WS_FTP Server

User Guide

IPSWITCH

File Transfer

CHAPTER 1 WS_FTP Server Overview

CHAPTER 2 Learning about WS_FTP Server Manager

CHAPTER 3 Configuring and Managing WS_FTP Server

CHAPTER 4 Configuring Hosts

CHAPTER 5 Configuring Listeners

CHAPTER 6 Managing User Accounts

CHAPTER 7 Managing User Groups

CHAPTER 8 Managing Folders and Files

CHAPTER 9 Using Rules and Notifications

CHAPTER 10 Using SSL

CHAPTER 11 Using SSH

CHAPTER 12 Using SCP2

CHAPTER 13 Managing Connections in Real-time

CHAPTER 14 Protecting against IP connection attacks

CHAPTER 15 Maintaining the Server

CHAPTER 16 Server Modules

APPENDIX A RFC 959 Highlights

About WS_FTP Server Web Transfer Module

Index

CHAPTER 1

WS_FTP Server Overview

In This Chapter

What is WS_FTP Server?

Ipswitch WS_FTP® Server is a highly secure, fully featured and easy-to-administer file transfer server for Microsoft Windows® systems. WS_FTP Server lets you create a host that makes files and folders on your server available to other people. Users can connect (via the Internet or a local area network) to your host, list folders and files, and (depending on permissions) download and upload data. Administrators can control access to data and files with granular permissions by folder, user, and group. Administrators can also create multiple hosts that function as completely distinct sites.

WS_FTP Server is proven and reliable. It is used by administrators globally to support millions of end users and enable the transfer of billions of files.

WS_FTP Server complies with the current Internet standards for FTP and SSL protocols. Users can connect to the server and transfer files by using an FTP client that complies with these protocols, such as Ipswitch WS_FTP Home or Ipswitch WS_FTP Professional.

WS_FTP Server with SSH also includes support for SFTP transfers over a secure SSH2 connection.

Our product offerings are described in WS_FTP Server product family.

System requirements for WS_FTP Server

WS_FTP Server requires:

- An Intel Pentium® 4, 1 GHz or higher (or an equivalent processor)

- 512 MB RAM minimum
- 250 MB of drive space
- NTFS formatted drive
- TCP/IP enabled network interface card (NIC)
- Microsoft® Windows® Server 2003 Service Pack 2 or later, Windows XP Professional Service Pack 3 or later

> ✓ If you will install the WS_FTP Server Web Transfer Module, you will need to also install Microsoft .NET 3.0. To install .NET 3.0, you need to have Windows® Server 2003 Service Pack 1 or later, or Windows XP Professional Service Pack 2 or later.

- Microsoft .NET Framework 2.0
- Microsoft Data Access Component (MDAC) 2.80 or later
- Microsoft Windows Installer 3.1 or later
- *Microsoft Windows Script Host 5.6 or later* (http://www.ipswitch.com/wsh56)
- Broadband connection to the Internet (recommended)
- During installation, you can select to use Microsoft Internet Information Services (IIS) as your web server (instead of WS_FTP's Web Server). If you choose this option, you need to have Microsoft Internet Information Services (IIS) 5.0 or later installed on your computer.
- During installation, you can select to use Microsoft SQL Server as your database for configuration data. if you choose this option, you must use one of the following versions: Microsoft SQL Server 2000, Microsoft SQL Server 2005, or Microsoft SQL Server 2005 Express.

Ipswitch Notification Server requires:

All requirements for WS_FTP Server (above), plus:

- Broadband or dial-up connection to the Internet (required for email notifications outside of the local area network)
- Modem and phone line (required for pager and SMS notifications)

WS_FTP Server Manager requires:

- Microsoft Internet Explorer 6 or later, Mozilla Firefox 2.0 or later, Netscape Navigator (or other Web browser that is CSS2 and HTML 4.01 compliant)
- Enabled Javascript support in the Web browser
- Enabled Cookie support in the Web browser

Installing WS_FTP Server on Windows 2008 Server

The WS_FTP Server installer automatically activates certain components in your Windows 2008 installation. This is necessary because after installation, Windows 2008 does not turn on non-core operating system components. However, before installing WS_FTP Server, you should be sure that these changes conform to your organization's security policies.

When you install WS_FTP Server, the install activates the following 2008 Server roles:

- ISAPI Extensions
- Windows Authentication
- ASP

> **Note**: If you are installing the WS_FTP Server Web Transfer Module on Windows 2008, there are additional components activated. See "System requirements for WS_FTP Server Web Transfer Module" below.

How FTP works

FTP is based on the client-server model of communication between computers: one computer runs a server program that makes information available to other computers. The other computers run client programs that request information and receive replies from the server.

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

A client-server session establishes two connections: a control channel that stays open for the entire session and a data channel that opens and closes to transfer data such as folder listings and files to or from the server as requested by the client. Normally, the control channel occurs on port 21, but WS_FTP Server can be configured to accept connections on any port.

The server runs continuously in the background and listens on a specified port (the standard port is 21) for a connection request from a client. When a client requests a connection, the server verifies the username and password and, if valid, listens to the control channel for the next command.

After a user logs on, his or her access to the host's folders and files is determined by permissions assigned to folders.

> **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 *the IEFT Web site* (http://www.ietf.org/).

How SSH works

SSH (Secure Shell) is a protocol for encrypting and securing various kinds of data transfers over a network or the Internet. SSH works by opening a secure channel between the SSH server and an authenticated user's computer. Many kinds of data may be sent or retrieved through this channel.

SSH can be understood as a large pipe: its purpose is to carry whatever is passed through it from one place to another without letting anything leak in or out.

WS_FTP Server with SSH uses SFTP (Secure File Transfer Protocol) over SSH2 to transfer files.

SFTP operates nearly identically to FTP, but all transmissions are secured under the SSH protocol.

Activating WS_FTP Server for new or upgraded licenses

There are four ways you can make a WS_FTP Server installation active:

- If you installed WS_FTP Server using an installation application downloaded from a link in a purchase confirmation email, then the program will be fully functional immediately after installation. No further action will need to be taken.
- If you downloaded the installation application from another source, when you run the installation, it will automatically ask you for your license serial number and attempt to activate.
- If the WS_FTP Server license is not activated during installation, or if you are upgrading from a previous WS_FTP Server version, you can manually activate WS_FTP Server (see below).
- If for some reason you cannot activate your license via Internet connection, you can opt for an offline activation. To force offline activation, on the Activation screen, clear the check mark for **Use active Internet connection**. You will then need to go to www.myipswitch.com, click on **Offline Activation**, and follow the instructions displayed.

To manually activate the license on an existing installation:

Note: Before you start the manual activation process, make sure that you have your product serial number, MyIpswitch account name, and password available for use during activation.

- Click **Start > Programs > Ipswitch WS_FTP Server > Activate or Refresh WS_FTP Server License**.

- or -

- If you run the WS_FTP Server installation, near the end, it will display a License dialog. Enter your serial number and click **Activate** to start the license activation process.

Follow the on-screen instructions, entering your product serial number, MyIpswitch account name, and password.

Note: When the activation is complete, a confirmation page indicates the license has been activated. If the activation does not complete successfully, you may be behind a proxy or firewall that is blocking the activation request. In this case, click the Offline button, then follow the onscreen instructions.

For more help and information about licensing, go to the MyIpswitch (www.myipswitch.com) licensing portal.

Sending feedback

We value your opinions on our products and welcome your feedback.

- To provide feedback on existing features, suggest new features or enhancements or suggest ways to make our products easier to use, fill out *the online product feedback form* (http://www.ipswitch.com/feedback).
- To provide feedback on this documentation, send email to wsftpserverauthor@alpha.ipswitch.com.

CHAPTER 2

Learning about WS_FTP Server Manager

In This Chapter

Understanding the server architecture

There are two primary components to WS_FTP Server.

- **Listener**. A listener acts as the gateway to one or more hosts. A listener accepts connections on a specific IP address and port over a specific protocol (either FTP or SSH), then routes the connection to the appropriate host.
  There are two types of listeners:
  - **FTP**. FTP listeners provide access to hosts via the FTP protocol. FTP listeners can be configured to provide simple FTP access, both FTP and SSL access, or SSL access only (Implicit SSL).
  - **SSH**. SSH listeners provide access to hosts using the SFTP protocol over SSH2.

> **Note:** When WS_FTP Server is installed, three listeners are created by default: one listens on all available IP addresses on port 21 for FTP connections; one listens on port 990 for Implicit SSL connections; and one listens on all available IP addresses on port 22 for SSH connections.

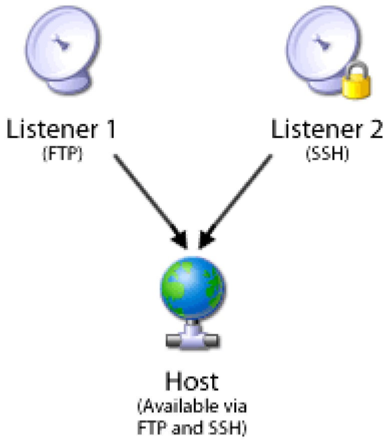
  For more information about listeners, see *Setting Up Listeners* (on page 55). For more information about SSL, see *Configuring SSL for a Host* (on page 58).

- **Host**. A host is the portion of the server that authenticates users and grants them access to the files and folders stored on the host. In addition to users and permissions, virtual folders, rules, notifications and SITE commands are defined and configured as part of the host. For more information about hosts, see *Setting Up Hosts* (on page 21).

Understanding the relationship between listeners and hosts

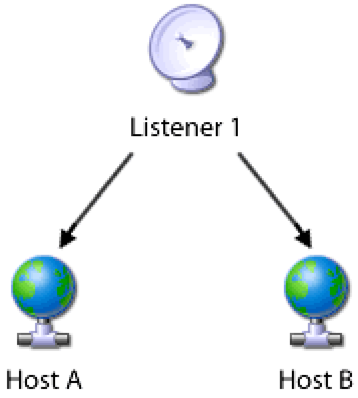
Listeners and hosts can relate to each other in multiple ways. Multiple listeners can point to a single host, or a single listener can point to multiple hosts. The following diagrams demonstrate various ways that listeners and hosts can relate to each other.

Multiple listeners accepting connections for one host



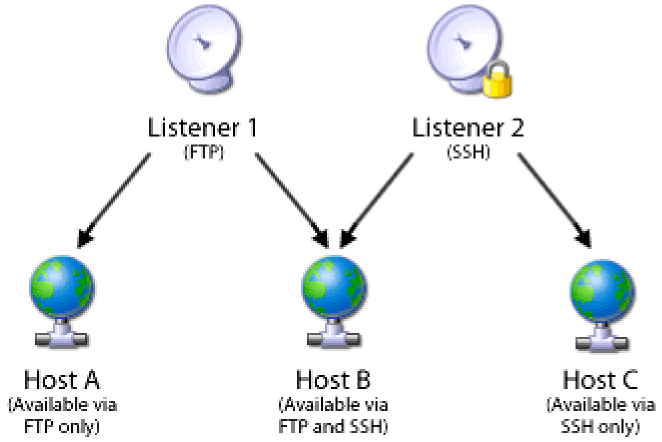
One listener accepting connections for multiple hosts

In this configuration, users are required to authenticate using both their user and host names.



Multiple listeners accepting connections for multiple hosts.

In this configuration, users are required to authenticate using both their user and host names.



Accessing the WS_FTP Server Manager

Ipswitch WS_FTP Server Manager is the web-based program used to manage the server and any hosts created on it. When you install the server, the server manager is also installed.

To access WS_FTP Server Manager:

1 Using one of the methods below, open the WS_FTP Server Manager.

- Double click the WS_FTP Server Manager icon on the desktop.
- On a computer that has Internet or network access to the server, open a web browser and enter `http://yourhostname.domainname.com/WSFTPSVR/`, replacing `yourhostname.domainname.com` with the host name you specified during installation.

The Ipswitch Web Admin login page appears.

2 In **Username**, enter the username of a system or host administrator. If you want to use a system or host administrator on a host other than the default host, enter the username, host separator and host name, such as `username@hostname`.

3 In **Password**, enter the password for the user you entered.

4 Click **Log In**.

Managing WS_FTP Server remotely

You can manage WS_FTP Server remotely by accessing the Web-based WS_FTP Server Manager from any computer with network or Internet access to the server. WS_FTP Server Manager fully supports Microsoft Internet Explorer, Mozilla Firefox, or Netscape Navigator Web browsers, but other Web browsers that are CSS2 and HTML 4.01 compliant may work as well.

To access the WS_FTP Server Manager remotely:

1 Enter the fully qualified domain name of the server in the address bar of your Web browser. The address should follow this format: `http://yourhostname.domainname.com/WSFTPSVR/`.

> **Note:** If you specified an alternative virtual folder under which to install the web files, enter that folder name in place of WSFTPSVR in the address above.

2 Enter your **Username**. If you have multiple hosts configured, you also may need to enter the host separator (the default is @) and the fully qualified domain name of the host, in the format of `username@yourhostname.domainname.com`.

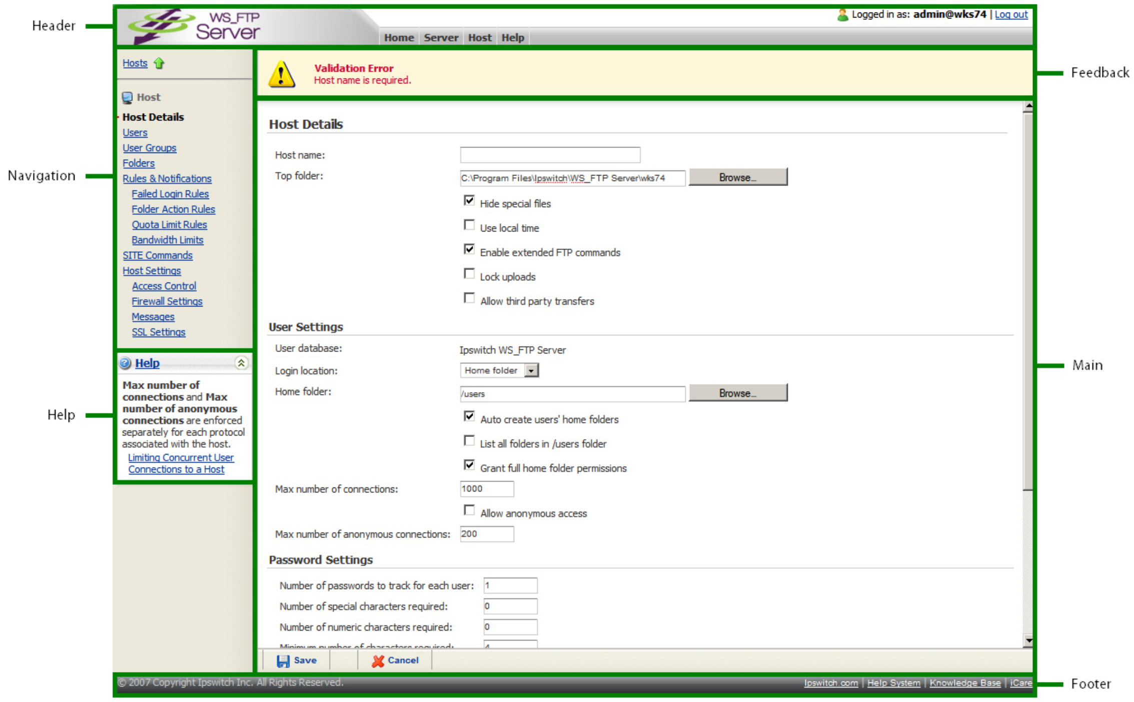
> **Tip:** If this is your first time logging in to the WS_FTP Server Manager, use the username you specified when you installed WS_FTP Server. If you accepted the defaults during the install, enter `admin`.

3 Enter your **Password**.

4 Click **Log In**.

Navigating the WS_FTP Server Manager

The WS_FTP Server Manager has a Web-based user interface.



Logged in as: **admin@wks74** | Log out

Validation Error
Host name is required.

Help

Max number of connections and **Max number of anonymous connections** are enforced separately for each protocol associated with the host.
Limiting Concurrent User Connections to a Host

Host Details

Host name:
Top folder: C:\Program Files\Ipswitch\WS_FTP Server\wks74

☑ Hide special files
☐ Use local time
☑ Enable extended FTP commands
☐ Lock uploads
☐ Allow third party transfers

User Settings

User database: Ipswitch WS_FTP Server
Login location: Home folder
Home folder: /users

☑ Auto create users' home folders
☐ List all folders in /users folder
☑ Grant full home folder permissions

Max number of connections: 1000

☐ Allow anonymous access

Max number of anonymous connections: 200

Password Settings

Number of passwords to track for each user: 1
Number of special characters required: 0
Number of numeric characters required: 0
Minimum number of characters required: 4

© 2007 Copyright Ipswitch Inc. All Rights Reserved.

The interface consists of five main regions that each perform a specific function.

- **Header**. The header contains the top menu, an indication of which user is logged in, and a link to log out.
- **Navigation**. The navigation area contains a link to the previous page, a contextual menu of links to pages that are relevant to the current page, and the help box.
- **Help**. Click to get help information about using the WS_FTP Server application.
- **Feedback**. This portion of the page displays informational messages about the processes you are completing. This area may display errors, helpful tips, evaluation status, and other information.
- **Main**. The main area contains the information and data for the selected page. If the page allows you to modify or create data, a **Save** (or **OK**) and **Cancel** button are anchored to the bottom left corner of the main area.
- **Footer**. In addition to copyright information, the footer displays links to the Ipswitch Web site, the help system and documentation for the product, the knowledge base, and the iCare campaign.

Note: Some pages are designed to act as dialogs, requiring that content be saved or the action cancelled. On these pages, the top menu in the header and the contextual menu in the navigation area are not displayed.

Using the top menu

The top menu, located in the header section of each page, provides quick access to almost every aspect of the WS_FTP Server Manager.

Home Menu

- **Home**. Select this option to return to the home page.

Server Menu

- **Listeners**. Select this option to manage listeners. From the listeners, you can configure SSH host keys and SSL certificates.
- **Hosts**. Select this option to manage hosts.
- **SSL Certificates**. Select this option to create, import or delete SSL certificates.
- **Log Viewer**. Select this option to view the server log statistical information about the server.
- **Notifications**. Select this option to view existing notifications or create new ones.
- **Session Manager**. Select this option to view statistics about the current sessions connected to the server and to forcefully terminate specific sessions.
- **Server Settings**
  - **Server Details**. Select this option to view information about the server and to configure the host separator for all hosts.
  - **Notification Server**. Select this option to specify the information needed to connect to the notification server.
  - **Log Settings**. Select this option to specify the information needed to connect to the log server. You can also specify the depth of detail that is logged.

- **Services**. Select this option to manage the WS_FTP Server services. From this page, you can view the current status of each service and start, stop or restart any of the services.
- **Modules** (on page 133). Select this option to open the Modules page, which show any separately purchased modules that you have installed. The modules extend WS_FTP Server functionality, for example, the Web Access module provides web-based transfer to your users.

Host Menu

- **Current host name**. Select this option (which displays as the host name of the current host) to open the home page for this host.
    - **Manage Hosts**. Select this option to open the host selection page used to change the current host.
- **Host Details**. Select this option to configure host, user and password options for the current host.
- **Users**. Select this option to manage users on the current host.
- **User Groups**. Select this option to manage user groups on the current host.
- **Folders**. Select this option to specify permissions on folders and to manage virtual folders.
- **Rules & Notifications**
    - **Failed Login Rules**. Select this option to configure rules that are triggered after multiple failed attempts to log in.
    - **Folder Action Rules**. Select this option to configure rules that are triggered when specified actions are performed on specified folders and files.
    - **Quota Limit Rules**. Select this option to configure the amount of disk space each user or user group can consume.
    - **Bandwidth Limits**. Select this option to configure how much bandwidth each user or user group can consume.
- **SITE Commands**. Select this option to configure and manage permissions to SITE commands for the current host.
- **Host Settings**
    - **Access Control**. Select this option to control access to the host by IP address.
    - **Firewall Settings**. Select this option to specify the IP address and port that the server uses in response to passive connections.
    - **Messages**. Select this option to specify welcome and exit messages for the host.
    - **SSL Settings**. Select this option to configure SSL settings specific to the host.

Help Menu

- **Help System**. Select this option to open the help file.
- **Support**
    - **Support Center**. Select this option to open the support center pages on the Ipswitch web site.

  - **Knowledge Base**. Select this option to open the knowledge base on the Ipswitch web site.
- **About Ipswitch**
  - **Ipswitch Web Site**. Select this option to open the Ipswitch web site.
  - **iCare**. Select this option to find out about iCare, Ipswitch's campaign to fight child poverty.
- **About this Product**. Select this option to view information about the product, including serial and activation numbers.

CHAPTER 3

Configuring and Managing WS_FTP Server

In This Chapter

Setting global options

After installation, WS_FTP Server is ready to work. You can use the default configuration for FTP connections (all IP addresses on the server on port 21 and all IP address on the server on port 990 for implicit SSL) or SSH connections (all IP addresses on the server on port 22). You can also set the options described in this section.

To view and set options for the WS_FTP Server configuration:

1 From the top menu, select **Server > Server Settings**. The Server Settings page opens.

2 Select one of the following links:

- **System Details**. Select this option to view information about the system and define the host separator.
- **Notification Server Settings**. Select this option to configure the notification server and notification logging.
- **Log Settings**. Select this option to configure the connection to the log server and select the level of detail to log.

Starting and stopping the server

You can use the Web-based WS_FTP Server Manager to start, stop or restart any of the services used by WS_FTP Server.

To start, stop or restart a service:

1. From the top menu, select **Server > Services**. The Services page opens.
2. If you are prompted for username and password, enter the username and password of a Windows user on the server computer. These credentials are required to access information about the services running on Windows.
3. Select the checkbox next to the name of the service you want to start, stop or restart. You can also select multiple checkboxes to start, stop or restart multiple services at one time.
4. Click the appropriate button for the action you want to perform: **Start**, **Stop** or **Restart**.

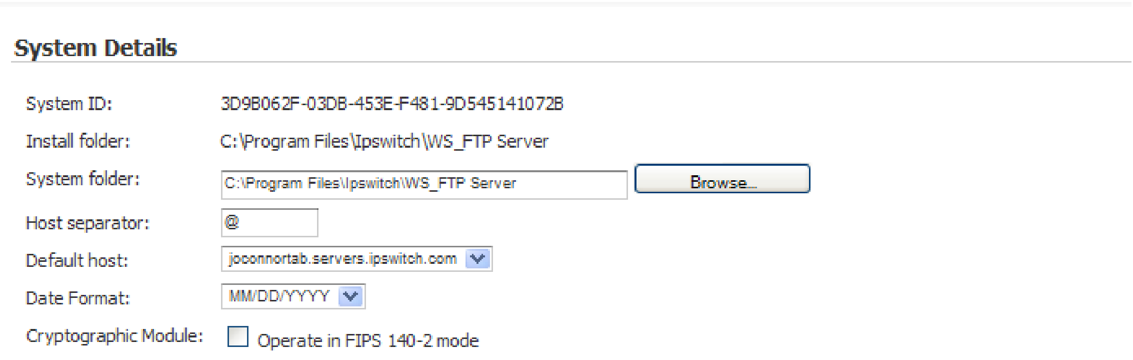
Changing the default host

The default host is used to determine which host to use when a user attempts to authenticate to a host or to the WS_FTP Server Manager. If the username entered exists on the default host and the password entered is correct, the user can authenticate without specifying the host separator and the host name.

There are two types of default hosts: the default host for the WS_FTP Server Manager and the default host for listeners.

To change the default host for the WS_FTP Server Manager:

1. From the top menu, select **Server > Server Settings > System Details**. The System Details page opens.



System Details

System ID:	3D9B062F-03DB-453E-F481-9D545141072B
Install folder:	C:\Program Files\Ipswitch\WS_FTP Server
System folder:	C:\Program Files\Ipswitch\WS_FTP Server
Host separator:	@
Default host:	joconnortab.servers.ipswitch.com
Date Format:	MM/DD/YYYY
Cryptographic Module:	□ Operate in FIPS 140-2 mode

2. In **Default host**, select the name of the host you want to serve as the default host for the WS_FTP Server Manager.
3. Click **Save**.

To change the default host for a listener:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.

3 In the **Hosts associated with this listener** list, select the checkbox next to the host name of the host you want to use as the current listener's default host. If only one host exists in the list, it is already the default.

4 Click **Set Default**. The select host is made the default host for the current listener.

5 Click **Save**.

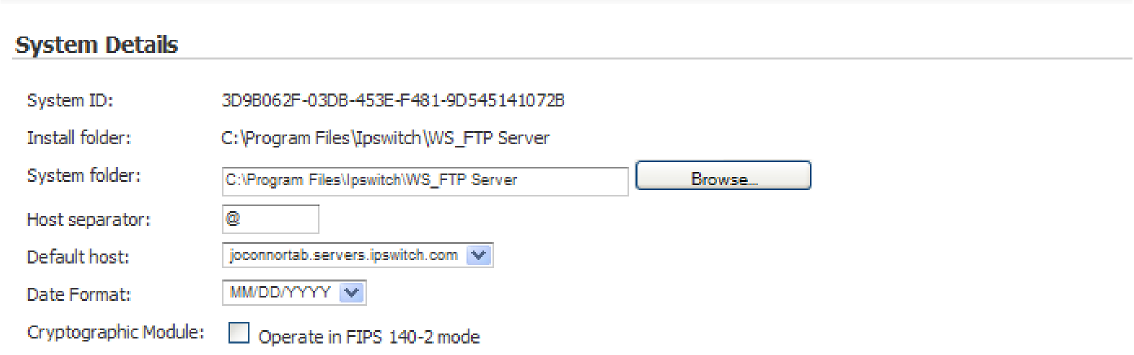
Changing the host separator

By default, WS_FTP Server allows users to authenticate to hosts other than the default host by including the host separator and the host name with the username, such as `username@hostname`.

Usernames cannot include the host separator. If you wish to use a different host separator (so that usernames can match email address, for example), you must change the host separator.

To change the host separator:

1 From the top menu, select **Server > Server Settings > System Details**. The System Details page opens.



System Details

System ID: 3D9B062F-03DB-453E-F481-9D545141072B

Install folder: C:\Program Files\Ipswitch\WS_FTP Server

System folder: C:\Program Files\Ipswitch\WS_FTP Server

Host separator: @

Default host: joconnortab.servers.ipswitch.com

Date Format: MM/DD/YYYY

Cryptographic Module: □ Operate in FIPS 140-2 mode

2 In **Host separator**, enter any single character that you want to use to separate usernames and host names.

Caution: If a username includes the character you specify as the host separator, that user will not be able to authenticate after you change the host separator.

3 Click **Save**.

Configuring DNS for hosts

Many 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 a host using its actual host name (for example, gyro.ipswitch.com) or IP address, it may be easier for users to remember or guess a name like ftp.ipswitch.com.

To create an alias, add an entry in your DNS records like the one below:

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

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

For more information, consult the documentation for your DNS system or contact your network administrator.

Activating FIPS Mode

You can configure WS_FTP Server to run in FIPS-validated mode.

FIPS (Federal Information Processing Standard) is a standard published by the U. S. National Institute of Standards and Technology (NIST), a non-regulatory agency of the U. S. Department of Commerce. NIST works to establish various standards that the U.S. military and various government agencies must abide by. Therefore, vendors, contractors, and any organization working with the government and military must also comply with these standards where they are required. Additionally, despite the fact that FIPS is a U.S.-developed standard, the Canadian government has similar policies requiring FIPS-validated software.

WS_FTP Server FIPS mode includes Triple DES, AES, and HMAC SHA-1. Other modes of encryption are not supported, as specified by FIPS 140-2.

