

Welcome	5
Titan FTP Administrator Help System	5
Navigating the Administrator	6
New Server Wizard	9
Titan FTP Service	15
System Requirements	16
Contact Us	17
Configuration Options	18
Domains Overview	19
Servers Overview	25
Where is it?	28
Configuration Options	28
Where is it?	30
Configuration Options	30
Where is it?	31
Configuration Options	31
Where is it?	32
Configuration Options	32
Where is it?	36
Configuration Options	36
File Permissions	36
Folder Permissions	36
Titan FTP Permissions	37
Where is it?	38
Configuration Options	38
Where is it?	40

Configuration Options	40
FIPS 140-2 Compliance Settings	43
Where is it?	45
Configuration Options	45
Where is it?	48
Configuration Options	48
Where is it?	49
Configuration Options	49
Where is it?	52
Configuration Options	52
Where is it?	53
Configuration Options	53
Where is it?	54
Configuration Options	54
Where is it?	55
Configuration Options	55
Server Statistics List	55
Where is it?	59
Configuration Options	59
Performance Tips	59
Where is it?	61
Configuration Options	61
Groups Overview	62
Where is it?	68
Configuration Options	68
Where is it?	70
Configuration Options	70
FIPS 140-2 Compliance Settings	71

Where is it?	73
Configuration Options	73
SFTP Options	73
Cipher/MAC Settings	73
Server host key settings	74
Where is it?	78
Configuration Options	78
Where is it?	80
Configuration Options	80
Where is it?	81
Configuration Options	81
Where is it?	82
Configuration Options	82
Where is it?	86
Configuration Options	86
File Permissions	86
Folder Permissions	86
Titan FTP Permissions	87
Where is it?	88
Configuration Options	88
Where is it?	90
Configuration Options	90
Users Overview	91
Inheritance	97
Advantages of Using Inherited Settings	97
FTP Commands	98
srxCfg Command Line Utility Overview	101
srxCOM Overview	102

Certificate Management	104
CRC File Integrity Checking	108
Custom Message Variables	109
Events Overview	115
Inheritance	117
Server Log Tab	118
Remote Administration	119
Routers and Firewalls	120
SFTP Support	121
Shared Attributes	122
SSL Support	129
UNC Accounts	130
User Authentication	131
Virtual Folders	132
Wildcards	134
FAQ	135
How to create a Hostkey pair:	139
Troubleshooting - set logging level to debug	139
Report Issues	140
Configuring a New Server	141
New User Wizard	143
New Group Wizard	146

Welcome



Titan FTP Administrator Help System

2018

Welcome to Titan FTP, the secure data storage and transfer solution. Titan FTP is highly customizable, to provide you the greatest balance of **efficiency**, **security**, and **convenience**.

Here are a few good places to get started with your new software

- [Navigating the Administrator](#)
- [New Server Wizard](#)
- [Configuring a New Server](#)
- [FAQ](#)

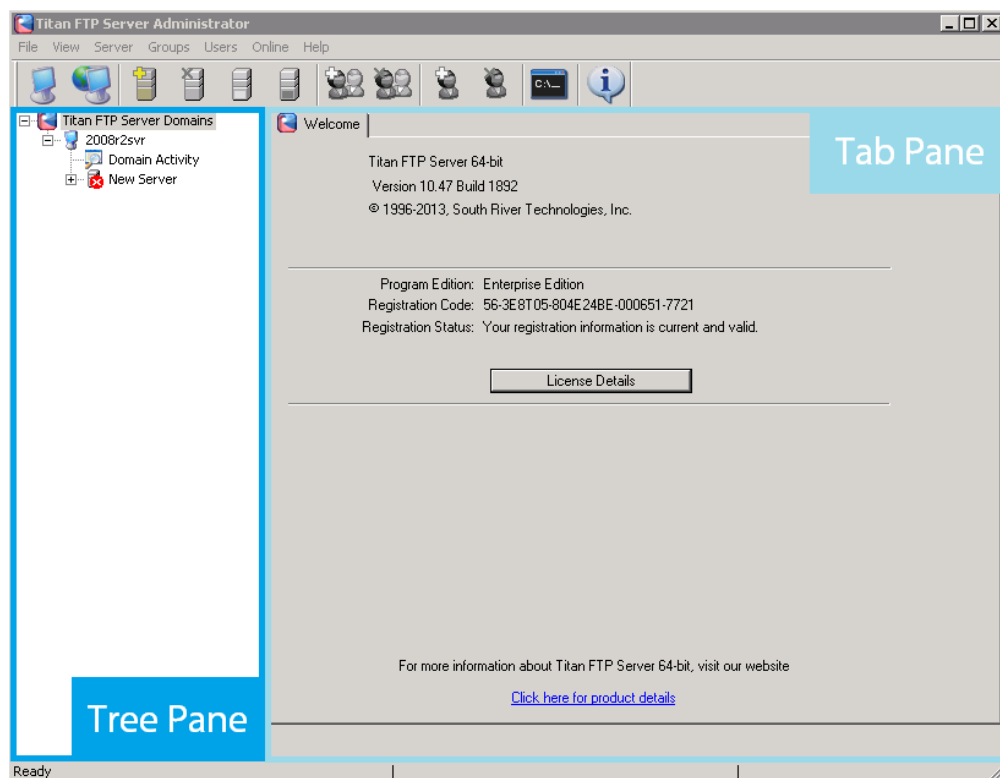
Can't find what you're looking for in this help system? Check out our online [QuickStart Guides](#) or [Submit a Ticket](#) through our free Knowledgebase.

Navigating the Administrator

The Titan FTP administrator is used to configure Servers, Groups, and Users, both locally and remotely.

To start the administrator, double-click the Administrator icon in the Titan FTP Program Group. There will also be a shortcut to the administrator on your Windows desktop.

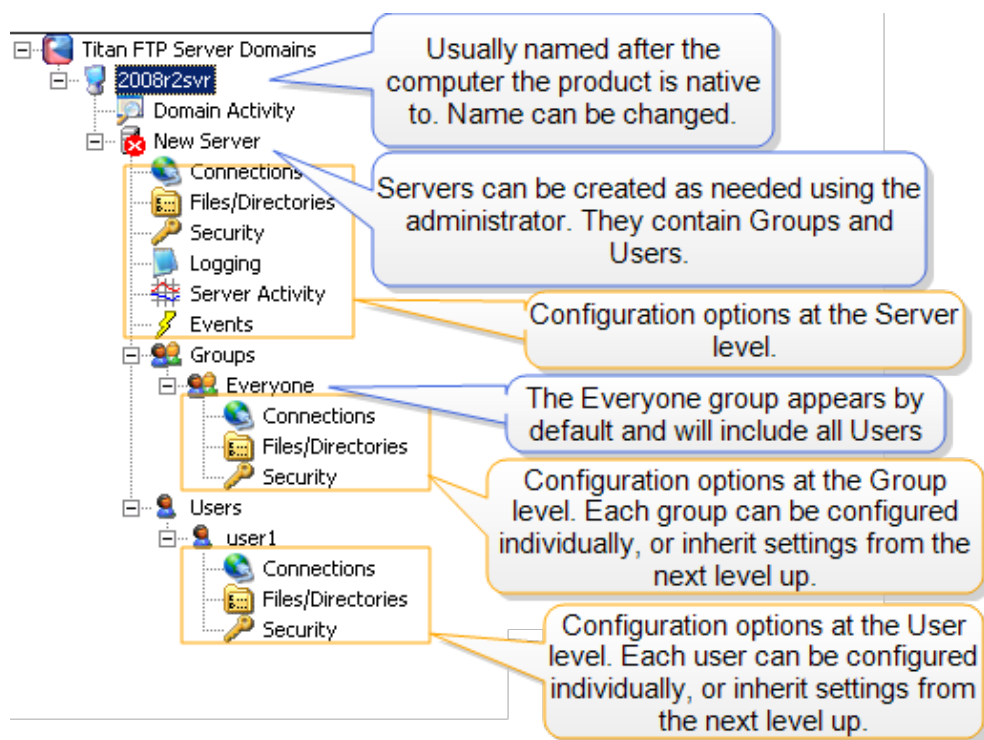
The administrator is a standard Windows application and contains a split screen with two panes separated by a vertical resizing bar:



Tree Pane

The left pane of the screen, or **Tree Pane**, displays the overall Titan FTP hierarchy of Domains, Servers, Groups, and Users (see Terminology). These can be expanded to reach subcategories with more specific settings, such as Security and Events.

There are several levels to this tree. Starting from the broadest and going to the most specific level of control:



- [Domains Overview](#) - A group of networked computers which exist as essentially one computer. Within each domain are individual servers.
- [Server](#) - A software construct that independently holds directories of data. Several servers can be linked, so and information can be shared between them. See Clustering. Servers contain groups and users.
- [Groups](#) - A category used to identify members and consolidate their privileges. Group members have all of the rights granted to the group, unless overridden at the User level.
- [Users](#) - Individual accounts with a username and password and a list of rights for how they may interact with the server.

Each level offers different configuration options, many of which can be inherited down through the chain.

See our topic on [Inheritance](#) for more information.

Tab Pane

The right pane of the screen, or **Tab Pane**, displays configuration information and options based on what is currently selected in the Tree Pane. When you click on items in the Tree Pane, the Tab Pane changes to display different Dialog Tabs. Each Dialog Tab in the Tab Pane displays information and options relevant to the selected item.

The administrator and the Titan FTP Service are different; the service may be running while the administrator isn't visible.

See our topic on the [Titan FTP Service](#).

New Server Wizard

New servers can be created and configured at any time using the New Server Wizard. The New Server Wizard can be launched from within the Titan FTP Server Administrator in two ways:

1. Right-click the Domain in the Tree Pane and select New Server Wizard from the context menu.
2. From the menu bar, select New Server, which will open the New Server Wizard.

The New Server Wizard walks you through the steps required to configure and connect a new server. You can modify the server configuration after the server has been created. There will be more features and configuration options available once the server is created. Use the Titan FTP Administrator to modify server properties.

Launching the New Server Wizard

[Launch the Titan FTP Server Administrator to create a new server...](#)

You can access the Administrator program by double-clicking on the Administrator icon in the Titan FTP Program Group. Once the Administrator program is running, select Server then New Server Wizard from the main menu bar to launch the Titan FTP New Server Wizard.

General Settings

[Enter the general information for your new server...](#)

Server Name: Enter a unique name for your server. This will identify it in the tree pane.

Server Description: Optionally enter a description for this server, such as its purpose or location.

IP Address: The IP Address the server will listen on. You can type a specific IP address, or you can select Any Available IP Address. We recommend Any Available IP Address if your network has a multiple IP addresses.

WAN Address: Enter the outward-facing IP address given to you by your ISP.

Data Directory: The base directory where all data will be stored.

Advanced Settings: Specify directory locations. Setting all directories in a single location from the start makes future configuration easier.

Log Directory: The directory to which the server will save its logs.

Start Server When Titan FTP Services starts: Select the check box to enable. When enabled, the server will automatically be started when Titan FTP starts.

Create standard unix directories (/bin, /incoming, /pub, /usr): Creates the standard Unix server folders under the Titan FTP server data folder, to create a cohesive unix layout.

Services

Use the check boxes to select services, or protocols, this server will handle when transferring files...

- FTP (typically port 21)
- FTPS (typically port 990)
- SFTP (typically port 22) (Only available in Enterprise Editions of Titan FTP Server)
- HTTP (typically port 80) (Only available with optional WebUI)
- HTTPS (typically port 443) (Only available with optional WebUI)

You must enable FTP access if you are using FTPS with explicit SSL (also known as AUTH SSL).

For more information, see our topics on the [AUTH](#) command or [SSL Support](#).

User Authentication

Titan FTP supports various methods of user authentication...

Select the desired authentication method from the dropdown list of authentication methods.

User Authentication Database: Select the appropriate user authentication method for your server.

Authentication Server Setup: If you are not using native Titan FTP authentication, select Authentication Server Setup to launch the User Authentication Wizard. The authentication wizard will help you to configure Titan FTP to work with your back end authentication server.

Auto Assign Home Directories: Enable this feature if you would like Titan FTP to automatically generate the user's home directory. If this feature is enabled, users will have their home directory created under the /usr/ folder in the Server Data Directory.

For more information, see our topic on the [User Authentication Wizard](#).

FTP Services

The FTP Services dialog allows you to configure the basic parameters necessary for running FTP on the server...

If you didn't select FTP in the Services section of the wizard, you won't see this step.

Enable FTP Services: Enable this option to have Titan FTP start the FTP server subsystems. If this option is disabled, FTP and FTPS will not be available on the server.

FTP Port: Select the appropriate port for FTP. The default port is port 21.

Enable anonymous FTP access: If this option is enabled, users will be able to connect to the Titan FTP server using anonymous as the username.

This server is sitting behind a router: Enable this option if Titan FTP will be installed behind a firewall or router. This feature is very important. If it is not configured properly, users will still be able to connect to your server, but they may not be able to transfer files or view directory listings.

Extern WAN IP address of router: If Titan FTP is behind a router/firewall, enter the public/external IP address of the router. This will be used by Titan FTP in the FTP PASV response. Titan FTP will return the external IP address to the client so that the client can then open a data connection back to Titan FTP by way of the router.

Use internal server IP in PASV response: If Titan FTP is behind a router/firewall, and you plan to have clients who are outside of the firewall and clients who are inside the firewall on your corporate LAN, then enable this feature so that local LAN clients can connect passively and receive the internal LAN IP from Titan FTP in the PASV response.

Note: You must enable FTP access if you are using FTPS with explicit SSL (also known as AUTH SSL).

For more information, see our topics on the [AUTH](#) command or [SSL Support](#).

FTPS/SSL Security Settings

The FTPS/SSL Services dialog allows you to configure the basic parameters necessary for running FTPS/SSL on the server...

Enable SSL/TLS access on this server: Enable this option to have Titan FTP start the FTPS server subsystems. If this option is disabled, FTPS will not be available on the server.

Enable explicit SSL/TLS access (User connects using the AUTH SSL command): Enable this option to use explicit mode FTPS. When you use explicit mode, the FTP client will send an AUTH SSL or AUTH TLS command to the server if it intends to secure the connection.

Enable implicit SSL/TLS (User connects to a special port for SSL/TLS services): Enable this option to use implicit mode FTPS. When you use implicit mode, FTPS is initiated to the FTP server on a separate secure port, usually port 990. All traffic over that port is secured.

Implicit SSL/TLS port: Use the up/down arrows to select the port. Port 990 is the default port for implicit SSL/TLS.

Use the following certificate for this server: Use the dropdown arrow to select the certificate, or click Certificate Management to create or import a certificate.

Enter the password associated with this certificate: Type the Password for the selected certificate.

Certificate Store Folder: This is the location where Titan FTP will store all certificates for this server.

Note: Local paths and UNC shares are supported; do not use a mapped drive because mapped network drives are not accessible from the Titan FTP service.

Ensure FIPS Compliance for SSL Titan FTP does not support SSL v2 and will reject any client that attempts a connection using SSL v2.

Require trusted certificates from clients who connect securely: If enabled, the client users will need to supply a trusted TLS certificate in order to connect to this server.

SFTP/SSH Settings

The SFTP/SSH dialog allows you to configure basic SFTP/SSH settings for this server...

See [SFTP Support](#) for more information.

Enable SFTP on this server: Enables/disables SFTP connections for the server. SFTP, SSH's Secure File Transfer Protocol, is a special subsystem of SSH and is different from FTP and FTPS.

SFTP Port: Port used for SFTP connections. The default SFTP port is port 22.

Use the following host key for this server: Select an existing host key to be used by the server. If no host keys are available, use the Host Key Management utility to create a new server host key pair.

Host Key Management: Launches the Titan FTP Host Key Management utility that allows you to create, import, export, and manage SSH host keys used by Titan FTP.

