server port, but it does not take effect until the server is restarted.
- After making changes remotely, select **Refresh** from the View menu (or press F5) to make the changes also appear under the Local System.

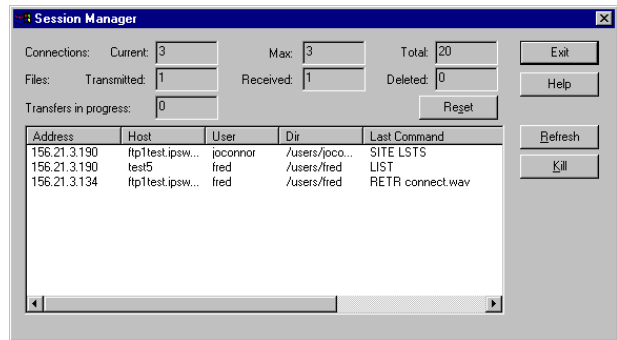
Click **Disconnect** to end the session and close the Server Manager.

Monitoring Active FTP Sessions

When connected to the FTP server from a remote system (or from the host on which it is installed), you can use the WS_FTP Server Manager to view and monitor active connections to the FTP server.

To view active sessions:

- 1 Use the WS_FTP Server Manager to connect to the FTP server.
- 2 In the left panel, select the IP Address of the remote FTP server. The server properties appear in the right panel.
- 3 Click **Session Manager**. The Session Manager window appears.



Server Statistics

The Session Manager window reports the following WS_FTP Server statistics. Connection and File statistics represent the count since the server was last started, or since the counter was reset.

Connection statistics: **Current** number of connections, **Maximum** number of concurrent connections, **Total** number of connections.

File statistics: the number of files **Transmitted** (uploaded), **Received** (downloaded), and **Deleted**

Transfers in progress: The number of file transfers in progress.

Click **Reset** to zero the counters within the WS_FTP Server. Note that these are the same values you can view and chart in the Windows NT Performance Manager (for more information, see “Monitoring FTP Server Statistics” on page 62).

Active Sessions

The Session Manager window shows all active connections from an FTP client (FTP sessions) or from a WS_FTP Server Manager to the FTP server. For each connection, the Session Manager shows:

Address. The IP address of the FTP client or remote WS_FTP Server Manager.

Host. The FTP host to which the client is connected. If there is only one FTP host on the WS_FTP Server, this column does not appear.

User. The User ID used to connect to the host.

Directory. The last directory accessed during this session.

Last Command. The last FTP command issued by the client or Server Manager.

Idle. The number of seconds the session has been idle. “Idle” means the server has not received a command or data from the client and has not sent a response or data to the client for the reported number of seconds. You can control the amount of idle time allowed for a session by setting a **Timeout** value in the host’s properties.

TA (Transfer Active). Indicates that a data channel is active for a session. If it shows a value of 1, the RETR or STOR command is currently active, which means data is being transferred (retrieved or stored). If it shows a value of 0, the data channel is inactive.

To update the list of active connections, click **Refresh**.

To end a session, select the session’s Address and click **Kill**. The listing automatically refreshes, but may take a few seconds.

Monitoring FTP Server Statistics

You can use the Windows NT Performance Manager to monitor statistics reported by the WS_FTP Server, including the number of concurrent connections, the total number of connections since the server started (or was reset), and the number of files transferred.

To display WS_FTP Server statistics:

- 1 From the Start menu, select **Programs->Administrative Tools (Common)->Performance Monitor**. The Windows NT Performance Monitor appears.
- 2 From File menu, select **New** to create a new chart. See the Performance Monitor's help system for information on using charts.
- 3 From the Edit menu, select **Add to Chart**. The Add to Chart dialog box appears.

In the **Computer** box, select the Windows NT name of the computer on which the WS_FTP server is installed. (The default is the local computer, but you can also connect to another computer on the local network.)

In the **Object** box, select **Ipswitch WS_FTP Server**. The WS_FTP server counters appear in the **Counter** list.

Select a counter and click **Add** to add it to the chart.

Click **Explain** to display a brief description of the counter.

- 4 To save the settings to a file, select **Save Chart Settings** from the File menu.

Reading the Log Files

This section shows a typical log file and describes the types of entries you will see in a log. The log file can be a valuable tool for managing your FTP server.

When you select the log option, a log file (*FSyyyymmnn.log*) is created daily in the FTP server directory. Events for all FTP hosts that are running on the server are logged to this file. The following shows some lines from a log file:

```
0915 12:17:00 (0000005c) 156.21.50.134:2040 connected to
156.21.50.190:21
0915 12:17:00 (0000005c) ftp4test.ipswitch.com S(0)
156.21.50.134 anon-guest@unknown logon success (A1)
0915 12:18:11 (0000005c) ntdoctest.lex.ipswitch.com S(0)
156.21.50.134 anon-guest@unknown logoff R:0 D:0 P:0
0915 12:18:11 (0000005c) 156.21.50.134 connection closed
```

The primary lines in the log file report a specific server event and use the following format:

Example	Description
0915	month (mm) and day (dd)
12:17:00	time of day the event occurred given in hours (hh), minutes (mm), seconds (ss)
(0000005c)	thread ID
ftp4test.ipswitch.com	name of the FTP host on the server.
S	Line type: U=user error; P=protocol error; N=network error; O=operating system error; S=success
156.21.50.134	address of the remote system
anon-guest@unkown	user ID of user logged on
Error	Message if error occurs
RECV	the FTP event

The STOR, STOU, APPE, RECV commands append “(nnnn bytes, nnnn ms)’ to the end of the line to indicate how many bytes were received or transmitted and how many milliseconds it took.