To configure WS_FTP Server to run in FIPS-validated mode:

1. Go to **Server Settings** > **System Details**.
2. Select the Cryptographic Module checkbox.
3. Navigate to the Services page.
4. Select the checkboxes next to each service.
5. Click the **Restart** button.

After restart, FIPS-validated mode will be activated.

> **Note**:With FIPS mode activated, non-FIPS connections *will still be allowed*, unless other connection modes are turned off. To restrict WS_FTP Server to FIPS-validated connections, you need to change the settings as described in the following procedure.

FIPS-related security settings:

1. Shut off all insecure listeners (with only FTPS and SFTP listeners remaining).
2. In the Server Manager, select **Server > Listeners**. The Listeners page opens.
3. Click the IP address of the listener you want to open. The Edit Listener page opens.
4. Click **Edit SSL Settings**. The Listener Encryption Settings page opens.
    1. For SSL type, select **SSL Enabled** (or **Implicit SSL**).
    2. Select the appropriate SSL certificate. You may need to create one.
    3. For SSL security level, select **Enable TLS Only**.
    4. Click **Save**.
5. Navigate to **Host > Host Settings > SSL Settings**.
    1. For **Minimum SSL level**, select **128** or **256**.
    2. Select **Force SSL**.

    Click **Save**.

CHAPTER 4

Configuring Hosts

In This Chapter

About hosts

To use the WS_FTP Server with a single host, the host uses the network host name and IP address of the computer on which you are installing the program.

For each host you add, consider the following:

- To create user accounts, choose whether you will create your own user database or use user accounts from an existing Windows NT, IMail Server user database on your PC, or external (ODBC) database. For more information, see *Configuring an external user database* (on page 24).
- By default, each user on the host will have a folder (with the same name as their username) for uploading and downloading files and 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 folder of the host. For more information, see *Configuring user settings* (on page 62).
- You can choose to provide anonymous access to the host. If you provide anonymous access, any user can log on to the host using a user account that belongs to the Anonymous group and an email address as the password. For more information, see *Enabling anonymous access* (on page 39).

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

Choosing host configuration

You can have multiple hosts on a single computer with each host functioning as a separate site. The first host you add should use the primary host name and IP address of the computer on which you have installed the program. The first host is set up during the program installation process.

Subsequent hosts can be configured in one of following ways:

- **Sharing a listener with the primary host**. If you configure a new host to share a listener with the primary host, users must include the host name and host separator with their username when they log in; for example, username@hostname or anonymous@hostname. This may present a problem for some older clients and Web browsers.

Note: Sharing a listener with the primary host may present a problem for some older clients and Web browsers. In previous versions of Ipswitch WS_FTP Server, a host that shared a listener with another host was referred to as a virtual host.

- **Using a different listener**. If you configure a new host to have a dedicated listener (either on the standard port on a different IP address or a nonstandard port on the IP address of the listener assigned to the primary host), users need to specify only their usernames to log in.

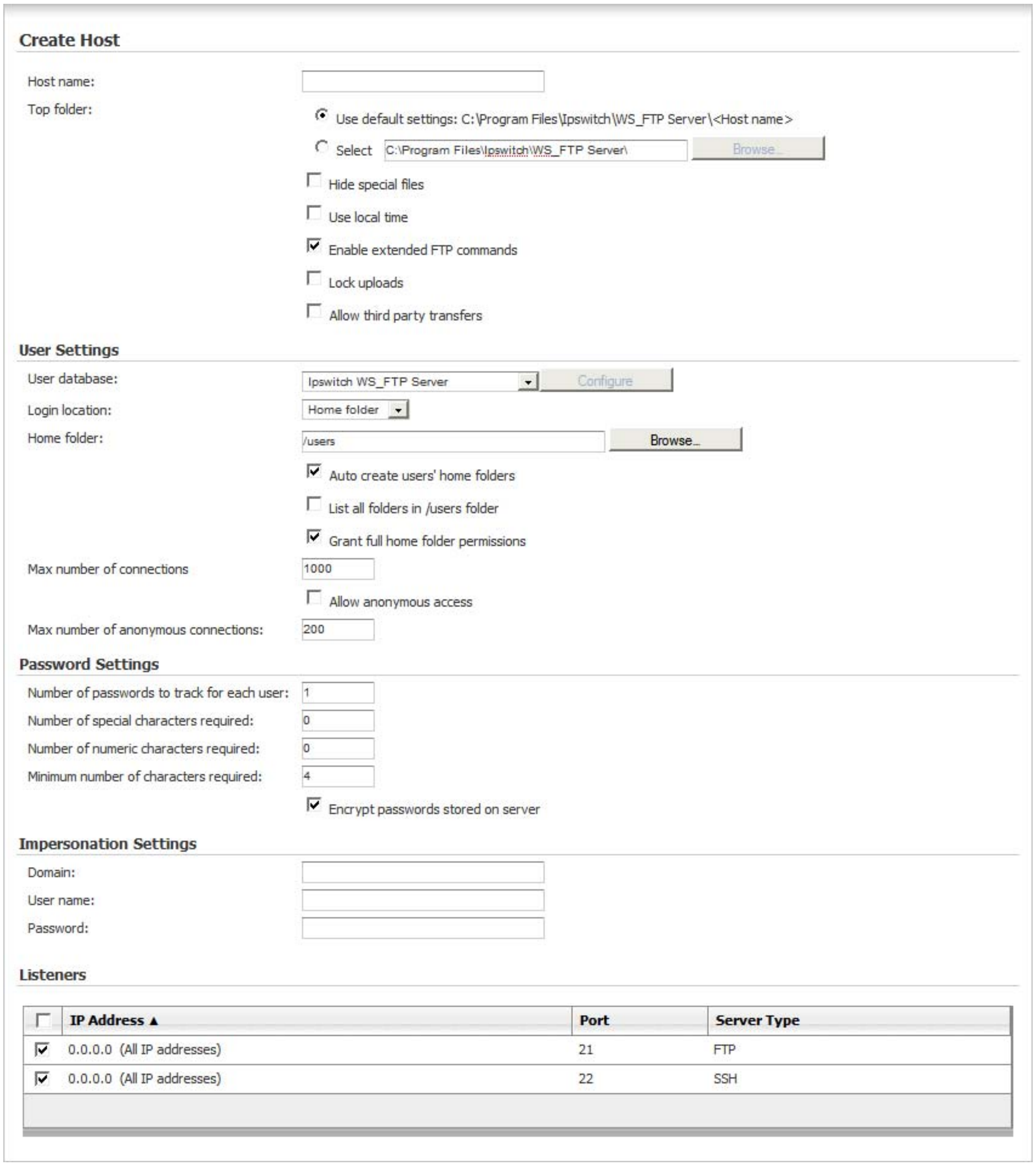
Setting up a host is a two step process. First you must configure the host, then you must assign a listener or listeners to the host.

Creating hosts

To create a new host:

1 From the top menu, select **Server > Hosts**. The Hosts page opens.

2 Click **Create**. The Create Host page opens.



Create Host

Host name:	
Top folder:	● Use default settings: C:\Program Files\Ipswitch\WS_FTP Server\<Host name>
	○ Select C:\Program Files\Ipswitch\WS_FTP Server\ Browse...
	□ Hide special files
	□ Use local time
	☑ Enable extended FTP commands
	□ Lock uploads
	□ Allow third party transfers

User Settings

User database:	Ipswitch WS_FTP Server Configure
Login location:	Home folder
Home folder:	/users Browse...
	☑ Auto create users' home folders
	□ List all folders in /users folder
	☑ Grant full home folder permissions
Max number of connections	1000
	□ Allow anonymous access
Max number of anonymous connections:	200

Password Settings

Number of passwords to track for each user:	1
Number of special characters required:	0
Number of numeric characters required:	0
Minimum number of characters required:	4
	☑ Encrypt passwords stored on server

Impersonation Settings

Domain:	
User name:	
Password:	

Listeners

□	IP Address ▲	Port	Server Type
☑	0.0.0.0 (All IP addresses)	21	FTP
☑	0.0.0.0 (All IP addresses)	22	SSH

3 Enter a **Host name** for the new host.

4 Modify the remaining settings as needed.

5 Under **Listeners**, select the listeners you want to allow clients to use to connect to this host.

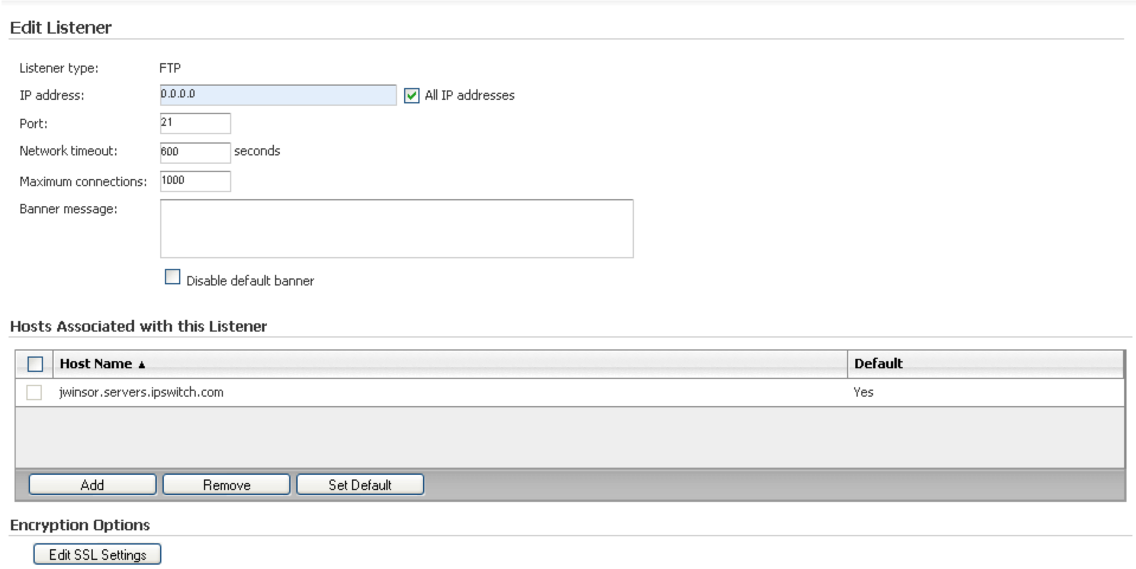
6 Click **Save**.The Hosts page reopens with the new host in the list of hosts.

Associating hosts with listeners

You select listeners to use with a host when you create a host. You can also associate a host with more or different listeners than you selected when you created the host.

To associate a host with a listener:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.



Edit Listener

Listener type: FTP

IP address: 0.0.0.0 ☑ All IP addresses

Port: 21

Network timeout: 600 seconds

Maximum connections: 1000

Banner message:

□ Disable default banner

Hosts Associated with this Listener

□	Host Name ▲	Default
□	jwinsor.servers.ipswitch.com	Yes

Encryption Options

> **Important:** If the listener you want to use is not in the list, you will need to configure it first. For more information, see *Configuring Listeners* (on page 55).

3. Under **Hosts Associated with this Listener**, click **Add**. The Select Host page opens.
4. Select the new host you created from the list, then click **OK**. The Listener Details page reopens with the new host listed under **Hosts Associated with this Listener**.
5. Click **Save**.

Configuring an external user database

WS_FTP Server hosts can be configured to use several types of user databases, allowing you to use an existing user database to minimize administration time and effort. Each WS_FTP Server host can use only one user database.

> **Note**: The type of user database used by a host must be selected when the host is initially created. User database type for a host cannot be changed after the host is created.

When you create a host that uses an external user database such as the Microsoft Windows user database, Microsoft Active Directory, or LDAP database, WS_FTP

Server replicates all users to the WS_FTP Server data store and stores additional information about each user (such as home folder location and folder permissions).

User passwords are not stored in the WS_FTP Server user database. When a user logs on to the WS_FTP Server host, the user is authenticated against the external user database.

If you create or delete a user on an external database, you must synchronize the database before the change appears in the WS_FTP Server Manager.

To select the user database:

1 From the top menu, select **Server > Hosts**. The Hosts page opens.
2 Click **Create**. The Create Host page opens.
3 In **User database**, select the type of database you want to use to authenticate users to this host.
   - **Ipswitch WS_FTP Server**. Select this option to use the native WS_FTP Server database.
   - **Microsoft Windows database**. Select this option to use a Microsoft Windows user database. By default, the users on the local computer are used, but you may also click **Configure** and provide additional information to use users on a domain.
   - **ODBC database**. Select this option to use any database that you can connect to using ODBC. You must click **Configure** and provide additional information before users can authenticate using this user database.
   - **Microsoft Active Directory database**. Select this option to use a Microsoft Active Directory user database. You must click **Configure** and provide more information before this option will work.
   - **Lightweight Directory Access Protocol (LDAP)**. Select this option to use a database that can connect using LDAP. Standard implementations of LDAP are supported, including Microsoft's Active Directory, OpenLDAP, and Novell's eDirectory. You must click **Configure** and provide additional information before users can authenticate using this user database.

> You can configure a Microsoft Active Directory database using the LDAP option, or the Microsoft Active Directory database option. The latter allows you to use Windows file permissions for the user folders.

   - **Ipswitch IMail Server database**. Select this option to use the user database from an Ipswitch IMail Server installed on the same computer as the WS_FTP Server. If Ipswitch IMail Server is not installed, this option is not available.

4 Click **Save**.

Microsoft Windows user database

If you select the Microsoft Windows user database option, all users in the Windows user database on your computer or on a specified domain are granted access (using their Windows username and password) to the host.

Using the WS_FTP Server Manager, you can display each user account and modify file transfer settings for an account, but you cannot add or delete user accounts. You must add or delete user accounts through Windows.

To configure a host to use a Microsoft Windows user database:

1 From the top menu, select **Host > Host Details**. The Host Details page opens.
2 Next to **User database**, click **Configure**. The User Database Configuration page opens.
3 Set the appropriate options.
   - **Domain controller**. Enter the host name of the domain controller for the domain to which the users that you want to grant access belong. To use the local users from the computer where WS_FTP Server is installed, enter a single period.
   - **Domain**. Enter the name of the domain to which the users you want to grant access belong. To use the local users from the computer where WS_FTP Server is installed, enter a single period.
   - **Use Microsoft Windows file permissions**. Select this option to use Microsoft Windows file permissions in addition to any permissions set within WS_FTP Server. For more information, see *Using Windows file permissions* (on page 36).
4 Click **Save**.
5 For WS_FTP Server to access the Microsoft Windows user database, you must change the user context under which WS_FTP Server is running using one of the following methods:
   - **Provide impersonation credentials for the host**. WS_FTP Server can impersonate any Windows user. For more information, see *Changing user context via user impersonation* (on page 37).
   - **Change the user context for WS_FTP Server services and the web server's virtual folder**. You can change the WS_FTP Server services to run as a Windows user who has access to the Microsoft Windows user database. For more information, see *Changing user context on the services* (on page 37).

Note: If you choose to change user context on WS_FTP Server services and the web server's virtual folder, you must restart all services before the changes become active.

ODBC user database

You can use an external database to hold all of the authentication information and properties for your users (with the exception of SSH user keys).

You must configure the ODBC user database before users can authenticate using this user database.

Before you can configure an ODBC user database, you must establish an ODBC system data source name through the Data Sources tool (found in the Windows Control Panel).

To configure an ODBC user database:

1 From the top menu, select **Host > Host Details**. The Host Details page opens.

2 Next to User database, click **Configure**. The User Database Configuration page opens.

3 Set the appropriate options.

- **Plug-in name**. This is the name of the user plug-in. This is provided as information only and cannot be edited.
- **Plug-in location**. This is the location of the DLL file for the user plug-in. This is provided as information only and cannot be edited.
- **Plug-in description**. This is a description of the plug-in that describes its function. This is provided as information only and cannot be edited.
- **ODBC User DLL**. Enter the full path to where the file obdcuser.dll was installed on the server. This is not the same as the ftpauthodbc.dll file listed in Plug-in location.
- **ODBC DSN**. Enter the source name created in the ODBC Source Administration tool described above.
- **Table name**. Enter the name of the database table that contains the correct fields. If you are using a Microsoft Access table with spaces in the name, you must enclose the table name in hard brackets; for example, `[Table Name]`.
- **User ID and Password**. If the database you are using requires authentication, enter a valid username and password.

4 Click **Save**.

Note: If you are configuring an external database that uses Windows credentials for authentication, such as Microsoft SQL Server, you must enter the credentials in the *host impersonation* (on page 37) fields on the Host Details page even if the credentials are already specified in the DSN and on the User Database Configuration page.

Microsoft Active Directory user database

You can use the Microsoft Active Directory user database option to grant users listed in the active directory access (using their Windows domain username and password) to a host.

Using the WS_FTP Server Manager, you can display each user account and modify file transfer settings for an account, but you cannot add or delete user accounts. You must add or delete user accounts through the Active Directory Users and Computers.

To configure Microsoft Active Directory user database:

1 From the top menu, select **Host > Host Details**. The Host Details page opens.

2 Next to **User database**, click **Configure**. The User Database Configuration page opens.

3 Set the appropriate options.

- **Organizational Unit**. Enter the fully distinguished name of the organizational unit that contains the users you want to grant access to the file transfer server

(Maximum length: 256 characters).
For example: OU=YourOrgUnit,DC=YourDomain,DC=com

- **Include users from nested OUs**. Select this option to grant access to all users contained in the organizational unit specified in **Organizational Unit** and all users in organizational units contained within the specified organizational unit. If this option is cleared, only the users in the specified organizational unit are granted access to WS_FTP Server; users in organizational units contained within the specified organizational unit are not granted access.
- **User Groups**. Specify the fully distinguished name for the user groups that contain the users you want to allow to authenticate to the file transfer server. You can specify multiple group distinguished names separated by the pipe character ("|") (Maximum length: 256 characters).

  For example: CN=Group1,OU=YourOrgUnit,DC=YourDomain,DC=com|CN=Group2,OU=AnotherOrgUnit,DC=YourDomain,DC=com

> **Note**: The organizational unit that a user group belongs to does not have to match or be contained within the organizational unit entered in the first field.
>
> **Tip**: For more information about distinguished names, see "LDAP Naming Model" in *How Active Directory Searches Work* (http://www.ipswitch.com/adsearch) on the Microsoft Web site.

- **Use Microsoft Windows file permissions**. Select this option to use Microsoft Windows file permissions in addition to any permissions set within WS_FTP Server. For more information, see *Using Windows file permissions* (on page 36).

> **Note**: If you opt to use Windows file permissions, users cannot authenticate over SSH using public key authentication. Since no key is associated with the Windows user account, users must authenticate using a password.

4 Click **Save**.

5 For WS_FTP Server to access the Microsoft Active Directory, you must change the user context under which WS_FTP Server is running using one of the following methods:

- **Provide impersonation credentials**. WS_FTP Server can impersonate any Windows user. For more information, see *Changing user context via user impersonation* (on page 37).
- **Change the user context for WS_FTP Server services and the virtual folder**. You can change the WS_FTP Server services to run as a Windows user who has access to the Active Directory. For more information, see *Changing user context on the services* (on page 37).

> **Note**: If you choose to change user context on WS_FTP Server services and the virtual folder, you must restart all services before the changes become active.

LDAP user database

You can use an external LDAP database to hold all of the authentication information and properties for your users.

You must configure the LDAP user database before users can authenticate using this user database. You can set a filter to determine which users in an LDAP user database should be added as WS_FTP Server users.

For a description of the LDAP feature in WS_FTP Server, see About LDAP.

To configure an LDAP user database:

1. From the top menu, select **Host > Host Details**. The Host Details page opens.
2. Next to **User database**, click **Configure**. The User Database Configuration page opens.
3. Set the appropriate options, then click **Save**.

Connection Settings

This section specifies the information used to connect to an LDAP database server.

- **Use SSL**. Select this option to connect via SSL on the specified port so that all communications between WS_FTP Server and the LDAP server are encrypted. The standard SSL port for LDAP is 636 (TCP).
- **Use mutual authentication**. Select this option if the LDAP server requests a client certificate to prove the client's identity. Your LDAP server administrator can tell you if a client certificate is needed. In many cases, you can use the default option **Default RSA SSL Certificate**. If you have a trusted SSL client certificate that you want to use, you can select the certificate from the list, provided it has been imported into the certificate store. For information on SSL certificates, see *Using SSL* (on page 101).
- **Primary host**. Enter the hostname or IP address of the LDAP server.
- **Port**. Enter the port on which the primary host's LDAP server is running. The default is port 389, or if SSL is selected, 636.
- **Secondary host**. Optionally, enter the hostname or IP address of a second LDAP server that will be queried if the connection to the primary host fails. The secondary host should be contain a mirrored version of the primary's LDAP database.
- **Port**. Enter the port on which the secondary host's LDAP server is running. The default is port 389, or, if SSL is selected, 636.

> Some LDAP servers allow you to connect anonymously (an anonymous bind). To do an anonymous bind, leave the **User name** and **Password** blank.

- **User name**. Enter the Distinguished Name (DN) used to authenticate to the LDAP database on the primary host. This user is used to run the query (specified below in the Directory Attributes section) that selects users from the LDAP database. The DN is the information required to authenticate to the LDAP

server, and depends on your LDAP server's configuration. The administrator of your LDAP server will know what is required, but typically you need to enter: your user name, called Common Name (CN), your Organizational Unit (OU), and your domain, called domain component (DC); for example:
cn=mjones, ou=georgia office, dc=domain1, dc=YourCompany, dc=com

The domain in this example is: domain1.YourCompany.com

If you specify a secondary host, the DN and password should be the same on both the primary and secondary hosts.

- **Password**. Enter the password for the DN.

> LDAP servers use the syntax "username@hostname," which means you need to change the host separator (default is @) used for WS_FTP Server hosts. The host separator is defined on the System Details page.
>
> To troubleshoot an LDAP connection error, see *Troubleshooting an LDAP connection and query* (on page 31).

Server Settings

This section contains options for working with the LDAP server.

- **Server type**. Select the type of server from the list of supported LDAP servers. The type selected will determine some of the default values displayed in the Directory Attributes options.
- **Network timeout**. The number of seconds after which the attempt to authenticate to the LDAP server, or search the LDAP database will be abandoned.
- **LDAP version**. This option identifies the version of LDAP used by the LDAP server you are connecting to. WS_FTP Server supports v2 and v3 of LDAP. The default is v3, which is the most recent specification. v3 is backwards compatible with v2.
- **Use server side paging**. Select this option to use paging on the LDAP server when synchronizing the LDAP user database with WS_FTP Server. If the LDAP database has a large number of users, this paging option can speed the synchronization. The option is selected by default.

  Synchronization of the LDAP user database with the WS_FTP Server database means that changes to the LDAP user database are written to the WS_FTP Server database. This is a one-direction update. Synchronization happens when:

  - A new user logs on to WS_FTP Server.
  - On the Users page, you (the WS_FTP Server administrator) select to Synchronize the databases.
- **Page size**. The page size to use for server side paging.

Directory Attributes

This section provides the information used to form the query of the LDAP database. The query returns the set of users to be added to the user database for the WS_FTP Server host.

- **Base DN**. Enter the DN of the object to be searched in the LDAP database. For example, to search for users in the domain, domain1.YourCompany.com, you would enter the DN as: dc=domain1,dc=yourCompany,dc=com
  - **Search subtrees**. Select this option to allow the search to access subtrees of the **Base DN**.

For the following options, the default value changes based on the **Server type** selected in the Server Settings section of this page.

- **User filter**. Enter an LDAP query that returns a specific list of users that you want to add to the user database for the WS_FTP Server host. You should use as specific a query as possible to return the best fit of users.

Tip: For more information about distinguished names and creating an LDAP query, see "LDAP Naming Model" in *How Active Directory Searches Work* (http://www.ipswitch.com/adsearch) on the Microsoft Web site. To troubleshoot an LDAP query, see *Troubleshooting an LDAP connection and query* (on page 31).

- **Login**. The LDAP object name for the user name. The default object returns the user name, which is required to create a WS_FTP Server user. If your LDAP database uses a non-standard schema, you will need to enter the object that defines the login user name.
- **Full name**. The LDAP object name for the user's full name. The default object returns the user's full name. This object is not required to create a WS_FTP Server user. If your LDAP database uses a non-standard schema, you will need to enter the object that defines the user's full name.
- **Email address**. The LDAP object name for the user's e-mail address. This object is not required to create a WS_FTP Server user. If your LDAP database uses a non-standard schema, you will need to enter the object that defines the user's email address.
- **Test**. The **Test** button runs a script that simulates a connection to the LDAP server and tests the query by using the information you have provided on this page. The test results are displayed in a log window, these results can be copied and pasted to an email or other report. You can use this log to determine if there is a connection error or if the specified query returns the appropriate list of users.

Troubleshooting an LDAP connection and query

In working with an LDAP database, we have found two general areas where problems occur:

- Making a connection to the LDAP server

- Getting the desired results (list of users) from an LDAP query.

This topic provides some ideas for troubleshooting both types of problems.

Testing the LDAP Connection and Query

On the LDAP Configuration page, the **Test** button runs a script that simulates a connection to the LDAP server and tests the query by using the information you have provided on this page. The test results are displayed in a log window, these results can be copied and pasted to an email or other report. You can use this log to determine if there is a connection error or if the specified query returns the appropriate list of users.

LDAP connection problems

To connect to your LDAP database, you will need:

- the IP address or hostname for the LDAP server
- an account (user name and password) on the LDAP database

The following errors indicate a connection error:

- LDAP server is down, or IP address or hostname is not valid:

```
Initializing LDAP...
Connecting...
Log entry: Command=ldap_bind : Message=Server Down
Disconnecting...
Initializing user search...
***Test Complete***
```

- User name or password is not valid:

```
Initializing LDAP...
Connecting...
Server asked for a client certificate.
Failed to match the client cert with server CA list.
Verifying server certificate...
Server certificate has been verified
Log entry: Command=ldap_bind : Message=Invalid Credentials
Disconnecting...
Initializing user search...
***Test Complete***
```

- If you select to use SSL and select a certificate to use, and the LDAP server does not allow the certificate, you'll see the following error:

```
Initializing LDAP...

Connecting...

Server asked for a client certificate.

Failed to match the client cert with server CA list.

Verifying server certificate...

Server certificate has been verified

Initializing user search...

Getting first user...

Processing retrieved user data...

Closing user search...

***Test Complete***
```

LDAP Queries

To get a list of users from your LDAP database, you need to know the structure (schema) of your database. This allows you to create a query that returns a specific list of users.