Host key password: Enter the password used to secure the private key portion of the selected host key. Titan FTP will not accept host key pairs that are not secured by a password. Passwords used to secure the private key portion of a host key pair must be at least 4 characters in length.

Host Key Folder: Enter the fully qualified path where Titan FTP SSH host keys will be stored.

Note: Local paths and UNC shares are supported; do not use a mapped drive because mapped network drives are not accessible from the Titan FTP service.

Kick user if they present an invalid host key: Enable this option to kick users if they do not present a valid, preconfigured host key.

HTTP/HTTPS Settings

The HTTP/HTTPS dialog allows you to configure basic HTTP/HTTPS settings for this server...

Enable HTTP browser based interface to Titan FTP : Select the check box to enable HTTP protocol on this server.

IP Address: Use the dropdown arrow to select your IP address. Any Available IP Address indicates that the server will listen on all IP addresses that are configured on the computer, along with the local IP address of 127.0.0.0, also known as localhost.

Port: Type in your port number. The default port is port 80.

Enable HTTPS/SSL browser based interface to Titan FTP : Select the check box to enable HTTPS protocol on this server.

IP Address: Use the dropdown arrow to select your IP address. Any Available IP Address indicates that the server will listen on all IP addresses that are configured on the computer, along with the local IP address of 127.0.0.0, also known as localhost.

Port: Type in your port number. The default port is port 443.

Use the following certificate for this server: Use the drop-down arrow to select the certificate to be used for this server.

Certificate Management: Launches the Certificate Manager, which can be used to create, import, and manage certificates.

Enter the password associated with this certificate: Type in the certificate password.

Require trusted certificates from clients who connect securely: If enabled, the client users will need to supply a trusted TLS certificate in order to connect to this server.

Web Services

Web Interface Services: Select the check box to enable access to this server using the Titan FTP Web User Interface (WebUI).

Disable the saving of Login credentials in Web Interface (AutoComplete): User's browsers will not be allowed to save passwords.

WebDAV Services: Enable this option to allow WebDAV (Web Based Distributed Authoring and Versioning) protocol support for the server. WebDAV allows locking of files to prevent conflicting save files and duplication. If enabled, WebDAV support will be active only on <url>/webdav/ URIs.

File Sharing Services: Enable this feature to allow File Sharing, QuickSend, QuickLinks, and DropZone within the WebUI.

Advanced

Require Logon to access QuickLinks: If enabled, named Cornerstone users will be required to log in before accessing quicklinks. For non-named/ad-hoc users (ie, users known only by their email addresses) will be required to enter their email address as a valid login verification before accessing the quicklink.

Enable sharing with public users (Ad-Hoc Sharing): If enabled, named cornerstone users will be permitted to share files and folders with non-named users by specifying a valid email address for the user.

Use HTML format for email: If enabled, emails will be sent out in html format. Recommended so that the QuickLink URL is more friendly.

Enable Active Directory Impersonation for Sharing: If enabled, Titan FTP will use the specified AD (Active Directory) user impersonation context when the recipient of a QuickLink clicks to access the file. This is very important when running in an environment where Titan FTP is using NTFS permissions and AD user credentials. Since the recipient of the QuickLink might not have an account on the local AD LAN, Titan FTP will need to be able to access the file on behalf of the end user. It will use these credentials to gain access to the file on behalf of the client user.

Advanced File Sharing

QuickSend Enabled: If enabled, a QuickSend box will appear in the lower left corner of the Web UI. This box will allow a named Titan FTPUser to drag and drop files from their local computer and share/send those files to another user securely.

QuickSend Data Directory: Specify a temporary location for QuickSend files.

DropZone Enabled: Enable this feature to allow the named Titan FTP server users to create DropZones allowing external clients to submit files with form data to Titan FTP.

Mail Services

Some features of Titan FTP, including the Events Manager, have the ability to send e-mail...

This page will allow you to configure the base e-mail settings to be used with Titan FTP.

For more information on these settings, see [Server Email Tab](#).

For more information on creating new servers, see the tutorial on [Configuring a New Server](#).

Titan FTP Service

Titan FTP runs as a system service or background process. You can configure Titan FTP to start with Windows, or you can configure it to require a manual start.

To check and/or modify the startup setting for the Titan FTP Server Service:

1. Click Start and then click Control Panel.
2. Navigate to **Administrative Tools** and double-click **Services**, or search for Services.
3. Right-click the Titan FTP **Daemon** and click **Properties**.
4. Select the **Startup type** you prefer from the dropdown menu.
 - Automatic (delayed start): The Titan FTP Service will start two minutes after the last boot task has ended when the computer starts. This is a way to start the service automatically without slowing normal boot processes.
 - Automatic: The Titan FTP Service will start along with the boot process of the computer.
 - Manual: Start the Titan FTP Service yourself every time you would like to run it.
 - Disabled: The Titan FTP Service will never run on this computer unless it is re-enabled.

Note: The Titan FTP Service will run under the context of the standard LocalSystem or LocalService Windows User Account. When a user connects to the Titan FTP server, the Windows User Account performs all file access on behalf of the logged in client user. Therefore, if there are files on a UNC Titan FTP will be accessing, the service must be re-configured to use a Windows User Account with proper NTFS (New Technology File System) permissions to the UNC share.

See our topic on using [UNC Accounts](#) with Titan FTP.

System Requirements

Titan FTP Server

- Windows 7, Windows 8, 2008, 2012
- Microsoft .Net v4.0 (required to use the WebUI features)

For Windows 64-bit platform, the Statistics/Tracking features in Titan FTP will require SQL Server 2005. Windows 32-bit can run on the default Microsoft Access.

Note: Windows Server 2003 is no longer supported. SRT will not be able to provide technical support for Titan FTP running on Windows 2003. Windows Server 2008 is the minimum OS requirement to utilize the WebUI of Titan FTP, which makes calls to the v6 Shell only available in newer OS.

WebUI

When accessing the server products from a browser, the following browsers are supported.

- Chrome v40 and later
- Safari v8 and later
- FireFox v35 and later
- Microsoft Internet Explorer v10 and later (required because IE9 and older do not fully support drag-drop, JQuery/HTML5)

Contact Us

Headquarters:	South River Technologies 1910 Towne Centre Blvd Suite 250 Annapolis, MD 21401 USA
Main:	443-603-0290
Toll Free:	1-866-861-9483
Fax:	1-410-266-1191
World Wide Web:	www.TitanFTP.com
Office hours:	Monday to Friday 8:30 A.M. to 5:30 P.M. Eastern Time, GMT-5:00
Sales Telephone:	1-410-266-0667
Sales Fax:	1-410-266-1191
Sales Email:	sales@southrivertech.com
Online Support:	https://titanftp.com/support/

For technical support questions, see our topic on [Report Issues](#).

Configuration Options

Titan FTP allows you to configure a wide variety of granular controls at several levels:

- [Domains Overview](#)
- [Servers Overview](#)
- [Groups Overview](#)
- [Users Overview](#)

The options start with the most general at the Domain level and move to the most specific at the User level. Many of the options on the lower levels of the tier system are inherited from the general settings by default. This can be changed on an individual basis.

For more information, see our topic on [Inheritance](#).

Domains Overview

A **Domain** is the physical computer on which Titan FTP is installed. The primary use of the domain is to provide a grouping for the server or servers running on that computer. You will use the [Titan FTP administrator](#) to connect to the domain and to configure your servers.

Once you have connected, the domain will display in the tree pane. Selecting the domain will bring up the **Local Administration** and **Remote Administration** tabs.

Local Domain Wizard

The first time the administrator is executed, the **Local Domain Wizard** will be launched.

The Local Domain Wizard ensures that your computer is properly configured. Along with other configuration options, you will need to specify the username and password to be used for local administration. Save this information; each time you run the administrator program and connect to the local domain, you will be prompted for the username and password for authentication.

The local domain name will appear in the Tree Pane of the administrator as the direct child of the Titan FTP Domains level of the tree.

Note: Recently, **Java Enterprise Server has started using port 31000**, which has been the default Local Administration Port for Titan FTP. Depending on which service starts first, Java Services may block the Titan FTP service and prevent it from starting. As a result, the Tray App will not be able to contact the service, and/or the administrator may not be able to log into the administrator console. This will also create conflicts with the srxCFG and srxCOM utilities. For information on changing your Local Administration Port, see our topic on [Local Administration Tab](#).

Local Administration Tab

The **Local Administration** tab will allow you to alter Titan FTP configuration options for servers within your local network.

Where is it?

The Local Administration tab can be found in the Titan FTP administrator by selecting the domain in the tree pan and selecting the Local Administration tab.

Configuration Options

Local Administration Settings: This text box contains your local IP Address, selected port, and admin username and password. See the **note** below about the default Local Administration Settings port 31000.

Administration IP Address: The IP address

Administration Port: By default, this is port 31000. See our **note** below.

Admin Username: The username with which you will need to log into the administration console. If you are logged in locally, you can choose to prevent remote administrators from changing this username by disabling **Allow Remote Admin to change local credentials** on the [Remote Administration Tab](#).

Password: The password with which you will need to log into the administration console. If you are logged in locally, you can choose to prevent remote administrators from changing this username by disabling **Allow Remote Admin to change local credentials** on the [Remote Administration Tab](#).

Domain Name: By default, this is the same name as the physical computer. You can change this name to any text. The local domain is not displayed to the client by default, but you can configure custom messages to display the name of the domain.

See our topic on [Custom Message Variables](#).

Domain Description - This text box provides you the option to further describe the domain.

Data Directory - The domain Data Directory setting defines the default storage location for Server data. This value is used to prime the Server Data Directory entry in the Server Wizard. For each new Server, the domain data directory and the new server name will be concatenated to produce the full path to the data directory where the Server data will be stored. This value can be either a fully qualified path, such as **C:\Mydata**, or a UNC name such as **\\Server\Share\MyData**.

Logfile Directory - The domain Log Directory setting defines the default storage location for Server logs. This value will be used to prime the Server Log Directory entry in the Server Wizard. For each new server, the domain log directory and the new server name will be concatenated to produce the full path to the log directory where the Server logs will be stored. This value can be either a fully qualified path, such as **C:\ MyLogs**, or a UNC name such as **\\Server\Share\MyLogs**.

Start Titan FTP Service when Windows Boots - This option allows you to configure whether or not the Titan FTP Service will start automatically when Windows starts. If this option is enabled, the Titan FTP Service starts automatically when Windows starts. Once the Service starts, any servers that you have configured to start when the Titan FTP Service starts will also launch. Titan FTP Service is installed as a Windows Service and follows the rules for starting automatically.

Start Titan FTP Tray Applet when Windows Starts - This option allows for the automatic launching of the Tray applet used to display/start/stop the Server Service.

Note: Recently, **Java Enterprise Server has started using port 31000**, which has been the default Local Administration Port for Titan FTP. Depending on which service starts first, Java Services may block the Titan FTP service and prevent it from starting. As a result, the Tray App will not be able to contact the service, and/or the administrator may not be able to log into the administrator console. This will also create conflicts with the srxCFG and srxCOM utilities. For information on changing your Local Administration Port, see our topic on [Local Administration Tab](#).

To change your Local Administrator Port

1. Stop/Close the Tray App and Admin App, and stop the Titan FTP Service in the Windows Control Panel.
2. Run RegEdit.
3. Go to **HKLM\Software\South River Technologies\Titan FTP Server\LDomain**.
4. Change the LASPort setting from 31000 to another large port number, such as 31100.
5. Close RegEdit.
6. In the Windows Control Panel, restart the Titan FTP Service.
7. Run the Admin utility and log in. You should see the new port number displayed in the login box..

Remote Administration Tab

The **Remote Administration** tab allows you to configure the Titan FTP administrator to connect to a Titan FTP Service installed on a remote computer, either on your intranet or over the Internet.

Where is it?

Before you can connect to this local domain from a remote location, you need to enable the Remote Administration feature for the local domain.

Configuration Options

Allow Remote Administration of this Domain: Enables remote administration to allow you to connect to this local domain and make changes from another location.

Administration IP Address: This is the address the local domain will listen on for remote administration connections.

Administration Port: This is the port the local domain will listen on for remote administration connections. This port cannot be the same port that is used for local administration. For example, if you have remote administration enabled, the Titan FTP Service will open two separate listener sockets, one on the **loopback: localport** for local administration and one on the **remoteaddress: remoteport** for remote administration.

Allow Remote Admin to change local credentials: This option, which allows a remote administrator to change the username and password fields on the [Local Administration Tab](#), is only available to local administrators, as a security precaution. Remote administrators will see the setting grayed out, whether it is enabled or not.

Domain Activity

Selecting the Domain category in the Tree Pane will open two tabs: **Domain Activity** and **IP/Ports In Use**.

If the Titan FTP Administrator application is connected to a remote domain, servers configured and running on the remote domain will be displayed on this tab.

Domain Activity Tab

The Domain Activity tab will display a list of servers currently configured and running on the domain to which the Administrator application is connected.

Click Domain Activity in the tree panel, then select the Domain Activity tab. For each server configured and running on the domain, this list will display the following:

Server Name: The name of the server as defined on the domain.

Start Time: The date and time that the server was started, in local 24-hour time.

Connections: The total number of active connections on the server. Connections represent any communication between the client and server, including uploads and downloads. There can be several connections to every session.

Active Sessions: The number of users currently logged into the server. Active sessions can continue briefly even after the client and server become disconnected.

Bytes Sent: The total number of bytes that have been sent by the server to the various client connections.

Bytes Received: The total number of bytes that have been received by the server from the various client connections.

File Bytes Sent: The number of bytes sent from the server that were specifically file data.

File Bytes Received: The number of bytes received by the server that were specifically file data.

Total Uploads: The total number of files that have been successfully uploaded to the server since the server was started.

Total Downloads: The total number of files that have been successfully downloaded from the server since the server was started.

Average KPS: The average KPS (kilobytes per second) for data transferred to and from the server since the server was started.

Domain IP/Ports In Use Tab

The IP/Ports In Use tab displays the IP addresses and ports the Titan FTP system is currently using.

To access the IP/Ports In Use tab, click Domain Activity in the Tree Pane and the IP/Ports In Use tab. There will be zero or more servers listed, depending on how many servers are configured on this domain.

For each server defined on the domain, FTP, FTPS, SFTP, or HTTP may be listed. This utility will not show non-Titan FTP IP addresses and ports that are in use. To display a complete list of all IP addresses and ports that are in use on the local computer, open a command prompt and use the **NETSTAT** utility.

Note: To diagnose which application is using a specific port, use the command line utility NETSTAT with the -b argument to display a list of IP addresses and ports that are in use on the computer. The -b argument will display the executable that is using the IP address/port.

Depending on the type of connection you have, either Local or Remote, you will see these types of servers in the list:

Local Administration Server: This is an internal system server that is used to interact with the Local Titan FTP Administrator. By default, this internal server will listen on IP address **127.0.0.1** (localhost), port **31000**.

Remote Administration Server: This is an internal system server that is used to interact with the Titan FTP Service from a remote Titan FTP Administration console. If Remote Administration is enabled on the domain, this server will listen on port **31001** for incoming connections from the Remote Titan FTP Administration utility.

Note: Recently, **Java Enterprise Server has started using port 31000**, which has been the default Local Administration Port for Titan FTP. Depending on which service starts first, Java Services may block the Titan FTP service and prevent it from starting. As a result, the Tray App will not be able to contact the service, and/or the administrator may not be able to log into the administrator console. This will also create conflicts with the srxCFG and srxCOM utilities. For information on changing your Local Administration Port, see our topic on [Local Administration Tab](#).

Servers Overview

Titan FTP supports the ability to configure multiple server instances under a single domain or physical computer. Each server instance listens on its own IP address and port combination, which provides the ability to have a virtually unlimited number of servers running simultaneously.

The Server level includes the widest variety of configuration options and the highest level of [inheritable](#) control. Many of the options available at the server level appear at the group and user level, and would only apply to that specific group or user if altered.