Note

The log file is created daily — you will need to delete old log files to keep the directory from filling up.

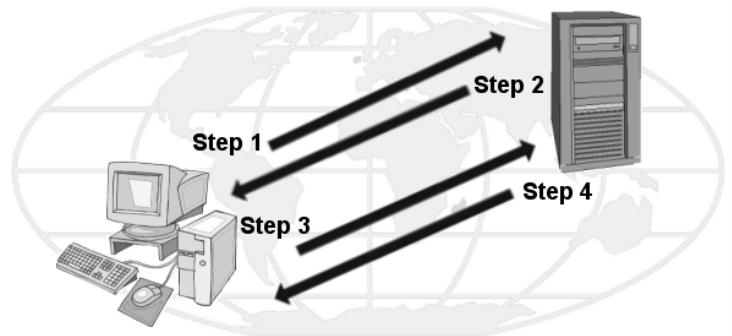
Chapter 5: SSL Configuration

This chapter describes what SSL is and how you can configure WS_FTP Server to allow secure (SSL) connections.

What is SSL?

SSL (Secure Socket Layer) is a protocol for encrypting and decrypting data sent across direct internet connections. When a client makes an SSL connection with a server, all data sent to and from that server is encoded with a complex mathematical algorithm that makes it extremely difficult to decode anything that is intercepted.

The following is a step by step illustration of how SSL works.



- Step 1.** The client makes the initial connection with the server and requests that an SSL connection be made.
- Step 2.** If the server is properly configured, the server will send to the client its certificate and public key.
- Step 3.** The client uses that public key to encrypt a session key and sends the session key to the server. If the server asks for the client's certificate in Step 2, the client must send it at this point.
- Step 4.** If the server is set up to receive certificates, it compares the certificate it received with those listed in its trusted authorities database and either accepts or rejects the connection.

If the connection is rejected, a fail message is sent to the client. If the connection is accepted, or if the server is not set up to receive certificates, it decodes the session key from the client with its own private key and sends a success message back to the client, thereby opening a secure data channel.

The key to understanding how SSL works is in understanding the parts that make SSL itself work. The following is a list of these parts and the roles each plays.

Client. Any FTP program that is able to make an SSL connection.

Certificate. The Certificate file holds the identification information of the client or server. This file is used during connection negotiations to identify the parties involved. In some cases, the client's certificate must be 'signed' by the server's certificate in order to open an SSL connection. Certificate files have the .crt ending.

Session Key. The session key is what both the client and the server use to encrypt data. It is created by the client.

Public Key. The public key is the device with which the client encrypts a session key. It does not exist as a file, but is a byproduct of the creation of a certificate and private key. Data encrypted with a public key can only be decrypted by the private key that made it.

Private Key. The private key decrypts the client's session key that is encrypted by a public key. The private key file has the .key ending. Private keys should NEVER be distributed to anyone.

Certificate Signing Request. A certificate signing request is generated each time a certificate is created. This file is used when you need to 'sign' a certificate. Once the Certificate Signing Request file is signed, a new certificate is made and can be used to replace the unsigned certificate.

How To Get Started

WS_FTP Server can be used without configuring the SSL Utility, but unless you select the **Disable SSL** option in the Host window, anyone will be able to make a secure connection with you. If you do not wish to use the SSL capabilities, you should select the **Disable SSL** option.

If you do want to allow users to make secure connections, follow these directions to set up your server.

- 1 The first step is to replace the default key and certificate installed with WS_FTP by creating a new certificate. Follow the directions for generating a certificate to accomplish this.

Note

The default key and certificate included with WS_FTP Server are exact copies of the files distributed to all users. If you do not generate a new certificate and set of keys, no data encrypted by your server will be completely secure.

- 2 On the Certificate Selection tab, replace the default values with the certificate, private key, and pass phrase generated with the Certificate Creation tab.
- 3 Determine what level of security you want for your server. For the highest security, click the Option tab and select the **Certificates are requested and verified upon connection** option. When this option is selected, the server requires the FTP client to send their certificate when attempting to log on.

If the certificate sent from the client to the server was not signed by a certificate on the host's Trusted Authorities database, the connection will fail. Read the Trusted Authorities section for more information on this process.

For the lowest level of security, you can stop after selecting a certificate on the Certificate Selection tab.