If there is a problem with the LDAP query you specified, the log will show the following:

```
Initializing LDAP...

Connecting...

Server asked for a client certificate.

Failed to match the client cert with server CA list.

Verifying server certificate...

Server certificate has been verified

Initializing user search...

Getting first user...

Processing retrieved user data...

Closing user search...

***Test Complete***
```

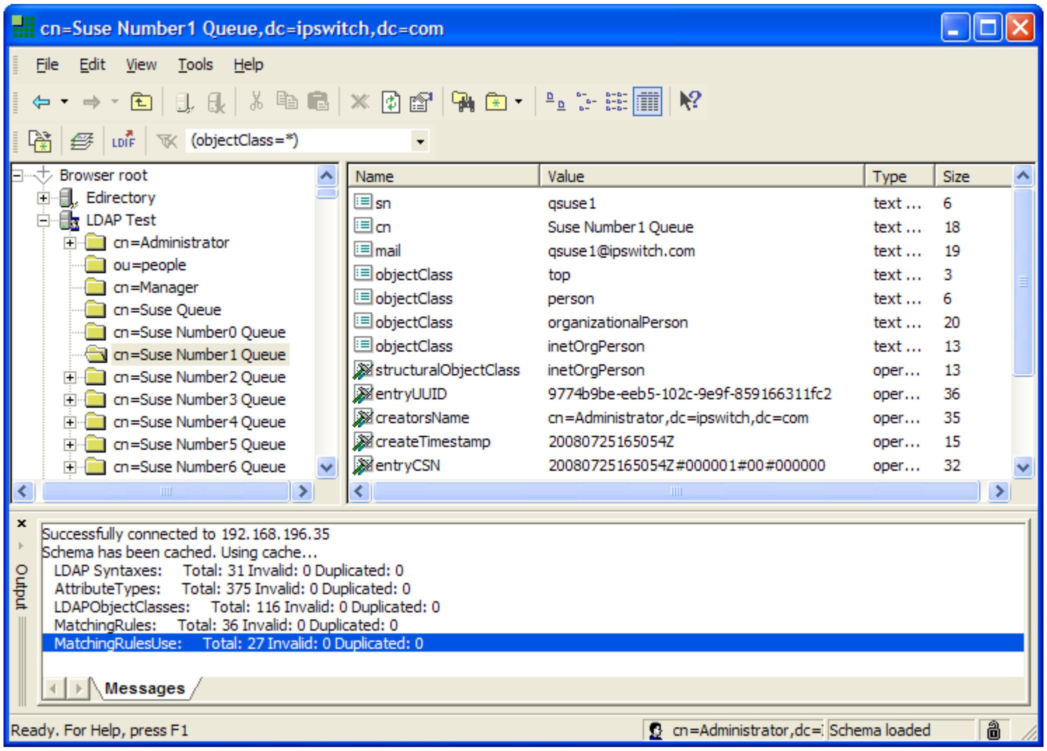
This section provides an example of how you can query an LDAP database (or Active Directory, which is an LDAP database) to return the specific list of users that you want to add to a WS_FTP Server host.

We first use an LDAP browser to view the LDAP database. This will allow us to see the database structure so we can set up an appropriate query when configuring the host in WS_FTP Server.

We use the Softera browser, which you can download from:
http://download.softerra.com/files/ldapbrowser26.msi
http://downlaod.softerra.com/files/ldapbrowser26.msi

Using Softerra, or another LDAP browser, we connect to the LDAP server using the following:

- IP address of LDAP Server: 192.168.196.135
- LDAP user name: cn=Suse Number1 Queue,dc=ipswitch,dc=com



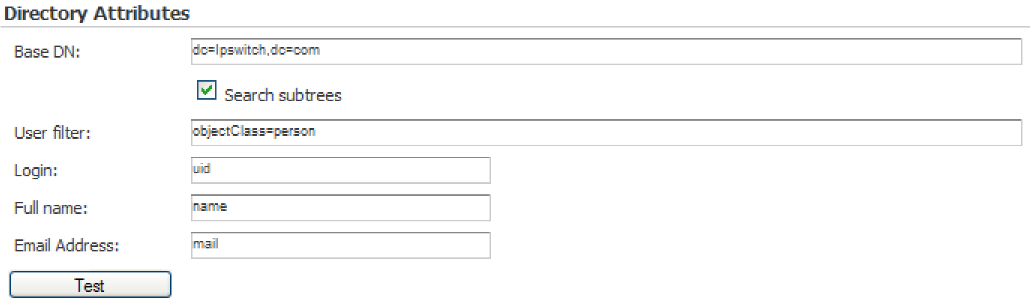
Name	Value	Type	Size
sn	qsuse1	text ...	6
cn	Suse Number1 Queue	text ...	18
mail	qsuse1@ipswitch.com	text ...	19
objectClass	top	text ...	3
objectClass	person	text ...	6
objectClass	organizationalPerson	text ...	20
objectClass	inetOrgPerson	text ...	13
structuralObjectClass	inetOrgPerson	oper...	13
entryUUID	9774b9be-eeb5-102c-9e9f-859166311fc2	oper...	36
creatorsName	cn=Administrator,dc=ipswitch,dc=com	oper...	35
createTimestamp	20080725165054Z	oper...	15
entryCSN	20080725165054Z#000001#00#000000	oper...	32

```
Successfully connected to 192.168.196.35
Schema has been cached. Using cache...
  LDAP Syntaxes:     Total: 31 Invalid: 0 Duplicated: 0
  AttributeTypes:    Total: 375 Invalid: 0 Duplicated: 0
  LDAPObjectClasses:    Total: 116 Invalid: 0 Duplicated: 0
  MatchingRules:    Total: 36 Invalid: 0 Duplicated: 0
  MatchingRulesUse:    Total: 27 Invalid: 0 Duplicated: 0
```

Ready. For Help, press F1 | cn=Administrator,dc= | Schema loaded

To view the structure of the LDAP database, we have selected LDAP Test (the name of our LDAP server) in the left pane. Each "cn" listed under LDAP test represents a user. If we start an LDAP query for users at the Base DN (dc=Ipswitch,dc=com), the query will return all of the users in this database.

On the LDAP Configuration page, this query would be specified as follows:



Directory Attributes

Base DN: dc=Ipswitch,dc=com

☑ Search subtrees

User filter: objectClass=person

Login: uid

Full name: name

Email Address: mail

If we use a Base DN that specifies a specific user (for example, cn=Suse Number1 Queue,dc=Ipswitch,dc=com), the query will return one user. Also note that this OpenLDAP database uses "sn" to identify the user's Login name, so sn is entered in the **Login** box.

Ipswitch IMail Server user database

If you select the IMail Server option, all users in the IMail Server user database on your local system will have access (using their IMail Server username and password) to the host.

You can view each user and modify settings for an account, but you cannot create or delete user accounts. You must create and delete user accounts through the IMail Server administrator.

Important: To use this option, Ipswitch IMail Server version 2006.1 or later must be installed on the same computer as Ipswitch WS_FTP Server.

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

Synchronizing external user databases

When you create a host that uses an external user database such as the Microsoft Windows user database, Microsoft Active Directory, or LDAP database, WS_FTP Server replicates all users to the WS_FTP Server data store and stores additional information about each user (such as home folder location and folder permissions).

User passwords are not stored in the WS_FTP Server user database. When a user logs on to the WS_FTP Server host, the user is authenticated against the external user database.

If you create or delete a user on an external database, you must synchronize the database before the change appears in the WS_FTP Server Manager.

Note: If you remove a user from an external user database, the user information and permissions remain in the WS_FTP Server database until the databases are synchronized. The user cannot, however, authenticate to the server even if the databases have not been synchronized. When the databases are synchronized, the user is removed and the user's home folder is moved to the Windows Recycle Bin.

To synchronize an external user database:

1 From the top menu, select **Host > Users**. The Users page opens.

2 Click **Synchronize**. WS_FTP Server synchronizes with the external user database.

Note: If you are viewing users on a host that does not use an external user database, the **Synchronize** button is not displayed.

Synchronizing external user databases from the command line

Using the ftpdbsync.exe command line utility, you can synchronize users on a host that uses an external user database.

Tip: You can schedule ftpdbsync.exe in Scheduled Tasks in the Windows control panel to automatically synchronize users from external databases on a regular interval.

To use ftpdbsync.exe:

1 From the Windows desktop, select **Start > Run**. The Run dialog appears.

2 Enter `cmd.exe` and click **OK**.

3 Change the directory to the WS_FTP Server directory. For a default installation, this location is `C:\Program Files\Ipswitch\WS_FTP Server\Utilities\`.

4 Enter `ftpdbsync <hostname>`, replacing `<hostname>` with the name of the host for which you want to synchronize users.

Using Windows file permissions

You can configure a host using a Microsoft Windows or Microsoft Active Directory user database to use Windows permissions for user permissions to files and folders on the file transfer server. This lets you consolidate your users and permissions so that you can minimize duplicated maintenance effort.

When this option is enabled, Windows file permissions are used in addition to the permissions explicitly configured in WS_FTP Server, with the most restrictive permission granted to the user.

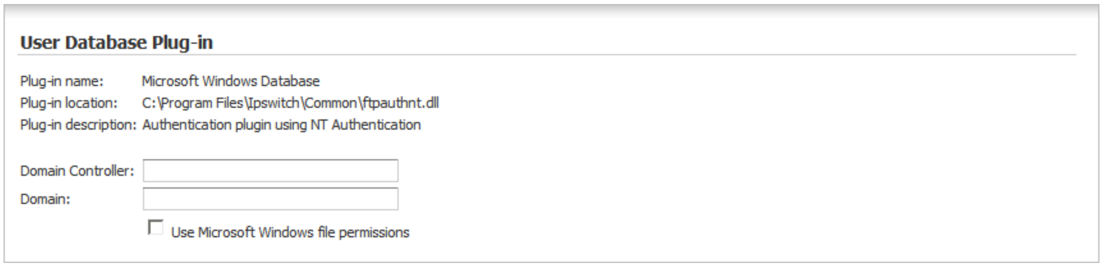
Note: If you opt to use Windows file permissions, users cannot authenticate over SSH using public key authentication. Since no key is associated with the Windows user account, users must authenticate using a password.

To use Windows file permissions:

1 From the top menu, select **Server > Hosts**. The Hosts page opens.

2 Click the **Host name** of the host you want to open. The host you select must use the Microsoft Windows or Microsoft Active Directory user database. The Host Details page opens.

3 Next to **User database**, click **Configure**. The User Database Plug-in page opens.



User Database Plug-in

Plug-in name: Microsoft Windows Database
Plug-in location: C:\Program Files\Ipswitch\Common\ftpauthnt.dll
Plug-in description: Authentication plugin using NT Authentication

Domain Controller:
Domain:
□ Use Microsoft Windows file permissions

4 Select **Use Windows file permissions.**

5 Click **Save**.

Changing user context via user impersonation

Impersonation settings are used to specify a Windows user account that WS_FTP Server uses to request access to folders used by a host. This includes local system folders and network folders specified with a UNC name.

This option may also be used to specify an account to use to access a Windows domain or an Active Directory user database.

To set user impersonation settings for a host:

1 From the top menu, select **Host > Host Details**. The Host Details page opens.

2 Under Impersonation Settings, set the appropriate options.

- **Domain**. Enter the name of the domain on which the user exists.
- **User name**. Enter the user name to use when requesting access to folders used by this host.
- **Password**. Enter the password to use when requesting access to folders used by this host.

3 Click **Save**.

Warning: The credentials saved to the database are encrypted. If you do not want to save your credentials to the database, however, you can change the user that the services and the IIS Web site run as to achieve the same effect for the entire server (if you use IIS as your web server). For more information, see *Changing user context on the services* (on page 37).

Changing user context on the services

If you want an alternative to using the *host-level impersonation settings* (on page 37), you can change the user context for the WS_FTP Server services and the virtual folder. This method changes the user context for all hosts on the server; you cannot have host-level control of the user context using this method.

To change the user context for the WS_FTP Server services:

1. From the Windows desktop of the computer where WS_FTP Server is installed, select **Start > Programs > Administrative Tools > Services**. The Services window opens.
2. Double-click the **Ipswitch WS_FTP Server** service. The **Ipswitch WS_FTP Server Properties (Local Computer)** window opens.
3. Select the **Logon** tab.
4. Select **This Account** and use the **Browse** button to locate the account you want this service to run as.
5. Enter and confirm the **Password** for the account you selected.
6. Click **OK**.
7. Repeat steps 2 through 6 for the **Ipswitch SSH Server** service.

To change the user context for the IIS virtual folder (if using Microsoft IIS as your web server):

1. From the Windows desktop of the computer where WS_FTP Server is installed, select **Start > Programs > Administrative Tools > Internet Information Services**. The Internet Information Services window opens.
2. Locate and right-click on the **WSFTPSVR** virtual folder, then select **Properties** from the context menu. The WSFTPSVR Properties window opens.
3. Select the **Directory Security** tab.
4. Under Anonymous access and authentication control, click **Edit**. The Authentication methods window opens.
5. Under anonymous access, enter the **Username** and **Password** of the user you want your web server's virtual folder to run as.
6. Verify that **Allow web server to control password** is cleared, then click **OK**.
7. Click **OK** to exit the WSFTPSVR Properties window.

Setting host options

After creating a file transfer host, you can set additional options or change existing host settings.

Setting folder listings to use local time

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

To use local time for file and folder listings:

1. From the menu, select **Server > Hosts**. The Hosts page opens.
2. Select a host from the list by clicking on the hyperlinked host name. The Host Details page opens.
3. Select **Use local time**.
4. Click **Save**.

Setting maximum number of connections

You can limit the number of users that can log on to the host at one time using the settings described here.

To set the maximum number of users:

1 From the top menu, select **Server > Hosts**. The Hosts page opens.
2 Select a host from the list by clicking on the hyperlinked host name. The Host Details page opens.
3 In **Max number of connections**, enter the maximum number of users (including anonymous users) that can connect to the host at the same time. The default is 1000 users.
4 In **Max number of anonymous connections**, enter the maximum number of anonymous users that can connect to the file transfer host at the same time. The default is 200 users.
5 Click **Save**.

Important: While limits are configured per host, they are enforced per protocol. If a host has two listeners associated with it, one FTP and one SSH, then the host will permit the maximum number of users and anonymous users to connect for each protocol. If **Max number of connections** is set to 10, for example, then the host will permit 10 users to connect via FTP and 10 via SSH (for a potential maximum of 20).

If a host has multiple listeners of the same protocol type, the limits are still enforced by protocol. For example, if a host has 3 SSH listeners and 2 FTP listeners, it will permit only 10 total FTP users and 10 total SSH listeners (for a potential maximum of 20) to connect concurrently.

Note: If the user limit is exceeded, a system administrator or host administrator can still log on using the Ipswitch Web Admin. Also, a system administrator can always log on using a client.

Entering zero for either option disables new connections. This provides a way to temporarily shut off access to the host, so you can update files. New connections are not allowed, but current connections will continue until the user logs off, the connection exceeds the timeout value, or the connection is terminated by an administrator. Setting **Max number of connections** to zero disables any new connections; setting **Max number of anonymous connections** to zero disables only new anonymous connections.

Enabling anonymous access

You can allow anonymous access to a host so that users can access specified folders on the host without needing a user account. Users can then log on using any username that you have designated as an anonymous user and their email address for the password (or no password).

When an anonymous user logs on to a host, they can perform any action which they are granted permission, either by a direct permission on the account or by the anonymous group, which all users marked as anonymous are automatically added to.

To enable anonymous access to the host:

1 From the menu, select **Server > Hosts**. The Hosts page opens.

2 Select a host from the list by clicking on the hyperlinked host name. The Edit Host page opens.

3 Select **Allow anonymous access**.

4 Click **Save**.

To designate a user as an anonymous user:

1 From the top menu, select **Host > Users**. The Users page opens.

2 In the list of users, select a user by clicking on the linked **Username**. The Edit User page opens.

3 In **User type**, select **Anonymous**.

4 Click **Save**.

Tip: You also set permissions for the anonymous user on any folders. For example, you can use folders or virtual folders to create a download or an upload folder for anonymous users.

Controlling access by IP address

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

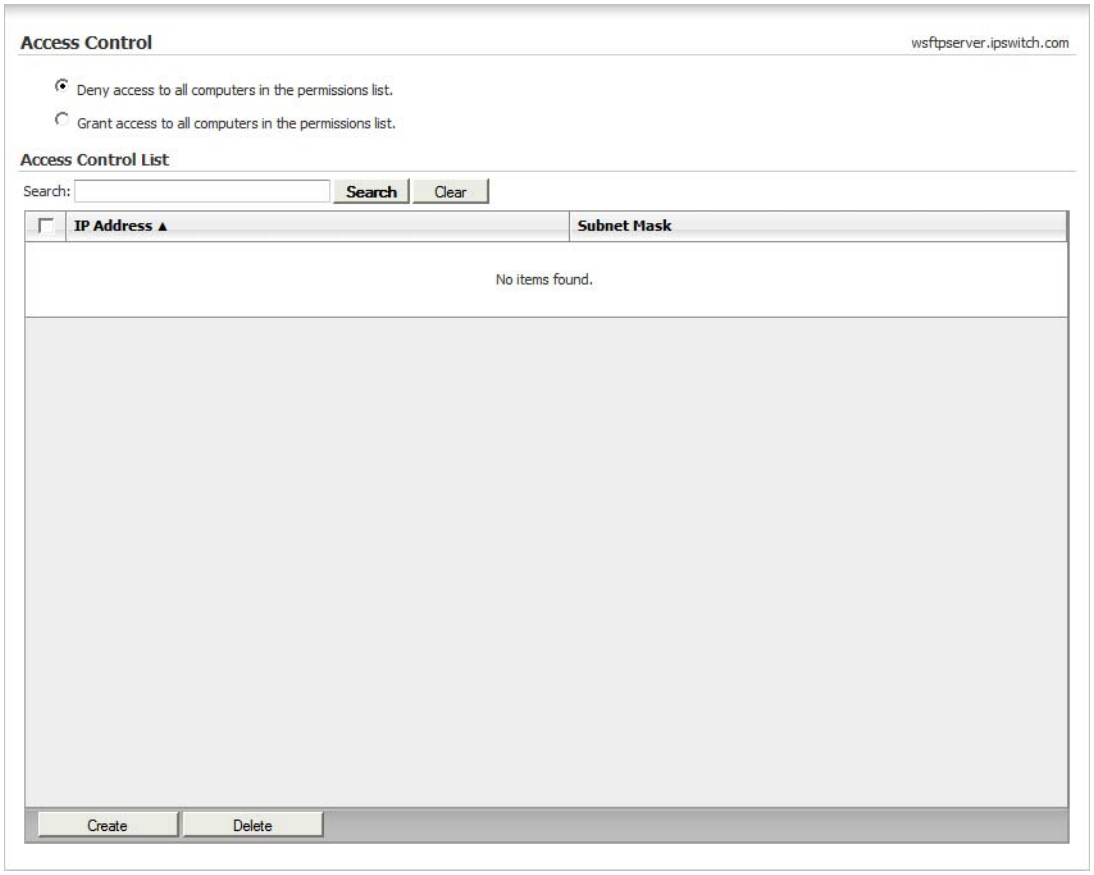
✓ We strongly recommend that the *IP Lockouts* (on page 128) feature be used instead of Access Control because IP Lockouts work at the server-level, blocking access when an offending IP address tries to establish a connection. As a result, the IP Lockouts feature is more efficient and secure, as it identifies an attack when the attack begins and it puts host resources out of reach.

When an IP address is added to Access Control and IP Lockouts is enabled, the IP address does not get added to the Blacklist. The Access Control setting will be used, so the IP address will be able to connect to the server, but then will be blocked at the host-level.

To control access to a specific computer or group of computers by IP address:

1 From the top menu, select **Host > Host Settings > Access Control**. The Access Control page opens.

2 Select whether you want to grant or deny access to, by default, all computers in the list.



Access Control

wsftpserver.ipswitch.com

● Deny access to all computers in the permissions list.

○ Grant access to all computers in the permissions list.

Access Control List

Search: [ ]

□	IP Address ▲	Subnet Mask

No items found.

3 Click **Create** to add another computer or group of computers to the IP Address list. The Create Access Control List Entry page opens.

4 Enter the appropriate information for each of the fields.

- **Define access controls for**. Select the type of access control entry.
  - **A single computer or IP address**. Select this option to grant or deny access to a single computer or IP address. If this option is selected, the **Net mask** field is disabled.
  - **A group of computers**. Select this option to grant or deny access to a group of computers or IP addresses.
- **IP address**. Enter the IP address of the computer to be added to the list.
- **Net mask**. If you are defining access for a group of computers, enter the subnet mask for the group. For example, if you have a class C address space of 156.21.50.0, enter a IP address of 156.21.50.0 and a net mask of 255.255.255.0. This will grant or deny access to the 254 systems with the IP address of 156.21.50.1 through 156.21.50.255.

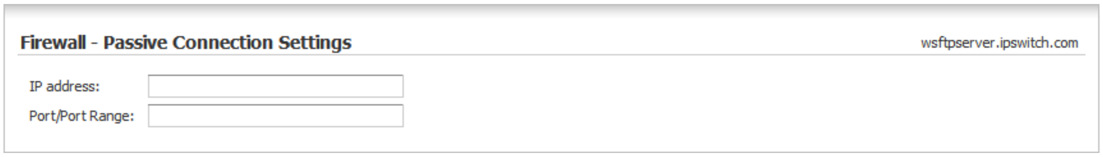
5 Click **Save**. The Access Control page opens again with the new entry listed in the IP Address list.

Using firewalls with WS_FTP Server

When you use a NAT (Network Address Translation) firewall, you may encounter problems when trying to use SSL encryption. A possible fix to this issue is to enter information on the Firewall - Passive Connection Settings page. The settings on this page set the file transfer host to respond to a PASV command by returning the IP address and port range of the NAT firewall. In many cases, this lets you use SSL through a NAT firewall.

To change firewall settings:

1. From the top menu, select **Host > Host Settings > Firewall Settings**. The Firewall - Passive Connection Settings page opens.



Firewall - Passive Connection Settings

wsftpserver.ipswitch.com

IP address:

Port/Port Range:

2. Set the appropriate options.
   - **IP address**. The IP Address to be used in response to a PASV request. This will be sent to the client instead of the host IP address. This should be the IP address of the NAT firewall.
   - **Port/Port Range**. The Port or Ports to be used with the IP address in response to a PASV request. Enter a single port number or a range of port numbers specified by #-# or #, #, #. In the #-# example, all ports between the two numbers are available for use. In the #, #, # example, only the specific ports are available. You can also use a combination of both port specification methods to specify multiple port ranges or ranges and specific ports.

Note: If you specify an IP address and not a port, the server will use any available port above 1024, but will still use the specified IP address in the response. If you specify a port or port range and not an IP address, the server will use its own IP address and only the specified ports.

3. Click **Save**.

What is a NAT firewall?

Because of the need for increased security, many businesses use a form of network protection called a firewall to prevent unauthorized access to or from their private networks. Firewalls can be software or hardware based, or they can be comprised of a combination of both. Part of this protection can include the use of a device or application called NAT.

NAT, or Network Address Translation, is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT box located where the LAN meets the Internet makes all necessary IP address translations. Additionally, NAT provides a type of firewall by hiding internal IP addresses, and it enables a company to use more internal IP addresses. Since they are used internally only, there is no possibility of conflict with IP addresses used by other companies and organizations.

Enabling disabled users

On occasion, users may disable their account after failing to login with the correct username and password with a certain number of failed attempts to authenticate. Use the following instructions to enable the user account login.

To enable a disabled user account:

1. From the top menu, select **Host > Users**. The Users page opens.
2. In the list of users, select a user by clicking on the linked **Username**. The Edit User page opens.
3. Clear **Disable Login**.
4. Click **Save**.

Using banner, welcome and exit messages

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

- **Banner Message**. The server sends this message to a user upon successful connection to a listener, before the user logs on to a host. You can use this message to tell users about the organization of your site, any rules, times of operation, mirror sites, or contact information. You can use the *message variables* (on page 44) to provide information, for example, that the 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* (on page 44) 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* (on page 44) to provide statistics for the FTP session, for example, the number of files received and sent by the user.

Note:Banner, welcome, and exit messages are not supported with SSH.

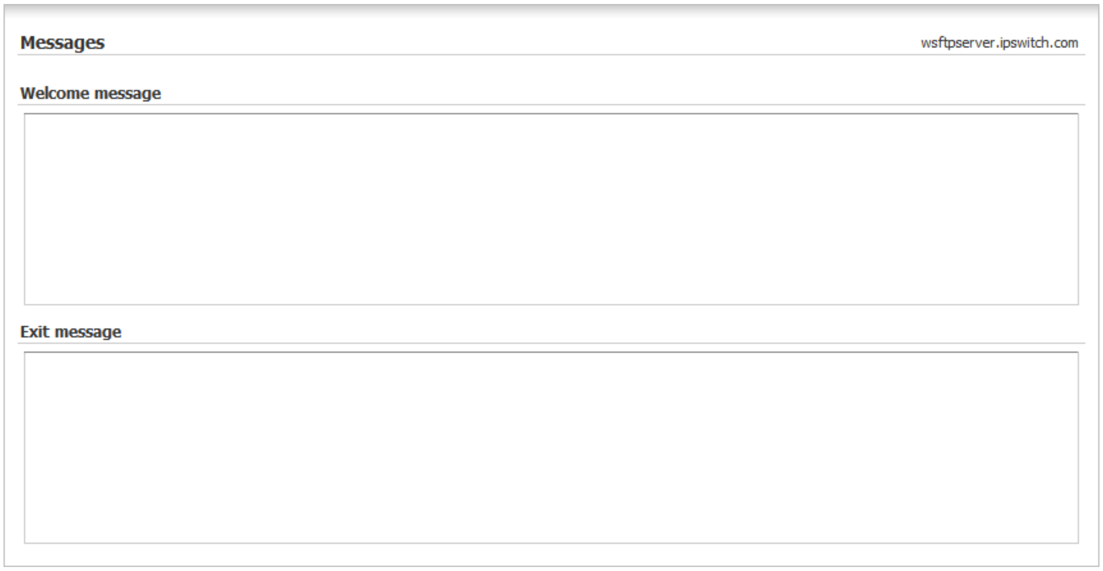
To create or edit a banner message:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the hyperlinked IP address of the listener you want to select. The Edit Listener page opens.
3. In **Banner message**, enter text for the message. You can use *message variables* (on page 44) in this message.
4. Click **Save**.

Tip: If a host uses multiple listeners, you must configure the banner message on each listener used by the host to make sure that all users connecting always get the same banner message. Similarly, if two hosts use one listener, users connecting to both hosts are presented the same banner message.

To create or edit a welcome or an exit message:

1 From the top menu, select **Host > Host Settings > Messages**. The Messages page opens.



2 In **Welcome message** and **Exit message**, enter text for the messages. You can use *message variables* (on page 44) in these messages.

3 Click **Save**.

Using message variables

For the Banner, Welcome and Exit messages, you can enter up to 70 standard ASCII characters. The messages can also contain the following variables:

Variable	Description	Valid in
`%a`	Current number of anonymous users for this host	Banner, Welcome, Exit
`%b`	Maximum number of anonymous users for this host	Banner, Welcome, Exit
`%d`	Number of files deleted by user	Exit
`%f`	Maximum number of files the user can have (or “unlimited”)	Welcome, Exit
`%e`	Number of files currently in user's home folder	Welcome, Exit
`%h`	Host name	Banner, Welcome, Exit
`%I`	IP address of remote user	Banner, Welcome, Exit
`%k`	Current number of users logged on	Banner, Welcome, Exit
`%l`	Maximum number of users that can log on	Banner, Welcome, Exit
`%n`	Full name	Welcome, Exit

Variable	Description	Valid in
`%p`	Number of days before the system resets the account's password	Welcome, Exit
`%q`	Maximum disk space the user can have (or “unlimited”)	Welcome, Exit
`%r`	Number of files the server received from the user	Exit
`%s`	Number of files the server sent to the user	Exit
`%u`	Username	Welcome, Exit
`%z`	Current disk space used by the user	Welcome, Exit

Disabling the default banner message

In some cases, you may opt to disable the banner message so that no identifying information about the server is displayed to potential hackers.

To disable the default banner message:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.
3. Select **Disable default banner**.
4. Click **Save**.

Setting timeouts for connections

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

To set the connection timeouts:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.
3. In **Network timeout**, enter a value in seconds.
4. Click **Save**.

Note: Since this setting is made on the listener, it applies to all hosts that use the listener. If a host uses multiple listeners, it is possible that there may be different timeouts set depending on which listener the client used to connect to the host.

Limiting connections to a host

You can limit how many authenticated users and anonymous users you want to let connect to a host at any given time.