Each server can be configured to store data in its own separate data directory, either on your local hard drive or on a shared network drive. Titan FTP supports both standard DOS path syntax and UNC paths.

Note: Do not use mapped drives or paths that point to a mapped drive. These are not accessible from the Titan FTP service; use a [UNC](#) path instead.

More on Servers

- [Creating Servers](#)
- [Configuring Servers](#)
- [Deleting Servers](#)
- [Backup and Restore Servers](#)

Connections General

The **Connections General** tab is used to configure general connection settings.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the Connections General tab at the **Server** level, expand the Server in the tree pane, click Connections, then click the Connections General tab.

To access these settings at the **Group** or **User** level, in the tree pane click the Group or User, click Connections, and then click the Connections General tab.

Configuration Options

Use Inherited Setting: This check box appears on the **Group** and **User** levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Max Concurrent Connections: The total number of concurrent sessions that may be established at once.

Idle Connection Time-out: The maximum amount of time, in minutes, the server will wait before dropping a user due to inactivity.

Max Connections/IP: The total number of concurrent connections a user can establish from any given IP address.

Max Upload Speed: The total KPS (Kilobytes Per Second) upload speed the server will allow from the user. If the user attempts to exceed this bandwidth allotment, the server will pause the transfer and slow it down to the proper speed.

Max Download Speed: The total KPS (Kilobytes Per Second) download speed the server will allow for data to be sent to the user.

Max Uploads/Session: The total number of files that may be uploaded per session. Once this limit has been reached, the user will not be able to upload/replace any files until they log out and log back in.

Max Downloads/Session: The total number of files that may be downloaded per session. Once this limit has been reached, the user will not be able to download any files until they log out and log back in.

Max File Upload Size: Specifies the maximum file size that can be uploaded by the user. Any attempt to upload a larger file will be aborted and the file will be deleted from the system.

Max File Download Size: Specifies the maximum file size that may be downloaded by this user. Any attempts to download files larger than this value will be denied.

Connections Advanced Tab

The **Connections Advanced** tab is used to configure advanced connection settings.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the Connections Advanced tab at the Server level, expand the Server in the tree pane, click Connections, then click the Connections Advanced tab.

To access these settings at the Group or User level, click the Group or User in the tree pane, click Connections, then click the Connections Advanced tab.

Configuration Options

Use Inherited Setting: This check box appears on the Group and User levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Disable account after X invalid password attempts: When enabled, the user account will be disabled after the specified number of consecutive incorrect password attempts.

Kick user after X consecutive bad commands: When enabled, the user connection will be dropped after the user types the specified number of invalid commands.

Disable user account afterwards: This option becomes available if you choose to kick the user after a certain number of bad commands. Select this to disable the account after the number is reached.

Ban access from IP address once this happens: This option becomes available if you choose to kick the user after a certain number of bad commands. Select this to ban the user's IP address from the server after the number is reached.

Allow PASV Mode Connections: When enabled, allows the server to be placed in [PASV](#) mode by the client. If this feature is disabled and the client attempts to issue a PASV command, they will receive a 502 Not Implemented response.

Allow EPSV Mode Connections: Similar to the PASV command, but used for IP v6 addressing. When enabled, allows the server to be placed in [EPSV](#) mode by the client. If this feature is disabled and the client attempts to issue a EPSV command, they will receive a **502 Not Implemented** response.

Limit PASV Port range from: Allows you to specify a specific range of ports that the server will use when the user issues a [PASV](#) command. This is useful if the server is behind a fire-wall/router and you only want to open a specified range of ports for use by the server.

Delete Partially Uploaded Files: When enabled, the server will delete any files that are not successfully uploaded. For example, if a [STOR](#) or [STOU](#) does not complete successfully, the file will be deleted from the server.

Block Anti-Timeout Schemes: When enabled, the server will ignore [NOOP](#) commands as attempts are made to keep the connection alive.

Block FTP Bounce Attacks and FXP: When enabled, the server will not accept any data connections from IP addresses other than the user's primary connection.

Allow change of password (SITE PSWD): When enabled, users are permitted to change their password using the [SITE PSWD](#) command.

Connections IP Access Tab

The **IP Access** tab is used to configure IP access restrictions, which affects specific users logging onto the Titan FTP server.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the IP Access tab at the **Server** level, in the tree pane expand the Server, click Connections, and then click the IP Access tab.

To access these settings at the **Group** or **User** level, in the tree pane expand Groups or Users, select the appropriate group or user, click Connections, and then click the IP Access tab.

Configuration Options

Use Inherited Setting: This check box appears on the **Group** and **User** levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Enable IP Access Restrictions: When enabled, IP Access restrictions will be applied at this level whenever a user attempts to connect.

Grant/Deny access to all IP Addresses by default: Select the default action that will be applied at this level when a connection attempt is made.

Except the addresses listed below: Use the Add button to enter a list of IP addresses that will be the exception to the default rule. For example, you can Deny Access by default and type a single IP address, which will then be the only IP address the user will be permitted to connect from.

Connections Upload/Download Ratios Tab

The **Upload/Download Ratios** tab is used to configure Upload/Download ratios.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the Upload/Download Ratios tab at the **Server** level, in the tree pane expand the Server and click Connections, and then click the Upload/Download Ratios tab.

To access these settings at the **Group** or **User** level, in the tree pane, expand Groups or Users, select the Group or User, click Connections, and click the Upload/Download Ratios tab.

Configuration Options

Use Inherited Setting: This check box appears on the Group and User levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Enable Upload/Download Ratios: When enabled, the user will have Upload/Download ratios applied to their sessions.

Count # of Files Per Session: Ratios will be applied at the file level on a per-session basis. Each time the user disconnects from the server, the counters are reset. If the user has multiple concurrent sessions open, statistics are applied for each individual session.

Count KBytes Per Session: Ratios will be applied at the file size level on a per-session basis. Each time the user disconnects from the server, the counters will be reset. If the user has multiple concurrent sessions open, statistics are applied for each individual session.

Count # of Files across All User Sessions: Ratios will be applied at the file level across all concurrent sessions for the user.

Count KBytes across All User Sessions: Ratios will be applied at the file size level across all concurrent sessions for the user.

Ratio: Enter the upload to download ratio for the user. For example, you may want to require that the user upload two files for every one file they download. The ratio would be Uploads 2, Downloads 1. You may also want to require that the user upload 1MB of data for each 1MB of data that they download, so the ratio would be Upload 1000, Download 1000, and select the Count KBytes option.

Free Files List: Use the New Free File Name form to add a list of files/file types that will be excluded from the ratios.

Connections Messages Tab

The **Messages** tab is used to configure custom messages. Any message displayed in the Messages tab list can be altered to show a custom message relevant to your server.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access these settings at the **Server** level, in the tree pane expand the Server, click Connections, then click the Messages tab.

To access these settings at the **Group** or **User** level, in the tree pane select the Group or User, click Connections, then click the Messages tab.

Configuration Options

Message Type: Select the message to customize. The current message will be displayed in the Message Text field. Most messages have a description of their meanings.

[Click here to see the list of messages and descriptions.](#)

Welcome Message - Displayed after a successful login.

Quit/Logout Message - Displayed as part of the [QUIT](#) response.

Kicked Message - Displayed when a user is kicked off the server.

Banned Message - Displayed to a banned user.

Max Connects Message - Displayed when Max Connections reached.

Max IP Message - Displayed when Max Connections from a single IP is reached.

Banned File Type Message - Displayed after an attempt to upload a banned file type.

Disk Quota Exceeded Message - Displayed to users after quota has been exceeded.

Expired Account Message - Displayed to a user with an expired account.

Account Disabled Message - Displayed to a user when their account has been disabled.

Maximum Upload File Size Exceeded Message - This message will display for users when the file size of an upload is larger than the limit set by the admin on the Connections General Tab in the **Max File Upload Size** field.

Maximum Download File Size Exceeded Message - This message will display to the user when the file size of a download is larger than the limit set by the admin in Connections General Tab in the **Max File Download Size** field.

Site-To-Site/FXP Error Message - Site-to-Site transfers (file transfers from one FTP server directly to another) are not enabled in Titan FTP by default. To enable secure Site-to-Site/FXP transfers, navigate to the Security category, select the FTPS/SSL tab, and check **Enable secure site-to-site (FXP) file transfers (CPSV/SSCN)**.

Maximum Number of Files Downloaded Message - This message is displayed when a user has exceeded the maximum number of allowed downloads in a specific session defined in the Connections, **Max Downloads/Session** field of the administrator.

Maximum Number of Files Uploaded Message - This message is displayed when a user has exceeded the maximum number of allowed uploads in a specific session defined in the Connections, **Max Uploads/Session** field of the administrator.

Banner Message - Displayed after connecting to the server

Anonymous access disabled Message - Anonymous access is disabled by default. It can be enabled in the admin by selecting your server in the left-hand tree-pane, navigating to the FTP tab, and checking **Allow Anonymous Access**. With anonymous access off, any user trying to log in anonymously will get the default error message.

Server Offline Message - Displayed when the server is offline or stopped. This message displays very rarely, when the server has begun the process of either starting or stopping, but isn't able to accept connections.

Server Going Offline Message - Displayed as the user is being kicked

SSL Banner Message - Displayed after connecting to the server on the Implicit SSL port.

SSL Disabled Message - Displayed in response to an [AUTH/PROT/PBSZ](#) command when SSL is not enabled.

SSL Required Message - Displayed when a user isn't using SSL and SSL is required.

Stat Message - Displayed in response to a [STAT](#) request.

Use Default/Inherited Setting: At the Server level, you can select this check box to use the default message for the selected Message Type. Clear this check box to customize the message. At the Group and User level, you can select this check box to use the inherited message for the selected Message type. Clear this check box to customize the message.

Message Text (limited to 1024 characters): Type the message to be displayed when this event occurs. Custom messages are limited to 1024 characters.

For more information, see the topic on [Custom Message Variables](#).

Files/Directories Tab

The **Files/Directories** tab is used to configure general file/directory settings.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access these settings on the **Server** level, expand the Server in the tree pane, click Files/Directories, then click the Files/Directories tab.

To access these settings at the **Group** or **User** level, in the tree pane, expand Groups or Users, select the Group or User, click Files/Directories, then click the Files/Directories tab.

Configuration Options

Use Inherited Setting: This check box appears on the **Group** and **User** levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Lock User(s) in Home Directory: Enable this feature to prevent the user from leaving the user's home directory and venturing "up" the tree. If the user's Home Directory is `c:\usr\test1\` and this feature is enabled, the user's Home Directory will appear as the root "/" when a [PWD](#) is performed from the client. The user will not be able to [CWD](#) or [CDUP](#) from the user's home directory. If this feature is not enabled, then the user's Home Directory will appear as `/usr/test1/` and the user will be able to CWD or CDUP to other directories in the system, provided that the user has adequate permissions.

Show Hidden Files: When enabled, Titan FTP will display hidden files in the directory listings that are sent to the client.

Hide directories users cannot enter: When enabled, Titan FTP will not display any folder-/directory entries that the user does not have adequate rights to.

Allow modification of file dates/times via [MDTM](#) command: When enabled, the user will be permitted to modify file dates/times by issuing the [SITE](#) MDTM command from the client.

Allow modification of file dates/times via [MFMT](#) command: When enabled, the user will be permitted to modify file dates/times by issuing the [SITE](#) MFMT command from the client.

Allow modification of file dates/times via [MFCT](#) command: When enabled, the user will be permitted to modify file dates/times by issuing the [SITE](#) MFCT command from the client.

[STOU](#) Prefix: The STOU command requires that all unique filenames have a prefix. Use the text box to customize the prefix.

STOU Extension: Use the text box to customize the STOU suffix (file extension).

Ban the following file types: Select this check box to ban certain file types. Use the text box to specify a list of file types that are prohibited from the server. Users will not be permitted to upload or rename a file that matches this filter. You must separate multiple entries with a semicolon.

Allow missing directory name in CWD command: When enabled, this feature will allow the FTP client to send a [CWD](#) command with no directory argument; the server will return the current working directory. Note that [RFC 959](#) requires that the CWD command contain a directory, so enabling this feature breaks compliance with the RFC.

Directory Access Tab

Use the **Directory Access** tab to grant or deny access to folders on the server. These settings can be configured at the Server, Group, and User levels. See Inheritance and Shared Attributes for more information.

Where is it?

To access these settings at the **Server** level, in the tree pane expand the Server, click Files/Directories and then click the Directory Access tab.

To access these settings at the **Group** or **User** level, in the tree pane select the Group or User, click Files/Directories, and then click the Directory Access tab.

Configuration Options

Directory Access is broken down into two categories, File Permissions and Folder Permissions. These options become available when a file in the list is selected. Click Add or Delete to alter the list's content.

Note: You can double-click the field to bring up the ACE (Access Control Entry) Editor window, where you can edit ACE path and detail information.

File Permissions

Read/Download Files: Allows users to download files from the server ([RETR](#)).

Write/Upload New Files: Allows users to upload files to the server ([STOR](#), [STOU](#)).

Append/Replace Files: Allows users to upload/replace/append existing files on the server.

Delete Files: Allows users to delete existing files from the server ([DELE](#)).

Rename Files: Allows users to rename existing files on the server ([RNFR](#)/[RNT0](#)).

Folder Permissions

Create Subdirectories: Allows users to create subdirectories within the current folder/directory ([MKD](#)).

Remove Subdirectories: Allows users to remove subdirectories from the current folder/directory ([RMD](#)).

Can View Directory Listing: Allows users to generate a directory listing of the contents of the folder ([LIST](#)/[NLST](#)).

Apply Rights to Subdirectories: Enable this check box to have these permissions, both File and Folder, propagated to all subdirectories of the specified path.

Titan FTP Permissions

Directory Access rules for the **User** are loaded first.

Directory Access rules for all **Groups** the user is a member of are loaded next. These Groups are loaded in the order in which they appear in the Groups tab of the User Configuration dialog. If a duplicate folder is encountered for which there are already Directory Access permissions specified, the SUM of the permissions is used.

Directory Access rules for the **Server** are loaded last. Again, if duplicates are located, they are summed together.

Example:

User A is a member of Group 1 and Group 2 for Server S.

User A has the following permissions: /pub/ - Read permissions

Group 1 has the following permissions: /pub/ - Write permissions

Group 2 has the following permissions: /pub/ - NO ACCESS AT ALL

Server S has the following permissions: /pub/ - LIST permissions

Outcome: User A will have READ, WRITE and LIST permissions to the /pub/ folder.

Virtual Folders Tab

Virtual folders are used to link or map external folders into a user's directory space. For Windows users, think of a virtual folder as a Windows shortcut. The link appears in one location while the data lives elsewhere. For UNIX users, virtual folders are very similar to symbolic links. Virtual Folders are commonly used to map network shares or folders from different drive letters into the server directory structure.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the Virtual Folders tab at the **Server** level, in the tree pane expand the Server, click Files/Directories, and click the Virtual Folders tab.

To access the Virtual Folders tab at the **Group** or **User** level, in the tree pane select the Group or User, click Files/Directories, and click the Virtual Folders tab.

Configuration Options

Using Virtual Folders

From the Virtual Folders tab:

1. Click Add to display the New Virtual Folder wizard.
2. To select the fully qualified path, browse to the physical folder location. You may select a folder on your local computer, or you may choose a network folder that has been previously shared. If you are mapping a UNC share, make sure the account under which the Titan FTP Service is running has access to the UNC. Click Next.
3. Select the default permissions for the virtual file and folder using the check boxes. Click Next.
4. The Actual Path of the folder is displayed and the Virtual Path is displayed. You can change the Folder Name as it will appear under the virtual path, or you can leave the default name (which is the same as the Actual Path name). A sample of what the final path will look like will be displayed. Click Finish to generate the virtual folder mapping.
5. The Virtual Path and the Actual Path should now be displayed in the Virtual Folders tab. Click Apply.