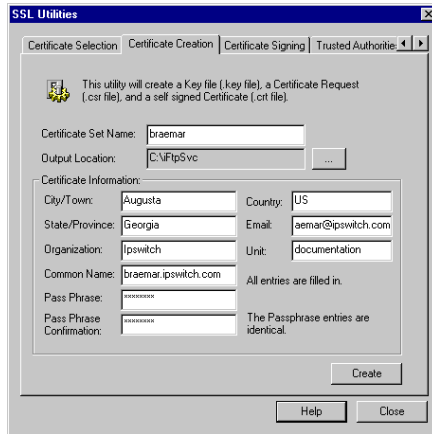
- 4 If you do want to limit which users can make an SSL connection to your server, add the certificate you are going to use to sign user certificates to the Trusted Authorities database for the host they have an account on. Read the Signing a Certificate section for more information on this process.

From here, WS_FTP server is ready to accept SSL connections.

Generating a Certificate

To create an SSL certificate:

- 1 From the File menu, select Configure SSL. The SSL Utilities dialog box appears.
- 2 Click the Certificate Creation tab.



- 3 Enter a name in the **Certificate Set Name** box. This will be the name of the certificate that is generated by WS_FTP Server.
- 4 Click the **Browse (...)** button in the **Output Location** box to select the folder you want the certificate created in.
- 5 Enter information in all of the Certificate Information boxes:
 - City/Town.** City or town where you are located. (Ex. Augusta)
 - State/Province.** State or Province where you are located. (Ex. Georgia)
 - Organization.** Company or individual user name.
 - Common Name.** This can be either the name of the person creating the certificate or the fully qualified domain name of the server associated with the host.
 - Pass Phrase.** Pass phrase that is to be used to encrypt the private key. It is important to remember this pass phrase. The pass phrase can be any combination of words, symbols, spaces, or numbers.

Pass Phrase Confirmation. Re-enter the same pass phrase as above.

Country. The country you are in. This must be a valid two letter country code. (Ex. US)

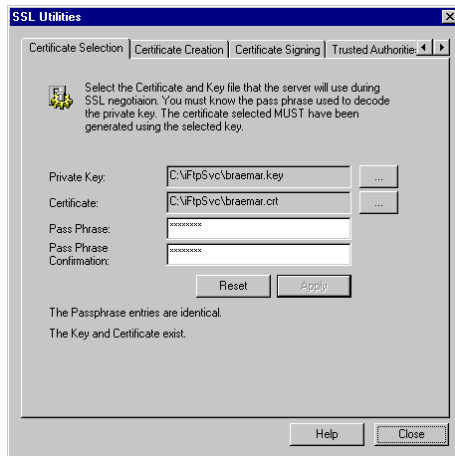
Email. E-mail address of the person the certificate belongs to.

Unit. Name of organizational unit. (Ex. Research and Development)

- 6 After all of the boxes are filled in correctly, click **Create** to generate the keys, certificate, and certificate signing request. If all of the boxes are not filled in, you can not create the certificate.

Selecting a Certificate

The Certificate Selection tab is used to choose which private key and certificate you want to use during SSL connection negotiations. If a new certificate has not been created, follow the directions for “Generating a Certificate” on page 68.



To select an SSL Certificate:

- 1 Click the **Browse (...)** button next to the **Private Key** box to select the private key you want to use during SSL negotiation.

- 2 Click the **Browse (...)** button next to the **Certificate box** to select the certificate you want to use during SSL negotiation. The certificate you use must have been created using the key you selected for the **Private Key** box.
- 3 Enter the pass phrase associated with that certificate in both the **Pass Phrase** and the **Pass Phrase Confirmation** boxes. A pass phrase can be any combination of words, symbols, or numbers. It is case sensitive and must be written exactly the same way each time it is used.

Without the correct pass phrase in both boxes, the certificate and private key cannot be verified and the selection cannot be saved.

- 4 Click **Apply** to save your entries.

Clicking the **Reset** button erases what you have done since the last time new settings were applied.

Signing Requirement Option

WS_FTP Server provides you with a signing requirement option for SSL connections.

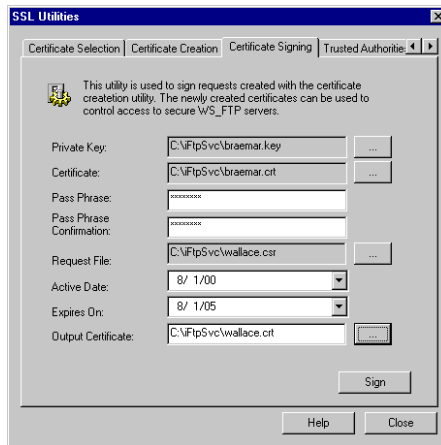


Certificates are requested and verified upon connection. When this option is selected, the server asks for a certificate from the user attempting to make a connection. That server then tries to verify that server against the certificates listed for that host on the Trusted Authorities tab. If the certificate is not listed there, for that host, then the SSL connection will fail.

Signing a Certificate

The Certificate Signing tab is used to sign requests with the private key and certificate you define. When a user wants to make an SSL connection with a host they have an account on, the user creates a certificate of their own and sends the generated request file to the server administrator. This is usually done through e-mail. Once the administrator has the file, they can sign the request and create a new certificate that can be sent back to the user. The user then uses that new certificate to make an SSL connection with the host.