To limit concurrent user connections to a host:

1 From the menu, select **Server > Hosts**. The Hosts page opens.

2 Select a host from the list by clicking on the linked host name. The Host Details page opens.

3 Enter the **Max number of connections** and **Max number of anonymous connections** you want to allow to connect to this host concurrently.

4 Click **Save**.

> **Important:** While limits are configured per host, they are enforced per protocol. If a host has two listeners associated with it, one FTP and one SSH, then the host will permit the maximum number of users and anonymous users to connect for each protocol. If **Max number of connections** is set to 10, for example, then the host will permit 10 users to connect via FTP and 10 via SSH (for a potential maximum of 20).
>
> If a host has multiple listeners of the same protocol type, the limits are still enforced by protocol. For example, if a host has 3 SSH listeners and 2 FTP listeners, it will permit only 10 total FTP users and 10 total SSH listeners (for a potential maximum of 20) to connect concurrently.

Deleting hosts

If a host is no longer needed, you can delete it. Deleting a host removes the host and all data associated with it, including users, groups and rules.

To delete a host:

1 From the top menu, select **Server > Hosts**. The Hosts page opens.

2 Select the checkbox next to the name of the host you want to delete.

3 Click **Delete**. The Delete Confirmation page opens.

4 To delete the host, click **Delete**. The host configuration is deleted from the server.

> **Note:** Deleting a host only removes the host configuration from the server. Files and folders that were created on the host by users or administrators are not removed.

Renaming hosts

You can change the name of a host in WS_FTP Server. If you rename a host without updating the Domain Name Service records that point to the host, the host may become inaccessible.

To rename a host:

1 From the top menu, select **Host > Host Details**. The Host Details page opens.

2 Enter a new **Host name**.

3 Click **Save**.

Managing hosts from the command line

You can add, modify or delete hosts using the host command line utility, iftpaddh.exe.

To start the Add Host Utility:

1. From the Windows desktop, select **Start > Run**. The Run dialog appears.
2. Enter `cmd.exe` and click **OK**.
3. Change the directory to the WS_FTP Server directory. For a default installation, this should be `C:\Program Files\Ipswitch\WS_FTP Server\`.
4. For a list of command options, enter `iftpaddh /?`.

Basic Command Syntax

The basic syntax for adding, modifying and removing a host is indicated below.

Adding a Host	`iftpaddh -add hostname [options]`
Modifying a Host	`iftpaddh -mod hostname [options]`
Deleting a Host	`iftpaddh -kill hostname`

Note: All arguments are case-sensitive and must be supplied as lower case.

Note: iftpaddh will fail if you do not have an active license. (Use the ipsactive command to launch the licensing application and enter your serial number.)

Arguments	**When to use**
`-add hostname`	Use to create a new host. Specify a name for the new host after -add.
`-mod hostname`	Use to modify a host. You must specify a host name after -mod.
`-kill hostname`	Use to delete a host. You must specify a host name after -kill.
`-l ip_address:port:protocol`	Use to specify a listener to associate with the host. You must specify the IP address, port and protocol for the listener you want to associate with the host. To use a listener listening on all IP addresses, enter 0.0.0.0 as the IP address. **Note**:If you enter SSH as your protocol, you must have a valid license that includes SSH support.

`-d directory`	Use to specify the top folder of the host. If a folder is not specified, the server will create a subfolder with the same name as the new host under the top folder of the server.
`-t number`	Use to specify the server time-out. The default is 600 seconds.
`-mu number`	Use to specify the maximum number of concurrent users. The default is 1000.
`-i address`	Use to specify the host IP address.
`-ma number`	Use to specify the number of maximum concurrent anonymous users. The default is 200.
`+anon`	Allow anonymous connections.
`-anon`	Disable anonymous connections.
`+hide`	Use to hide files and folders whose names begin with the dollar sign ($).
`-hide`	Use to show files and folders whose names begin with the dollar sign ($).
`+lt`	Use the server's local time instead of Greenwich Mean Time (GMT).
`-lt`	Use GMT instead of the server's local time.
`+ext`	Enable extended commands for the host (such as FEAT, HOST, LANG, MDTM, MLST, OPTS, XAUT, AUTH SSL and AUTH TLS).
`-ext`	Disable extended commands for the host (such as FEAT, HOST, LANG, MDTM, MLST, OPTS, XAUT, AUTH SSL and AUTH TLS).
`+tpt`	Allow third-party transfers.
`-tpt`	Disable third-party transfers.
`-rd`	Use to delete all files and folders associated with the host. By default, all files and folders remain when a host is removed.

About Impersonation Settings

Impersonation settings are used to specify Windows user accounts that WS_FTP Server uses in requesting access to folders and files on a specific computer.

The following information may be useful in determining what impersonation settings are in effect and have priority. For instance, you might ask, “I’ve entered these impersonation settings. Why aren’t they being used?”

Also, as part of your security planning and management, this information might be helpful in keeping track of the Windows users present on WS_FTP Server.

There are three kinds of impersonation settings that WS_FTP Server may use. In general, WS_FTP Server prefers them in the following order: Windows database users > Host Impersonation Settings > Web Client Impersonation Settings. But there are exceptions, which are described below.

Host Impersonation Settings

The host impersonation specifies the Windows user account and credential at the WS_FTP Server host level.

When do I need to create or modify host impersonation settings?

In many cases, you will not need to. By default, when you install WS_FTP Server or create a new host, the system uses the local machine user to carry out tasks.

In cases where you do not want to use the local machine user, for security purposes, you may want to create a different account and an impersonation setting.

When you choose to enter new host impersonation settings, these settings apply to the WS_FTP Server Web Transfer Module as well (see below).

How do I find host impersonation settings in the WS_FTP Server Web Administration application?

On the “Host Detail Settings” page. You can find this page at: Host > Host Detail Settings.

Are there cases where host impersonation settings will not be used by the system?

Yes. If you use an external Windows database (see below), then the user for the database takes precedence over the both the host impersonation settings and the local machine user. Also, if you specified an executable to run in the “Rules and Notifications” feature, if an executable is triggered by WS_FTP Server Server, it will still run using the local machine user, regardless of what you entered in the Host Impersonation settings.

WS_FTP Server Web Transfer Module Impersonation Settings

The WS_FTP Server Web Transfer Module impersonation account specifies a user for all WS_FTP Server hosts using the WS_FTP Server Web Transfer Module.

When do I need to modify WS_FTP Server Web Transfer Module impersonation settings?

You create WS_FTP Server Web Transfer Module impersonation settings during the WS_FTP Server Web Transfer Module install. Generally, these do not need to change, unless you want to create a different user for security purposes.

If for some reason you delete these impersonation settings, the system will use the Network Service account to access files and folders. The Network Service account has, by design, very limited privileges, and attempts to read or write files using this account will most likely fail.

How do I find WS_FTP Server Web Transfer Module impersonation settings?

In the “Web Access Settings” page. You can find this page by navigating to: Module > Web Access Settings.

Are there cases where WS_FTP Server Web Transfer Module impersonation settings are not used by the system?

Yes. If there are impersonation settings that you have configured for the host, or if you use an external Windows database, these take precedence over the WS_FTP Server Web Transfer Module impersonation settings.

The exception is if you have specified an executable to run in the “Rules and Notifications” feature. If the event was triggered by the WS_FTP Server Web Transfer Module, it will run using the WS_FTP Server Web Transfer Module impersonation settings, even if you have an external Windows database, or a host impersonation setting.

External Windows Database User

When you connect a host to a Microsoft Windows database, Microsoft Active Directory database, or LDAP database, the system employs the Windows user for the external database to access your file system. This user takes precedence over other impersonation settings in almost all cases. (See below.)

When do I need to modify external Windows database user settings?

In the Windows database software, you should be sure that the user accessing the host directory has adequate permissions to do so.

Are there cases where external Windows database user impersonation settings are not used by the system?

Yes. If you specified an executable to run in the “Rules and Notifications” feature, and if the executable was triggered by the WS_FTP Server Web Transfer Module, it will still run using the WS_FTP Server Web Transfer Module impersonation settings. If it was triggered by WS_FTP Server, it will run as the local machine user. The system handles executables this way regardless of whether or not you are using an external Windows database.

Configuring SITE commands

SITE commands are customized FTP commands that FTP clients can issue to execute applications on the server.

You can configure a SITE command to execute any program or application that you could run if you were logged onto the server.

For example, a server administrator could create a SITE command called UNZIP that could be issued by clients to decompress ZIP archive files previously uploaded to the server.

To use this SITE command, the client sends `UNZIP filename.zip` to the server. Ipswitch WS_FTP Professional can send this command using the QUOTE feature. To learn how to issue text commands in another client, consult that client's documentation.

Note: The Windows user your file transfer services are running as (usually `IPS_<WS_FTP Server admin username>`) must have permissions to the executable that is run by the SITE command. If the user does not have permission to run the executable, the SITE command fails.

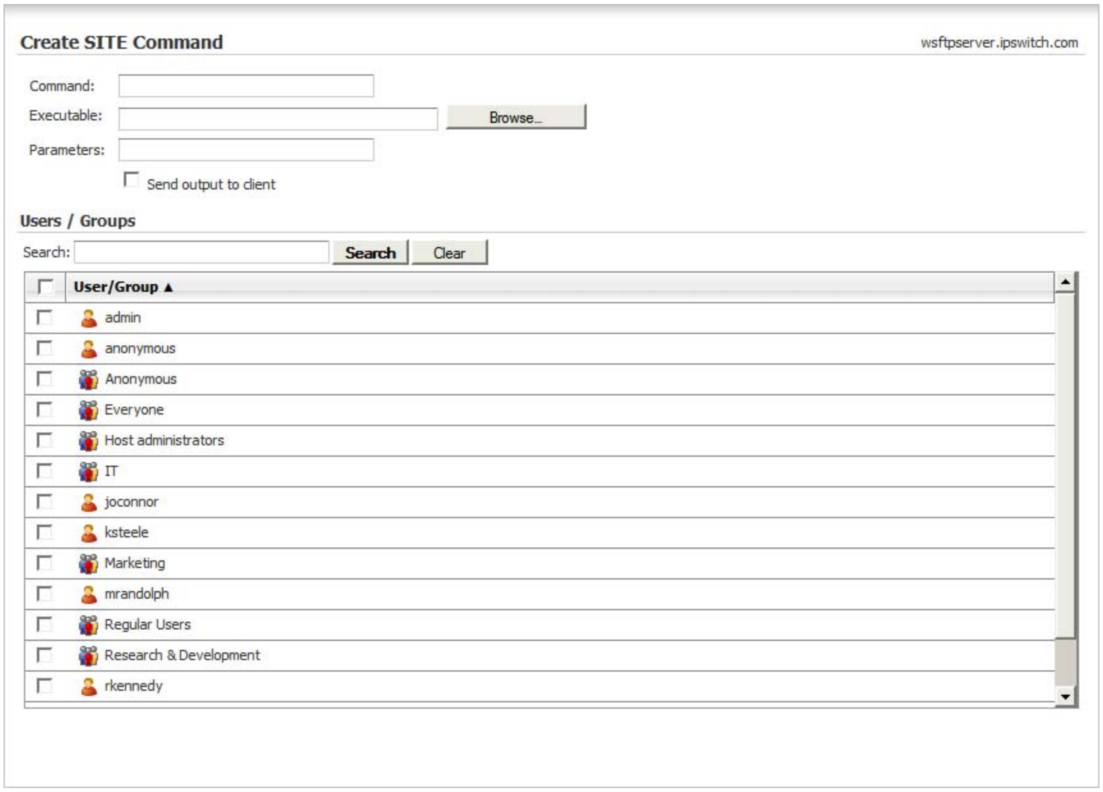
Creating a SITE command

SITE commands are configured per host. To have the same SITE command on multiple hosts, you must configure it for each host separately.

To create a new SITE command:

1 From the top menu, select **Host > SITE Commands**. The SITE Commands page opens.

2 Select **Create**. The Create Site Command page opens.



Create SITE Command

wsftpserver.ipswitch.com

Command:

Executable: Browse...

Parameters:

□ Send output to client

Users / Groups

Search: Search Clear

□	User/Group ▲
□	admin
□	anonymous
□	Anonymous
□	Everyone
□	Host administrators
□	IT
□	joconnor
□	ksteele
□	Marketing
□	mrandolph
□	Regular Users
□	Research & Development
□	rkennedy

3 Set the appropriate options.

- **Command**. Enter a name for this command. This is the name users must issue to use this command.
- **Executable**. eEnter or browse to select the executable or bat file that should be executed when a user issues this command.
- **Parameters**. Enter any arguments to pass to the executable when the command is triggered. 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. Spaces are delimiters for arguments, so a single argument with a space will be treated as two, unless the entire argument is in quotation marks.
- **Send output to client**. Select this option to return the output of the executable and parameters to the user's client.
- **Permissions list.** This list contains all of the users and user groups on this host. Select the users and groups you want to grant permission to execute this SITE command by clicking the checkbox next to user or user group name.

4 Click **Save**.

Securing SITE commands

SITE commands can be configured to allow remote users to perform almost any action that they could perform if they were logged into the server's operating system. As such, it is extremely important that users' permission to SITE commands be strictly controlled.

To specify access to a SITE Command:

1. From the top menu, select **Host > SITE Commands**. The SITE Commands page opens.
2. Click the hyperlinked name of the SITE command you want to edit. The Edit Site Command page opens.
3. Under **Permissions list**, select the users you want to grant permission to execute this SITE command.
   - To add a new user or group to this list, click **Add**.
   - To remove a user or group from this list, select the checkbox beside the user or group name, then click **Remove**.
4. Click **Save** to finalize the changes.

CHAPTER 5

Configuring Listeners

In This Chapter

About listeners

Listeners are a combination of an IP address and port number on which a server is configured to allow connections. You can configure as many listeners as you want, up to one per port on each available IP address.

There are two kinds of listeners: FTP and SSH. FTP listeners provide access to hosts using basic FTP and SSL (implicit and explicit). SSH listeners provide access to hosts using the SFTP protocol over SSH.

By default, WS_FTP Server creates three listeners:

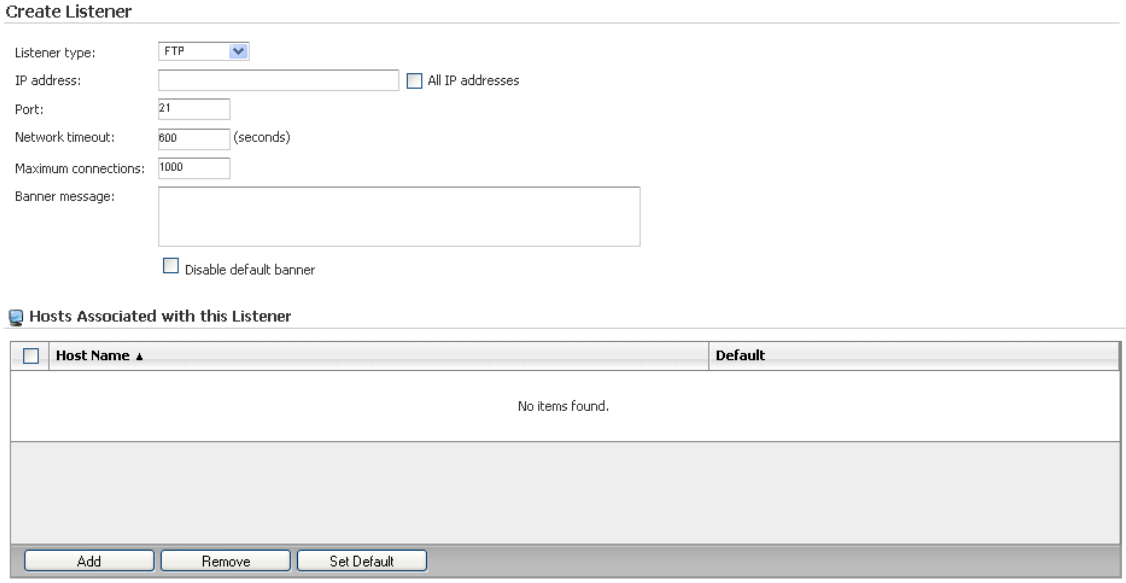
- **FTP (FTP and Explicit SSL)**. This listener accepts connections on all available IP addresses on the computer on port 21 for FTP connections.
- **SSH**. This listener accepts connections on all available IP addresses on the computer on port 22 for SSH connections.
- **FTP (Implicit SSL)**. This listeners accepts connections on all available IP addresses on the computer on port 990, and it requires SSL encryption.

Creating Listeners

To configure a new listener:

1 From the top menu, select **Server > Listeners**. The Listeners page opens.

2 Click **Create**. The Create Listener page opens.



Create Listener

Listener type:	FTP
IP address:	□ All IP addresses
Port:	21
Network timeout:	600 (seconds)
Maximum connections:	1000
Banner message:	
	□ Disable default banner

Hosts Associated with this Listener

□	Host Name ▲	Default

No items found.

How to get here

This page is used to create a new listener on the server.

- **Listener type**. Select the type of listener you are configuring.
  - **FTP.** Select this option to accept connections using the FTP protocol. FTP listeners are used for FTP and SSL connections.

Tip: To configure an SSL listener, select FTP as the Listener type. After saving the listener, you can configure specific SSL settings by editing the listener.

  - **SSH/SFTP**. Select this option to accept connections using the SFTP protocol over an SSH tunnel.

Note: Listener type is only available in Ipswitch WS_FTP Server with SSH. If you only have Ipswitch WS_FTP Server installed, this option does not appear.

- **IP address**. Enter the IP address on which you want the server to accept connections.
- **All IP addresses**. Select to enable this listener to accept connections on the specified port for all IP addresses configured on the server.

Note: If you have a listener accepting connections on all IP addresses, you cannot create other listeners using that same port.

- **Port** (21 by default for FTP listeners; 22 by default for SSH/SFTP listeners, if available). Enter the port on which you want the server to accept connections.

- **Network timeout** (600 by default). Enter the number of seconds after which the client is disconnected if the server has not received a command or any data from the client.
- **Data channel timeout** (60 by default). Enter the number of seconds after which the client is disconnected that the server will abandon the transfer of an uploaded file and release the lock from any partially uploaded file.
- **Maximum connections** (1000 by default). Enter the total number of connections you want this listener to accept. This number limits connections to the server through this listener for all hosts associated with this listener. All connections beyond the limit are immediately terminated.
- **Banner message**. Enter the message you want the server to send to a user upon successful connection, before the user logs on. You can use this message to tell users about the organization of your host, any rules, times of operation, mirror sites, or contact information. You can use *message variables* (on page 44) to provide information to the user (for example, that the host has reached the maximum number of concurrent users).

  Disable default banner. Select this option to prevent the server from sending the default banner message, which identifies the server as Ipswitch WS_FTP Server.

Note: In addition to the Banner message, you can set Welcome and Exit messages that are displayed when a client authenticates and disconnects, respectively. Welcome and Exit messages only apply to FTP listeners.

- **Enable Secure Copy (SCP2)**. Select this option to allow an SCP client to connect to the SSH server. This setting applies only to SSH listeners. For more information, see *Using SCP* (on page 119).

Hosts Associated with this Listener

This list displays the hosts that use this listener. From this list, you can perform the following actions:

- **Associate a host with this listener**. Select **Add** to associate an existing host with this listener.
- **Remove a host from this listener**. Select a host, then select **Remove** to break the association between the host and this listener. After removing a host, you can no longer negotiate connections to the host on this listener.
- **Define a default host for this listener**. Select a host from the list and then click **Set Default** to define that host as the default host on this listener. Any users who authenticate without providing a host are assumed to be accessing this host. If the list of hosts is empty, you must click **Add** and select a host to add to the list before you can select a default host.

Note: SSL and SSH options cannot be configured while creating a listener. To configure SSH or SSL, you must edit the listener after it is saved.

Configuring listeners for SSH

For a host to be accessible via SSH, clients must connect to the host using the IP address and port of an SSH listener.

To configure a host to be accessible via SSH:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.
3. Under **Hosts Associated with this Listener**, verify that the host you want to be accessible via SSH is listed. If it is not, add the host before proceeding to the next step. Fore more information, see *Associating a Host with a Listener* (on page 23).
4. By default, the SSH listener uses a SSH host key that WS_FTP Server generates when you install the program. This key is unique to your server. For information on how to change this key, see *Selecting an SSH Host Key* (on page 114).

Configuring listeners for SSL

For a host to be accessible via SSL, clients must connect to the host using the IP address and port of an SSL-enabled listener.

To configure a host to be accessible via SSL:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.

> **Note**: Since SSL can be configured only on FTP listeners, make sure that you select a listener that displays FTP in the Server type column.

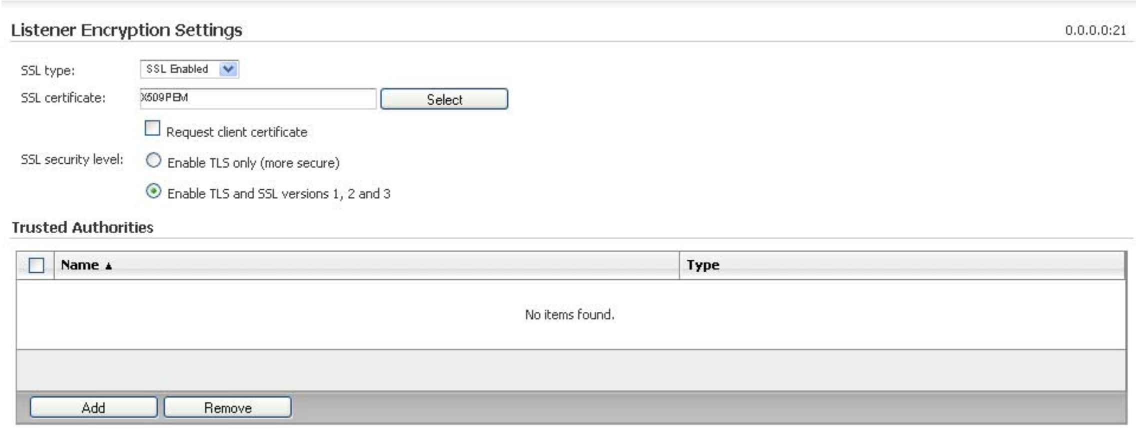
3. Under **Hosts Associated with this Listener**, verify that the host you want to be accessible via SSL is listed. If it is not, add the host before proceeding to the next step. For more information, see *Associating a Host with a Listener* (on page 23).
4. Verify that the listener has the **SSL type** set to **SSL enabled** or **Implicit SSL**.
5. Next, specify the SSL certificate for the listener to use to negotiate SSL connections.

To specify an SSL certificate:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.

> **Note**: Since SSL can be configured only on FTP listeners, make sure that you select a listener that displays FTP in the Server type column.

3 Under **Encryption Options**, click **Edit SSL Settings**. The Listener Encryption Settings page opens.



Listener Encryption Settings 0.0.0.0:21

SSL type: SSL Enabled

SSL certificate: X509PEM

□ Request client certificate

SSL security level:
○ Enable TLS only (more secure)
● Enable TLS and SSL versions 1, 2 and 3

Trusted Authorities

□	Name ▲	Type
	No items found.	

4 Verify that the certificate listed in **SSL certificate** is the certificate you want to use. If no certificate is listed, or if a certificate other than the one you want to use is listed, click **Select**. The Select SSL Certificate page opens. From this page, you can select, create or import a certificate to use.

Caution: The certificate applied to the listener is the SSL certificate used for all hosts assigned to this listener when a client attempts an SSL connection. Changing the certificate listed in SSL certificate affects all hosts assigned to this listener.

In addition to the SSL settings configured on the listener, there are several options that are host-specific. To edit these options, select **Host > Host Settings > SSL Settings** from the top menu.

CHAPTER 6

Managing User Accounts

In This Chapter

How user accounts work

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

If you selected the Microsoft Windows, Ipswitch IMail Server, or external (ODBC) user databases, you may already have a list of users for the host. In this case, you cannot use the WS_FTP Server Manager to add or delete users, but you can set additional user options in the Host Details page in the User Settings section.

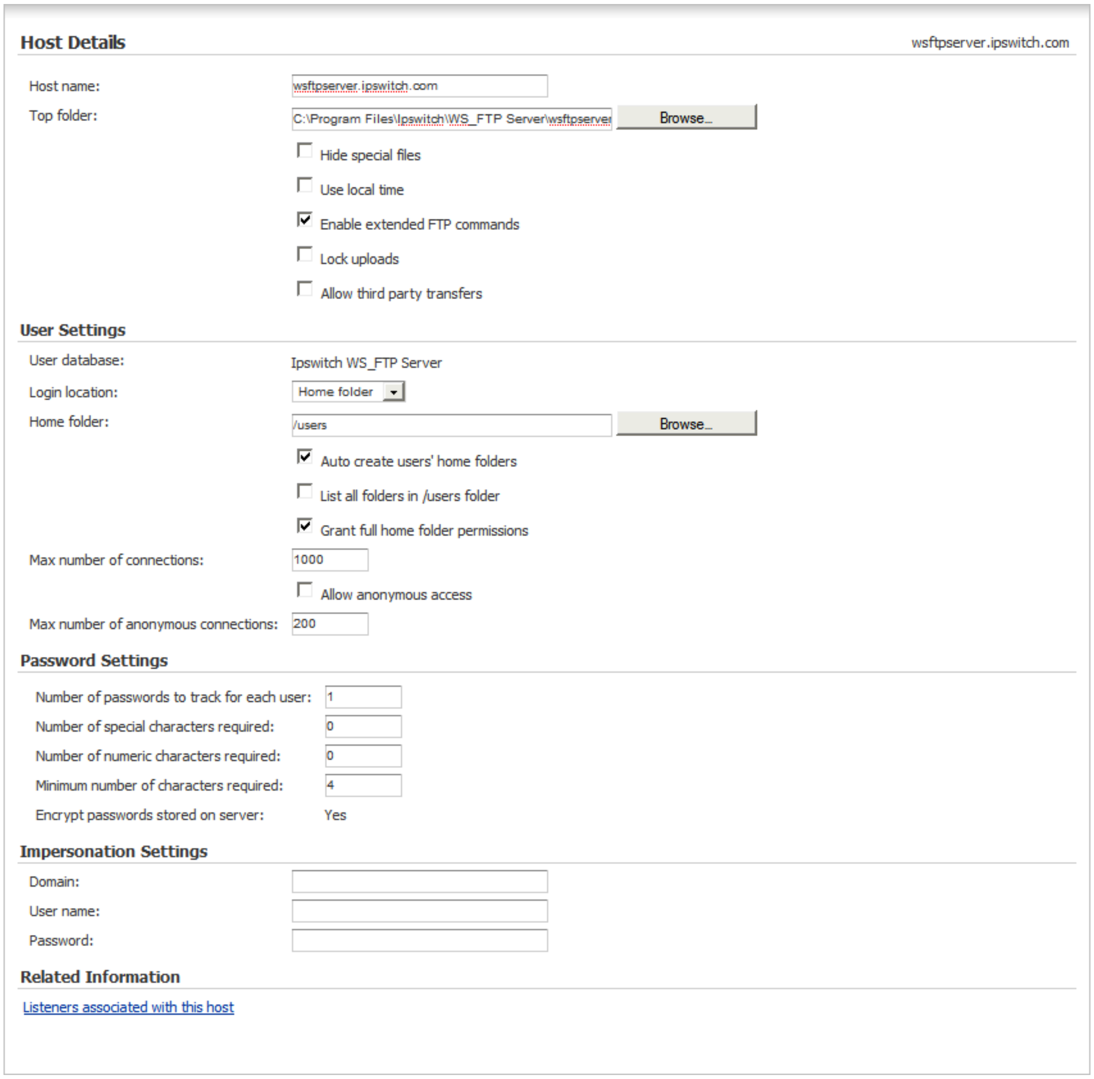
If you are using a user database other than the WS_FTP Server internal database, you must use the other database's method to add or remove user.