Virtual folder updates are not real-time. If a user is connected to the server when you make changes to the Virtual Folder list, users will need to log out and log back into the system to see the virtual folder changes.

If mapping a [UNC](#) share, make sure the account under which the Titan FTP Service is running has access to the UNC. Otherwise, you will need to add the appropriate username and password under the UNC accounts tab.

See our topic on [Virtual Folders](#).

If you attempt to create a virtual folder to a mapped network drive, Titan FTP will replace the drive mapping with the actual UNC name. Titan FTP Service does not have access to mapped drives, only to UNC shares.

If you would like more information about configuring group level virtual folders, see the [Using Group Level Folders QuickStart Guide](#).

Disk Quotas

The **Disk Quotas** tab is used to configure disk quota limits.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access these settings at the **Server** level, in the tree pane expand the Server, click Files/Directories, and then click the Disk Quotas tab.

To access these settings at the **Group** or **User** level, in the tree pane expand the Server, expand the Group or User, click Files/Directories, and click the Disk Quotas tab.

Configuration Options

Use Inherited Setting: This check box appears on the **Group** and **User** levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Enable Disk Quotas: When enabled, the server will have a limited amount of storage space. The rest of the disk quota options are unavailable unless disk quotas are enabled.

Current Disk Usage: Shows the amount of storage currently being used by this server.

Maximum Disk Usage: Specifies the maximum number of kilobytes of data the server will be permitted to store.

Recalculate: Recalculates the current disk usage.

Explore: Launches Explorer so you can browse the server's data directory. This is useful if you need to purge invalid files, or if you want to see how space is being used.

Free Files List: Type names of files/file types that will not be included in the quota calculations and use the Add or Remove buttons to compile a list.

Directories

The **Directories** tab contains a consolidated list of the directories specified for Titan FTP, for easy access and editing.

User Home Directory: The root directory under which all user directories will default. This can also be set at the [Group](#) or User level by altering the home directory.

Logfile Directory: The domain Log Directory setting defines the default storage location for Server logs. This value will be used to prime the Server Log Directory entry in the Server Wizard. For each new server, the domain log directory and the new server name will be concatenated to produce the full path to the log directory where the Server logs will be stored. This value can be either a fully qualified path, such as **C:\ MyLogs**, or a UNC name such as **\\Server\Share\MyLogs**.

System Database Directory: For Titan this is typically the directory used for the legacy Statistics database. For Cornerstone this directory is used to signal the Cornerstone server that something in the configuration has been changed. In a clustered Cornerstone Environment, this directory should live on a UNC and be shared by all nodes in the cornerstone cluster so that if one cluster node updates the database, it's propagated across all node clusters.

Temporary Cache Directory: This is used for temporary file storage. A great example is in the WebUI when someone wants to download a folder. The contents of the folder will be zipped up and this directory is used to temporarily store the zip file during download

SSL Certificate Store Directory: The directory in which your SSL certificates are stored. They are accessible from within Titan FTP via any Certificate Management button.

SSH Host Key Directory: The directory in which your SSH keys are stored. They are accessible from within Titan FTP via any Host Key Management button.

PGP Keyring Directory: The directory in which your PGP keys are stored.

Reports Directory: The directory in which your custom reports will appear after generation.

Backups Directory: This directory is available for use as a backup directory and can be leveraged in the Events Manager through the use of the %SVR.BACKUPSDIR% [variable](#).

FTPS/SSL Tab

The **FTPS/SSL** tab is used to configure secure FTP/S (FTP over SSL) settings used by Titan FTP .

For more information about the SSL features supported by Titan FTP, see [SSL Support](#).

Where is it?

To access the FTPS/SSL tab, expand the Server in the tree pane and click Services. Select the FTPS/SSL tab.

Configuration Options

Enable SSL/TLS access on this server: Enables the added protection of basic FTPS services. If enabled at this level, these options become available at the Group and User levels.

Security Protocols: TLS is the newer and more secure version of SSL. Select the highest/maximum supported SSL version used by Titan FTP. The minimum supported protocol is SSL v3.0. Titan FTP does not support SSL v.2 and will reject any client connection presenting SSL v.2 messages. For more on this, see the FIPS-SSL topic.

Enable explicit SSL/TLS access (User connects using the [AUTH](#) SSL command): When this option is enabled, Titan FTP will allow incoming connections on the standard FTP port, and once connected, the remote FTPS client may issue the AUTH SSL or AUTH TLS command to initiate the secure handshake process with the Titan FTP server.

Enable implicit SSL/TLS (User connects to a special port for SSL/TLS services): When this option is enabled, Titan FTP will accept secure connections on the Implicit SSL/TLS port. Any inbound connection on this port will imply that it is secure and Titan FTP will immediately initiate a secure handshake with the remote client before any FTP commands are accepted from the client.

Implicit SSL/TLS port: Select the port number that Titan FTP will use for inbound SSL connections. The default Implicit SSL port is port 990.

Encrypt data channel by default (Used if client does not issue [PROT](#) command): Protect the data channel by encrypting all communications by default. If a client makes a PROT command, that value will override this setting.

Enable CCC (Clear Command Channel): This option enables Titan FTP support for the CCC command. The CCC command can be issued by a remote FTPS client and will cause Titan FTP to fall out of secure mode and back into unsecure mode. This option is useful for clients who only

need to secure the authentication portion of the session. Once the USER/PASS has completed, some clients will use CCC to return to unsecure mode, which is faster.

Enable secure site-to-site (FXP) file transfers ([CPSV/SSCN](#)): Enables FXP site-to-site transfers. FXP indicates a direct server-to-server file transfer.

Require all FTP connections to be secure: Prevents normal FTP connections from being established. When enabled, the user must use Explicit or Implicit SSL or the connection will be terminated.

Disable weak encryption protocols (for PCI Compliance): Allows Titan FTP to run at a forced-elevated level of security. This is the most secure mode, but older clients may not have sufficiently modern technology to connect.

Server Certificate Settings

Require trusted certificates from clients who connect securely: This feature requires that all FTPS clients provide a trusted certificate to connect. This is the most secure method of connecting, but it requires that trusted keys be distributed offline to each user.

Use the following certificate for this server: Select a certificate to use for this server.

Certificate Management: Click Certificate Management to create or import certificates.

Certificate Password: Type the Password for the selected certificate.

Certificate Store Folder: This is the location where Titan FTP will store all certificates for this server.

Note: Local paths and [UNC](#) shares are supported; do not use a mapped drive because mapped network drives are not accessible from the Titan FTP service.

FIPS 140-2 Compliance Settings

Ensure FIPS Compliance for SSL: This option enables/disables FIPS mode for SSL.

You must enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** settings in the operating system if you intend to enable FIPS-SSL compliance on Titan FTP. If you enabled FIPS-SSL compliance in Titan FTP server without enabling the cryptography settings on the operating system, the Titan FTP server will not start. You must also configure your browser to use TLS or SSL v.3. If your browser is configured for SSL v.2, your browser will fail to connect to Titan FTP.

Titan FTP does not support SSL v2 and will reject any client that attempts a connection using SSL v2.

If you would like more information about configuring Titan FTP Server FTPS/SSL settings, please see the Titan FTP [Server FTPS/SSL & Public Key Security QuickStart Guide](#).

For more information about configuring FIPS mode, see the topic on [FIPS-SSL](#).

Flood Protection Tab

The **Flood Protection/DoS** tab is used to manage flood protection configuration options for the server.

Flood protection is designed to limit a hacker's ability to flood your server with multiple connections over a short period of time. Many times this is used to produce a DoS (Denial of Service) attack, which is designed to cripple the server so that it is unable to service existing or new connections properly.

Titan FTP has the ability to track incoming connections based on IP address and time since last connection. If Cornerstone finds that a client IP address has attempted to connect to the Titan FTP server more than X number of times in Y seconds, Titan FTP flags this client IP address as Flooding the server and closes the incoming connection as well as preventing any future connections from that IP address.

Note: Use the banning features carefully to avoid banning valid clients. Sometimes a client will use multiple connections to transfer many very tiny files to the Titan FTP server. If the files are transferred very quickly, this will cause the client to open and close many connections. Titan FTP may erroneously flag this as a flooding attempt and ban the client IP from connecting.

Where is it?

To access the Flood Protection/DoS tab, click the Server in the tree pane, click the Security item, then select the Flood Protection/DoS tab.

Configuration Options

Flood Protection

Enable Flood Protection (DoS/Hammering): Enable this feature to have Cornerstone track incoming connections and look for flooding/DoS attacks. If this option is enabled, the following options become available:

X Connections received from an IP address within Y Seconds: Set the thresholds for the minimum number of connections and minimum seconds that must elapse before the client IP is flagged as flooding. It is recommended that the Number of Connections is set high and the Number Of Seconds is set low to prevent incorrect flagging of valid clients. The default setting is: 200 connections received from an IP address within 5 seconds.

Ban IP Address Forever: If this option is selected, Cornerstone will add the client IP address to the list of IP addresses that are banned from accessing the server.

For more information on the banned IP list, see Server > Connections > IP Access.

Ban IP Address for X Minutes: If this option is selected, connections from the client IP address will be prevented for the predefined number of minutes. Once that time period has expired, the IP address is removed from the banned list and the client will be allowed to connect. The default setting is: Ban IP address for 60 minutes.

Flush Hammering Cache: Resets the banned members list to allow those who might have been accidentally added to reconnect without restarting the server.

Currently Blocked IP Addresses Window: This window appears when you click the Flush Hammering Cache button. It displays all IP addresses that are currently banned from the server, as well as the date on which they were banned, and how long since that time in minutes. You can selectively remove IP addresses, or all addresses, from the list, allowing them to login to the server.

Remove All: This will remove all banned IPs from the list, which will allow them to attempt to access the server again.

Remove: Select one or more IPs from the banned list and remove them, allowing those users to attempt to reconnect.

OK: Closes the window, saving all changes made to the list.

Cancel: Closes the window without committing the changes.

Hacking Protection

Enable Username/Password Hacking Protection - When this option is enabled, the following options become available:

X hack attempts received from an IP Address within Y seconds -

Ban IP Address Forever - If this option is selected, Cornerstone will add the client IP address to the list of IP addresses that are banned from accessing the server.

For more information on the banned IP list, see Server > Connections > IP Access.

Ban IP Address for X Minutes - If this option is selected, connections from the client IP address will be prevented for the predefined number of minutes. Once that time period has expired, the IP address is removed from the banned list and the client will be allowed to connect. The default setting is: Ban IP address for 60 minutes.

Flush Hacking Cache - Resets the banned members list to allow those who might have been accidentally added to reconnect without restarting the server.

Server Log Tab

The **Server Log** tab is used to view the Server Log in real-time.

Where is it?

To access the Server Log tab, in the tree pane expand the server, click Logging, and select the Server Log tab.

Configuration Options

Auto-refresh list every X seconds: Enable this option schedules the logfile viewer to automatically refresh the screen after the specified interval has elapsed. For efficiency, the most recent entries are listed. For a complete listing of the entire logfile, click View Entire Logfile.

Refresh: Click Refresh to force an immediate refresh of the log viewer.

View Entire Logfile: Opens the complete logfile in a text editor.

Clear Log Window: Clears the Log Window. To view the erased text, click View Entire Logfile.

Server Log Tab

The **Server Log** tab is used to view the Server Log in real-time.

Where is it?

To access the Server Log tab, in the tree pane expand the server, click Logging, and select the Server Log tab.

Configuration Options

Auto-refresh list every X seconds: Enable this option schedules the logfile viewer to automatically refresh the screen after the specified interval has elapsed. For efficiency, the most recent entries are listed. For a complete listing of the entire logfile, click View Entire Logfile.

Refresh: Click Refresh to force an immediate refresh of the log viewer.

View Entire Logfile: Opens the complete logfile in a text editor.

Clear Log Window: Clears the Log Window. To view the erased text, click View Entire Logfile.

Log Settings Tab

The **Log Settings** tab is used to configure the logging options for the server.

Where is it?

To access the Log Settings tab, expand the Server in the tree pane, click Logging, and select the Log Settings tab.

Configuration Options

Enable Logging to File: Enables logging to a disk file. This is highly recommended.

Enable Logging to Screen: Select to enable logging to the Activity screen in the Titan FTP administrator.

Prefix logfile name with machine name: Forces Titan FTP servers to name log files with both the name of the computer on which they are stored and the date, which gives them a unique name if the files are merged into a single location at a later date.

Use Unicode formatted logfiles: File characters will be saved using Unicode, which allows for a greater variety of characters, especially international alphabets.

Log Directory: Specifies the location where log files will be stored.

Explore Log Directory: Launches Windows Explorer to browse the contents of the Log Directory for this server.

Logfile Format: Use the dropdown arrow to select the output format for the server log file.

Log Fields: Select the log fields to be included in each log entry (Date, Time, ServerID/Socket#, Message).

Information Level: Choose the level of information to be recorded in the log file. Word Wrap - When enabled, each line in the log file is limited to the specified number of characters.

Rotate Log: Select the rotation schedule for log files. Logs accumulate in a single file until they are rotated. On rotation, a new file is created, with a filename based on the Date+#milliseconds_since_midnight. The rotation schedule dictates how often a new log file is created. Selecting "never" is highly discouraged as log files can become rather large.

Rotate Log Now: Rotates the log immediately. A new log file will be created based on the current date. If a log file already exists for the current date, a number will be appended to the log file until a unique name is found. If Anti-Virus software is installed on the same computer as the Titan FTP service, it is highly recommended that the anti-virus software be configured so that it does not actively scan the Titan FTP log file subdirectories. Contention between the anti-virus software actively scan-

ning the Titan FTP log files and service attempting to write to those files could cause performance issues with the Titan FTP server.

Advanced Settings Button: Click this to launch the Advanced Settings window.

Log Rotation Interval: Specify the number of minutes between checks to see if it is time to rotate the logs, which will create a new file.

Maximum Log Size (MB): Specify a maximum size for the log files before they are rotated. If this file size is exceeded, instead of adding to the previous file, a new file will be started.

Server Activity Tab

The **Server Activity** tab shows information about current connections to the server.

Where is it?

To access the Server Activity tab, in the tree pane expand the Server, click Server Activity, and then click the Server Activity tab.

Configuration Options

Auto-refresh list every X seconds: Use the check box to enable this option. When this option is enabled, the list will be refreshed automatically after each interval. The refreshed list will be incorporated in real time.

Refresh: Refreshes the list immediately to show any alterations.

Kick User(s): This option will log the selected user off of the server. All sessions for this user will be disconnected, but they will not be banned. They will be permitted to log back into the server. To Kick and Ban a user, use the Events Management features of Titan FTP.

Spy on User(s): Opens up a new [Spy User window](#) to view the selected user(s) server activities.

Kick Session(s): Terminates the currently selected user session. If the user is connected multiple times and has multiple sessions open, the remaining sessions will remain active.

Spy on Session(s): Shows all activities of the currently selected user session. Spying on a session allows you to view the logging information specific to the user session. This option opens a [Spy Session window](#) to spy on the selected session(s).

Session List: Displays a list of active sessions. A session is an open connection between a user and the server.

Server Activity Tab

The **Server Activity** tab shows information about current connections to the server.

Where is it?

To access the Server Activity tab, in the tree pane expand the Server, click Server Activity, and then click the Server Activity tab.

Configuration Options

Auto-refresh list every X seconds: Use the check box to enable this option. When this option is enabled, the list will be refreshed automatically after each interval. The refreshed list will be incorporated in real time.

Refresh: Refreshes the list immediately to show any alterations.

Kick User(s): This option will log the selected user off of the server. All sessions for this user will be disconnected, but they will not be banned. They will be permitted to log back into the server. To Kick and Ban a user, use the Events Management features of Titan FTP.

Spy on User(s): Opens up a new [Spy User window](#) to view the selected user(s) server activities.