If the **Certificates are requested and verified upon connection** option found on the SSL Option tab is selected, the certificate the administrator uses to sign the certificate signing request must be listed in the Trusted Authorities tab for that host. If not, any SSL connection that tries to use that certificate will fail.



To sign a certificate:

- 1 In the **Private Key** box, select the private key you want to use to sign the request by clicking on the **Browse (...)** button and selecting the file.
- 2 In the **Certificate** box, select the certificate associated with that private key.

- 3 Enter the pass phrase associated with that private key/certificate in both the **Pass Phrase** box and the **Pass Phrase Confirmation** box.
- 4 In the **Request File** box, select the request file you want to sign by clicking on the Browse (...) button and selecting the file.
- 5 In the **Active Date** box, enter the date the certificate is activated, or use the pull-down button to select the date from a calendar.
- 6 In the **Expires On** box, enter the date the certificate expires on, or use the pull-down button to select the date from a calendar.
- 7 In the **Output Certificate** box, enter the file name and complete path of the certificate that is to be generated by signing the request. You can click the **Browse (...)** button to enter the name and select the folder you want to create the file in.

Note

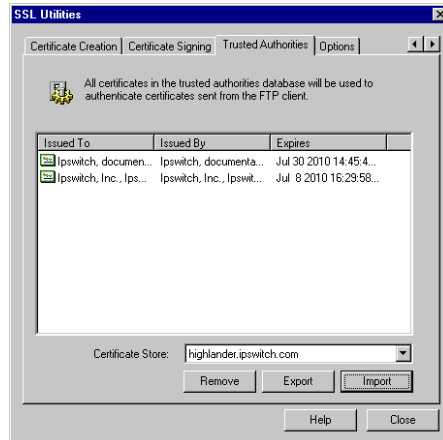
Usually, the output certificate file uses the same name as the request file.

- 8 Click the **Sign** button to sign the request and create the new certificate.

The certificate that was created should now be sent back to the user. If the certificate file used to sign the request is not listed in the Trusted Authorities tab for that host, you should add it now.

Trusted Authorities

The Trusted Authorities tab stores a list of certificate names that are recognized by the host you identify in the Certificate Store box (In WS_FTP Pro, the Certificate Store box does not appear). If you use the Certificates are requested and verified upon connection option found on the SSL Option tab, any user that tries to make an SSL connection must have their certificate signed by a certificate that has been added to this host's database, or have the certificate itself in the database.



Certificate Display

Issued To. Who the certificate was issued to.

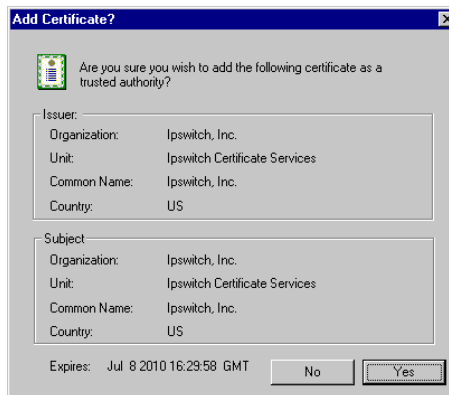
Issued By. Who the certificate was signed by.

Expires. Date on which the certificate expires.

Adding a Certificate

To add a certificate to the database:

- 1 Click the **Import** button and select the path and file name for the certificate. The Add Certificate? dialog box appears.



- 2 Review the information and click **Yes** to add the certificate to the database.

Exporting a Certificate

To export a certificate from the Trusted Authorities database:

- 1 Select the certificate you want to copy out of your database.
- 2 Click the **Export** button.
- 3 Select the folder you want to copy the certificate to and enter the name you want to save the certificate file as.
- 4 Click **OK**.

Removing a Certificate

To remove a certificate:

- 1 Select the certificate to be removed.
- 2 Click **Remove**.
- 3 A warning appears advising you to export the certificate before you remove it. Removing the certificate deletes the certificate file.
- 4 Click **OK** to remove the certificate.

Appendix A: Highlights of RFC 959

This appendix includes some highlights of RFC 959, “File Transfer Protocol.” This information is provided here for those advanced users who want to know more about how FTP works. It will also assist those wishing to interpret the messages at the bottom of the WS_FTP Pro Classic main window or in the log window. Topics included here are:

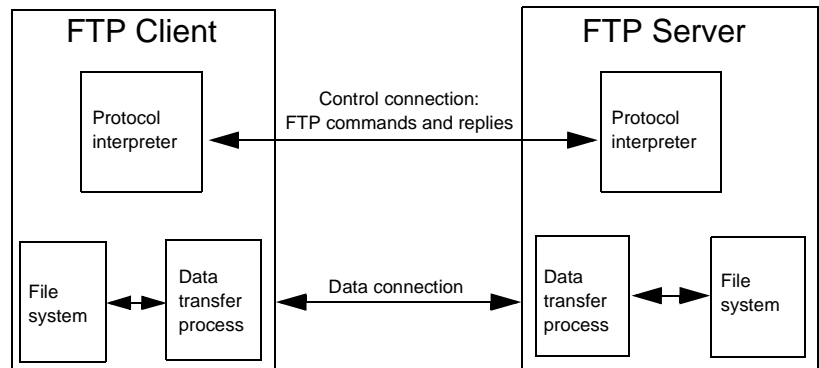
- Basics
- FTP Commands
- FTP Replies (three-digit “error codes”)

For more detailed information, see the RFC itself.