Setting user options for hosts

You can specify the user database type, home folder that opens when users log in, maximum number of connections, maximum number of anonymous connections, and password settings for each user.

To select user settings:

1 From the top menu, select **Host > Host Details**. The Host Details page opens.



Host Details wsftpserver.ipswitch.com

Host name: wsftpserver.ipswitch.com

Top folder: C:\Program Files\Ipswitch\WS_FTP Server\wsftpserver [Browse...]

☐ Hide special files

☐ Use local time

☑ Enable extended FTP commands

☐ Lock uploads

☐ Allow third party transfers

User Settings

User database: Ipswitch WS_FTP Server

Login location: Home folder

Home folder: /users [Browse...]

☑ Auto create users' home folders

☐ List all folders in /users folder

☑ Grant full home folder permissions

Max number of connections: 1000

☐ Allow anonymous access

Max number of anonymous connections: 200

Password Settings

Number of passwords to track for each user: 1

Number of special characters required: 0

Number of numeric characters required: 0

Minimum number of characters required: 4

Encrypt passwords stored on server: Yes

Impersonation Settings

Domain:

User name:

Password:

Related Information

Listeners associated with this host

2 Set the appropriate options.

- **Login location**. Select the folder that should be displayed to users after successfully logging in.
  - **Home folder**. Users are shown their home folder after successfully logging in.
  - **Root folder**. Users are shown the root folder after successfully logging in.
- **Home folder**. Enter the path of the user's home folder.
- **Auto-create users' home folders** (selected by default). If selected, user folders are automatically created when a new user is added to this host.

Caution: If **Auto-create user folders** is cleared, users will be connected to the root directory even if **Login location** is set to Home folder. Administrators must manually create a home folder for the user before they will be able to log in to it. If the users are logged in to the root directory because they have no home folder, and the user is locked to his home folder, the user will not be able to see or do anything once logged on.

- **List all folders in /users folder**. If selected, all users can view all folders in the /users folder. If cleared, all folders except the user's home folder are hidden.

Note: System and host administrators can always see all folders in the /users folder.

- **Grant full home folder permissions** when creating user (selected by default). When selected, new users are granted full permissions to their user home folders when they are created.
- **Max number of connections** (1000 by default). Enter the total number of users who can be logged in at any given time. This includes both anonymous and authenticated users.
- **Allow anonymous access**. If selected, anonymous users can access the host. If cleared, users must authenticate with valid credentials before they can gain access to the host.
- **Max number of anonymous connections** (200 by default). Enter the total number of anonymous users *per server* who can be logged in at any given time. "Per server" here means that each different server--FTP and SSH--can have this number of connections. (For instance, if you have both FTP and SSH server installed, and this number is set to 200, it will be possible to have 400 anonymous connections, provided that the Max number of connections is 400 or greater.)

3 Click **Save**.

You can configure a host on WS_FTP Server to require user passwords to meet minimum security standards.

To configure minimum standards for user passwords:

1 From the top menu, select **Host > Host Details**. The Host Details page opens.

2 Set the appropriate options.

- **Number of passwords to track for each user**. Enter the number of expired passwords to remember. If users are forced to change their passwords, they will not be allowed to use any of their former passwords that are remembered.
- **Number of special characters required**. Enter the number of non-alphanumeric characters that users are required to have in their passwords.
- **Number of numeric characters required**. Enter the number of numeric characters that users are required to have in their passwords.
- **Minimum number of characters required** (4 by default). Enter the minimum number of characters that users are required to have in their passwords.

- **Encrypt passwords stored on server** (selected by default). Select this option to encrypt all user passwords stored on the server. If you are using an external database for user authentication that is accessed by other applications, you may need to clear this option.

> **Caution**: **Encrypt passwords stored on server** cannot be changed after a host is created.

3 Click **Save**.

Changing user passwords

System administrators can change the password of any user on the server, and host administrators can change the password of any user on their host.

To change a user's password:

1 From the home page, select **Hosts**. The Hosts page opens.
2 Click the **Host name** of the host you want to open. The Host Details page opens.
3 From the left navigation menu, select **Users**. The Users page opens.
4 In the list of users, select a user by clicking on the linked **Username**. The Edit User page opens.
5 Click **Change Password**. The Change Password page opens.
6 Enter and confirm a new password for the user, then click **Save**.

Enabling disabled users from the command line

If a system administrator user account is disabled due to too many failed login attempts, you may find yourself in a situation where you cannot authenticate to the WS_FTP Server Manager. In this case, you can use iftpaddu.exe command line utility to enable the user account.

To enable a disabled system administrator account using the command line utility:

1 Log on to the operating system of the computer where WS_FTP Server is installed.
2 Select **Start > Run**. The Run dialog appears.
3 Enter `cmd.exe` and click **OK**. The command line window opens.
4 Enter `iftpaddu.exe -mod -h <host name> -u <user name> +active`, where `<user name>` is the name of the user you want to restore and `<host name>` is the name of the host to which the user belongs.
5 Press the Enter key. A message appears indicating whether or not your command succeeded. If the command succeeded, you can log on to the WS_FTP Server Manager using a Web browser.

Resetting a user's failed login count

If you have failed login rules configured to disable an account after a certain number of failed attempts to authenticate, you may need to reset a user account's failed login count to reactive the account.

To reset a user's failed login count:

1. From the top menu, select **Server > Hosts**. The Hosts page opens.
2. Select a host from the list by clicking on the hyperlinked host name. The Host Details page opens.
3. Select **Users** from the left navigation menu. The Users page opens.
4. Select a user from the list by clicking on the hyperlinked username. The Edit User page opens.
5. Click the **Reset** button next to **Failed login count**.

Understanding administrator privileges

Host administrators and system administrators have different permissions in the WS_FTP Server Manager and when connected using a file transfer client. The table below explains the permissions each type of administrators has in each case.

Connecting via:	Host Administrator	Server Administrator
WS_FTP Server Manager	Full control over the host to which they belong, except the following: ▪ Host administrators of hosts using an alternative user database cannot configure the user database plugin. ▪ When creating virtual folders, host administrators cannot see any folders that are not located below the top folder of the host. When viewing virtual folders that point to a physical folder that is not located below the top folder of the host, the host administrator cannot modify the location of the physical folder to which the virtual folder points. ▪ When creating or modifying rules, host administrators cannot configure or modify any executables that are run when the rule is triggered. ▪ Host administrators cannot create or delete SITE commands, but can manage which users can trigger SITE commands created by a system administrator. No control over server-wide settings, except the following: ▪ Host administrators can use the Log Viewer to view logs for their host only. ▪ Host administrators can create, manage and delete notifications.	Full control over all hosts on the server. Full control over all server-wide settings.
File Transfer Client	Full permissions to all folders on the host to which the user account belongs.	Full permissions to all folders on the host to which the user account belongs.

Granting administrative privileges

You can grant administrative privileges to any user on any host.

To grant administrative privileges:

1 From the top menu, select **Host > Users**. The Users page opens.

In the list of users, select a user by clicking on the linked **Username**. The Edit User page opens.

2 In **User type**, select an administrator type:

- **Host administrator**. Select this option to grant this user host administrator privileges. Host administrators have full permissions to all folders on the host and can manage the host through the Ipswitch Web Admin.
- **System administrator**. Select this option to grant this user system administrator privileges. System administrators have full permissions to all folders on the hosts and can manage all aspects of all hosts through the Ipswitch Web Admin.

3 Click **Save**.

Creating user accounts

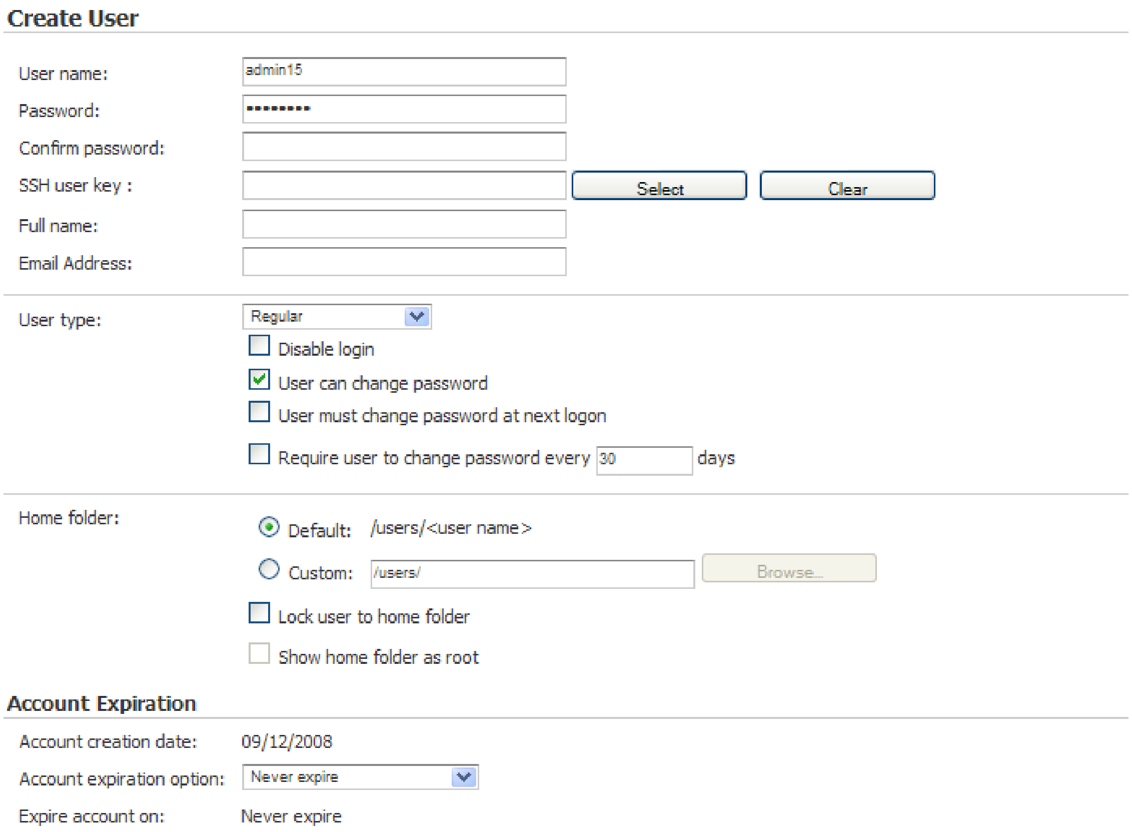
After you have configured a host, you can add users to the host.

Note: If you are using a Microsoft Windows user database, Ipswitch IMail database, or some ODBC databases, you must use the respective database management tools to create and delete users. After the user is created, you can modify other settings in WS_FTP Server Manager.

To create a new user on a host:

1 From the menu, select **Hosts > Users**. The Users page opens.

2 Click **Create**. The Create User page opens.



Create User

User name: admin15

Password: ••••••••

Confirm password:

SSH user key :

Full name:

Email Address:

User type: Regular

□ Disable login

☑ User can change password

□ User must change password at next logon

□ Require user to change password every 30 days

Home folder:

● Default: /users/<user name>

○ Custom: /users/

□ Lock user to home folder

□ Show home folder as root

Account Expiration

Account creation date: 09/12/2008

Account expiration option: Never expire

Expire account on: Never expire

3 Enter the appropriate information for each of the fields.

- **Username**. Enter the username for this user. The username is provided to authenticate with the server.
- **Password**. Enter a password for this user.
- **Confirm password**. Re-enter the password for this user.
- **SSH user key**. SSH user host keys are one of the methods used by SSH listeners to authenticate users. Click **Select** to select, import or create an SSH user host key. To clear the selected key, click **Clear**.
- **Full name**. Enter the full name of the user if desired.
- **Email address**. Enter a valid email address for this user. This email address can be referenced in *notifications* (on page 94) by using the notification variable: %emailaddress
- **User type**. Select a user type.
  - **Regular**. Select this option to make this user a regular user.
  - **Anonymous**. Select this option to designate this user as an anonymous user.
  - **Host administrator**. Select this option to grant this user host administrator privileges. Host administrators have full permissions to all folders on the host and can manage the host through the Ipswitch Web Admin.

  - **System administrator**. Select this option to grant this user system administrator privileges. System administrators have full permissions to all folders on the hosts and can manage all aspects of all hosts through the Ipswitch Web Admin.

- **Disable login**. Select this option to disable this user account. If this option is selected, this user cannot log in to the server.
- **User can change password**. Select this option to allow this user to change his or her password. This option is not available on hosts that use Microsoft Windows, Microsoft Active Directory or Ipswitch IMail user databases.
- **User must change password at next logon**. Select this option to force the user to change his or her password the next time he logs in to the FTP server or the SSH server. This option is disabled by default. This option is available only if **User can change password** is enabled.

  For the FTP Server:

  When the user attempts to log in from the client, the FTP server returns:

  560 Password expired, use 'pass oldpassword newpassword'

  The user must then log in and, in the Password box, enter the old password and the new password, separated by a space: '**oldpassword newpassword**'

  The password is reset to the new password.

  For the SSH Server:

  The SSH Server issues an SSH_MSG_USERAUTH_PASSWD_CHANGEREQ packet to the client. In response to this message, the client should prompt the user for the new password.

  In either case (FTP or SSH), the server ensures that the new password meets criteria for any password rules for the host. If the password is accepted, the server resets the **User must change password at next logon** option.
- **Require user to change password every x number of days**. When this option is selected, users are required to change their password at least once during the time frame specified. If a user fails to change his password during the allotted time, he cannot authenticate to the server. If this option is selected, the number of days remaining before this user must change his password is listed below this field. This option is available only if **User can change password** is enabled.
- **Home folder**. Select whether you want this user's home folder to be created in the default location or a custom location. If you select **Custom**, enter the full path to the folder or click Browse to locate it.
- **Lock user to home folder**. Select this option to prevent this user from navigating outside their home folder.
- **Show home folder as root.** This option can be used only if **Lock user to home** folder is selected. If this option is selected, the user's home folder will be displayed to the user as the root of the FTP directory's path. (For instance, if the user chooses the following directory: /Users/ThisUsersHome/OneOfMyFolders, if this option is selected, the user will only see /OneOfMyFolders.)

System and host administrators can always see the full path to the user's home folder.

The log file will always show the full path to the user's home folder.

Notifications will display the full path to system and host administrators, and if **Show home folder as root** is selected, will not display the full path to a user.

To select the home folder options for all users on the host, use the *iftpaddu command line* (on page 72) options (+lock for **Lock user to home folder** and +root for **Show home folder as root**). The iftpaddu command supports the WS_FTP Server user database, but cannot be used with external user databases.

- **Account creation date**. Today's date is displayed.
- **Account expiration option**. This option is used to specify when and how a user account should expire.
  - **Never expire**. Select this option if you do not want the user account to expire.
  - **Expire on the expiration date**. This option expires the account on the specified date.
- **Expire account on**. If you have selected **Expire on the expiration date**, a date field appears here. Using the calendar (📅), select the date after which you want this account to expire.

4 Click **Save**.

Note: If you want to create a user account on a host other than the current host, you can switch hosts by selecting **Host > Current Host > Change Hosts** from the menu. Select the host you want to create a user account for, then follow the steps as listed above.

Setting users' home folders

Users have full permissions to their home folders. Even if users do not log in to their home folders, you can specify a home folder for the user.

To set a user's home folder:

1 From the top menu, select **Host > Users**. The Users page opens.

2 In the list of users, select a user by clicking on the linked **Username**. The Edit User page opens.

3 In **Home folder**, enter the full path to a user's home folder (relative from the file server root) or click **Browse** to locate one.

4 Click **Save**.

Note: If you want to keep a user from navigating outside their home folder, select the **Lock user to home folder** option. If you want to hide the path to the user's home folder, as displayed in the FTP client, select **Show home folder as root**.

Renaming a user account

System administrators can change the name of any user on the server, and host administrators can rename any user on their host.

To rename a user:

1. From the home page, select **Hosts**. The Hosts page opens.
2. Click the **Host name** of the host you want to open. The Host Settings page opens.
3. From the left navigation menu on the left, select **Users**. The Users page opens.
4. In the list of users, select a user by clicking on the linked **Username**. The Edit User page opens.
5. In **Username**, enter new name for the user.
6. Click **Save**.

Deleting user accounts

You can delete a user from the current host. When you delete a user, the user is removed from all groups and rules, and you can optionally choose to delete the files and folders in the user's home folder.

To delete a user from the current host:

1. From the top menu, select **Host > Users**. The Users page opens.
2. Select the checkbox next to the name of the user you want to delete.
3. Click **Delete.** The Delete Confirmation page opens.
4. If you want to remove the user's home folder (and all files and folders contained within it), select **Delete the home folder and all subfolders for the following user(s)**.

Note: When you delete a user's home folder, it is moved to the Windows Recycling Bin. If you delete something in error, you can restore it from the Recycling Bin.

5. To delete the user, click **Delete.** The user is deleted from the server.

Note: When the user account is deleted, the user is removed from all groups and rules. If you recreate the user, you must manually add the user to each group and rule to return to the state before the user was deleted.

Disabling user accounts

You can disable a user account without deleting the account, so that the account can be easily re-enabled without creating a new account for the user.

To disable a user account:

1 From the top menu, select **Host > Users**. The Users page opens.

2 In the **Username** list, click the user you want to disable. The Edit User page opens.

3 Click **Disable login**.

4 Click **Save**.

Managing users from the command line

You can add, modify or delete users on a host using the user command line utility `iftpaddu.exe`.

Important: You cannot use this utility to add users to a host that uses a Microsoft Windows user database, Ipswitch IMail database, or External ODBC database.

To run the Add User Utility:

1 From the Windows desktop, select **Start > Run**. The Run dialog appears.

2 Enter `cmd.exe` and click **OK**.

3 Change the directory to the WS_FTP Server directory. For a default installation, this should be `C:\Program Files\Ipswitch\WS_FTP Server\`.

4 For a list of command options, enter `iftpaddu /?`.

Basic Command Syntax

The basic syntax for adding, modifying and removing a user, as well as the syntax to change permissions for all users on the server at once, are indicated below.

Adding a User	`iftpaddu -u userid -h hostname [-n "full name"] [-p password] [options]`
Modifying a User	`iftpaddu -mod -u userid -h hostname [-n "full name"] [-p password] [options]`
Deleting a User	`iftpaddu -kill -u userid -h hostname`
Modifying All Users on a Host	`iftpaddu -all -h hostname [options]`

Note: All arguments are case-sensitive and must be supplied as lower case.

Note:When using the +/-root and +/-lock command line switches, the command lock switch must precede the root switch, otherwise the the command line will fail.

Arguments	When to use
-add	Use when you want to add a new user. If -add, - mod, -kill or -all are not specified, -add is assumed.
-mod	Use when you want to modify an existing user.
-kill	Use to delete a user. You must also specify a username using -u userid.
-all	This argument can be used in conjunction with the active, chgpass, sysadm, hostadm, lock and g (group) arguments to modify all users on the server.
-f filename	Specifies an external file from which to read additional arguments.
-u username	Adds a username, where username the user you want to add. This is the only required argument. Only one username can be added in a single command.
-h hostname	Specifies the user's host, where hostname is the name of the file transfer host. The primary FTP host is used if no host is specified.
-n "full name"	Specifies the *full name* of the user. The full name must be enclosed in quotes if it contains any spaces.
-p password	Specifies the password for a user. If you omit this argument when adding a user, the user's password defaults to "password."
+g groupname	Adds the user to the specified group.
-g groupname	Removes the user from the specified group.
-s	Sets the quota space for the user. (The minimum to enter is 1024. Less than this number will enter a "0" as the quota space.)
-x	Sets the file count quota for the user.
+active	Enables the user to log on. This is the default setting when adding a new user.
-active	Disables the user account, so the user cannot log in.
+chgpass	Enables the user to change password from an FTP client.
-chgpass	Disables the user's ability to change password from an FTP client.
+forcechgpass	Forces the user to change the password on next login from an FTP client. For more information on functionality of this option, see the "User must change password at next logon" option in *Creating user accounts* (on page 67).
-forcechgpass	Disables the force change password option.
+hostadm	Grants the user Host Administrator permissions.
-hostadm	Removes Host Administrator permissions from the user.
-list	Outputs a list of the commands needed to generate all of the users on a host in a format that can be used with the -f argument. If -u is specified, only the commands needed to generate the specified user are output. Examples: iftpaddu -u admin -h serverhostname -list iftpaddu -h serverhostname -list

`+lock`	Locks a user to their home folder.
`-lock`	Unlocks a user from their home folder.
`+root`	Displays the user home folder as root (/), effectively hiding the path to the location. To set this option, +lock must also be set for the user.
`-root`	Displays the full path to the user's home folder, for example /users/fredf
`+sysadm`	Grants the user System Administrator permissions.
`-sysadm`	Removes System Administrator permissions from the user.

CHAPTER 7

Managing User Groups

In This Chapter

How user groups work

You can create custom user groups for the current host. For example, you may want to create groups for Marketing, Accounting, Product Development, and others so that users only have access to specified files and folders based on the group permissions.

Once you create a user group, you can manage permissions to folders, rules and SITE commands for the entire group as easily as you manage permissions for a single user.

Creating user groups

To create a user group:

1. From the top menu, select **Host > User Groups**. The User Groups page opens.
2. Select **Create**. The Create User Group page opens.
3. Set the appropriate options.
   - **Name**. Enter or modify the name assigned to the user group.
   - **Description**. Enter or modify the description. This description is for your reference only.
   - **Users.** This list shows all of the users who are members of this group. To add another user to the group, click **Add.** To remove a user or users from the group, select the checkbox next to the user's name, then click **Remove**.
4. Click **Save**.

Adding users to user groups

After you have created a user group, you can add additional users to it.

To add a user to a user group:

1 From the top menu, select **Host > User Groups**. The User Groups page opens.

2 Select the user group to which you want to a add a user. The Edit User Group page opens.

3 Click A**dd**. The Select User page opens.

4 Select a user from the **Username** list, then click **OK**. The user displays in the list.

5 Click **Save**.

Adding Users to a User Group

If you decide you do not want a user to be part of a group, you can remove that user from the group.

To remove a user from a user group:

1 From the top menu, select **Host > User Groups**. The User Groups page opens.

2 Select the name of the user group you want to edit. The Edit User Group page opens.

3 Select the checkbox next to the name of the user you want to remove from the group, then click **Remove**. The user is removed from the group.

4 Click **Save**.

Deleting user groups

You can delete a user group from the current host. When you delete a user group, all permissions assigned to that user group are lost; if a user has permission to a folder by virtue of membership in a user group that is deleted, the user can no longer access that folder.

To delete a user from the current host:

1 From the top menu, select **Host > User Groups**. The User Groups page opens.

2 Select the checkbox next to the name of the user group you want to delete.

3 Click **Delete.** The Delete Confirmation page opens.

4 To delete the user group, click **Delete.** The user group is deleted from the server.

CHAPTER 8

Managing Folders and Files

In This Chapter

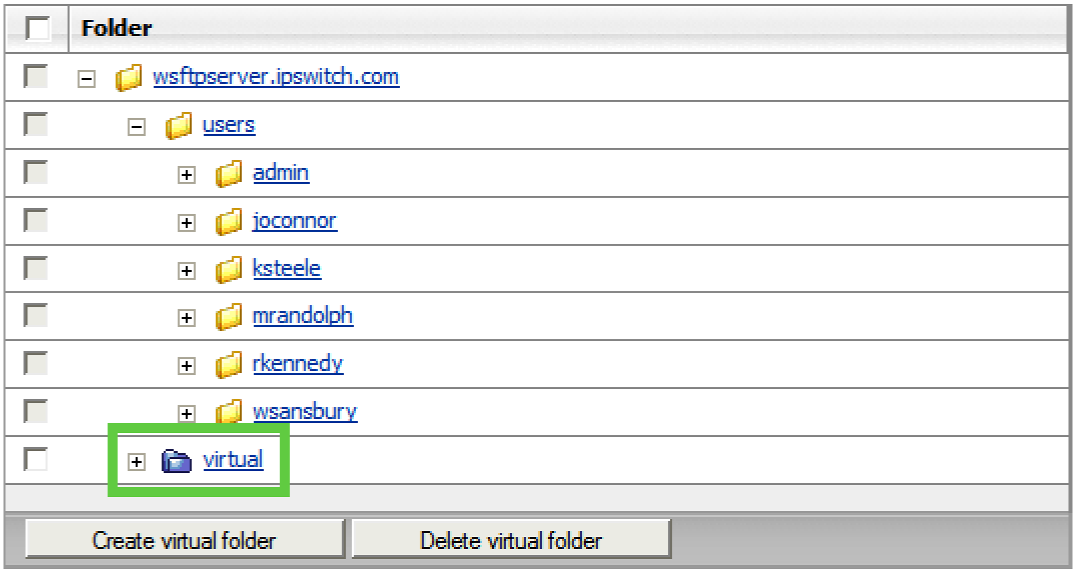
Managing folders

For the most part, folder management for the remote (FTP or SSH) file system is done through standard methods of managing folders on the operating system. With Windows Explorer, you can find the top folder of a host (for example `C:\Program Files\Ipswitch\WS_FTP Server\MyHost`) and create , rename, or delete folders under that host. For security reasons, you cannot manage physical folders remotely using WS_FTP Server Manager. You must log on to the server directly.

You can, however, manage virtual folders and folder permissions for all folders via WS_FTP Server Manager.

About user home folders

Each user has a designated home folder, which usually resides in the WS_FTP Server host's top directory, under /users.



When a user logs in using an FTP client, the client shows the home folder as the current directory, for example: /users/wsansbury

WS_FTP Server offers several options for setting up the user home folder, setting access, and determining how the home folder is displayed by the FTP client.

Host-level options, which apply to all users on the host, are set on the Host Details page (from the top menu, select **Host > Host Details**).

User-level options, which apply to an individual user, are set on the Edit Users page (from the top menu, select **Host > Users** and either select an existing user or create a new user).

About virtual folders

Virtual folders are folders that you create in the FTP or SFTP file system that can point to any folder on the server's physical file system. Normally, folders do not appear to users unless they are children of the top folder of the host. By creating a virtual folder, you can tell the server to include a folder that is not a child of the top folder of the host when returning the directory listing for that host.

For example, if you created a folder located at `C:\Documents\` that you wanted to include under a host named `MyHost` whose top folder is `C:\Program Files\Ipswitch\WS_FTP Server\MyHost`, you could create a virtual folder in the root of the MyHost host and point it to `C:\Documents\`.

Creating, editing, and deleting virtual folders

Virtual folders are folders that you create in the FTP or SFTP file system that can point to any folder on the server's physical file system. After you create a virtual folder, you can edit the folder to change most of the settings selected when you created the folder.

To create or edit a virtual folder:

1. From the top menu, select **Host > Folders**. The Folders page opens.
2. Click **Create Virtual Folder**. The Create Virtual Folder page opens.

   - OR -

   Click a hyperinked folder name. The Edit Folder page opens.
3. Set the appropriate options.
   - **Folder name**. Enter a name for the virtual folder. This name will identify the folder to users who log in to the server.
   - **Full path.** Select the physical location on the folder. You may either enter the path manually or select it by clicking Browse.

> **Tip:** You can use a network share anywhere that you specify a physical folder on the server. To do this, you must enter the UNC path to the shared folder. You must also specify an Impersonation account that allows the WS_FTP Server to access the UNC path. The Impersonation Settings are configured on the same page (Host Details page) as the Top folder.
> If using Microsoft IIS, you must also give permissions to the shared folder to the Windows user account under which your web server's `WSFTPSVR` folder is running. If that user cannot access the shared folder through the Windows explorer, you cannot access the folder via the WS_FTP Server Manager.