Kick Session(s): Terminates the currently selected user session. If the user is connected multiple times and has multiple sessions open, the remaining sessions will remain active.

Spy on Session(s): Shows all activities of the currently selected user session. Spying on a session allows you to view the logging information specific to the user session. This option opens a [Spy Session window](#) to spy on the selected session(s).

Session List: Displays a list of active sessions. A session is an open connection between a user and the server.

Spy Session

The **Spy Session** window is useful for tracking the activities of a single user session. Keep in mind that multiple sessions can exist for the same user name. This viewer allows you to monitor the current session activity only. To view activity from all sessions, use the Spy User feature.

For more information on configuring a spy tab, see the [Where is it?](#).

Where is it?

To access the Spy Session window, from the tree pane expand the Server, click Server Activity, and then click Spy on Session(s) to launch the window.

Configuration Options

Auto-refresh: When this option is enabled, the list will be refreshed automatically after each interval. If this option is not enabled, you can refresh the viewer manually by clicking Refresh.

Refresh: Click Refresh to manually refresh the viewer at any time.

Kick Session: Click Kick Session to kick the selected user session from the server.

Close: Click Close to close the Spy viewer for this session.

Spy User

The **Spy User** window is useful for tracking the activities of a single user. Keep in mind that multiple sessions can exist for the same username. This viewer allows you to watch all activity from all sessions for the currently selected user.

Where is it?

To access the Spy User window, from the tree pane expand the Server and click the [Server Activity tab](#). Select the user you would like to track, and click Spy on User(s). The Spy User window will launch.

Configuration Options

Auto-refresh: When this option is enabled, the list will be refreshed automatically after each interval. If this option is not enabled, you can refresh the viewer manually by clicking Refresh.

Refresh: Click Refresh to refresh the viewer manually .

Kick User: Click Kick User to kick the selected user from the server. All sessions for this user will be disconnected, but they will not be banned. They will be permitted to log back in to the server. To Kick and Ban a user, use the Events Management features of Titan FTP.

Close: Use this button to close the Spy viewer for this user.

Statistics Tab

The **Statistics** tab displays a list of useful data concerning the variable settings in Titan FTP.

Where is it?

The Statistics tab can be found by selecting the Server, clicking on Server Activity, and the Statistics tab.

Configuration Options

Auto-refresh list every X seconds: Use the check box to enable this option. When this option is enabled, the list will be refreshed automatically after each interval.

Refresh Now: Immediately updates all statistics listed.

Server Statistics List

- Is Online
- Server Start Time
- Running Time
- Active SSL Connections
- Active Sessions
- Active Public Sessions
- I/O Buffer Count
- I/O Buffer SSL Count
- Allocated User Params
- Open file handles
- Transactions/last second
- Transactions Total
- Total Bytes Sent
- Total Bytes Received

File Transfer Statistics

- Total File Uploads: Number of files uploaded since the server started
- Total File Transfer Bytes Uploaded: Total bytes uploaded for the Total Files

- Total File Downloads: Number of files downloaded since the server started
- Total File Transfer Bytes Downloaded: Total bytes downloaded for the total files downloaded

File System I/O Statistics

- File Read Requests: Total number of file system READ() requests for file downloads since the server started
- File Write Requests: Total number of file system WRITE() requests to file uploads since the server started.

Event Handlers Tab

The **Event Handlers** tab is used to view, create, modify, and delete Event Handlers. Event Handlers trigger customized actions based on events and conditions. Read the Introduction to Event Handling for an overview. Titan FTP also provides pre-configured event handlers; Pre-configured event handlers are listed on the Event Handlers tab.

Where is it?

To access the Event Handlers tab, in the tree pane of the Titan FTP administrator, expand the Server, click Events, and then click the Event Handlers tab.

Configuration Options

The Event Handlers tab contains a list of currently configured events. If you haven't configured any, this list will be blank.

Add: Adds a new Event Handler for this server to this list.

Edit: Click to edit an existing Event Handler's configuration settings.

Enable/Disable: Enables or disables Event Handlers, which will display a green icon when enabled and a red icon when disabled.

Remove: Select the Event and click Remove to remove one or more Event Handlers.

Run Now: Use this option to force the execution of the selected Event. Please note that some events will not fire properly because they rely on a connection context, user login, client ip address, etc., which are only available in a live environment. Run Now is most useful for exercising events which might run on a scheduled basis, or for events that do not rely on a user connection.

Display System Events: This option allows you to view, enable, and disable certain system defined events. These are advanced events and should not be modified, enabled, or disabled unless instructed to do so by SRT support representatives.

Expand any event on your list for a tree view of its details. For more information, see the topics on [Events](#), [Conditions](#), and [Actions](#).

Performance Tips

The Event Handler system is designed for efficient performance, but it is possible to design an Event Handler that will slow down the server. Consider these factors while configuring events to preserve system performance:

Logging: When you create a custom log, ensure that the file is periodically rotated or renamed to prevent large file sizes. Appending to large files (1MB+) will cause a noticeable delay, especially if the log is updated frequently.

Flag for admin review: This action is not designed to be triggered frequently and will cause the Flagged Events list to become bloated. As this list grows, especially beyond a few hundred entries, performance will deteriorate.

Send email: Depending on your email system, sending email frequently could slow performance. In addition, many email servers include spam countermeasures that may block emails or even black-list the sender.

For more information on configuring events in Titan FTP, see our the Events section of the Tutorials in this help.

Event Handlers Tab

The **Event Handlers** tab is used to view, create, modify, and delete Event Handlers. Event Handlers trigger customized actions based on events and conditions. Read the Introduction to Event Handling for an overview. Titan FTP also provides pre-configured event handlers; Pre-configured event handlers are listed on the Event Handlers tab.

Where is it?

To access the Event Handlers tab, in the tree pane of the Titan FTP administrator, expand the Server, click Events, and then click the Event Handlers tab.

Configuration Options

The Event Handlers tab contains a list of currently configured events. If you haven't configured any, this list will be blank.

Add: Adds a new Event Handler for this server to this list.

Edit: Click to edit an existing Event Handler's configuration settings.

Enable/Disable: Enables or disables Event Handlers, which will display a green icon when enabled and a red icon when disabled.

Remove: Select the Event and click Remove to remove one or more Event Handlers.

Run Now: Use this option to force the execution of the selected Event. Please note that some events will not fire properly because they rely on a connection context, user login, client ip address, etc., which are only available in a live environment. Run Now is most useful for exercising events which might run on a scheduled basis, or for events that do not rely on a user connection.

Display System Events: This option allows you to view, enable, and disable certain system defined events. These are advanced events and should not be modified, enabled, or disabled unless instructed to do so by SRT support representatives.

Expand any event on your list for a tree view of its details. For more information, see the topics on [Events](#), [Conditions](#), and [Actions](#).

Performance Tips

The Event Handler system is designed for efficient performance, but it is possible to design an Event Handler that will slow down the server. Consider these factors while configuring events to preserve system performance:

Logging: When you create a custom log, ensure that the file is periodically rotated or renamed to prevent large file sizes. Appending to large files (1MB+) will cause a noticeable delay, especially if the log is updated frequently.

Flag for admin review: This action is not designed to be triggered frequently and will cause the Flagged Events list to become bloated. As this list grows, especially beyond a few hundred entries, performance will deteriorate.

Send email: Depending on your email system, sending email frequently could slow performance. In addition, many email servers include spam countermeasures that may block emails or even black-list the sender.

For more information on configuring events in Titan FTP, see our the Events section of the Tutorials in this help.

Flagged Events Tab

The **Flagged Events** tab displays a list of events triggered on the server.

Where is it?

To access the Flagged Events tab, expand the Server in the tree pane, click Events, and then click the Flagged Events tab.

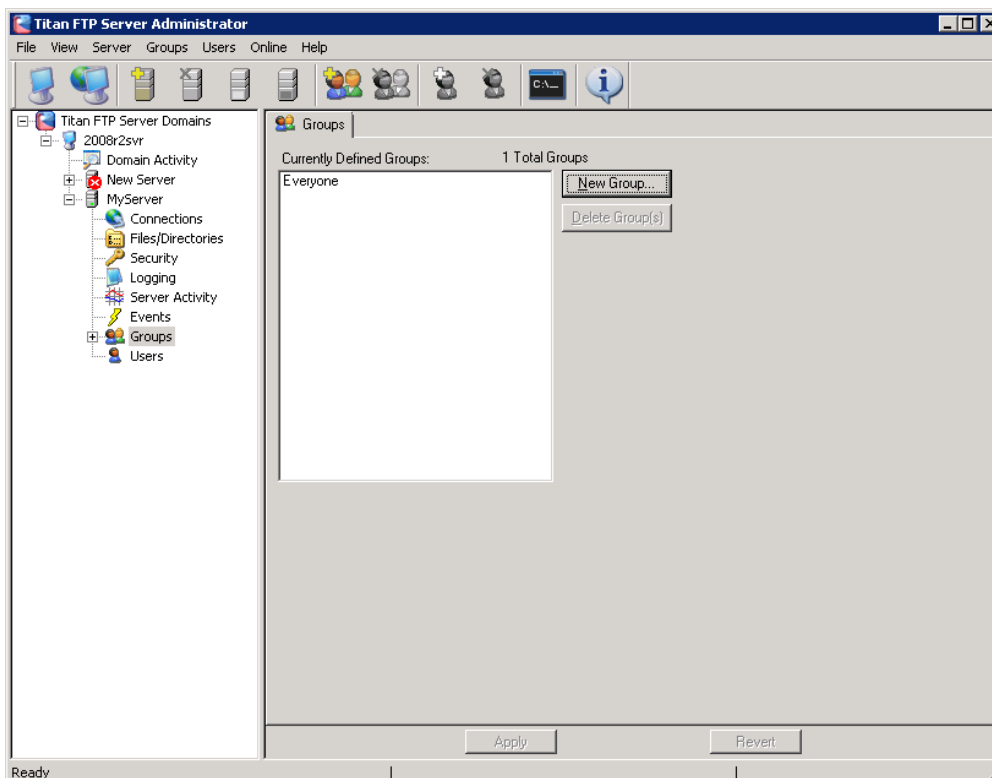
Configuration Options

Flagged events are special events a Titan FTP Administrator can set up to activate under certain conditions. When the event is triggered, it is stored in this tab and saved for administrative review.

Remove From List: Once the event has been reviewed by the Administrator, the event can be removed from the list. To remove the event, select the event and click Remove From List.

Groups Overview

The **Groups** configurations in Titan FTP provide the ability to associate multiple users with similar characteristics and permissions.



Groups contains a list of currently defined groups and allows you to create groups, using the New Group Wizard, and delete them. By default, Titan FTP will generate a global system group called **Everyone**. The Everyone Group will always exist and cannot be deleted. All users are members of the Everyone group, so care should be taken when adjusting the access permissions for this group.

For more information, see our topic on the [New Group Wizard](#).

Where is it?

To access the Groups tab, select a Server in the tree pane and click Groups.

Configuration Options

Currently Defined Groups: List of groups registered with this server, including the number total listed to the right.

New Group: Click to launch the New Group Wizard, which will lead you through the process of naming a new group, selecting the directory the group will draw members from, and adding initial members. The members list for each group can be changed later.

Delete Group(s): Select the group you wish to delete and select Delete Group(s). You will be prompted to confirm that you wish to delete the group.

Flush Cache: This feature is only available for servers using LDAP or AD for user authentication. Immediately updates all group information.

You can set up an unlimited number of Groups for each server. Each Group can have zero or more Users. You can also add the same user to multiple groups.

Note: If you add a user to multiple groups, that user [inherits](#) the sum or culmination of the **Directory Access Permissions** for all of the groups.

Titan FTP Groups are not the same as Windows User Groups. If you would like to disable a group after you have created it, you must first change the Group Home Directory to No group directory.

Creating Groups

There are three methods for creating a Group in Titan FTP:

1. Expand the Server and right-click on the Groups tree pane. Select New Group. The New Group Wizard will launch.
2. Click Groups in the tree pane of the Titan FTP Administrator. A list of groups is then generated and displayed in the tab pane. Click New Group. The New Group Wizard will launch.
3. From the menu bar, select Groups > New Group Wizard.

For more information, see our topic on the [New Group Wizard](#).

Deleting Groups

There are three ways to delete groups in Titan FTP. When you delete a group from the system, all users who are members of that group are removed from the group and their **Directory Access Permissions** are updated. If you would like to disable a group after you have created it, you must first change the **Group Home Directory** to **No group directory**.

1. In the tree pane, right-click the Group you would like to delete and select Delete Group from the context menu. You will be prompted to confirm the deletion of the group.
2. In the tree pane, select the Group you would like to delete. From the Titan FTP Administrator menu bar, select Groups, Delete Group. You will be prompted to confirm the deletion of the group.
3. In the tree pane, click Groups. A list of groups is generated and displayed in the tab pane. Select the Group you would like to delete and click Delete. You will be prompted to confirm the deletion of the group.

[Adding and Removing Group Members](#)

Users can be added to any number of Groups. Users must be created in the Users section of the administrator before they can be added to a group.

See our topic on [Users Overview](#).

To add a user to a group, select the group in the tree pane of the Titan FTP Administrator and then click the Users tab. Make the appropriate changes in group membership and then click Apply to save the changes.

If a user is a member of multiple groups, the user will inherit the sum or culmination of the Directory Access Permissions for the various groups.

Example

User A is a member of Group 1 and Group 2.

Group 1 has Read permissions to folder /F/.

Group 2 has Write permissions to folder /F/.

This means that User A will have Read AND Write permissions to folder /F/.

Group General Tab

The **Group General** tab is used to configure general group settings.

Where is it?

To access the a specific group's General tab, in the tree pane click the group name and the Group General tab.

Configuration Options

Group Name: Displays the Group Name. Use this text box to change the group name. You cannot change the group name for the Everyone group.

Group Home Directory: These options specify the kind of group home directory to be used. The Group home directory can be used to ensure that group members are organized according to Group settings, rather than having to set these values at the individual User level. Care must be taken to ensure that users that are members of multiple groups have the correct home directory.

- **No group directory (home directory set at user level):** This group does not have a home directory. Home directories will default to the Server home directory. The home directory can be changed on an individual user level.
- **User home directories default to group directory:** Select this value to cause any users that are members of this group to use the Group Home Directory as their home directory.
- **User home directories default to subdirectory of group directory:** Select this value to cause any users that are members of this group to have their own subdirectory created under the Group Home Directory.

Group Directory: If the group is defined to have user home directories based on a group directory, this is where the base group directory will be set.

Expiration Date: This setting allows expiration date values to be set at the Group level, thus preventing them from having to be set at the User level. As of this date, all members of the group will be denied access to the server.

Always Allow Login (even if max connections exceeded): This setting allows you to give members of a Group the ability to always be able to connect to the server, even if the maximum number of logins has been reached.

Group-Level Users Tab

Groups Users Tab

The **Users** tab is used to manage group membership.

Where is it?

To access the Users tab, in the tree pane select the Group and click the Users tab.

Configuration Options

Members of: Lists the groups this user is a part of. To add groups, select a group in the Not a member of list and use the arrows to shunt the group back and forth until the member is a part of the appropriate groups. Click Apply when you have completed your changes.

Not a member of: Lists all groups this member is not currently a member of. To add members to a group, select a group from the list and use the arrow buttons to shunt the user to the Members list. Click Apply when you have completed your changes.

FTP Tab

The **FTP** tab allows you to configure FTP settings used by Titan FTP.

Where is it?

To access the FTP tab, expand the Server in the tree pane and click Services. Select the FTP tab.

Configuration Options

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

To access the FTP tab at the User or Group levels, select the appropriate Group or User in the tree pane and click the FTP tab.

Enable FTP access on this server: This option enables/disables a user's ability to connect to the server using FTP.