Basics

FTP (File Transfer Protocol) is a specification for how files can be transferred over the Internet. FTP is a client-server protocol in which FTP client software on one system communicates with FTP server software on another. The communication between the FTP client and server is an exchange of commands and replies which are transmitted over a “control connection” between the two systems; this control connection follows the Telnet model.

Files are transferred between the client and server over a second connection, a full duplex connection known as the “data connection.” This connection is between the client’s “data transfer process” and the server’s data transfer process (or between two servers’ data transfer processes).



Both the client and the server have a protocol interpreter. The protocol interpreters receive commands or replies, send commands or replies, and govern the data connection. The server's protocol interpreter listens for a connection from a client's protocol interpreter.

In an "active" transfer, the FTP server's data transfer process initiates, or establishes, the data connection to the FTP client, setting up the parameters for data transfer and storage.

In a "passive" transfer, the server's data transfer process is placed in a passive state to *listen for*, rather than *initiate*, a connection to the data port. In this case, the FTP client initiates the data connection.

FTP Commands

The standard commands that an FTP client (such as WS_FTP Pro) issues to an FTP server are listed here with a brief explanation that has been adapted from RFC 959. The command syntax is presented using BNF (Backus-Naur Form) notation where applicable.

FTP commands may be in any order except that a "rename from" command must be followed by a "rename to" command and the REST (restart) command must be followed by the interrupted service command (e.g., STOR or RETR).

ABOR (ABORT)

ABOR <CRLF>

This command tells the server to abort the previous FTP service command and any associated transfer of data.

ACCT (ACCOUNT)

ACCT <SP> <account-information> <CRLF>

The argument field is a Telnet string identifying the user's account. The command is not necessarily related to the USER command, as some sites may require an account for login and others only for specific access, such as storing files.

ALLO (ALLOCATE)

ALLO <SP> <decimal-integer> [<SP> R <SP>
<decimal-integer>] <CRLF>

This command is required by some servers to reserve sufficient storage to accommodate the file to be transferred.

APPE (APPEND) (with create)

```
APPE <SP> <pathname> <CRLF>
```

This command causes the server's data transfer process to accept the data transferred and to store the data in a file at the server site. If the file specified in *pathname* exists at the server site, then the data is appended to that file; otherwise the file specified in *pathname* is created at the server site.

CDUP (CHANGE TO PARENT DIRECTORY)

```
CDUP <CRLF>
```

This command is a special case of CWD which allows the transfer of directory trees between operating systems having different syntaxes for naming the parent directory.

CWD (CHANGE WORKING DIRECTORY)

```
CWD <SP> <pathname> <CRLF>
```

This command allows the user to work with a different directory or dataset without altering his login or account information.

DELE (DELETE)

```
DELE <SP> <pathname> <CRLF>
```

This command causes the file specified in *pathname* to be deleted at the server site.

FEAT

```
FEAT <CRLF>
```

This command causes the FTP server to list all new FTP features that the server supports beyond those described in RFC 959. A typical example reply to the FEAT command might be a multi-line reply of the form:

```
C> FEAT
S> 211-Extensions supported
S> SIZE
S> MDTM
S> MLST size*;type*;perm*;create*;modify*;
S> LANG EN*
S> REST STREAM
S> TVFS
S> UTF8
S> 211 end
```

HELP (HELP)

```
HELP [<SP> <string>] <CRLF>
```

This command causes the server to send a list of supported commands and other helpful information.

LIST (LIST)

```
LIST [<SP> <pathname>] <CRLF>
```

This command causes a list of file names and file details to be sent from the FTP site to WS_FTP Pro.

MDTM (MODIFICATION TIME)

```
MDTM <SP> <pathname> <CRLF>
```

This command can be used to determine when a file in the server NVFS was last modified.

MKD (MAKE DIRECTORY)

```
MKD <SP> <pathname> <CRLF>
```

This command causes the directory specified in *pathname* to be created as a directory (if *pathname* is absolute) or as a subdirectory of the current working directory (if *pathname* is relative).

MLSD

```
MLSD [<SP> <pathname>] <CRLF>
```

If WS_FTP Pro detects that the server is an MLSD server, this command is sent to the server instead of the LIST command.

MLST

```
MLST [<SP> <pathname>] <CRLF>
```

This command causes the server to provide data about the single object named, whether a file or directory.

MODE (TRANSFER MODE)

```
MODE <SP> <mode-code> <CRLF>
```

The argument is a single Telnet character code specifying the data transfer mode. The following codes are assigned for transfer modes: S - Stream, B - Block, C - Compressed. The default transfer mode is Stream.