   - **Only viewable with 40-bit SSL or higher**. Select this option to make this folder viewable via FTP only if the user has logged in using 40-bit SSL or higher.
   - **Only viewable with 128-bit SSL or higher**. Select this option to make this folder viewable via FTP only if the user has logged in using 128-bit SSL or higher.
   - **Virtual display location**. Select where you want this virtual folder to display.
     - **Not displayed**. Select this option to exclude this virtual folder from folder listings. Users who know virtual folder name can still access it by providing the folder name manually.
     - **Display at root**. Select this option to display this virtual folder as a subfolder of the server root folder.

- **Display in user**. Select this option to display this virtual folder as a subfolder of each user's home folder.

> ✓ **Important**: If you change the virtual display location of a virtual folder for which folder action rules are configured, you must update the folder action rules to use the new file path. If you do not do this, the folder action rules will not work.

4 Under **Permissions**, modify user permissions to the folder as needed.

5 Click **Save**.

Permissions

This section of the page displays and lets you manage user permissions for this folder. By default, users do not have permissions to new folders. To view or grant permissions to the folder, use the Permissions options.

> **Note**: Permission settings take effect the next time the user connects.

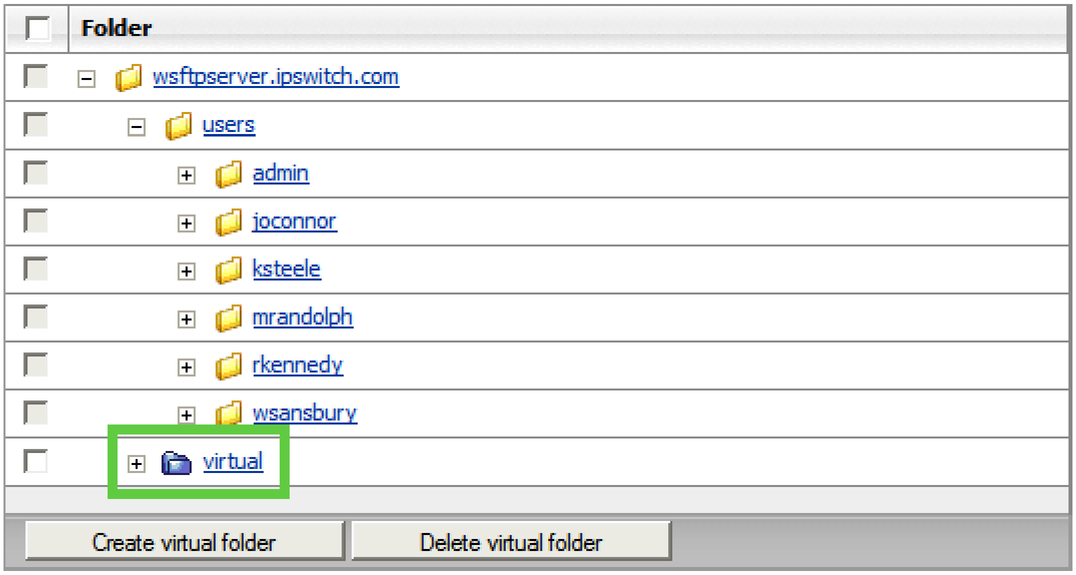
You can perform the following tasks related to user permissions on a folder:

- **Add permissions to this folder**. To add a permission to this folder, click **Add**.
- **View or modify permissions to this folder**. Click a user or user group name to open the Edit Permissions page. From there, you can view or modify the permission.
- **Remove permissions from this folder**. Select a permission by selecting the checkbox beside the user's or group's name. Select multiple permission by selecting multiple checkboxes. Once you have made your selection, click **Remove** to remove the selected permissions from this folder.

For more information, see *Using WS_FTP Server Manager to Manage Permissions* (on page 84).

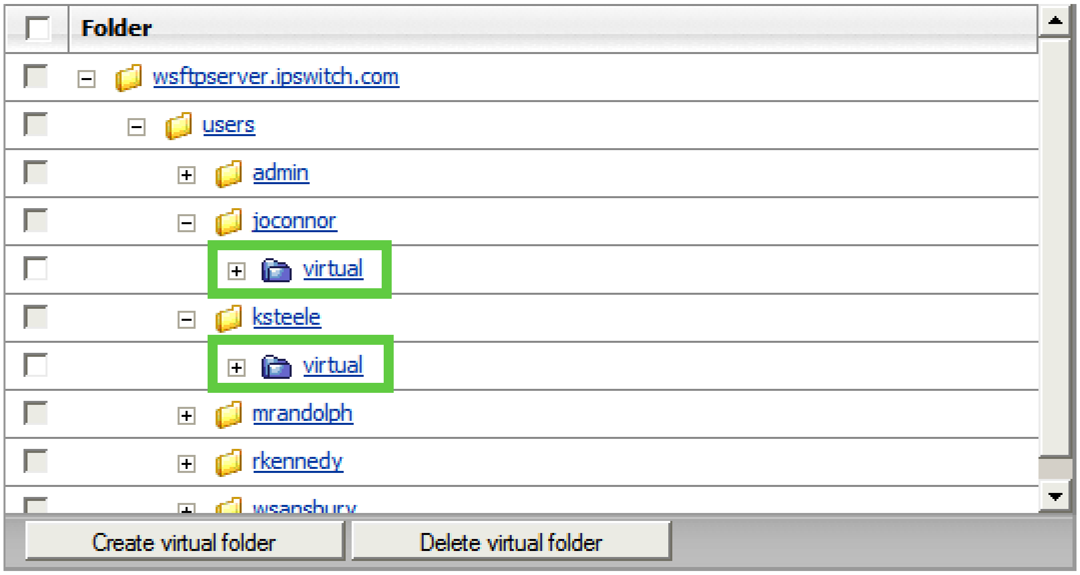
Understanding limitations of virtual folders

A virtual folder can be created as a subfolder of the root folder



- OR -

as a subfolder of every user's home folder



- If a user's home folder is set to a custom location (outside of the /users folder under the top folder of the host), then virtual folders configured to display in a users' home folders are not displayed.
- A virtual folder cannot contain another virtual folder. If a file structure is created where one virtual folder could conceivably contain another, the second virtual folder is not displayed.

- If the physical folder the virtual folder references is changed or deleted, the virtual folder is still displayed to users, but it cannot be accessed. Users attempting to access a virtual folder that points to a nonexistant physical folder receive the following error message: `550 CWD virtual: access denied`.
- If you use the WS_FTP Server Web Transfer Module, the physical folder that a virtual folder points to needs to have the WS_FTP Server Web Transfer Module Impersonation User assigned to it, with full permissions (as would be the case with a conventional, physical folder).

Managing folder permissions

After you have created folders on the file transfer host, you need to specify appropriate permissions for users or groups of users for each folder or virtual folder on an file transfer host. You can manage folder permissions from the:

- WS_FTP Server Manager Folder Permission page to manage WS_FTP Server database, Microsoft Windows database, Ipswitch IMail Server database, or an ODBC database.

  - OR -
- Windows file/folder Security Tab to manage a Microsoft Windows Database.

Understanding folder permissions

Folder permissions govern which users and group can perform various actions on a folder or its contents.

There are two main types of permissions:

- **Permit**. Permit permissions grant users or groups access to the folder on which the permission is applied.
- **Deny**. Deny permissions are used when you want to specifically deny a user or group permission to a folder. Deny permissions take precendence over all other permissions, so a deny permission guarantees that a user cannot perform the action indicated in the permission.

For each permission, you can also indicate which actions you want to permit or deny:

- **Read**. This option refers to downloading files from the server.
- **List**. This option refers to retrieving a folder listing, which shows the files in the folder, from the server.
- **Write**. This option refers to uploading files to the server.
- **Delete**. This option refers to deleting files or folders from the server.
- **Rename**. This option refers to changing the name of a file or folder already on the server.
- **Create folder**. This option refers to creating a new folder under the folder where the permission is set.

Finally, you can also choose to have a permission apply only to files that match a specified **file mask**. To match all files, enter `*`.

For each permission, you can choose to have the option propagate down to all subfolders of the folder where the permission is set by selecting **Include subfolders**.

User and group permissions are aggregated. WS_FTP Server evaluates permit permissions first, then deny permissions to determine the actual permissions granted.

For example, if a user has the following permissions set

- Permit Read and List permission propagated from a parent folder
- Permit Write permission set on the current folder
- Deny Read permission set on the current folder

he or she can List and Write on the current folder.

Permissions and administrators

By default, host and system administrators are granted full permissions to all folders on the host to which they belong. However, host and system administrators are bound by deny permissions. It is possible to deny them access to any folder by creating a deny permission on that folder.

Permissions and users' home folders

When a user is created, WS_FTP Server automatically generates a permit permission granting the user full permissions to his or her home folder.

Permissions and virtual folders

Permissions set to include subfolders on a parent folder of a virtual folder are not applied to the virtual folder or any folders underneath it. Virtual folders do not inherit permissions from parent folders.

How to stop a propagated permission

When a permission set on a parent folder is propagated to a child folder and you want to remove or change the permission on the child folder, you can add another permission with the same mask at that level. For example, if the parent folder grants a user Read, List and Write permissions, and you want to remove Write permissions on the child folder, you can enter another permission on the child that specifies only Read and List for the User. This removes the Write permission.

Note: If a folder is governed by permissions marked include in subfolders on a parent folder, the permissions are not displayed on the child folder. Permissions that are included in subfolders are displayed only at the parent folder level.

How WS_FTP Server determines permissions

WS_FTP Server uses this method to determine if a user has permission to complete an action:

- WS_FTP Server checks its internal permissions first.
  - If the user does not have permission, the server returns a permissions error.
  - If the user has permission to complete the action in the WS_FTP Server internal permissions, the Windows permissions are checked.
    - If the user does not have permission, the server returns a permissions error.
    - If the user has permission, the action is completed.

Note: To use Windows file permissions exclusively, we recommend granting the Everyone group full permission to the root of your host and propagate the permissions to subfolders. If the host includes any configured virtual folders, grant the Everyone group full permission to each virtual folder and propagate the permissions to subfolders.

You can manage user/group folder permissions from the Folder Permission page.

To grant or change permissions to a folder for a user or group:

1. From the top menu, select **Host > Folders**. The Folders page opens.
2. Click the hyperlinked name of the folder you want to open. The Edit Folder page opens.
3. In the User/Group list, click the hyperlinked name of the user or group for which you want to change permissions. The Folder Permission page opens.
4. Set the appropriate options.
   - **User** or **Group**. The user or group to which this permission applies is listed here.
   - **File mask**. Enter a file mask. Permissions are granted only to files that match the file mask.
   - **Permission Type**:
     - **Allow**. Select this option to permit access to the following permission options.
     - **Deny**. Select this option to not permit access to the following permission options.
   - **Select/Deselect All**. Select to grant full permissions. Clear to remove all permissions.
   - **Read**. Select this option to grant permissions to read files.
   - **List**. Select this option to grant permission to list the files in the folder.
   - **Write**. Select this option to grant permission to add files or modify files to the folder.
   - **Delete**. Select this option to grant permission to delete files from the folder.
   - **Rename**. Select this option to grant permission to rename files or folders in the folder.

- **Create folder**. Select this option to grant permission to create subfolders in the folder.
- **Include subfolders**. Select this option to extend the permissions assigned to this folder to all folders beneath it.

5 Click **Save**.

Using Windows permissions

For hosts that use the Microsoft Windows or Microsoft Active Directory user database, you can manage user/group folder permissions from the Windows file/folder Security Tab.

> **Important:** WS_FTP Server uses the highest permission restriction level to determine permission priority. For example, you can restrict users from areas that Windows permissions would allow by setting stronger permissions on the folder in the WS_FTP Server Manager.

To grant or change user/group folder permissions:

1 Double-click the **My Computer** icon on the desktop, then navigate to the folder on which you want to set permissions.

2 Right-click on the folder name to display a context-sensitive menu for the folder, and select **Properties**. The Properties dialog box opens.

3 Click the **Security** tab to display a security-related properties page for this folder.

4 Set the folder permissions for groups and users as required.

Checking file integrity

WS_FTP Server includes support for file integrity checking. File integrity checking works by using an algorithm to calculate a unique number based on the contents of a file. When the same algorithm is run on the client computer before transferring the file and on the server computer after transferring the file, the results of the algorithm's computation can be compared to detect any corruption that may have occured during the transfer. If the transfer succeeded without corruption, the two values are identical.

The table below indicates the algorithms supported during FTP and SSH/SFTP connections as well as the command the client must issue to check the integrity of a file using one of the supported algorithms.

Algorithm	Client command	FTP	SSH/SFTP
SHA512	XSHA512	✓	✓
SHA256	XSHA256	✓	✓
SHA1	XSHA1	✓	✓
CRC32	XCRC	✓	

MD5	XMD5	✓	✓

An algorithm must be supported by both the server and the client to be used in file transfer checking. To determine which algorithms are supported by your file transfer client, consult its user documentation.

Note: For file integrity checking to work, the **Enable extended FTP commands** option must be enabled on the Host Details page of the host on which you want to support file integrity checking.

CHAPTER 9

Using Rules and Notifications

In This Chapter

Rules overview

The rules feature lets you define actions and notifications that are triggered by specific events. You can set up rules to prevent or allow actions (such as downloading a file or creating a folder) and to send notifications via email, pager or SMS. A rule can also execute a program on the server when the event occurs.

Rules can be applied to any combination of users and user groups.

There are four types of rules:

- **Failed Login Rules** can be configured to trigger a notification and/or disable a user account after the specified number of failed login attempts. For more information, see *Creating a Failed Login Rule* (on page 89).
- **Folder Action Rules** are used to trigger a notification when a user performs a specified folder or file action on the server, including uploading a file or folder, downloading a file or folder, renaming a file or folder, deleting a file or folder, or creating a folder. Folder action rules can be configured to execute when one of these events succeeds and/or fails. For more information, see *Creating Folder Action Rules* (on page 91).

- **Quota Limit Rules** are used to govern the amount of disk space and the number of files users can upload to their home folders. For more information, see *Creating a Quota Limit Rule* (on page 92).
- **Bandwidth Limits** are used to throttle the amount of bandwidth a connection can consume. For more information, see Creating a Bandwidth Limit.

About bandwidth limits

Bandwidth limits are used to throttle the amount of bandwidth a connection can consume. When a user who is governed by a bandwidth limit initiates a file transfer, the server transfers the file at a steady pace that will not exceed the specified bandwidth limit.

In situations where users share a server, bandwidth limits can be employed to ensure that no user or group can consume all of the bandwidth available to the server, which could effectively cause a denial of service for other users.

Since bandwidth limits cannot be exceeded, bandwidth limits are the only type of rule that does not trigger notifications.

Note: Bandwidth limits throttle bandwidth by connection, not by user. This means that a user with a client that supports making multiple simultaneous connections, such as Ipswitch WS_FTP Professional, can consume the full amount of bandwidth available, up to the bandwidth limit, for each connection.

Creating bandwidth limits

Bandwidth limits are used to govern the amount of bandwidth each connection to this host can consume.

To create a new Bandwidth Limit:

1. From the top menu, select **Server > Hosts**. The Hosts page opens.
2. Select a host from the list by clicking on the hyperlinked host name. The Host Details page opens.
3. Select **Bandwidth Limits** from the left navigation menu. The Bandwidth Limits page opens.
4. Click **Create**. The Create Bandwidth Limit page opens.
5. Enter the appropriate values for each field.

Name. Enter a name for this rule. This name is for your reference only and can include up to 256 characters.

Limit. Specify the maximum amount of bandwidth you want to allow users and groups to which this limit is applied to consume.

Users/Groups. This list contains all of the users and groups configured on the host. Select the checkboxes next to the users and groups to whom you want this rule to apply.

Note: Bandwidth limits throttle the amount of bandwidth each user can consume per connection. If a user makes multiple connections simultaneously, each connection is allowed the maximum bandwidth.

About failed login rules

Failed login rules can be configured to trigger a notification and/or disable a user account after the specified number of failed login attempts.

A failed login occurs each time someone attempts to log in with an invalid username or an incorrect password. The server keeps track of each failed login attempt for each user. If there is a failed login rule applied to a user, the server triggers the rule when the number of failed login attempts exceeds the maximum specified in the rule.

The server can differentiate between failed login attempts caused by invalid passwords and failed login attempts caused by a disabled account or an account with an expired password. You can specify which of these types of failed login attempts the server should use when deciding to send a notification.

Creating failed login rules

Failed login rules are configured per host. To have the same failed login rule on multiple hosts, you must configure it for each host.

To create a new failed login rule:

From the top menu, select **Server > Hosts**. The Hosts page opens.

1. Select a host from the list by clicking on the hyperlinked host name. The Host Details page opens.
2. Select **Failed Login Rules** from the left navigation menu. The Failed Login Rules page opens.
3. Click **Create**. The Create Failed Login Rule page opens.
4. Set the appropriate options.
   - **Name**. Enter a name for this rule. This name is for your reference only and can include up to 256 characters.
   - **Failed login limit**. Specify the number of failed login attempts you want to allow before this rule is triggered.

- **Users/Groups**. This list contains all of the users and groups configured on the host. Select the checkboxes next to the users and groups to whom you want this rule to apply.
- **Rule Notifications**. This section is used to select one or more notifications to send and to specify the criteria that trigger the notifications for this rule. Notifications can be triggered when any of the following actions succeed or fail: failed attempts exceed allowed attempts, expired account, invalid user, password expired.
- **Send notifications when rule is triggered as a result of:**
  - **Failed attempts exceeding allowed attempts**. Select this option to send notifications hen a user fails to log in more times than is allowed.
  - **Expired account**. Select this option to send notifications when a user attempts to log in with an account that has expired.
  - **Invalid user**. Select this option to send notifications when someone attempts to log in using an incorrect user name.
  - **Password expired**. Select this option to send notifications when someone attempts to log in using a user account with an expired password.
- **Notification**. This list contains all of the notifications configured on the current host. Select the checkboxes beside the notifications you want to associate with this rule. To configure a new notification and associate it with this rule, click **Create**.
- **Executable** (optional). Enter the full path and file name of the program you want to run on the server when this rule is triggered.
- **Arguments** (optional). Enter the arguments to pass to the executable, if necessary.

Tip: You can specify *message notification variables* (on page 99) as arguments to pass to the executable.

Note: Executables are separate programs that WS_FTP Server runs for you under certain conditions. Depending on the volume of traffic on your server and the number of times an executable is run, these programs may consume considerable resources and may cause performance issues.

5 Click **Save**.

About folder action rules

Folder action rules are used to trigger a notification when a user performs a specified folder or file action on the server. The rules can be configured to execute when the following events are attempted, succeed, or fail:

- uploading a file or folder
- downloading a file or folder

- renaming a file or folder
- deleting a file or folder
- creating a folder

You can apply folder action rules to files and folders selectively by specifying a mask. Multiple entries must be separated with a comma. Use the asterisk (*) as a wildcard matching any number of characters and the question mark (?) as a wildcard matching a single character.

Creating folder action rules

Folder action rules are configured per host. To have the same folder action rule on multiple hosts, you must configure it for each host.

To create a new folder action rule:

1 From the top menu, select **Server > Hosts**. The Hosts page opens.

2 Select a host from the list by clicking on the hyperlinked host name. The Host Details page opens.

3 Select **Folder Action Rules** from the left navigation menu. The Folder Action Rules page opens.

4 Click **Create**. The Create Folder Action Rule page opens.

5 Enter the appropriate values for each field.

- **Name**. Enter a name for this rule. This name is for your reference only and can include up to 256 characters.
- **File mask**. Specify a mask for this rule. The rule only applies to the files and folders that match the specified mask. Multiple entries must be separated with a comma. For example: *.exe, readme.txt, *.gif

Tip: Enter *.* to match all files. Enter * to match all files and folders or any number of characers. Enter a question mark (?) as a wildcard matching a single character.

- **File path** (/ by default). Enter or browse to select the folder you want this rule to apply to. This path is relative to the root of the host.

Note: If the file path specified is a virtual folder set to display in users' home folders, the rule only applies to the instance of the virtual folder located at the specific file path displayed. To apply the rule to the virtual folder under all users' home folders, you must create one rule for each user's home folder.

- **Include subfolders** (selected by default). Select this option to apply this rule to the subfolders of the folder specified in **File path**.
- **Users/Groups**. This list contains all of the users and groups configured on the host. Select the checkboxes next to the users and groups to whom you want this rule to apply.
- **Rule Notifications**. This section is used to select one or more notifications to send and to specify the criteria that trigger the notifications for this rule.

Notifications can be triggered when any of the following actions succeed or fail: upload, download, rename, delete, create folder.

- **Notification**. This list contains all of the notifications configured on the current host. Select the checkboxes beside the notifications you want to associate with this rule. To configure a new notification and associate it with this rule, click **Create**.
- **Executable** (optional). Enter the full path and file name of the program you want to run on the server when this rule is triggered.
- **Arguments** (optional). Enter the arguments to pass to the executable, if necessary.
- **Tip**: You can specify *message notification variables* (on page 99) as arguments to pass to the executable.

6 Click **OK** to save the new folder action rule.

About quota limit rules

Quota limit rules are used to govern the amount of disk space and the number of files users can upload to their home folders. Quota limit rules prevent a user from performing an action that would cause the limits specified in the rule to be exceeded.

Unlike failed login rules and folder action rules, which send notifications when the rule is triggered, quota limit rules can be configured to send notifications as a warning prior to the absolute limit being reached. For example, a quota limit rule that specifies a limit of 20 MB in the home folder can be configured to also send notifications as a warning when the size of the user's home folder reaches 18 MB.

If your users have the WS_FTP Professional client, the FTP and SSH servers can send the user's remaining disk space to the FTP client, which will display the data at the bottom of the remote file list. When you create a Quota Limit Rule, this functionality is enabled.

Creating quota limit rules

Quota limit rules are configured per host. To have the same quota limit rule on multiple hosts, you must configure it for each host.

To create a new Quota Limit Rule:

1 From the top menu, select **Server > Hosts**. The Hosts page opens.

2 Select a host from the list by clicking on the hyperlinked host name. The Host Details page opens.

3 Select **Quota Limit Rules** from the left navigation menu. The Quota Limit Rules page opens.

4 Click **Create**. The Create Quota Limit Rule page opens.

5 Enter the appropriate values for each field.

- **Name**. Enter a name for this rule. This name is for your reference only and can include up to 256 characters.
- Do not allow uploads if:
  - **Number of files in user's home folder and its subfolders exceeds ... files**. When the user attempts an action that would cause the total number of files in the user's home folder (and its subfolders) to exceed the specified number, the action is not permitted. If you do not want to limit the number of files in the user's home folder, enter 0.
  - **Size of user's home folder exceeds ... [KBs, MBs, GBs]**. When the user attempts an action that would cause the total size of the files and folders in the user's home folder to exceed the specified amount, the action is not permitted. If you do not want to limit the size of the user's home folder, enter 0.

> If your users have the WS_FTP Professional client, the FTP and SSH servers can send the user's remaining disk space to the FTP client, which will display the data at the bottom of the remote file list. When you create a Quota Limit Rule, this functionality is enabled.

- **Users/Groups**. This list contains all of the users and groups configured on the host. Select the checkboxes next to the users and groups to whom you want this rule to apply.
- **Rule Notifications**. This section is used to select a notification (or notifications) and to specify the criteria that trigger the notifications for this rule. **Send notification when rule is triggered as a result of**:
  - **Number of files in user's home folder and its subfolders exceeds ... files**. When the total number of files in the user's home folder (and its subfolders) grows larger than the specified number, any notifications attached to this rule are triggered. If you do not want to limit the number of files in the user's home folder, enter 0.
  - **Size of user's home folder exceeds ... [KBs, MBs, GBs]**. When the user's home folder grows larger than the specified maximum amount of disk space, any notifications attached to this rule are triggered. If you do not want to limit the size of the user's home folder, enter 0.
- **Notification**. This list contains all of the notifications configured on the current host. Select the checkboxes beside the notifications you want this rule to apply to. To configure a new notification and associate it with this rule, click **Add**.
- **Execute the following program when the rule is triggered**. Select the option to enable a selected program to run when a rule is triggered.
  - **Executable (optional)**. Enter the full path and file name of the program you want to run on the server when this rule is triggered. Click **Browse** to browse for the program file name.
  - **Arguments (optional)**. Enter the arguments to pass to the executable, if necessary.

6 Click **Save** to save the new Quota Limit Rule.

About notifications

Notifications can be used with rules to monitor the WS_FTP Server and send a message or take an action when an event occurs.

A file transfer event, such as a file upload or download, can trigger a notification that sends a message to a user or launches an application. Notifications help you respond to events that occur on the server and automate certain responses, for example:

- Inform the server administrator when a disk quota or failed login limit is exceeded.
- Inform a user that a file has arrived on the server and is ready for download.
- Inform a user or administrator that a particular file has been downloaded.

Notification Types

There are three types of notifications. The notifications define how a message is sent and to whom the message is sent.

- **Email**. Sends a message to an email address. For more information, see *Creating an Email Notification* (on page 96).
- **Pager**. Sends a message to a pager via a dial-up modem. For more information, see *Creating a Pager Notification* (on page 97).
- **SMS**. (Short Message Service) sends messages of up to 160 characters (225 characters using the 5-bit mode) to mobile phones that use Global System for Mobile communication (GSM). SMS is similar to paging; however, SMS messages do not require the mobile phone to be active and within range. Instead, the message will be held for a number of days until the phone is active and within range. SMS messages are transmitted within the same cell or to anyone with roaming service capability. They can also be sent to digital phones from a web site equipped with PC Link or from one digital phone to another. For more information, see Creating an SMS Notification.

Note: The program notifications feature of previous versions of WS_FTP Server is now included in rules. For more information about creating a rule that launches an application or a batch file, see *Rules Overview* (on page 87).

Configuring the Notification Server

To use Email, SMS, or Pager Notifications, you must first configure the WS_FTP Server and the Ipswitch Notification Server to communicate with each other. You can configure WS_FTP Server to use a Notification Server installed on the same computer as WS_FTP Server, or you can use a Notification Server located on another computer.

To configure the Notification Server:

1 From the top menu, select **Server > Server Settings > Notification Server**. The Notification Server Settings page opens.

Note: You must be logged in as a system administrator for the Notification Server Settings link to appear.

2 Enter the appropriate information for each of the fields.

- **Notification server IP address.** Enter the IP address of the Notification Server that you want WS_FTP Server to use to send notifications. If you are using Notification Server installed on the same computer as WS_FTP Server, enter `127.0.0.1`.
- **Port**. Enter the port you want Ipswitch Notification Server to listen on for connections from WS_FTP Server.
- **Retries**. Enter the number of times you want Ipswitch Notification Server to attempt to send a notification. If the notification cannot be successfully sent within this number of tries, the notification is logged as failed.
- **Logging level**. Specify the level of detail the server provides to the enabled log servers.
  - **None**. No data is captured or supplied to the log server.
  - **Errors Only**. Only events that register as errors are logged.
  - **Normal** (selected by default). In addition to errors, the following events are logged: uploading, downloading, deleting and renaming a file; removing and creating a folder; user authentications; and issuing a SITE command.
  - **Verbose**. In addition to everything logged in Normal, the following events are logged: connecting and disconnecting; changing working directory; negotiating SSL, including cipher, type and strength; negotiating SSH, including ciphers and MACs; and any other command sent to the server.

Caution: Verbose mode produces a large quantity of log entries and should only be used for brief periods of troubleshooting.

- **Enable WS_FTP Logging**. Select this option to enable logging to an Ipswitch Log Server.
  - **Log server IP address** (127.0.0.1 by default). Enter the host name or IP address of the log server.
  - **Port** (5151 by default). Enter the port over which the connection to the log server should be made.
- **Enable Syslog**. Select this option to enable logging to a syslog server.
  - **Log server IP address**. Enter the host name or IP address of the syslog server.
  - **Port**. Enter the port over which the connection to the log server should be made.