IP Address: The IP Address the server will listen on. You can type a specific IP address, or you can select Any Available IP Address. We recommend Any Available IP Address if your computer has a multiple IP addresses.

FTP port: Enter the port the server will use to accept FTP connections. The default FTP port is 21.

FTP send buffer size: This value defines the size of the buffer used to send data to the remote client during file downloads. If you experience very slow transmission rates between Titan FTP and the client, your network could have a high latency rate. Increasing/decreasing this value could help improve performance on high latency networks.

FTP receive buffer size: This value defines the size of the buffer used to receive data from the remote client during file uploads. Increasing or decreasing this value could help improve performance on high latency networks.

NLST Returns File names AND directory/folder names: When enabled, this option forces [NLST](#) to return directory/folder names in addition to returning file names.

Exclusively lock file during upload: When enabled, Titan FTP will create an exclusive lock on the server file while it is being uploaded from the client.

Allow Anonymous Access: When selected, enables the Anonymous user account.

Check Anonymous Password: Requires that the password for Anonymous access be of the **x@y** format (usually specifying an e-mail address). Checking is only performed to ensure that the format is correct. No checking is performed to ensure that the email address and/or domain are valid.

Server Time Zone: Allows you to specify the time zone the server will "virtually" exist in. By default, this is the local time zone. Modifying the time zone will alter how the file dates and times are displayed to the user through a client.

Adjust for Daylight Saving Time: When selected, compensates for Daylight Saving Time.

FTPS/SSL Tab

The **FTPS/SSL** tab is used to configure secure FTP/S (FTP over SSL) settings used by Titan FTP .

For more information about the SSL features supported by Titan FTP, see [SSL Support](#).

Where is it?

To access the FTPS/SSL tab, expand the Server in the tree pane and click Services. Select the FTPS/SSL tab.

Configuration Options

Enable SSL/TLS access on this server: Enables the added protection of basic FTPS services. If enabled at this level, these options become available at the Group and User levels.

Security Protocols: TLS is the newer and more secure version of SSL. Select the highest/maximum supported SSL version used by Titan FTP. The minimum supported protocol is SSL v3.0. Titan FTP does not support SSL v.2 and will reject any client connection presenting SSL v.2 messages. For more on this, see the FIPS-SSL topic.

Enable explicit SSL/TLS access (User connects using the [AUTH](#) SSL command): When this option is enabled, Titan FTP will allow incoming connections on the standard FTP port, and once connected, the remote FTPS client may issue the AUTH SSL or AUTH TLS command to initiate the secure handshake process with the Titan FTP server.

Enable implicit SSL/TLS (User connects to a special port for SSL/TLS services): When this option is enabled, Titan FTP will accept secure connections on the Implicit SSL/TLS port. Any inbound connection on this port will imply that it is secure and Titan FTP will immediately initiate a secure handshake with the remote client before any FTP commands are accepted from the client.

Implicit SSL/TLS port: Select the port number that Titan FTP will use for inbound SSL connections. The default Implicit SSL port is port 990.

Encrypt data channel by default (Used if client does not issue [PROT](#) command): Protect the data channel by encrypting all communications by default. If a client makes a PROT command, that value will override this setting.

Enable CCC (Clear Command Channel): This option enables Titan FTP support for the CCC command. The CCC command can be issued by a remote FTPS client and will cause Titan FTP to fall out of secure mode and back into unsecure mode. This option is useful for clients who only

need to secure the authentication portion of the session. Once the USER/PASS has completed, some clients will use CCC to return to unsecure mode, which is faster.

Enable secure site-to-site (FXP) file transfers ([CPSV/SSCN](#)): Enables FXP site-to-site transfers. FXP indicates a direct server-to-server file transfer.

Require all FTP connections to be secure: Prevents normal FTP connections from being established. When enabled, the user must use Explicit or Implicit SSL or the connection will be terminated.

Disable weak encryption protocols (for PCI Compliance): Allows Titan FTP to run at a forced-elevated level of security. This is the most secure mode, but older clients may not have sufficiently modern technology to connect.

Server Certificate Settings

Require trusted certificates from clients who connect securely: This feature requires that all FTPS clients provide a trusted certificate to connect. This is the most secure method of connecting, but it requires that trusted keys be distributed offline to each user.

Use the following certificate for this server: Select a certificate to use for this server.

Certificate Management: Click Certificate Management to create or import certificates.

Certificate Password: Type the Password for the selected certificate.

Certificate Store Folder: This is the location where Titan FTP will store all certificates for this server.

Note: Local paths and [UNC](#) shares are supported; do not use a mapped drive because mapped network drives are not accessible from the Titan FTP service.

FIPS 140-2 Compliance Settings

Ensure FIPS Compliance for SSL: This option enables/disables FIPS mode for SSL.

You must enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** settings in the operating system if you intend to enable FIPS-SSL compliance on Titan FTP. If you enabled FIPS-SSL compliance in Titan FTP server without enabling the cryptography settings on the operating system, the Titan FTP server will not start. You must also configure your browser to use TLS or SSL v.3. If your browser is configured for SSL v.2, your browser will fail to connect to Titan FTP.

Titan FTP does not support SSL v2 and will reject any client that attempts a connection using SSL v2.

If you would like more information about configuring Titan FTP Server FTPS/SSL settings, please see the Titan FTP [Server FTPS/SSL & Public Key Security QuickStart Guide](#).

For more information about configuring FIPS mode, see the topic on [FIPS-SSL](#).

SFTP/SSH Tab

The **SFTP/SSH** tab is used to configure SFTP/SSH settings for this server.

FIPS compliance is only available in Cornerstone MFT Server. For more information, contact sales@southrivertechnologies.com.

Where is it?

To access the SFTP/SSH tab, expand the Server in the tree pane, click the Services category, then select the SFTP/SSH tab.

Configuration Options

Enable SFTP on this server (SSH's Secure File Transfer Protocol) on this server:

Enables/disables SFTP connections for the server. SFTP is a special subsystem of SSH and is different from FTP and FTPS. If this option is not enabled, no other options will be accessible on this tab.

SFTP Options

SFTP Port: Port used for SFTP connections. Default SFTP port is port 22.

SFTP Version: Select the highest version of SFTP the server will accept. Clients will negotiate with the server and the highest version supported by both the client and the server support will be used. Titan FTP currently supports versions 3, 4, 5, and 6 of the SFTP protocol.

Use Zlib compression: Enable zlib compression to increase transfer throughput. Exclusively lock file during upload - When enabled, Titan FTP will create an exclusive lock on the server file while it is being uploaded from the client.

Cipher/MAC Settings

Cipher preferences: Select one or more encryption ciphers to be supported by the server. During the SSH handshake, Titan FTP presents a list of supported ciphers to the SFTP client. The client will do the same, and the two parties will negotiate on a commonly supported cipher.

Note: The cipher used to send data from the client to the server may be different than the cipher used to send data from the server to the client.

MAC preferences: Select one or more MAC (Message Authentication Code) algorithms that will be supported by the server. The list of supported MACs is presented to the SFTP client during the handshake.

Key Exchange Algorithms: Select one or more KEX (Key Exchange Algorithms) to be supported by the server.

Note: The SHA1 based algorithms is discourage. SHA1 has been deemed unsecure as of 2017. SHA1 support is included for legacy support only. SRT recommends SHA2 or SHA3 based algorithms.

Server host key settings

Kick user if they present an invalid host key: Users attempting to access the server with an incorrect host key will be logged out.

Require trusted host keys when accessing this server: Enable this feature to require users to present a valid Username and public host key when connecting to the system. When this feature is enabled, Titan FTP will only allow Public-Key authentication. The service will enable the AM_PUBLICKEY flag, 0x04h, and return "publickey" as an acceptable authentication method. When this option is enabled, AM_PASSWORD, 0x02, "password" authentication is disabled and logging in with a password is not permitted.

Allow trusted host keys when accessing this server: Titan FTP will advertise to the client that it accepts password and/or key authentication. The client will need to present their valid Username with **either** a valid password **or** a valid public host key. The authentication process should go on silently in the background if only keys are required to log in. The service will enable **both** the AM_PUBLICKEY (0x04) **and** AM_PASSWORD (0x02), and it will return both "publickey" and "password" as valid authentication methods.

If neither Require or Allow trusted host keys is enabled: Clients who connect to the SFTP service will be required to present both their valid Username and Password in order to connect. The service will enable AM_PASSWORD (0x02) and return only "password" as a valid authentication method.

Use the following host key for this server: Select an existing host key to be used by the server. If no host keys are available, use the Host Key Management utility to create a new server host key pair.

Enter the password associated with this host key: Enter the password used to secure the private key portion of the selected host key.

Note: Titan FTP will not accept host key pairs that are not secured by a password. Passwords used to secure the private key portion of a host key pair must be at least 4 characters in length.

Host Key Folder: Enter the fully qualified path where Titan FTP SSH host keys will be stored.

Note: Local paths and UNC shares are supported. Do not use a mapped drive, as mapped network drives are not accessible from the Titan FTP service. Titan FTP does not accept connections from SSH v.1.x clients. SSH v.2 is required to connect to a Titan FTP server.

If you would like more information about configuring Titan FTP Server SFTP settings & Host Key Management, please see the Titan FTP SFTP & Host Key Management Quick Start Guide.

See SFTP Support for more information.

Connections General

The **Connections General** tab is used to configure general connection settings.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the Connections General tab at the **Server** level, expand the Server in the tree pane, click Connections, then click the Connections General tab.

To access these settings at the **Group** or **User** level, in the tree pane click the Group or User, click Connections, and then click the Connections General tab.

Configuration Options

Use Inherited Setting: This check box appears on the **Group** and **User** levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Max Concurrent Connections: The total number of concurrent sessions that may be established at once.

Idle Connection Time-out: The maximum amount of time, in minutes, the server will wait before dropping a user due to inactivity.

Max Connections/IP: The total number of concurrent connections a user can establish from any given IP address.

Max Upload Speed: The total KPS (Kilobytes Per Second) upload speed the server will allow from the user. If the user attempts to exceed this bandwidth allotment, the server will pause the transfer and slow it down to the proper speed.

Max Download Speed: The total KPS (Kilobytes Per Second) download speed the server will allow for data to be sent to the user.

Max Uploads/Session: The total number of files that may be uploaded per session. Once this limit has been reached, the user will not be able to upload/replace any files until they log out and log back in.

Max Downloads/Session: The total number of files that may be downloaded per session. Once this limit has been reached, the user will not be able to download any files until they log out and log back in.

Max File Upload Size: Specifies the maximum file size that can be uploaded by the user. Any attempt to upload a larger file will be aborted and the file will be deleted from the system.

Max File Download Size: Specifies the maximum file size that may be downloaded by this user. Any attempts to download files larger than this value will be denied.

Connections Advanced Tab

The **Connections Advanced** tab is used to configure advanced connection settings.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the Connections Advanced tab at the Server level, expand the Server in the tree pane, click Connections, then click the Connections Advanced tab.

To access these settings at the Group or User level, click the Group or User in the tree pane, click Connections, then click the Connections Advanced tab.

Configuration Options

Use Inherited Setting: This check box appears on the Group and User levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Disable account after X invalid password attempts: When enabled, the user account will be disabled after the specified number of consecutive incorrect password attempts.

Kick user after X consecutive bad commands: When enabled, the user connection will be dropped after the user types the specified number of invalid commands.

Disable user account afterwards: This option becomes available if you choose to kick the user after a certain number of bad commands. Select this to disable the account after the number is reached.

Ban access from IP address once this happens: This option becomes available if you choose to kick the user after a certain number of bad commands. Select this to ban the user's IP address from the server after the number is reached.

Allow PASV Mode Connections: When enabled, allows the server to be placed in [PASV](#) mode by the client. If this feature is disabled and the client attempts to issue a PASV command, they will receive a 502 Not Implemented response.

Allow EPSV Mode Connections: Similar to the PASV command, but used for IP v6 addressing. When enabled, allows the server to be placed in [EPSV](#) mode by the client. If this feature is disabled and the client attempts to issue a EPSV command, they will receive a **502 Not Implemented** response.

Limit PASV Port range from: Allows you to specify a specific range of ports that the server will use when the user issues a [PASV](#) command. This is useful if the server is behind a fire-wall/router and you only want to open a specified range of ports for use by the server.

Delete Partially Uploaded Files: When enabled, the server will delete any files that are not successfully uploaded. For example, if a [STOR](#) or [STOU](#) does not complete successfully, the file will be deleted from the server.

Block Anti-Timeout Schemes: When enabled, the server will ignore [NOOP](#) commands as attempts are made to keep the connection alive.

Block FTP Bounce Attacks and FXP: When enabled, the server will not accept any data connections from IP addresses other than the user's primary connection.

Allow change of password (SITE PSWD): When enabled, users are permitted to change their password using the [SITE PSWD](#) command.

Connections IP Access Tab

The **IP Access** tab is used to configure IP access restrictions, which affects specific users logging onto the Titan FTP server.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the IP Access tab at the **Server** level, in the tree pane expand the Server, click Connections, and then click the IP Access tab.

To access these settings at the **Group** or **User** level, in the tree pane expand Groups or Users, select the appropriate group or user, click Connections, and then click the IP Access tab.

Configuration Options

Use Inherited Setting: This check box appears on the **Group and User levels**. When selected, the values will be inherited from the next level up in the inheritance chain . Clear this check box to override the inherited values.

Enable IP Access Restrictions: When enabled, IP Access restrictions will be applied at this level whenever a user attempts to connect.

Grant/Deny access to all IP Addresses by default: Select the default action that will be applied at this level when a connection attempt is made.

Except the addresses listed below: Use the Add button to enter a list of IP addresses that will be the exception to the default rule. For example, you can Deny Access by default and type a single IP address, which will then be the only IP address the user will be permitted to connect from.

Connections Upload/Download Ratios Tab

The **Upload/Download Ratios** tab is used to configure Upload/Download ratios.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the Upload/Download Ratios tab at the **Server** level, in the tree pane expand the Server and click Connections, and then click the Upload/Download Ratios tab.

To access these settings at the **Group** or **User** level, in the tree pane, expand Groups or Users, select the Group or User, click Connections, and click the Upload/Download Ratios tab.

Configuration Options

Use Inherited Setting: This check box appears on the Group and User levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Enable Upload/Download Ratios: When enabled, the user will have Upload/Download ratios applied to their sessions.

Count # of Files Per Session: Ratios will be applied at the file level on a per-session basis. Each time the user disconnects from the server, the counters are reset. If the user has multiple concurrent sessions open, statistics are applied for each individual session.

Count KBytes Per Session: Ratios will be applied at the file size level on a per-session basis. Each time the user disconnects from the server, the counters will be reset. If the user has multiple concurrent sessions open, statistics are applied for each individual session.

Count # of Files across All User Sessions: Ratios will be applied at the file level across all concurrent sessions for the user.

Count KBytes across All User Sessions: Ratios will be applied at the file size level across all concurrent sessions for the user.

Ratio: Enter the upload to download ratio for the user. For example, you may want to require that the user upload two files for every one file they download. The ratio would be Uploads 2, Downloads 1. You may also want to require that the user upload 1MB of data for each 1MB of data that they download, so the ratio would be Upload 1000, Download 1000, and select the Count KBytes option.

Free Files List: Use the New Free File Name form to add a list of files/file types that will be excluded from the ratios.

Connections Messages Tab

The **Messages** tab is used to configure custom messages. Any message displayed in the Messages tab list can be altered to show a custom message relevant to your server.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access these settings at the **Server** level, in the tree pane expand the Server, click Connections, then click the Messages tab.

To access these settings at the **Group** or **User** level, in the tree pane select the Group or User, click Connections, then click the Messages tab.

Configuration Options

Message Type: Select the message to customize. The current message will be displayed in the Message Text field. Most messages have a description of their meanings.

[Click here to see the list of messages and descriptions.](#)

Welcome Message - Displayed after a successful login.