Note

This “transfer mode” is not equivalent to the “transfer mode” of the WS_FTP Pro user interface. The “transfer mode” referred to in WS_FTP Pro and its documentation is handled by the **TYPE** command.

NLST (NAME LIST)

NLST [<SP> <pathname>] <CRLF>

This command causes a list of file names (with no other information) to be sent from the FTP site to WS_FTP Pro.

NOOP (NOOP)

NOOP <CRLF>

This command does not affect any parameters or previously entered commands. It specifies no action other than that the server send an OK reply.

OPTS (OPTIONS)

OPTS <SP> <parameter> <CRLF>

This command allows an FTP client to define a parameter that will be used by a subsequent command.

PASS (PASSWORD)

PASS <SP> <password> <CRLF>

The argument field is a Telnet string specifying the user's *password*. This command must be immediately preceded by the user name command, and, for some sites, completes the user's identification for access control.

PASV (PASSIVE)

PASV <CRLF>

This command requests the server's data transfer process to "listen" on a data port (which is not its default data port) and to wait for a connection rather than initiate one upon receipt of a transfer command. The response to this command includes the host and port address this server is listening on.

PORT (DATA PORT)

PORT <SP> <host-port> <CRLF>

This specifies an alternate data port. There are defaults for both the client and server data ports, and under normal circumstances this command and its reply are not needed.

PWD (PRINT WORKING DIRECTORY)

PWD <CRLF>

This command causes the name of the current working directory to be returned in the reply.

QUIT (LOGOUT)

QUIT <CRLF>

This command terminates a USER and, if file transfer is not in progress, closes the control connection. If file transfer is in progress, the connection will remain open for result response and the server will then close it.

QUOTE

QUOTE <string> <CRLF>

The QUOTE command lets you enter any *standard* FTP command. WS_FTP Pro sends it to the FTP site, unedited; it is up to you to determine the command syntax depending on the FTP site you are connected to.

REIN (REINITIALIZE)

REIN <CRLF>

This command terminates a USER, flushing all I/O and account information, except to allow any transfer in progress to be completed. A USER command may be expected to follow.

REST (RESTART)

REST <SP> <marker> <CRLF>

The argument field represents the server marker at which file transfer is to be restarted. This command does not *cause* file transfer but skips over the file to the specified data checkpoint. This command shall be immediately followed by the appropriate FTP service command which causes file transfer to resume.

RETR (RETRIEVE)

RETR <SP> <pathname> <CRLF>

This command causes the server to transfer a copy of the file specified in *pathname* to the client. The status and contents of the file at the server site are unaffected.

RMD (REMOVE DIRECTORY)

RMD <SP> <pathname> <CRLF>

This command causes the directory specified in *pathname* to be removed as a directory (if *pathname* is absolute) or as a subdirectory of the current working directory (if *pathname* is relative).

RNFR (RENAME FROM)

RNFR <SP> <pathname> <CRLF>

This command specifies the old *pathname* of the file which is to be renamed. This command must be immediately followed by a “rename to” command specifying the new file pathname.

RNTO (RENAME TO)

RNTO <SP> <pathname> <CRLF>

This command specifies the new *pathname* of the file specified in the immediately preceding “rename from” command. Together the two commands cause a file to be renamed.

SITE (SITE PARAMETERS)

SITE <SP> <string> <CRLF>

This allows you to enter a command that is *specific to the current FTP site*. WS_FTP Pro prefixes your entry with the word SITE. WS_FTP Pro sends it to the FTP site, unedited; it is up to you to determine the command syntax depending on the FTP site you are connected to.

SITE CPWD

SITE CPWD <SP> <string> <CRLF>

This is a special command you can enter using WS_FTP Pro when the FTP server is a WS_FTP Server from Ipswitch. It changes the user’s password.

SIZE (SIZE OF FILE)

SIZE <SP> <pathname> <CRLF>

This command is used to obtain the transfer size of a file from the server: that is, the exact number of octets (8 bit bytes) which would be transmitted over the data connection should that file be transmitted. This value will change depending on the current STRUcture, MODE and TYPE of the data.

SMNT (STRUCTURE MOUNT)

SMNT <SP> <pathname> <CRLF>

This command allows the user to mount a different file system data structure without altering his login or accounting information.

STAT (STATUS)

STAT [<SP> <pathname>] <CRLF>

This command causes a status response to be sent over the control connection in the form of a reply.

STOR (STORE)

STOR <SP> <pathname> <CRLF>

This command causes the FTP server to accept the data transferred via the data connection and to store the data as a file at the FTP server. If the file specified in *pathname* exists at the server site, then its contents shall be replaced by the data being transferred. A new file is created at the FTP server if the file specified in *pathname* does not already exist.

STOU (STORE UNIQUE)

STOU <CRLF>

This command behaves like STOR except that the resultant file is to be created in the current directory under a name unique to that directory. The “250 Transfer Started” response must include the name generated.

STRU (FILE STRUCTURE)

STRU <SP> <structure-code> <CRLF>

The argument is a single Telnet character code specifying the file structure described in RFC 959. The following codes are assigned for structure: F - File (no record structure) R - Record structure P - Page structure. The default structure is File.