3 Click **Save**.

About email notifications

Email messages are delivered via an SMTP gateway, which will probably be the same relay for all email addresses. However, you can have notifications that use different SMTP servers.

Creating email notifications

After you create an email notification profile, you can add it as a rule notification on one of the rules pages:

- *Failed Login Rules page* (on page 89)
- *Folder Action Rules page* (on page 91)
- *Quota Limit Rules page* (on page 92)
- Bandwidth Limit Rules page

To create an email notification:

1. From the top menu, select **Server > Notifications**. The Notifications page opens.
2. Click **Create Email**. The Create Email Notification page opens.
3. Enter the appropriate information for each of the fields.
   - **Name**. Enter a name for this notification. This name is for your reference only and will never be displayed to the notification recipient.
   - **Description**. Enter or modify the description. This description is for your reference only.
   - **HELO text**. When the Notification server sends an SMTP message, the first message it sends identifies the Notification server to the mail server (for example, HELO "foo.ipswitch.com"). A mail server can decide to accept or refuse further messages based on the identity. By default, the hostname of the local machine is used in the HELO message. You can override the default value by entering a different hostname in this box.

⚠ **Caution**: Many mail servers will reject a message if the hostname cannot be resolved to a valid IP address.

   - **Email server**. Enter the IP address or host name of the mail server through which you want to send this notification. You must possess appropriate permissions to send mail through this server.
   - **Use SMTP Authentication.** Check this box if your SMTP server requires authentication. WS_FTP Server will use the username and password that you enter below.
   - **Username.** Enter the username for authentication to your SMTP server (if required).
   - **Password.** Enter the password for authentication to your SMTP server (if required).

- **From address**. Enter the email address from which the notification should appear to have been sent.
- **To address**. Enter the address of the recipient of the notification. You can send a notification to multiple recipients by entering multiple email addresses separated by commas.

> **Note**:WS_FTP Server can automatically enter the email address of the user who initiated the action (for example, a folder action or quota limit warning). To set this up, enter the notification variable %Emailaddress in the **To address**, and make sure a valid email address is entered in the **Edit User** page.
>
> **Caution**: Entering more than two or three email addresses in the To address field may cause the performance time of the notification to decrease significantly. In these cases, you should create an email list in your email server and enter its address in the To address field.
>
> **Tip:** You can specify a friendly name for From address and To address by using this format: Frank Gibson <frankgibson@ipswitch.com>

- **Subject**. Enter a subject for the Email notification. You can use *notification variables* (on page 99) in this field.
- **Message**. Enter the message that should be sent with this notification. You can use *notification variables* (on page 99) in this field.

4 Click **Save**.

About pager notifications

Pager messages are delivered via a terminal service provider. You can define a notification to send a message to a pager when an FTP event occurs. WS_FTP Server supports PageNet, TAP (Telocator Alphanumeric Protocol) , SMS-TAP, UCP-SMS (British Telecom), and NTT (Nippon Telegraph and Telephone) pager services.

Creating a pager notification

After you create a pager notification profile, you can add it as a rule notification on one of the rules pages:

- *Failed Login Rules page* (on page 89)
- *Folder Action Rules page* (on page 91)
- *Quota Limit Rules page* (on page 92)
- Bandwidth Limit Rules page

To create a pager notification:

1 From the top menu, select **Server > Notifications**. The Notifications page opens.

2 Click **Create Pager**. The Create Pager Notification page opens.

3 Enter the appropriate information for each of the fields.

- **Initialization string**. Enter an initialization string for the modem. This string should contain the modem commands for "Command Echo Off" (EO), "Result Codes On" (QO), "Verbal Results" (V1), "Result Codes Displayed" (X4), and "Local Echo OFF" (F1). The recommended string to use is: ATEO QO V1 X4 F1.
- **COM port**. Select the COM port to which your modem is connected.
- **Baud rate**. Select the speed (measured in bits per second) at which the serial port will communicate with the modem. Consult the documentation for your modem if you are unsure of the appropriate selection.
- **Data bits**. Select the type of data bit transmission to be used for communications with the selected serial port. Select from 6, 7, or 8.
- **Parity**. Select the form of parity checking you want the modem to use. Parity checking can be specified as even (a successful transmission will form an even number), odd or none. No parity means the modems will not transmit or check a parity bit and the server will assume that there are other forms of error checking being used.
- **Stop bits**. Select whether to use 1 or 2 bits to signal the end of a unit of transmission.

4 Click **Save**.

About SMS notifications

Short Message Service (SMS) is similar to paging. However, SMS messages do not require the mobile phone to be active and within range and will be held for a number of days until the phone is active and within range. SMS messages are transmitted within the same cell or to anyone with roaming service capability.

SMS notification services are provided by a number of different providers in one of two ways: Email, where a specifically formatted email message is sent to an address or dialup, the protocol used in common pagers which requires a modem and the phone number of the provider and recipient.

Because multiple methods can be used to provide SMS service, there are no common settings for SMS notifications. Each notification is tied to a provider, which may support either or both of the delivery methods mentioned.

Creating SMS notifications

After you create an SMS notification profile, you can add it as a rule notification on one of the rules pages:

- *Failed Login Rules page* (on page 89)
- *Folder Action Rules page* (on page 91)
- *Quota Limit Rules page* (on page 92)
- Bandwidth Limit Rules page

To create an SMS notification:

1. From the top menu, select **Server > Notifications**. The Notifications page opens.
2. Click **Create SMS**. The Create SMS Notification page opens.
3. Enter the appropriate information for each of the fields.
   - **Name**. Enter a name for this notification. This name is for your reference only and will never be displayed to the notification recipient.
   - **Description**. Enter or modify the description. This description is for your reference only.
   - **SMS provider**. Click **Select** to choose a provider for this notification.
   - **Delivery mode**. Select the radio button for the delivery mode you want to use with this notification. Depending on the provider selected, only one option may be available.
     - **Email**. Enter the email address to which you want to send the notification.
     - **Dialup**. Enter the telephone number to dial when this notification is initiated.
   - **Message**. Enter the message that should be sent with this notification. You can use *notification variables* (on page 99) in this field.
4. Click **Save**.

Using notification variables

The following variables can be specified in a message of a notification or in the parameters of an executable attached to a rule.

Variable	Description
`%Event`	The type of rule that triggered the notification.
`%Dir`	The name of the directory where the action was attempted.
`%File`	The name of the file the action was attempted on, including the full file path relevant to root.
`%ToFile`	The new name of a file that was renamed.
`%FmFile`	The former name of a file that was renamed.
`%User`	The username of the user that attempted the action.
`%Emailaddress`	The email address, as specified on the Edit User page, of the user that attempted the action.
`%Status`	The status of the attempted action, either Success or Fail.
`%SimpleName`	The name, without any path information, of the file the action was attempted on.
`%Timestamp`	The date and time the notification was triggered.

`%TransferType`	Retrieves the values "ASCII" or "Binary," depending on the type of transfer (available for Folder Action and Quota Rules only).
`%ClientIPAddress`	The IP address of the FTP client that performed the action triggering the notification (this variable is not available for Failed Login Rules).
`%HostName`	The WS-FTP server host of the user attempting the action.
`%FileSize`	The file size of the file uploaded or downloaded (available only for Successful Upload, Successful Download, and Failed Download events occurring under Folder Action Rules).

CHAPTER 10

Using SSL

In This Chapter

What is SSL?

SSL (Secure Sockets 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 the 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 a standard SSL connection:

Step 1 Client connects and requests SSL encryption

Step 2 Server sends its certificate and public key to client

Step 3 Client encrypts session key using server's public key and sends it to server

Step 4 Server decodes session key and uses it to open and encrypt secure data channel

Tip: For additional security, the server can require a certificate from the client, which is compared to a trusted authorities database to determine whether the client should be allowed to connect. If this option is enabled, the server requests the client certificate between steps 2 and 3; the client sends its certificate and the server checks to see if it has been signed by a certificate in the trusted authorities database.

If the server is not configured to accept SSL connections, or if the server requires client certificates and none is provided or the provided certificate is not found in the trusted authorities database, then the connection is rejected and the server sends a message to the client indicating a failed connection.

Understanding SSL terminology

To understand how SSL works, you must understand the various terms used to describe the parts of the SSL connection. The following is a list of these parts and the role each plays.

- **Client**. Any FTP program that is able to make an SSL connection.
- **Certificate**. The file that contains 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. The server stores certificate files in its database, so no physical file exists. The certificate includes the public key.
- **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 belongs to the server, but is used by the client to encrypt a session key. It does not exist as a file, but is a byproduct of the creation of a certificate and a private key. Data encrypted with the public key can be decrypted only by the corresponding private key.
- **Private key**. The private key is used by the server to decrypt the session key. The server stores private keys in its database, so no physical file exists. Private keys should be guarded like a password and NEVER shared with 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 signed certificate is made, which can replace the unsigned certificate.

SSL Terminology

To understand how SSL works, you must understand the various terms used to describe the parts of the SSL connection. The following is a list of these parts and the role each plays.

- **Client**. Any FTP program that is able to make an SSL connection.
- **Certificate**. The file that contains 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. The server stores certificate files in its database, so no physical file exists. The certificate includes the public key.
- **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 belongs to the server, but is used by the client to encrypt a session key. It does not exist as a file, but is a byproduct of the creation of a certificate and a private key. Data encrypted with the public key can be decrypted only by the corresponding private key.
- **Private key**. The private key is used by the server to decrypt the session key. The server stores private keys in its database, so no physical file exists. Private keys should be guarded like a password and NEVER shared with 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 signed certificate is made, which can replace the unsigned certificate.

Choosing a type of SSL

There are two types of SSL that can be used by a listener.

- **Implicit SSL**. With Implicit SSL, the server listens for connections on a special port (usually 990). When a connection is made, SSL negotiations are handled before any other activity, including authentication. Using this option, it is impossible for a non-SSL connection to be made on the listener, but users must know to connect on the special port.
- **SSL enabled** (sometimes called *Explicit SSL or AUTH SSL*). With this option, an SSL connection is made after the client connects and requests an SSL connection. If the SSL command is not issued, the connection continues as a standard FTP connection. SSL enabled connections may occur on any port, but most often port 21 is used (the same port as standard FTP).

The following SSL options can be used to provide increased security for connections.

- **Request client certificates**. This listener-level option adds a second layer of authentication by requiring users to present an SSL certificate of their own as part of the authentication process. If the certificate is not signed by a certificate in the trusted authorities database, the connection is terminated. This option can be used with Implicit SSL or SSL enabled (Explicit SSL).
- **Force SSL**. When selected, this host-level option forces clients to invoke SSL before authenticating. If the client attempts to authenticate before establishing an SSL connection, the server reports an error explaining to the client that SSL is required. This option is only valid with SSL enabled (Explicit SSL).
- **Minimum SSL strength**. This host-level option forces the server to require a specific cipher strength or higher to secure SSL connections. The server can require 128 and 256-bit cipher strength, or it can allow any SSL connection regardless of cipher strength.
- **Force SSL on data channel**. When this host-level option is enabled, the server encrypts all of the data sent over the data channel. Enabling this option improves security, but it may also negatively impact the speed of transfers.

- **Allow Clear Command Channel (CCC)**. When this host-level option is enabled, clients can issue the CCC command to revert a secured command channel to unsecured. If cleared, CCC commands fail. Clear this option to prevent users from converting an SSL connection to an unsecured standard FTP connection.

> **Note**: If users are having difficulty accessing the server over SSL using passive mode and through a firewall, enabling this option may help by sending the IP address and port that the server should use to establish the connection with the client in a clear, unencrypted format.

Configuring implicit SSL

Implicit SSL settings apply only to FTP listeners and are typically a listener on port 990. Use the following settings to configure Implicit SSL settings.

To configure Implicit SSL:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.

> **Note**: Since SSL can be configured only on FTP listeners, make sure that you select a listener that displays FTP in the Server type column.

3. Under **Encryption Options**, click **Edit SSL Settings**. The Listener Encryption Settings page opens.
4. Set the appropriate options.
   - **SSL type** (Clear Only enabled by default). Select the type of SSL connection to attempt when a request comes in to the current listener.
     - **Clear only**. No SSL connection is allowed.
     - **SSL enabled**. An SSL connection is made after the client connects and issues the appropriate command. If the SSL command is not issued and you are not forcing SSL, the connection is made as a standard FTP connection.
     - **Implicit SSL**. An SSL connection is made immediately upon connection. With Implicit SSL, it is impossible for a non-SSL connection to be made on this listener. The default port for Implicit SSL listeners is 990.
   - **SSL certificate**. Displays the SSL certificate currently applied to the current listener. This is the SSL certificate that the server sends to identify itself to client that connect to this listener. To select an SSL certificate, click **Select**.
   - **Request client certificate**. If selected, the listener will request an SSL client certificate before allowing the user to authenticate. In order for the client to authenticate, the client certificate must be signed by a certificate in the **Trusted Authorities** list.
   - **SSL security level**. Select the versions of SSL and TLS that you want to allow clients to use to connect.

   - **TLS only (more secure)**. Select this option to require clients to negotiate SSL connections using TLS version 1.0 or higher. This option provides the greatest security, but may cause some clients to fail to connect.
   - **Enable TLS and SSL versions 1, 2 and 3** (selected by default). Select this option to allow clients to connect using any version of SSL or TLS. This option works with most clients, but does not protect the server from security vulnerabilities in older versions of SSL.
- **Trusted Authorities**. This list contains a list of certificates which the server trusts to sign client certificates. When **Request client certificate** is enabled and a client attempts an SSL connection, the server prompts the client for a client certificate. The server then checks to see if the client certificate is signed by any of the certificates in the trusted authorities list. If not, the connection is terminated.
   - To add a certificate to this list, click **Add**.
   - To remove a certificate from this list, click **Remove**.

5 Click **Save**. The Edit Listener page opens.

6 In the **Port** box, enter **990**. For more information, see *Setting Up Listeners* (on page 55).

7 Click **Save**.

Common SSL configurations

The table below includes some common SSL configurations and the options that must be set to produce each.

	SSL Type	**Force SSL**	**Request client certificates**
Client may connect using SSL, but it is not required.	SSL Enabled	No	No
Clients must use SSL (option 1).	SSL Enabled	Yes	No
Clients must use SSL (option 2).	Implicit SSL	Not applicable*	No
Clients must use SSL and submit a client certificate to prove identity (option 1).	SSL Enabled	Yes	Yes
Clients must use SSL and submit a client certificate to prove identity (option 2).	Implicit SSL	Not applicable*	Yes

* Force SSL option only affects SSL enabled listeners.

Selecting an SSL certificate

While SSL connections are commonly thought of as being made to a host, SSL negotiations actually occur at the listener level, before a host is defined. As such, the SSL certificate is applied to the listener.

To select an SSL certificate:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.

> **Note**: Since SSL can be configured only on FTP listeners, make sure that you select a listener that displays FTP in the Server type column.

3. Under **Encryption Options**, click **Edit SSL Settings**. The Listener Encryption Settings page opens.
4. Next to **SSL Certificate**, click **Select**. The Select SSL Certificate page opens.
5. Select the certificate you want to associate with this listener, then click **OK**. The Edit Listener page opens again, with the SSL certificate you selected displayed in **SSL Certificate**.
6. Click **Save**.

If the SSL certificate you want to use is not listed, you can import a certificate from another program. For more information, see *Importing an SSL Certificate* (on page 106).

If you do not have an SSL certificate yet, WS_FTP Server can create one. For more information, see *Creating an SSL Certificate* (on page 107).

Importing an SSL certificate

If you have an SSL certificate from a certificate authority or from another application, WS_FTP Server can import it and use it for SSL connections to a listener.

To import an SSL certificate and apply it to a listener:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.

> **Note**: Since SSL can be configured only on FTP listeners, make sure that you select a listener that displays FTP in the Server type column.

3. Under **Encryption Options**, click **Edit SSL Settings**. The Listener Encryption Settings page opens.
4. Next to **SSL Certificate**, click **Select**. The Select SSL Certificate page opens.
5. Click **Import**. The Import SSL Certificate page opens.
6. Enter the appropriate information for each of the fields.

- **Name**. Enter a name for your certificate. This name is for your reference and is never displayed to users.
- **Certificate**. Enter the full path and file name of a certificate file on your computer, or click **Browse**.
- **Key File**. Enter the full path and file name of a key file on your computer, or click **Browse**.
- **Passphrase**. Enter the passphrase needed to decrypt this certificate.

7 Click **Save**. The Select SSL Certificate page reopens with the imported certificate included in the list.

8 Select the certificate you just created, then click **OK**. The Listener Encryption Settings page opens again, with the SSL certificate you imported displayed in **SSL Certificate** box.

9 Click **Save**.

Creating an SSL certificate

Ipswitch WS_FTP Server can generate SSL certificates for you to apply to listeners.

To create an SSL certificate and apply it to a listener:

1 From the top menu, select **Server > Listeners**. The Listeners page opens.

2 Click the **IP address** of the listener you want to open. The Edit Listener page opens.

Note: Since SSL can be configured only on FTP listeners, make sure that you select a listener that displays FTP in the Server type column.

3 Under **Encryption Options**, click **Edit SSL Settings**. The Listener Encryption Settings page opens.

4 Next to **SSL Certificate**, click **Select**. The Select SSL Certificate page opens.

5 Click **Create**. The Create SSL Certificate page opens.

6 Enter the appropriate information for each of the fields.

- **Name**. Enter a name for the certificate. This name is for your reference and is never displayed to users.
- **Expire date**. Enter an expiration date for the certificate, or click the calendar icon to browse for one.
- **Passphrase**. Enter the passphrase for the certificate. The passphrase is used to encrypt the key file.
- **Confirm passphrase**. Re-enter the same passphrase as above.
- **City/Town**. Enter the name of the city or town where you are located (for example, Augusta).
- **State/Province**. Enter the name of the state or province where you are located (for example, GA).
- **Country**. Enter the two-character code of the country where you are located (for example, US).

- **Common name**. Enter the host name that users enter to access the host this certificate will be applied to (for example, ftp.ipswitch.com).
- **Email**. Enter the email address of the person responsible for this certificate.
- **Organization**. Enter the name of your company or, if you are running the server privately, your name (for example, Ipswitch, Inc.).
- **Unit**. Enter the name of the organizational unit (for example, Information Technology).
- **Key size**. Select the key size for the certificate. A higher key size creates a more secure key, but takes longer to generate.

> If you plan to purchase a certificate from a Certificate Authority, you can still select any of the available key sizes. For general information about purchasing a certificate, see the *FAQ on Verisign's site* http://www.verisign.com/ssl/ssl-information-center/ssl-basics/index.html.

-

7. Click **Save**. The Select SSL Certificate page reopens with the new certificate included in the list.
8. Select the certificate you just created, then click **OK**. The Listener Encryption Settings page opens again, with the SSL certificate you created displayed in **SSL Certificate** box.
9. Click **Save**.

Disabling SSL

The default installation of Ipswitch WS_FTP Server allows SSL enabled (Explicit SSL) and Implicit SSL connections. If you do not want to allow SSL connections, you must make changes to the default configuration.

To turn off SSL for a listener:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the listener you want to open. The Edit Listener page opens.

> **Note**: Since SSL can be configured only on FTP listeners, make sure that you select a listener that displays FTP in the Server type column.

3. Under **Encryption Options**, click **Edit SSL Settings**. The Listener Encryption Settings page opens.
4. Change **SSL type** to **Clear Only**, then click **Save**.

Requiring SSL for specific folders

Folders can be configured to appear only to clients who have connected with a minimum SSL strength. If a client is not using SSL or is using a lower strength of SSL than is required, the folder is not displayed in the file listing and cannot be accessed.

To require a minimum strength of SSL for a folder to display:

1 From the top menu, select **Server > Hosts**. The Hosts page opens.
2 Click the **Host name** of the host you want to open. The Host Settings page opens.
3 From the left navigation menu, select **Folders**. The Folders page opens.
4 Click the **Folder** you want to open.
5 Select:

- **Only viewable with 40-bit SSL or higher**
- **Only viewable with 128-bit SSL or higher**

If you specify 40- or 128-bit, the folder is not shown to clients connected without SSL or with an SSL strength lower than the specified strength.

Note: Minimum SSL strength to view affects FTP listeners only. Clients connected over SSH/SFTP can view the folder regardless of this option selection.

6 Click **Save**.

Requesting client certificates

The server can require all authenticating users to present a client certificate as an extra measure of security. The client certificate proves the client's identity to the server. Client certificates must be signed by a trusted authority.

When a client presents a certificate, it is compared to the certificates maintained in the trusted authorities database. If the certificate used to sign the client certificate is found in the trusted authorities database, the client is authenticated and the connection continues; if not, the connection is terminated.

To add a certificate to the trusted authorities database:

1 From the top menu, select **Server > Listeners**. The Listeners page opens.
2 Select the listener for which you want to specify an SSL certificate to add to the listener's trusted authorities database by clicking on the listener's hyperlinked IP address. The Edit Listener page opens.
3 Under **Encryption Options**, click **Edit SSL Settings**. The Listener Encryption Settings page opens.
4 Under **Trusted Authorities**, click **Add**. The Select Trusted Authorities page opens.

5 Click **Import** and select the certificate you want to trust, or click **Create** to create a new certificate. For more information, see Import Trusted Authorities or *Creating an SSL Certificate* (on page 107).

6 Click **Save**. The previous page reopens with the new certificate included in the list.

7 Select the certificate you just created, then click **OK**. The Listener Encryption page opens again with the certificate you imported displayed in the Trusted Authorities list.

8 Click **Save**.

To remove a certificate from the trusted authorities database:

1 From the top menu, select **Server > Listeners**. The Listeners page opens.

2 Select the listener for which you want to specify an SSL certificate to remove from the listener's trusted authorities database by clicking on the listener's hyperlinked IP address. The Edit Listener page opens.

3 Under **Encryption Options**, click **Edit SSL Settings**. The Listener Encryption Settings page opens.

4 Select the certificate in the Trusted Authorities list that you want to remove.

5 Click **Remove**.

Note: When you remove a certificate from the trusted authorities database, it is not deleted. The certificate can still be accessed by selecting **Server > SSL Certificates**. You can delete the certificate from the server there if desired.

6 Click **Save**.

Signing SSL certificates

When a user wants to make an SSL connection with a host that requests client certificates, the user creates a certificate of their own and sends the generated certificate signing request to the server administrator, usually via email. The administrator uses this page to sign the request, which creates a new certificate that can be sent back to the user. The user can then use that certificate to make an SSL connection with the host.

To sign an SSL certificate signing request:

1 From the main menu, select **Server > SSL Certificates**. The SSL Certificates page opens.

2 At the bottom of the page, select the **Sign SSL Certificate** link. The Select a Certificate Signing Request (CSR) to sign page opens.

3 Select whether you want to **Upload** a certificate signing request (as a .csr file) or **Select a CSR to sign** from the certificates database. (All certificates listed in the Select a CSR to sign list have valid certificate signing requests. Only imported certificates for which no .csr file was included are not listed.)

4 Select the certificate with which you want to sign the certificate signing request. You can use an SSL certificate in the certificates database to sign a certificate signing request.

5 Specify the **Active Date** and **Expires on** date for the new signed certificate. The certificate is not valid before the activation date or after the expiration date.

6 Click **OK**. The SSL Certificates page opens with a link to download the new signed certificate in the message bar at the top of the page.

CHAPTER 11

Using SSH

In This Chapter

What is SSH?

SSH (Secure Shell) is a protocol for encrypting and securing various kinds of data transfers over a network or the Internet. SSH works by opening a secure channel between the SSH server and an authenticated user's computer, through which many kinds of data may be sent or retrieved.

SSH can be understood as a large pipe: its purpose is to carry whatever is passed through it from one place to another without letting anything leak in or out.

The WS_FTP SSH Server uses SFTP (SSH File Transfer Protocol) over SSH2 to transfer files.

How does SSH work?

When an SSH client connects to the SSH server, the client and the server each send a key to the other. If the keys are trusted, the client and server then negotiate a secret key which is used to encrypt all data exchanged between the two.

Once the secure channel is negotiated and the user is authenticated, files can be transferred through the secured SSH pipeline using SFTP.

Understanding SSH terminology

- **RSA** and **DSA**. RSA and DSA are two of the encryption algorithms that can be used to generate keys. Ipswitch WS_FTP Server supports both types of keys.
- **Host key**. The host key is the key that the server presents to the client to prove its identity.
- **User key**. The user key is the key that the client presents to the server to prove its identity.
- **MAC.** Message Authentication Code is a secret code agreed upon by the client and the server during SSH negotiations. The MAC is used to verify the integrity of packets sent between the two.
- **Cipher**. Ciphers are cryptographic algorithms used to encrypt SSH connections.

Selecting methods of authentication

Ipswitch WS_FTP Server supports two methods of authenticating over SSH.

- **Public key**. Public key authentication is the preferred authentication method for SSH. Clients authenticate by sending a key which the server matches to the key associated with the user. If the match is successful, the client is authenticated.
- **Password**. Password authentication works much like FTP authentication. Users present a username and password to the server, which verifies that the password supplied is the password for the user supplied. If the passwords match, the client is authenticated.

To configure authentication methods for an SSH listener:

1 From the top menu, select **Server > Listeners**. The Listeners page opens.

2 Click the **IP address** of the listener you want to open. The Edit Listener page opens.

3 At the bottom of the page, click **SSH Settings**. The Listener Encryption Settings (SSH) page opens.

4 Under **Authentication Method**, select the checkboxes next to the authentication methods you want to allow.

Note: If you choose to allow both authentication methods, user can authenticate using a public key OR a password; both are not required.

Selecting an SSH host key

SSH host keys are used to verify the identity of the server to connecting clients. SSH host keys are sent as soon as a client connects to a listener. If the client recognizes and trusts the key, and the server does the same for the key sent by the client, they establish an SSH connection.

SSH host keys are always used in SSH negotiations. An SSH host key is required regardless of the SSH authentication method used.

To select an SSH host key to apply to a listener:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Select the listener you want to specify an SSH host key for by clicking on its hyperlinked IP address. The Edit Listener page opens.
3. Click **SSH Settings**. The Listener Encryption Settings (SSH) page opens.
4. Next to **RSA host key** or **DSA host key**, click **Select**. The Select SSH Host Key page opens.
5. Select the host key you want to apply to the listener, then click **OK**. The Edit Listener page opens again.
6. Click **Save**.

If you do not have an SSH host key yet, WS_FTP Server can create one. For more information, see *Creating an SSH Host Key* (on page 115).

Creating an SSH host key

To create an SSH host key and apply it to a listener:

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Select the listener you want to specify an SSH host key for by clicking on its hyperlinked IP address. The Edit Listener page opens.
3. Click **SSH Settings**. The Listener Encryption Settings (SSH) page opens.
4. Next to **RSA host key** or **DSA host key**, click **Select**. The Select SSH Host Key page opens.
5. Click **Create**. The Create SSH Host Key page opens.
6. Enter the appropriate information for each of the fields.
   - **Name**. Enter a name for the key. This name is for your reference and is never displayed to users.
   - **Type**. The type of key, DSA or RSA, that you want to generate is displayed here.
   - **Passphrase** (optional). Enter a passphrase to encrypt the host key.
   - **Key size**. Select the key size for the key. A higher key size creates a more secure key, but takes longer to generate.
7. Click **Save**. The Select SSH Host Key page reopens with the new host key included in the list.
8. Select the host key you just created, then click **OK**. The Edit Listener page opens again.
9. Click **Save**.