Quit/Logout Message - Displayed as part of the [QUIT](#) response.

Kicked Message - Displayed when a user is kicked off the server.

Banned Message - Displayed to a banned user.

Max Connects Message - Displayed when Max Connections reached.

Max IP Message - Displayed when Max Connections from a single IP is reached.

Banned File Type Message - Displayed after an attempt to upload a banned file type.

Disk Quota Exceeded Message - Displayed to users after quota has been exceeded.

Expired Account Message - Displayed to a user with an expired account.

Account Disabled Message - Displayed to a user when their account has been disabled.

Maximum Upload File Size Exceeded Message - This message will display for users when the file size of an upload is larger than the limit set by the admin on the Connections General Tab in the **Max File Upload Size** field.

Maximum Download File Size Exceeded Message - This message will display to the user when the file size of a download is larger than the limit set by the admin in Connections General Tab in the **Max File Download Size** field.

Site-To-Site/FXP Error Message - Site-to-Site transfers (file transfers from one FTP server directly to another) are not enabled in Titan FTP by default. To enable secure Site-to-Site/FXP transfers, navigate to the Security category, select the FTPS/SSL tab, and check **Enable secure site-to-site (FXP) file transfers (CPSV/SSCN)**.

Maximum Number of Files Downloaded Message - This message is displayed when a user has exceeded the maximum number of allowed downloads in a specific session defined in the Connections, **Max Downloads/Session** field of the administrator.

Maximum Number of Files Uploaded Message - This message is displayed when a user has exceeded the maximum number of allowed uploads in a specific session defined in the Connections, **Max Uploads/Session** field of the administrator.

Banner Message - Displayed after connecting to the server

Anonymous access disabled Message - Anonymous access is disabled by default. It can be enabled in the admin by selecting your server in the left-hand tree-pane, navigating to the FTP tab, and checking **Allow Anonymous Access**. With anonymous access off, any user trying to log in anonymously will get the default error message.

Server Offline Message - Displayed when the server is offline or stopped. This message displays very rarely, when the server has begun the process of either starting or stopping, but isn't able to accept connections.

Server Going Offline Message - Displayed as the user is being kicked

SSL Banner Message - Displayed after connecting to the server on the Implicit SSL port.

SSL Disabled Message - Displayed in response to an [AUTH/PROT/PBSZ](#) command when SSL is not enabled.

SSL Required Message - Displayed when a user isn't using SSL and SSL is required.

Stat Message - Displayed in response to a [STAT](#) request.

Use Default/Inherited Setting: At the Server level, you can select this check box to use the default message for the selected Message Type. Clear this check box to customize the message. At the Group and User level, you can select this check box to use the inherited message for the selected Message type. Clear this check box to customize the message.

Message Text (limited to 1024 characters): Type the message to be displayed when this event occurs. Custom messages are limited to 1024 characters.

For more information, see the topic on [Custom Message Variables](#).

Files/Directories Tab

The **Files/Directories** tab is used to configure general file/directory settings.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access these settings on the **Server** level, expand the Server in the tree pane, click Files/Directories, then click the Files/Directories tab.

To access these settings at the **Group** or **User** level, in the tree pane, expand Groups or Users, select the Group or User, click Files/Directories, then click the Files/Directories tab.

Configuration Options

Use Inherited Setting: This check box appears on the **Group** and **User** levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Lock User(s) in Home Directory: Enable this feature to prevent the user from leaving the user's home directory and venturing "up" the tree. If the user's Home Directory is `c:\usr\test1\` and this feature is enabled, the user's Home Directory will appear as the root "/" when a [PWD](#) is performed from the client. The user will not be able to [CWD](#) or [CDUP](#) from the user's home directory. If this feature is not enabled, then the user's Home Directory will appear as `/usr/test1/` and the user will be able to CWD or CDUP to other directories in the system, provided that the user has adequate permissions.

Show Hidden Files: When enabled, Titan FTP will display hidden files in the directory listings that are sent to the client.

Hide directories users cannot enter: When enabled, Titan FTP will not display any folder-/directory entries that the user does not have adequate rights to.

Allow modification of file dates/times via [MDTM](#) command: When enabled, the user will be permitted to modify file dates/times by issuing the [SITE](#) MDTM command from the client.

Allow modification of file dates/times via [MFMT](#) command: When enabled, the user will be permitted to modify file dates/times by issuing the [SITE](#) MFMT command from the client.

Allow modification of file dates/times via [MFCT](#) command: When enabled, the user will be permitted to modify file dates/times by issuing the [SITE](#) MFCT command from the client.

[STOU](#) Prefix: The STOU command requires that all unique filenames have a prefix. Use the text box to customize the prefix.

STOU Extension: Use the text box to customize the STOU suffix (file extension).

Ban the following file types: Select this check box to ban certain file types. Use the text box to specify a list of file types that are prohibited from the server. Users will not be permitted to upload or rename a file that matches this filter. You must separate multiple entries with a semicolon.

Allow missing directory name in CWD command: When enabled, this feature will allow the FTP client to send a [CWD](#) command with no directory argument; the server will return the current working directory. Note that [RFC 959](#) requires that the CWD command contain a directory, so enabling this feature breaks compliance with the RFC.

Directory Access Tab

Use the **Directory Access** tab to grant or deny access to folders on the server. These settings can be configured at the Server, Group, and User levels. See Inheritance and Shared Attributes for more information.

Where is it?

To access these settings at the **Server** level, in the tree pane expand the Server, click Files/Directories and then click the Directory Access tab.

To access these settings at the **Group** or **User** level, in the tree pane select the Group or User, click Files/Directories, and then click the Directory Access tab.

Configuration Options

Directory Access is broken down into two categories, File Permissions and Folder Permissions. These options become available when a file in the list is selected. Click Add or Delete to alter the list's content.

Note: You can double-click the field to bring up the ACE (Access Control Entry) Editor window, where you can edit ACE path and detail information.

File Permissions

Read/Download Files: Allows users to download files from the server ([RETR](#)).

Write/Upload New Files: Allows users to upload files to the server ([STOR](#), [STOU](#)).

Append/Replace Files: Allows users to upload/replace/append existing files on the server.

Delete Files: Allows users to delete existing files from the server ([DELE](#)).

Rename Files: Allows users to rename existing files on the server ([RNFR](#)/[RNTD](#)).

Folder Permissions

Create Subdirectories: Allows users to create subdirectories within the current folder/directory ([MKD](#)).

Remove Subdirectories: Allows users to remove subdirectories from the current folder/directory ([RMD](#)).

Can View Directory Listing: Allows users to generate a directory listing of the contents of the folder ([LIST](#)/[NLST](#)).

Apply Rights to Subdirectories: Enable this check box to have these permissions, both File and Folder, propagated to all subdirectories of the specified path.

Titan FTP Permissions

Directory Access rules for the **User** are loaded first.

Directory Access rules for all **Groups** the user is a member of are loaded next. These Groups are loaded in the order in which they appear in the Groups tab of the User Configuration dialog. If a duplicate folder is encountered for which there are already Directory Access permissions specified, the SUM of the permissions is used.

Directory Access rules for the **Server** are loaded last. Again, if duplicates are located, they are summed together.

Example:

User A is a member of Group 1 and Group 2 for Server S.

User A has the following permissions: /pub/ - Read permissions

Group 1 has the following permissions: /pub/ - Write permissions

Group 2 has the following permissions: /pub/ - NO ACCESS AT ALL

Server S has the following permissions: /pub/ - LIST permissions

Outcome: User A will have READ, WRITE and LIST permissions to the /pub/ folder.

Virtual Folders Tab

Virtual folders are used to link or map external folders into a user's directory space. For Windows users, think of a virtual folder as a Windows shortcut. The link appears in one location while the data lives elsewhere. For UNIX users, virtual folders are very similar to symbolic links. Virtual Folders are commonly used to map network shares or folders from different drive letters into the server directory structure.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access the Virtual Folders tab at the **Server** level, in the tree pane expand the Server, click Files/Directories, and click the Virtual Folders tab.

To access the Virtual Folders tab at the **Group** or **User** level, in the tree pane select the Group or User, click Files/Directories, and click the Virtual Folders tab.

Configuration Options

Using Virtual Folders

From the Virtual Folders tab:

1. Click Add to display the New Virtual Folder wizard.
2. To select the fully qualified path, browse to the physical folder location. You may select a folder on your local computer, or you may choose a network folder that has been previously shared. If you are mapping a UNC share, make sure the account under which the Titan FTP Service is running has access to the UNC. Click Next.
3. Select the default permissions for the virtual file and folder using the check boxes. Click Next.
4. The Actual Path of the folder is displayed and the Virtual Path is displayed. You can change the Folder Name as it will appear under the virtual path, or you can leave the default name (which is the same as the Actual Path name). A sample of what the final path will look like will be displayed. Click Finish to generate the virtual folder mapping.
5. The Virtual Path and the Actual Path should now be displayed in the Virtual Folders tab. Click Apply.

Virtual folder updates are not real-time. If a user is connected to the server when you make changes to the Virtual Folder list, users will need to log out and log back into the system to see the virtual folder changes.

If mapping a [UNC](#) share, make sure the account under which the Titan FTP Service is running has access to the UNC. Otherwise, you will need to add the appropriate username and password under the UNC accounts tab.

See our topic on [Virtual Folders](#).

If you attempt to create a virtual folder to a mapped network drive, Titan FTP will replace the drive mapping with the actual UNC name. Titan FTP Service does not have access to mapped drives, only to UNC shares.

If you would like more information about configuring group level virtual folders, see the [Using Group Level Folders QuickStart Guide](#).

Disk Quotas

The **Disk Quotas** tab is used to configure disk quota limits.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

Where is it?

To access these settings at the **Server** level, in the tree pane expand the Server, click Files/Directories, and then click the Disk Quotas tab.

To access these settings at the **Group** or **User** level, in the tree pane expand the Server, expand the Group or User, click Files/Directories, and click the Disk Quotas tab.

Configuration Options

Use Inherited Setting: This check box appears on the Group and User levels. When selected, the values will be inherited from the next level up in the inheritance chain. Clear this check box to override the inherited values.

Enable Disk Quotas: When enabled, the server will have a limited amount of storage space. The rest of the disk quota options are unavailable unless disk quotas are enabled.

Current Disk Usage: Shows the amount of storage currently being used by this server.

Maximum Disk Usage: Specifies the maximum number of kilobytes of data the server will be permitted to store.

Recalculate: Recalculates the current disk usage.

Explore: Launches Explorer so you can browse the server's data directory. This is useful if you need to purge invalid files, or if you want to see how space is being used.

Free Files List: Type names of files/file types that will not be included in the quota calculations and use the Add or Remove buttons to compile a list.

Users Overview

If your server is configured for [standard Titan FTP Authentication](#), new user accounts can be created directly within the Administration program. From here, you can also launch the New User Wizard.

Where is it?

To access the Users tab, in the tree pane, expand your server and click Users.

Configuration Options

Currently Defined Users: List of users registered with this server, including the number total listed to the right.

New User: Click to launch the [New User Wizard](#).

Delete User(s): Select the group you wish to delete and select Delete Group(s). You will be prompted to confirm that you wish to delete the group.

Flush Cache: Immediately updated all user information. This feature is only available for servers using LDAP or AD for user authentication.

Creating Users

When you create a new user, the New User Wizard will launch. There are three ways to access the wizard and create a new user. Open your Titan FTP administrator and:

1. In the tree pane, right-click on Users and select New User. The New User Wizard will launch.
2. In the tree pane select Users, and then on the Users tab click New User.
3. In the tree pane select Users. On the menu bar select Users, New User Wizard.

Deleting Users

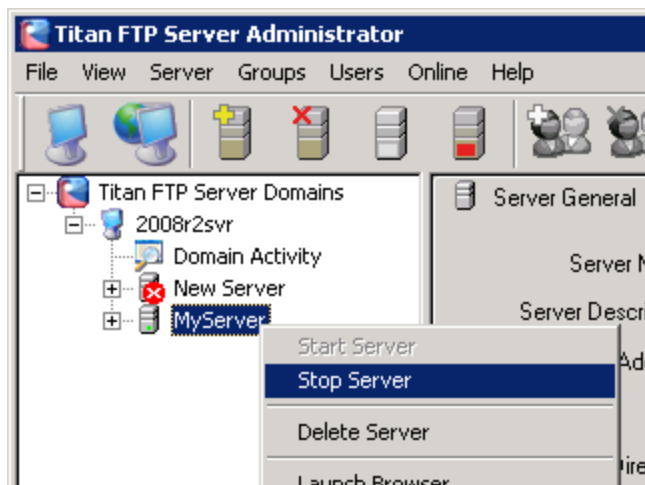
Deleting a user is **permanent**. If you are unsure about deleting a user account from the system, you

may want to **Disable** the account. When you delete a user account, Titan FTP will also remove the user from all groups.

If your server is configured for standard Titan FTP Authentication, you can delete users using the Titan FTP administrator in three ways:

1. In the tree pane under the appropriate server, expand Users and right-click the user you want to delete. Select Delete User from the context menu. You will be prompted to confirm the deletion of the user.
2. In the tree pane under the appropriate server, expand Users and select a user to delete. From the menu bar click Users, Delete User. You will be prompted to confirm the deletion of the user.
3. In the tree pane under the appropriate server, select Users. A list of users is generated and displayed in the tab pane. Select the user from the list and click Delete. You will be prompted to confirm the deletion of the user.

Note: You cannot delete a server if it is running. In order to delete the server, you must stop it by either clicking the Stop Server button in the menu or right-clicking the server in the tree pane to bring up the context menu and selecting Stop Server.



The server can be restarted in the same fashion.

User General Tab

The **User General** tab is used to configure User settings on an individual basis.

Where is it?

To access the User General tab, expand your server in the left tree pane, expand Users, select a User, and click the User General tab (this should show first by default).

Configuration Options

Use Inherited Setting: This check box appears on the Group and User levels. When selected, the values will be inherited from the next level up in the inheritance chain . Clear this check box to override the inherited values.

Account Enabled: When checked, the user account will be fully functional. If disabled, the user will no longer be able to log in using this account. When a user is banned from the server, the account will be disabled.

Username: The name attached to the account.

Password: The password attached to the username on this account.

Confirm Password: This must match the password.

Password Type: Set the security requirements of the password for this account. Anonymous (anything) is the lowest security option and is not recommended.

Users Full Name: Optional. The name of the user for this account.

Email Address: Optional. An email address attached to this account. We recommend including a valid email address, in case a user needs to receive notifications from the administrator.

Home Directory: The directory that will display automatically to the user.

Use Inherited Setting: This check box appears on the Group and User levels. When selected, the values will be inherited from the next level up in the inheritance chain . Clear this check box to override the inherited values.

Expiration Date: Optional. You can set an expiration date for the account, on which it will be automatically disabled.

Use Inherited Setting: This check box appears on the Group and User levels. When selected, the values will be inherited from the next level up in the inheritance chain . Clear this check box to override the inherited values.

Always Allow Login (even if max connections exceeded): Optional. When enabled, the user will be able to access the server, even if the maximum number of concurrent users has been exceeded (this setting is on the [Connections General](#) tab).

Use Inherited Setting: This check box appears on the **Group and User levels**. When selected, the values will be inherited from the next level up in the inheritance chain . Clear this check box to override the inherited values.

User-Level Groups Tab

The **Users** tab is used to manage group membership.

Where is it?

To access the Groups tab, in the tree pane expand Users and select the user, then click the Groups tab.

Configuration Options

Members of: Lists the groups this user is a part of. To add groups, select a group in the Not a member of list and use the arrows to shunt the group back and forth until the member is a part of the appropriate groups. Click Apply when you have completed your changes.

Not a member of: Lists all groups this member is not currently a member of. To add members to a group, select a group from the list and use the arrow buttons to shunt the user to the Members list. Click Apply when you have completed your changes.