SYST (SYSTEM)

SYST <CRLF>

This command is used to find out the operating system of the server.

TYPE (REPRESENTATION TYPE)

TYPE <SP> <type-code> <CRLF>

The argument specifies the file type. The following codes are assigned:

A = ASCII (text files)

N = Non-print (files that have no vertical format controls such as carriage returns and line feeds)

T = Telnet format effectors (files that have ASCII or EBCDIC vertical format controls)

E = EBCDIC (files being transferred between systems that use EBCDIC for internal character representation)

C = Carriage Control (ASA) (files that contain ASA [FORTRAN] vertical format controls)

I = Image (binary files)

L = Local byte size (files that need to be transferred using specific non-standard size bytes)

The default representation type is ASCII Non-print.

USER (USER NAME)

```
USER <SP> <username> <CRLF>
```

The argument field is a Telnet string identifying the user. The user identification is that which is required by the server for access to its file system.

FTP Replies

In the protocol conversation between an FTP client (such as WS_FTP Pro) and an FTP server, at least one server reply is sent to the FTP client in response to an FTP command. A reply consists of a three-digit code, followed by one line of text, and terminated by the Telnet end-of-line code.

Positive Preliminary Replies

These types of replies indicate that the requested action was taken and that another reply is to follow.

- 110** Restart marker reply.
- 120** Service ready in nnn minutes.
- 125** Data connection already open; transfer starting.
- 150** File status okay; about to open data connection.

Positive Completion Replies

These type of replies indicate that the requested action was taken and that the server is awaiting another command.

- 200** Command okay.
- 202** Command not implemented, superfluous at this site.
- 211** System status, or system help reply.
- 212** Directory status.
- 213** File status.
- 214** Help message on how to use the server or the meaning of a particular non-standard command. This reply is useful only to the human user.
- 215** NAME system type. Where NAME is an official system name.

- 220 Service ready for new user.
- 221 Service closing control connection. Logged out if appropriate.
- 225 Data connection open; no transfer in progress.
- 226 Closing data connection. Requested file action successful (for example, file transfer or file abort).
- 227 Entering Passive Mode (h1,h2,h3,h4,p1,p2).
- 230 User logged in, proceed.
- 250 Requested file action okay, completed.
- 257 "PATHNAME" created.

Positive Intermediate Replies

These types of replies indicate that the requested action was taken and that the server is awaiting further information to complete the request.

- 331 User name okay, need password.
- 332 Need account for login.
- 350 Requested file action pending further information.

Transient Negative Completion Replies

These types of replies indicate that the command was not accepted; the requested action was not taken. However, the error is temporary and the action may be requested again.

- 421 Service not available, closing control connection. This may be a reply to any command if the service knows it must shut down.
- 425 Can't open data connection.
- 426 Connection closed; transfer aborted.
- 450 Requested file action not taken. File unavailable (e.g., file busy).
- 451 Requested action aborted: local error in processing.
- 452 Requested action not taken. Insufficient storage space in system.

Permanent Negative Completion Replies

These types of replies indicate that the command was not accepted; the requested action was not taken. The FTP client is "discouraged" from repeating the same exact request.

- 500** Syntax error, command unrecognized. This may include errors such as command line too long.
- 501** Syntax error in parameters or arguments.
- 502** Command not implemented.
- 503** Bad sequence of commands.
- 504** Command not implemented for that parameter.
- 530** Not logged in.
- 532** Need account for storing files.
- 550** Requested action not taken. File unavailable; e.g., file not found, no access.
- 551** Requested action aborted: page type unknown.
- 552** Requested file action aborted. Exceeded storage allocation for current directory or dataset.
- 553** Requested action not taken. File name not allowed.

Index

Numerics

550 reply 85

A

ABOR (command) 76
access control 25
ACCT (command) 76
active transfers 76
Add User utility 48
adding

- user accounts 42
- user groups 51
- virtual folders 53

administrator permissions 47
aliases 28
ALLO (command) 76
anonymous logons 2
anonymous users

- disabling access 22
- enabling access 22
- permissions 22
- setting maximum 21

APPE (command) 77
ASA (FORTRAN) 82
ASCII files 82

B

banner messages 23
binary files 82

C

CDUP (command) 77
Certificate 66
Certificate Signing Request 66

changing passwords 51
Client 66
configuring

- FTP hosts 13
- FTP server 11

connections

- setting timeouts 20

control connection 75
CPWD command 51
CWD (command) 77

D

data connection 75, 76
data transfer process 75
DELE (command) 77
deleting

- FTP hosts 31
- user groups 53
- users 48
- virtual folders 58

directories

- initial 3
- logon 3

disk space

- setting user quotas 46

domain name server 14
domain name servers

- setting FTP alias 28

E

EBCDIC 82
encryption 5
Event Commands 32
exit messages 23
external user database 17

- configuring 17

F

FEAT (command) 77

files

- granting permissions 55
- hiding 23
- setting user quotas 46

files installed 7
folders 3

- deleting virtual folders 58
- disable access to public 46
- granting permissions 55
- hiding 23
- messages 25
- renaming virtual folders 58
- see also virtual folders