Selecting an SSH user key

SSH user keys are used to authenticate users connecting over SSH. For a user to authenticate, the key the client sends must be associated with the user account on the server.

SSH user keys are only used when a listener uses public key authentication.

WS_FTP Server can create SSH user keys, or you can import keys created in another application.

To select an SSH user key to assign to a user:

1 From the top menu, select **Host> Users**. The Users page opens.
2 Select the user for whom you want to create a key by clicking on the hyperlinked username. The Edit User page appears.
3 Next to **SSH user key**, click **Select**. The Select SSH Key page opens.
4 Select the key you want to associate with this user, then click **Save**.

If the SSH user key you want to use is not listed, you can import a key from another program. For more information, see *Importing an SSH User Key* (on page 116).

If you do not have an SSH user key yet, WS_FTP Server can create one. For more information, see *Creating an SSH User Key* (on page 116).

Importing an SSH user key

If you have an SSH user key from another application (such as an SSH client), you can import it for use with WS_FTP Server.

To import an SSH user key and associate it with a user:

1 From the menu, select **Server > Hosts**. The Hosts page opens.
2 Select the host to which the user for whom you want to import a key belongs by clicking on the hyperlinked host name. The Host Settings page opens.
3 From the left navigation menu, select **Users**. The Users page opens.
4 Select the user for whom you want to import a key by clicking on the hyperlinked username. The Edit User page appears.
5 Next to **SSH user key**, click **Select**. The Select SSH Key page opens.
6 Click **Import**. The Import SSH User Key page opens.
7 Enter the appropriate information for each of the fields.
   - **Name**. Enter a name for the key. This name is for your reference and is never displayed to users.
   - **User key (public)**. Enter the full path and file name of a key file on your computer, or click **Browse**.
8 Click **Save**.

Creating an SSH user key

To create an SSH key and assign it to a user:

1 From the menu, select **Server > Hosts**. The Hosts page opens.
2 Select the host to which the user for whom you want to create a key belongs by clicking on the hyperlinked host name. The Host Settings page opens.
3 From the left navigation menu, select **Users**. The Users page opens.

4 Select the user for whom you want to create a key by clicking on the hyperlinked username. The Edit User page appears.

5 Next to **SSH user key**, click **Select**. The Select SSH Key page opens.

6 Click **Create**. The Create SSH User Key page opens.

7 Enter the appropriate information for each of the fields.

- **Name**. Enter a name for the key. This name is for your reference and is never displayed to users.
- **Type** (RSA by default). Select the type of key, DSA or RSA, that you want to generate.
- **Passphrase** (optional). Enter a passphrase to encrypt the key.
- **Key size**. Select the key size for the key. A higher key size creates a more secure key, but takes longer to generate.

8 Click **Save**.

Specifying MACs and ciphers

You can control which MACs and ciphers are used by a particular SSH listener.

To view the MACs and ciphers used by an SSH listener:

1 From the top menu, select **Server > Listeners**. The Listeners page opens.

2 Click the **IP address** of the listener you want to open. The Edit Listener page opens.

At the bottom of the page, click **SSH Settings**. The Listener Encryption Settings (SSH) page opens.

To remove a MAC or cipher from an SSH listener:

1 Select the radio button next to the name of the MAC or cipher you want to remove.

2 Click **Remove**. The page reloads with the selected MAC or cipher removed from the list.

To add a cipher to an SSH listener:

1 Click **Add** below the list of ciphers. The Add Cipher page opens.

2 Select the cipher you want to add.

> **Note**: If nothing appears in the list, all available MACs are already assigned to the SSH listener.

3 Click **Save**.

To add a MAC to an SSH listener:

1 Click **Add** below the list of MACs. The Add MAC page opens.

2 Select the MAC you want to add.

Note: If nothing appears in the list, all available MACs are already assigned to the SSH listener.

3 Click **Save**.

CHAPTER 12

Using SCP2

In This Chapter

What is SCP?

SCP (Secure Copy) is a protocol that uses SSH to provide "remote copy" capability in a secure environment. Traditionally, "remote copy" was used to transfer files within a secure internal network. SCP leverages SSH to provide authentication and secure transfer.

SCP2 support in WS_FTP Server with SSH

There is no published RFC that describes SCP protocol. There are several implementations of SCP, with some variation in the features implemented. WS_FTP Server with SSH supports SCP2 protocol (i.e. SCP over SSH2).

In addition, the WS_FTP implementation of SCP2 has the benefit of leveraging any users, rules, and notifications created for the WS_FTP server host.

Supported SSH clients include:

- OpenSSH: Designed as part of the OpenBSD project, but portable to a number of UNIX-like operating systems.

  http://www.openssh.org/ http://www.openssh.org/
- PuTTY: A free telnet and SSH Client for Windows and Unix platforms.

Enabling SCP2 connections in WS_FTP SSH server

1. From the top menu, select **Server > Listeners**. The Listeners page opens.
2. Click the **IP address** of the SSH listener you want to open. The Edit Listener page opens.
3. Select the option **Enable Secure Copy (SCP2)** (i.e. SCP protocol over SSH2).

   After restarting the SSH server, SCP2 clients can connect to the SSH listener for the selected host. WS_FTP SSH Server uses the host's users, rules, and notifications while executing SCP commands received from the SCP2 client. The server logs the status of execution of SCP commands into the WS_FTP server log. In WS_FTP Server Manager, the **Session Manager** can be used to view statistical information about SCP2 connections and data transferred over SCP2 connections.

> SCP2 connections apply only to the SSH listener for the selected host.

Examples of SCP2 transfers

The following examples show how you would use the PuTTY tool to transfer files using SCP.

Specifying the WS_FTP hostname on the SCP command line:

The syntax of (PuTTY) SCP command-line is:

```
pscp [-pqrvBC46] [-F ssh_config] [-S program] [-P port] [-c cipher] [-i
identity_file] [-o ssh_option] [[user@]machine1:]file1 [...]

[[user@]machine2:]file2
```

In this command line:

- machine-names (e.g. machine1, machine2) indicate the computer-name (and NOT the name of WS_FTP host).
- `user` can be any WS_FTP Server user.

If the ‘username’ does not explicitly include a WS_FTP hostname, WS_FTP SSH server will use the default hostname for authenticating the user.

For example, to connect to the default host of WS_FTP SSH server running on machine ‘MACHINE1’ with the credentials of USER1, use: USER1@MACHINE1 in the SCP command-line.

If the username explicitly includes the WS_FTP hostname (separated by current host separator character), WS_FTP SSH server uses the specified hostname for authenticating the user.

For example, if the current host separator character for WS_FTP server is *****, then, to connect to the host HOST2 of WS_FTP SSH server running on machine MACHINE2 with the credentials of USER2, use: `USER2*HOST2@MACHINE2` in the SCP command-line.

Downloading files

Using the PSCP (PuTTY) SCP tool, to download the file a.txt to the current directory on the client machine from the home folder of User1 (of the default host) of WS_FTP Server with SSH running on Machine1 using the credentials of User1, use the following command:

```
PSCP.exe -P 22 -l User1 -pw password -2 -4 -scp User1@Machine1:./a.txt
```

To download the folder ‘MyDocuments’ (and all files/sub-folders underneath this folder) to the current directory on client machine from the home folder of User1 (of the default host) of WS_FTP Server with SSH running on Machine1 using the credentials of User1, use the following command:

```
PSCP.exe -r -P 22 -l User1 -pw password -2 -4 -scp
User1@Machine1:./MyDocuments .
```

Uploading files

Using the PSCP (PuTTY) SCP tool, to upload the file a.txt from the current directory on the client machine to the home folder of User1 (of the default host) of WS_FTP Server with SSH running on Machine1 using the credentials of User1, use the following command:

```
PSCP.exe -P 22 -l User1 -pw password -2 -4 -scp a.txt User1@Machine1:.
```

To upload the folder ‘MyDocuments’ (and all files/sub-folders underneath this folder) from the current directory on client machine to the home folder of User1 (of the default host) of WS_FTP Server with SSH running on Machine1 using the credentials of User1, use the following command:

```
PSCP.exe -r -P 22 -l User1 -pw password -2 -4 -scp MyDocuments
User1@Machine1:.
```

If you are uploading from a Unix system, remember that file names on the WS_FTP Server are not case sensitive, as it runs on Windows operating systems.

Summary of supported SCP2 options

The following table summarizes handling of server-side options on the command-line for OpenSSH SCP and PuTTY's PSCP programs in WS_FTP SSH server. Remaining options are not applicable for the server since they are handled on the client side.

Purpose	OpenSSH SCP Option	PuTTY SCP (PSCP.EXE)	Handling in WS_FTP Server with SSH
Cipher for encryption of data transfer	-c cipher Selects the cipher to use for encrypting the data transfer. This option is directly passed to ssh(1).	-load *session* Loads settings from the saved session (configured using PuTTY.exe) This session can specify the encryption algorithm.	Supported
Private key file for authentication	-i *identity file* Selects the file from which the identity (private key) for RSA authentication is read. this option is directly passed to ssh(1).	-i *key* private key file (in .PPK format) for authentication	Supported
Preserve file attributes (modification times, access times, and modes) from the original file	-p	-p	Supported
Recursive copy of entire directories	-r	-r	Supported
Verbose mode	-v	-v	Not supported
Enable Compression	-C	-C	Supported
Port to which to connect to on the remote host	-P *port* Note that this option is written with a capital P, because -p is reserved for preserving the times and modes of the file in rcp.	-P *port*	Supported
SCP version	-2 SCP2 support -1 SCP1 support	-2 SCP2 support -1 SCP1 support	Supports -2 only

Use of IPv4/IPv6	-4 Forces scp to use IPv4 addresses only. -6 Forces scp to use IPv6 addresses only	-4 Forces scp to use IPv4 addresses only. -6 Forces scp to use IPv6 addresses only	Supports -4 only
Server side wildcards	* Match 0 or more characters ? Match a single character	-unsafe Allows server side wildcards. * Match 0 or more characters ? Match a single character	Supports * and ?
Directory listing on remote server	Not available	-ls For example, pscp -ls fred@example.com:dir1	Not supported. An SCP server cannot implement this option because SCP protocol does not have a mechanism to list files within a directory. While PSCP supports the option (ls) to list files, it may not work with all servers.

References:

- OpenSSH, 1999a: SCP Man Page. http://www.eos.ncsu.edu/remoteaccess/man/scp.html
- PuTTY: Using PSCP to transfer files securely. http://the.earth.li/~sgtatham/putty/0.60/htmldoc/Chapter5.html#pscp

CHAPTER 13

Managing Connections in Real-time

In This Chapter

Monitoring active sessions

You can use the session manager to view and monitor active connections to the server.

To view active sessions:

1. From the top menu, select **Server > Session Manager**. The Session Manager page opens.
2. All active sessions are listed in the Sessions section of the page. For each session, the following information is listed:
    - **Client Address**. This column shows the IP address of the client.
    - **Host**. This column shows the host to which the client is connected.
    - **User**. This column shows the user name that the client used during authentication.
    - **Directory**. This column shows the name of the folder where the client is currently active.
    - **Last Command**. This column shows the last command issued by the client.
    - **KB Sent**. This column shows the number of kilobytes sent from the server to the client during the current session.
    - **KB Received**. This column shows the number of kilobytes the server received from the client during the current session.
    - **Idle Time**. This column indicates the amount of time that has elapsed since the client issued the last command.
    - **Transfer Active**. This column indicates whether or not the client is currently transferring a file.
    - **Listener Type**. This column indicates the type of listener, FTP or SSH, to which the client is connected.

Terminating an active session

You can forcefully terminate any connection to the server that is visible in the session manager.

To terminate a session:

1. From the top menu, select **Server > Session Manager**. The Session Manager page opens.
2. Select the checkbox next to each session that you want to end.
3. Click **End Session**. The sessions are marked for termination. It may take up to fifteen seconds for sessions marked for termination to actually terminate.

Viewing server statistics

The session manager reports the following statistics about the server. Statistics are aggregated for all servers using the shared configuration database from the last service restart time of each service.

Connections

- **Current connections**. This value represents the total number of connections to the servers that are active when the page rendered.
- **Highest concurrent connections**. This value represents the highest number of concurrent connections recorded at one time.
- **Connection attempts**. The number of times connections were attempted, including cases where username and/or password authentication was *not* attempted.
- **Logon attempts**. The number of times that username and/or password authentication has been attempted.

Files

- **Sends in progress**. This value represents the number of transfers from the server to clients ("downloads" from the client perspective) that are in progress.
- **Receives in progress**. This value represents the number of transfers from clients to the server ("uploads" from the client perspective) that are in progress.
- **Files sent**. This value represents the number of files sent from the server to clients.
- **Files received**. This value represents the number of files sent from clients to the server.
- **Files deleted**. This value represents the number of files deleted from the server.

CHAPTER 14

Protecting against IP connection attacks

In This Chapter

About IP Lockouts

The IP Lockouts feature is designed to thwart dictionary attacks, which can shut down a server by flooding it with connection requests. WS_FTP Server can monitor connection attempts, identify possible abuse, and deny access to the FTP and SSH servers for the offending IP address.

You can set the criteria (connection attempts within a time period) which the IP Lockouts feature uses to block an IP address. If an IP address meets the criteria it is added to the Blacklist and blocked from further connection attempts. You can also specify how long an IP address remains on the blacklist.

Dictionary attacks are usually run by a script, which attempts to make connections randomly. When the connection attempts fail (due to being locked out), the script moves on to another server. So, in most cases, you do not need to keep the IP address in the Blacklist indefinitely. If a previous offender (IP address) tries again, the same IP Lockout Settings apply.

The Blacklist is maintained in the WS_FTP Server database and runs in memory whenever the FTP or SSH servers are running. For this reason, and because dictionary attacks are usually random, it is not necessary to keep entries in the Blacklist indefinitely.

For trusted IP addresses, you can bypass the IP Lockouts feature by adding the IP addresses to the Whitelist.

To enable IP Lockouts, see *Configuring IP Lockouts* (on page 128).

✓ We strongly recommend that the *IP Lockouts* (on page 128) feature be used instead of Access Control because IP Lockouts work at the server-level, blocking access when an offending IP address tries to establish a connection. As a result, the IP Lockouts feature is more efficient and secure, as it identifies an attack when the attack begins and it puts host resources out of reach.

When an IP address is added to Access Control and IP Lockouts is enabled, the IP address does not get added to the Blacklist. The Access Control setting will be used, so the IP address will be able to connect to the server, but then will be blocked at the host-level.

Configuring IP Lockouts

You can use the IP Lockouts settings to protect your FTP and SSH servers against repeated failed connections. For a description of the IP Lockouts feature, see *About IP Lockouts* (on page 127).

To enable IP Lockouts, or configure settings:

From the top menu, select **Server > IP Lockouts**. The IP Lockouts page opens.

This page is used to navigate to the pages associated with IP Lockouts.

- IP Lockouts Settings. Select this option to modify settings that determine if and when to block access from an IP address to your FTP and SSH servers.
- Blacklist. Select this option to to view the IP addresses that are not allowed to attempt to connect to the server (FTP or SSH), or to manually add an IP address to the Blacklist.

CHAPTER 15

Maintaining the Server

In This Chapter

Backing up WS_FTP Server

Batch scripts are provided to help you back up the configuration data store for your installation of WS_FTP Server. These files are located in the `C:\Program Files\Ipswitch\WS_FTP Server\utilities\` folder. These scripts are written to work with a standard installation. For installations with PostgreSQL in a location other than `C:\Program Files\PostgreSQL\bin\`, you must edit each file and change the location specified in the `%BINPATH%` variable.

To backup WS_FTP Server:

1 Run `backup_registry.bat` to export the registry keys for WS_FTP Server.

> **Note**: If your configuration includes a remote Ipswitch Notification Server or Ipswitch Log Server, you must copy `backup_registry.bat` to the remote servers and execute it there. For Ipswitch Notification Server, you must still back up the ips_notifications database using `INS_backup.bat` on the server where the PostgreSQL database server is installed.

2 Run `wsftp_backup.bat` to export the WS_FTP Server configuration data, located in the `ws_ftp_server` database, from the PostgreSQL database.

3 If your configuration includes an Ipswitch Notification Server, run `ins_backup.bat` to export the Ipswitch Notification Server configuration data, located in the `ips_notifications` database, from the PostgreSQL database.

4 Back up the files and folders located in the top folders of each host.

> **Warning**: The scripts provided will not back up host folders and files. You must manually back up the folders and files located under the host top folder.

Back up utilities

These utilities must be run from the command line interface. To open the command line interface, from the Windows desktop, select **Start > Run** and enter `cmd.exe`.

You can also schedule these scripts to run as a Windows scheduled task. For more information, consult the help system for your operating system.

WSFTP_backup.bat

Exports a backup of the WS_FTP Server database (ws_ftp_server) from the PostgreSQL database server to a file named `WSFTP_<timestamp>.backup`, with `<timestamp>` replaced by the current date and time.

Usage `WSFTP_backup.bat username password`

- **username**. The admin user for the PostgreSQL database
- **password**. The password for the admin user for the PostgreSQL database

INS_backup.bat

Exports a backup of the Ipswitch Notification Server database (ips_notifications) from the PostgreSQL database server to a file named `INS_<timestamp>.backup`, with `<timestamp>` replaced by the current date and time.

Usage `INS_backup.bat username password`

- **username**. The admin user for the PostgreSQL database
- **password**. The password for the admin user for the PostgreSQL database

backup_registry.bat

Exports the WS_FTP Server, Ipswitch Log Server and Ipswitch Notification Server registry hives to files named `IPS_Log_Server_<timestamp>.reg`, `IPS_Notification_Server_<timestamp>.reg` and `WS_FTP_Server_<timestamp>.reg`. with `<timestamp>` replaced by the current date and time.

Usage `backup_registry.bat`

Restoring WS_FTP Server from backup

In addition to the batch scripts provided to help you back up WS_FTP Server, one is provided to help you restore a backup.

This script, named `restore_backup.bat`, is located in the `C:\Program Files\Ipswitch\WS_FTP Server\utilities\` folder. This script is written to work with a standard installation. For installations with PostgreSQL in a location other than

C:\Program Files\PostgreSQL\bin\, you must edit the file and change the location specified in the %BINPATH% variable.

To restore WS_FTP Server from backup:

1. If you backed up the registry keys using backup_registry.bat, double-click on each registry file (IPS_Log_Server_<timestamp>.reg, IPS_Notification_Server_<timestamp>.reg and WS_FTP_Server_<timestamp>.reg. with <timestamp> replaced by the date and time when the backup was generated) to restore the backup data to the Windows registry.
2. Run restore_backup.bat to restore the WS_FTP Server configuration data to the ws_ftp_server database. The backup file is named wsftp_<timestamp>.backup, with <timestamp> replaced by the date and time when the backup was generated.
3. If you backed up an Ipswitch Notification Server database, run restore_backup.bat to restore the Ipswitch Notification Server configuration data to the ips_notifications database. The backup file is named ins_<timestamp>.backup, with <timestamp> replaced by the date and time when the backup was generated.

Note: You must run restore_backup.bat on the computer where PostgreSQL server is installed even if you are restoring configuration for a remote Ipswitch Notification Server.

Restore utility

This utility must be run from the command line interface. To open the command line interface, from the Windows desktop, select **Start > Run** and enter cmd.exe.

restore_backup.bat

Restores a backup of the WS_FTP Server or Ipswitch Notification Server database created with WSFTP_backup.bat or INS_backup.bat.

Usage restore_backup.bat username password dbname backupfile

- **username**. The admin user for the PostgreSQL database
- **password**. The password for the admin user for the PostgreSQL database
- **dbname**. The name of the PostgreSQL database to restore
- **backupfile**. The name of the file to restore; if located in another folder, provide the entire path, enclosing it in double quotes if it includes any spaces.

Warning: Use of restore_backup.bat will overwrite all changes made to the database since the backup file was created.

Note: restore_backup.bat does not restore the Windows registry keys. To do this, you must manually merge each key by double-clicking on it in the Windows explorer.

Prior to running restore_backup.bat, you must stop the WS_FTP Server, SSH Server, and your web server's services.

`Restore_backup.bat` will generate the following error:

```
pg_restore: [archiver (db)] Error while PROCESSING TOC:
pg_restore: [archiver (db)] Error from TOC entry 321; 2612 16386
PROCEDURAL LANGUAGE plpgsql
pg_restore: [archiver (db)] could not execute query: ERROR:  language
"plpgsql" already exists
    Command was: CREATE PROCEDURAL LANGUAGE plpgsql;
```

This error is expected and is not fatal.

Maintaining the WS_FTP Server data store

WS_FTP Server stores user and configuration data in a PostgreSQL database. In most cases, this database will not require any maintenance. If, however, you modify the configuration data of the server often (adding and removing users, folder permissions, rules or notifications), you may need to run periodic maintenance tasks on the database server.

To perform this routine maintenance, use the maintain_db.bat file located in the `C:\Program Files\Ipswitch\WS_FTP Server\Utilities\` folder.

Usage

```
maintain_db.bat username password
```

- **username**. The admin user for the PostgreSQL database
- **password**. The password for the admin user for the PostgreSQL database

CHAPTER 16

Server Modules

In This Chapter

About Server Modules

If your Ipswitch WS_FTP Server installation includes modules (purchased separately from Ipswitch WS_FTP Server), then you will see them displayed on the Modules page.

To navigate to the Modules page, click **Home > Modules**.

- WS_FTP Server Web Transfer Module

  WS_FTP Server Web Transfer Module is a web application that runs with Microsoft Internet Information Server (IIS) and lets your WS_FTP Server users access their accounts via a browser (using HTTP/S).

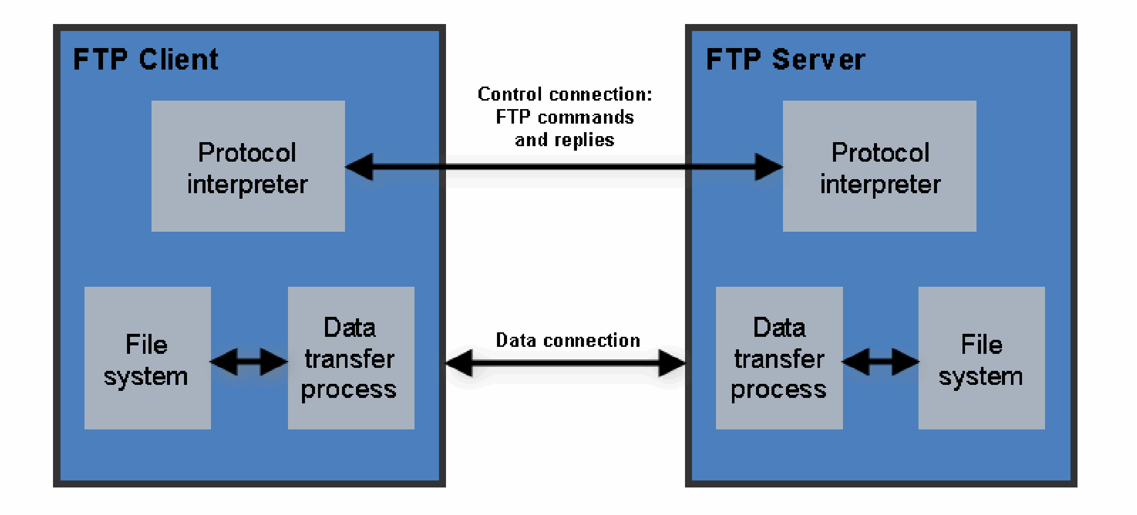
APPENDIX A

RFC 959 Highlights

Overview of RFC 959

File Transfer Protocol (FTP) 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 that 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 FTP 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

(for example, 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 modeis 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.

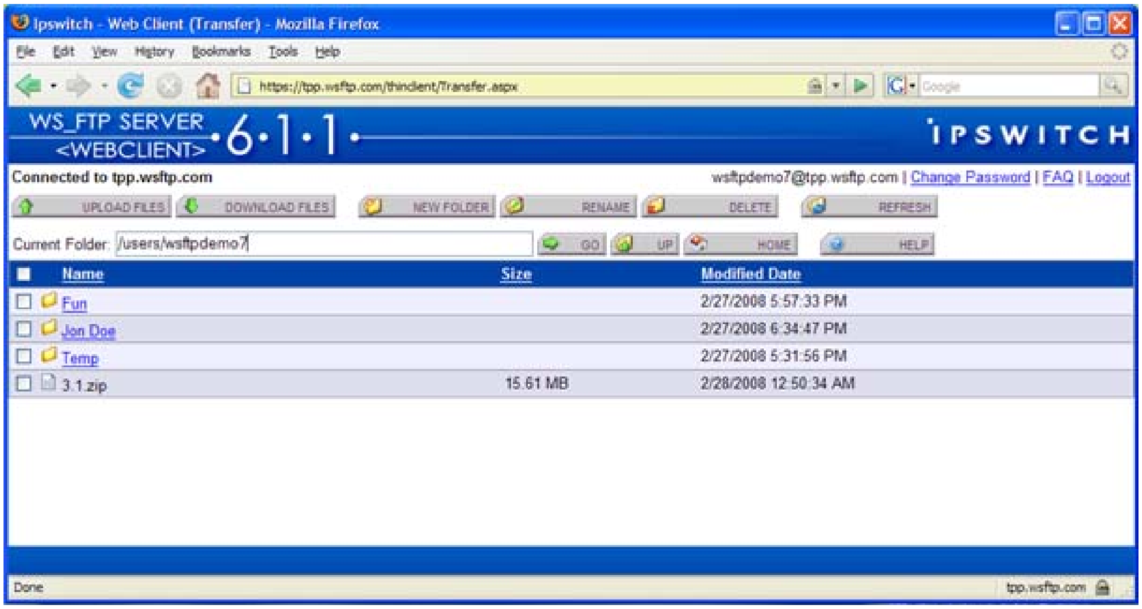
About WS_FTP Server Web Transfer Module

WS_FTP Server Web Transfer Module is a web application that runs with Microsoft Internet Information Server (IIS) and lets your WS_FTP Server users access their accounts via a browser (using HTTP/S).

No installation is required for the end user. The end user will open a web address in a browser and log on to their account using the Web Transfer Client.

You can enable Web Transfer access to any of your WS_FTP Server users. All existing user settings, rules, and notifications apply to the WS_FTP Server Web Transfer Module account.

For the end user, the Web Transfer Client offers easy, secure access via a browser, basic upload and download operations, and no client installation or maintenance.


Ipswitch - Web Client (Transfer) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tpp.wsftp.com/thinclient/Transfer.aspx
Google
WS_FTP SERVER
<WEBCLIENT>
6.1.1
IPSWITCH
wsftpdemo7@tpp.wsftp.com | Change Password | FAQ | Logout
UPLOAD FILES
DOWNLOAD FILES
NEW FOLDER
RENAME
DELETE
REFRESH
GO
UP
HOME
HELP
Done
tpp.wsftp.com

Connected to tpp.wsftp.com

Current Folder: /users/wsftpdemo7

	Name	Size	Modified Date
□	Fun		2/27/2008 5:57:33 PM
□	Jon Doe		2/27/2008 6:34:47 PM
□	Temp		2/27/2008 5:31:56 PM
□	3.1.zip	15.61 MB	2/28/2008 12:50:34 AM

For the administrator, WS_FTP Server Web Transfer Module provides secure file transfer via HTTPS, offers quick setup and rollout, and works the same across different operating systems and browsers.

To navigate to the Modules page, click **Home > Modules**. If you have the WS_FTP Server Web Transfer Module installed, you will see the following options:

- **User Web Access**. Use this page to give your users web access via the Web Transfer Client.
- **Web Access Settings**. If you installled the WS_FTP Server Web Transfer Module on a remote computer, use this page to specify a Windows account for the Web Transfer Client to use.

Index