FTP 1
FTP (File Transfer Protocol) 2, 59

- basics of RFC 959 75
- client 75
- server 75

FTP clients

- password change 50
- WS_FTP Pro 4, 51

FTP hosts

- adding additional 28
- adding first host 14
- deleting 31
- options 20, 28
- renaming 31
- setting a DNS alias 28
- setting maximum users 21
- setting timeout 20
- setting up 13
- with IP address 29
- without IP address 29

FTP protocol commands 76
FTP protocol replies 83
FTP Server

- log files 63

FTP server

- configuring 11
- managing remotely 59
- monitoring performance

- 62
- setting access 25
- statistics 61, 63
- using local time 23

FTP sessions 62

FTP sites

- see FTP hosts

G

groups

- deleting 53

H

HELP (command) 78

hidden files and folders 23

host administrator 47

I

installing

- files installed 7

installing the server 7

IP addresses

- denying access 25
- granting access 25

K

Keys

- private 66
- public 66
- session 66

L

LIST (command) 78

log files

- reading 63

logon directories 3

logons

- anonymous users 22
- disabling 45
- setting options 44

M

MDTM (command) 78

messages

- banner, welcome, exit 23
- change directory 25
- for files and folders 25

MKD (command) 78

MLSD (command) 78

MLST (command) 78

MODE (command) 78

N

non-print files 82

NOOP (command) 79

O

OPTS (command) 79

P

PASS (command) 79

passive transfers 76

passwords

- changing from FTP client 50
- disabling change 46
- encryption 5

PASV (command) 79

performance monitoring 62

permissions 3, 56

- anonymous users 22
- for folders 53
- granting for folders 55
- how they work 41
- notes 56

- options 56

PORT (command) 79

Private Key 66

protocol interpreter 76

protocol stack

- see TCP/IP stack

public directories, setting

- access 46

public folders 3, 42

- disabling access 45

PWD (command) 79

Q

QUIT (command) 80

QUOTE (command) 80

R

REIN (command) 80

release notes 8

remote management 59

removing the server 7

renaming

- FTP hosts 31
- users 48
- virtual folders 58

Request for Comments

- see RFCs

REST command 76

RETR (command) 76, 80

RFC 959 75

RFCs

- where to find 1

RMD (command) 80

RNFR (command) 81

S

security 5

Server Manager

- see WS_FTP Server

- Manager
 - Session Key 66
 - Session Manager 61
 - sessions
 - viewing active 61, 62
 - sign-off messages 23
 - sign-on messages 23
 - SITE (command) 81
 - Site Commands 34
 - site commands
 - adding a site command 34
 - modifying 37
 - permissions 38
 - SITE CPWD (command) 81
 - SITE CPWD command 51
 - SIZE (command) 81
 - SMNT (command) 81
 - SSL
 - generating a certificate 68
 - selecting a certificate 69
 - signing a certificate 71
 - trusted authorities 72
 - adding a certificate 73
 - exporting a certificate 74
 - removing a certificate 74
 - SSL (definition) 65
 - certificate 66
 - certificate signing request 66
 - client 66
 - private key 66
 - public key 66
 - session key 66
 - STAT (command) 81
 - statistics
 - FTP server 61, 63
 - log files 63
 - STOR (command) 76, 82
 - STOU (command) 82
 - STRU (command) 82
 - SYST (command) 82
 - system administrator 47
 - system requirements 7
- T**
- TCP/IP stack 7
 - Telnet 75, 82
 - time
 - using local time 23
 - timeouts 20
 - transfer modes 78
 - TYPE (command) 78, 82
- U**
- USER (command) 83
 - user accounts 2
 - adding 42
 - how they work 41
 - user accounts, disabling 46
 - user authorization 15
 - user databases
 - external user database 15
 - IMail Server 16
 - Windows NT 15
 - user groups 3
 - adding 51
 - adding and removing users 52
 - deleting 53
 - user icons 47
 - users
 - adding groups 51
 - adding with command line 48
 - administrator permissions 47
 - changing passwords 50
 - deleting 48
 - directories 45
 - disabling logon 45
 - disabling password change 46
 - Host Administrator 47
 - passwords 45
 - renaming 48
 - setting disk quotas 46
 - setting file quotas 46
 - setting logon options 44
 - setting max anonymous 21
 - setting max concurrent 21
 - setting maximum 21
 - setting options 44
 - System Administrator 47
- V**
- viewing active sessions 61
 - virtual folders 42
 - adding 54
 - granting permissions 55
 - setting up 53
 - virtual hosts
 - see FTP hosts
- W**
- welcome messages 23
 - Windows NT
 - Performance Monitor 62
 - WS_FTP Pro client 4
 - WS_FTP Server 81
 - configuring 11
 - how it works 2
 - installing 7
 - major features 3
 - removing 7
 - security 5
 - session manager 61
 - setting access 25
 - system requirements 7
 - what is? 1
 - WS_FTP Server Manager 5
 - using remotely 59