Inheritance

Titan FTP supports the ability to set Shared Attributes at the Server, Group, or User level.

If an attribute is set at the Server level, every Group can inherit the value.

If an attribute is set at the Group level, every user who is a member of that group can inherit the value.

Inheritance at the Group and User level is controlled by the Use Inherited Setting check box. For certain attributes, such as directory permissions and virtual folders, the Server and Group level values are always inherited.

Advantages of Using Inherited Settings

Setting attribute values at the Server or Group level and then enabling Use Inherited settings at the Group or User level provides several advantages, including organization and simplification.

Rather than setting values for each user, you can set these values at the Server or Group level and minimize the amount of work required when you add new users or update attribute values.

FTP Commands

This section outlines the list of FTP commands currently implemented by Titan FTP.

Standard Commands

ABOR - Instructs the server to abort the current command.

APPE - Appends data to an existing file.

CDUP - Changes the current working directory to the parent directory.

CWD - Changes the current working directory to the relative or absolute path specified.

DELE - Deletes the specified file object.

HELP - Displays a list of implemented commands.

LIST - Generates a list of files for the specified (or current) directory. The file list is returned on a data connection.

NLST - Generates a list of filenames for the specified (or current) directory. The filename list is returned on a data connection.

MKD - Creates a folder.

MODE - Specifies the data transfer mode. Stream and zlib are supported.

NOOP - Pings the server to keep the control connection alive.

PASS - Sends the user's password to the server.

PASV - Instructs the server to go into passive mode and return an IP/Port combination to be used for a data connection.

PORT - Instructs the server to use the supplied IP/Port combination during the establishment of the next data connection.

PWD - Displays the current working directory.

QUIT - Terminates the user's session and closes the control connection.

REIN - Reinitializes the control connection. The currently authenticated user is cleared out and reset for a new USER.

REST - Specifies an offset for restarting a data transfer.

RETR - Used to retrieve a file from the server.

RMD - Removes/Deletes a directory folder from the server. The folder must be empty.

RNFR - Renames a file/folder. Used in conjunction with RNTD.

RNTO - Renames a file/folder. Used in conjunction with RNFR.

SITE - Special command used to issue site-specific instructions to Titan FTP Server.

STAT - Displays status information.

STOR - Instructs the server to begin storing a file that will be sent over the data connection.

STOU - Instructs the server to generate a unique filename used to store data being sent over the data connection.

STRU - Specifies the structure of data on the server. File format is currently supported.

SYST - Displays the system type for the server.

TYPE - Sets the data representation on the server.

USER - Sends the username to the server.

Advanced Commands

AUTH - Used to initiate an SSL encrypted session.

COMB - Combines file segments into a single file on the server.

CCSN - Used during secure FXP to set the handshaking role of the server.

CPSV - Used during secure FXP to set the handshaking role of the server. This is an alternate form of CCSN.

DQTA - Returns disk quota information.

EPRT - Similar to the PORT command, but for IP v6 addressing.

EPSV - Similar to the PASV command, but used for IP v6 addressing.

FEAT - Displays a list of extensions supported by the server.

MFMT - Change Last Modified Time for a file.

MFCT - Change File Creation Time for a file.

MDTM - Displays/sets date/time information for files.

MLSD - Generates/displays directory information over the control connection.

MLST - Displays file information over the control connection.

OPTS - Allows for the configuration/enabling of special options supported by the server.

PBSZ - Sets the Protected Buffer Size for an SSL data connection.

PROT - Sets the Protection Level for an SSL data connection.

SIZE - Returns the size of a supplied file.

SSCN - Specifies the size of the protected buffer on an SSL connection.

XCRC - Performs a CRC-32 checksum of the user supplied filename.

SITE Commands

SITE PSWD - Used to modify the current user's password on the server.

SITE ZONE - Used to display the current time zone setting for the server.

srxCfg Command Line Utility Overview

The srxCfg utility is a program that allows administrators to configure the Titan FTP server from a command prompt. The basic syntax is as follows:

```
srxCfg.exe /ADMINUSER=<adminusername> /ADMINPASS=<adminpass> ADMINHOST-  
T=<machinename_or_ip> /ADMINPORT=<adminport> /CMD=<command> /SERVER=<  
ftpservername> [/OUTFILE=<filename.ext>] [/CMDFILE=<filename.ext>]  
[/attr=<value>]
```

Note: /SERVER specifies the name of the Titan FTP server to execute the command against. If the Titan FTP server name is long or contains spaces, use double-quotes around the name.
For Example: /SERVER="My FTP Server", or /server=server1, or /SERVER="server1"

See our topics on different parameters accepted by Titan FTP Server:

[Required Parameters](#)

[Conditional Parameters](#)

[Optional Parameters](#)

srxCOM Overview

srxCOM is a COM/Scripting interface that can be used to configure Servers, Groups, and Users. The scripting engine is installed with Titan FTP.

Interface Name: srxCom.SRXTitan

Implementation DLL: srxCom.dll

Methods

General

[SRX_Connect\(\)](#) - Opens a connection to the Cornerstone Service.

[SRX_Disconnect\(\)](#) - Closes an existing connection.

[SRX_GetErrStr\(\)](#) - Retrieves an error string for the supplied error code.

Server-level Commands

[SVR_Create\(\)](#) - Creates a new server instance.

[SVR_Delete\(\)](#) - Deletes an existing server instance.

[SVR_Enum\(\)](#) - Generates a list of servers.

[SVR_Start\(\)](#) - Starts an server.

[SVR_Stop\(\)](#) - Stops an server.

[SVR_Restart\(\)](#) - Restarts an server.

[SVR_GetAttr\(\)](#) - Retrieves a configuration attribute for an server.

[SVR_SetAttr\(\)](#) - Sets/Modifies a configuration attribute for an server.

[SVR_GetSessions](#) - Generates a list of sessions for an server.

Group-level Commands

[GRP_Create\(\)](#) - Creates a new group for the specified server.

[GRP_Delete\(\)](#) - Deletes an existing group from the specified server.

[GRP_Enum\(\)](#) - Generates a list of groups defined for the specified server.

[GRP_GetMembers\(\)](#) - Generates a list of members/users for the specified server/group.

[GRP_SetMembers\(\)](#) - Changes the members list for the specified server/group.

[GRP_GetAttr\(\)](#) - Retrieves an attribute for the specified server/group.

[GRP_SetAttr\(\)](#) - Changes an attribute for the specified server/group.

User-level Commands

[USR_Create\(\)](#) - Creates a new user for the specified server.

[USR_Delete\(\)](#) - Deletes an existing user from the specified server.

[USR_Enum\(\)](#) - Generates a list of users defined for the specified server.

[USR_GetAttr\(\)](#) - Retrieves an attribute for the specified server/user.

[USR_SetAttr\(\)](#) - Changes an attribute for the specified server/user.

VB 6 Example

```
Dim srxcom

Set srxcom = CreateObject("srxCom.SRXCornerstone") ' instantiate the
object

srxcom.SRX_Connect("localhost",31000,"Administrator","MyPassword")

srxcom.SVR_Create("fred", "1.2.3.4", 12, "C:\fred", 0)

srxcom.SRX_Disconnect
```

Certificate Management

Certificates provide an essential layer of security to file transfers by verifying the origin of information transfers. An electronic document can be signed with a certificate and bound to the sender's public key, which creates a unique signature that can only be decoded by the matching private key.

Titan FTP's Certificate Manager allows you to **create** new certificates, **import** previously-made certificates and private keys, and **sign** your own certificates. Once you have certificates stored in Titan FTP, you can also use the Certificate Manager to **Delete**, **Export**, **Update**, or **View** the Properties of your certificates.

To find the Certificate Manager, launch the Titan FTP Administrator, expand your Server, and select Security. Under the FTPS/SSL tab, enable SSL/TLS and click the **Certificate Management...** button.

The Certificate Manager is accessible from other locations in Titan FTP; it will appear on any screen that deals with SSL, including during the Server Creation Wizard.

[Create a New Certificate](#)

1. Click Create to create a certificate. This will launch the SSL Certificate Wizard.
2. You must supply valid information for each field for the certificate to validate. The Common Name (CN) is the name of the server. Avoid using special characters (though the asterisk (*) symbol is valid when used as a [wildcard](#) to cover many different domains). Please note that some Certificate Authorities do not allow you to abbreviate the State/Province name. Click Next.
3. Select a desired key length for your certificate. Longer key lengths provide better security but result in slower performance. Shorter keys run faster but are less secure. Key lengths of 2048 bits or larger are recommended for secure environments. Click Next.
4. Your certificate name will populate automatically. Create a Private Key password. Your password is case sensitive and must be at least four characters with no spaces. After you confirm your password, click Next.

There are three options available for generating your certificate:

- **Self-sign this certificate**—Self-signed certificates are relatively insecure. In general, this option should only be used for testing purposes and should not be used in a production environment.
- **Generate CSR for signing by a Trusted Certificate Authority**—Select this option if you would like to generate a Certificate Signing Request (CSR) to send to an external Certificate Authority (CA) or Trusted Authority for signing. Once the CSR has been signed and your certificate generated, you will be able to update your CSR and use your newly signed certificate. Export the certificate request to a

directory by using the “...” browse button. For more information about generating a CSR for signing by a Trusted Certificate Authority, see the section on Generating & Updating a CSR.

- **Sign this certificate using the following Trusted Certificate**—Select this option if you would like to sign this new certificate using a trusted certificate already in your certificate store.

Click Finish when you are done configuring these options and Close the window.

To configure Titan FTP to start using the certificate, select Security in the tree pane and select the FTPS/SSL tab. Select your new certificate and enter the corresponding password.

Import a Certificate

Click Import to import an already-existing certificate and private key.

Import Certificate provides two options for importing your certificate, which depend on whether your certificate is stored in one file or two:

- **Import my Certificate and Private Key from a single file (PKCS#12)**—Use the “...” browse button to browse to your .p12 file. Type your Private Key password, confirm your password, and type a name used to identify this certificate in the system. When you are finished, click Import.
- **Import my Certificate and Private Key from separate files**—Use the “...” button to browse to your .crt file. If you would also like to Import your Private Key Information, select this check box and browse to your .key file.

You must then type your Private Key password and confirm your password. Type a name used to identify this certificate in this system. When you are finished, click Import.

Your certificate will be imported and added to the Certificate list.

Sign a CSR

Select Sign CSR. The Certificate Signing Wizard will launch.

The Certificate Signing Wizard provides two options for signing your certificate:

- **Sign a CSR in local store**—Use the dropdown arrow to select your certificate and type your password. Click Next when you are finished.
- **Select an external CSR**—Use the “...” button to browse to and save the certificate. Click Next when you are finished.

Select the certificate name using the dropdown arrow. Type the password used to access the keypair for the selected certificate. You can change the Valid From and Valid To dates by using the dropdown arrow. Click Finish.

Your certificate should appear in the Certificate List.

Generating & Updating a CSR

Having a certificate signed by a Certificate Authority (CA) adds a robust layer of authenticity and security to your certificate. If you opted to create a certificate and have it signed by a Certificate Authority, follow these steps:

1. After selecting Generate CSR for signing by a Trusted Certificate Authority, export the certificate request to a directory by using the “...” browse button. Be sure to take note of where you save the .csr file; you will need to access it again to send it to the Certificate Authority. Click Finish.
2. You will see a message indicating that your CSR has been successfully exported to the directory you specified. Click Close to close the Certificate Manager.

Sending the CSR to the Certificate Authority

1. Open your .csr file in a WordPad or other text editor. Copy the text of the entire file, including the words “Begin Certificate Request” and “End Certificate Request”.
2. You must choose a Certificate Authority. There are many to choose from, such as:
 - <https://www.thawte.com>
 - <http://www.verisign.com>
 - <http://www.digicert.com>

The CA’s website should include a place for you to paste your CSR and provide any additional information required by the Certificate Authority. After you submit your Certificate Signing Request, the CA will verify the information and create a certificate for you. The time necessary to create a certificate varies from authority to authority, so check with the specific CA for turn-around times.

To Update CSR in Cornerstone MFT

After the Certificate Authority approves your CSR, it will email you a secure link to access your certificate. Copy your certificate to WordPad and save in .crt format. When you name your .crt file, do not use extra periods or special characters. Be sure to take note of where you save the .crt file; you will need to access it again to update the certificate stored in the server.

1. Launch the Cornerstone MFT Certificate Manager. Select Update CSR. Do not choose Import—this will invalidate your CSR.
2. The Update CSR Utility will launch. Use the dropdown arrow to select the CSR File you would like to update with a signed certificate. Once updated, the CSR will become a valid certificate associated with your key pair. Type your password.

Use the “...” button to browse to the location of your certificate file. When you are finished, click Update. Click OK.

Your CSR is now upgraded to a verified certificate file. You may now use the certificate.

CRC File Integrity Checking

Titan FTP supports the ability for the client to verify that a file has been successfully transferred to the server without corruption. This is accomplished by requesting that the server perform a **Cyclic Redundancy Check**, or **CRC-32**, on the file once it has been uploaded.

What does a CRC do?

A CRC performs a mathematical calculation on a block of data and returns a number that represents the content and organization of that data. The CRC returns a number that uniquely identifies the data. CRC is the operation that generates a "fingerprint" for a block of data. The actual number, or fingerprint, that is used to identify the data is called a checksum.

Once the file has been uploaded, the client issues the `XCRC <filename>` command to the server. The server will perform the CRC-32 on the file and return the 4-byte "fingerprint" for the specified file. The CRC fingerprint will be returned in hexadecimal. The client application can compare this fingerprint to the CRC-32 fingerprint generated locally to determine if the file has been modified, corrupted, or altered during its transfer to the server.

For more information on the syntax and return values, see our topic on [XCRC](#).

Custom Message Variables

Custom variables are used to dynamically generate strings that reflect the current status of variables. Variables are commands entered between a pair of percent symbols (ex, %EXAMPLE%).

Where is it?

Variables can be used throughout the Titan FTP administrator, and in several locations you can find a Show Variables button to bring up a window with a list of available variables.

General Message Variables

%TIME% - Current system date/time in yyyy/mm/dd format.

%SYSTIME% - System time formatted according to the clock's settings.

%TIMEONLY% - Current system time, formatted according to the system clock settings (including punctuation, month/day/year order, etc.).

%DATEONLY% - System date, in yyyy/mm/dd format.

%DATETIMEEX% - Draws on the server date and time of an event.

%MONTHONLY% - Generates digits for the month, MM

%YEARONLY% - Generates digits for the year, YYYY

%DAYONLY% - Generates digits for the day, DD

%SYSDATE% - System date according to system clock.

%SYSDATETIME% - Date and time according to the system clock.

%VER% - The current version of the server. Version information will be displayed as X.XX.

%DOMAINNAME% - The name of the domain on which the server is running. By default, this is the name of the physical machine, but it can be customized by the Administrator to be any text string.

%COMMAND% - The last command to be received by the server in the context of this server-connection.

%RETCODE% - The last return code to be sent to the client in the context of this server/connection.

%EVENTTEXT% - Text describing the current [event](#), if any, that is being processed.

%FILEPATH% - The complete filename, including path, of the last file to be accessed by the server-connection. Resolves the last file acted upon.

%FILEPATH.PATH% - Full file path, without the name.

%FILEPATH.NAME% - File name, without the path.

%FILEPATH.NAME.NAME% - File name, without the extension.

%FILEPATH.NAME.EXT% - File extension, without the path or name.

Example:

For a file named **fred.txt** uploaded to **c:\srtMftData\MyServer\Michael\subdir\fred.txt**:

%FILEPATH% would be c:\srtMftData\MyServer\Michael\subdir\fred.txt

%FILEPATH.NAME% would be fred.txt

%FILEPATH.NAME.NAME% would be fred

%FILEPATH.NAME.EXT% would be txt

%RELFILEPATH% - The full path, relative to the home directory.

%RELFILEPATH.PATH% - The file path, without the name, relative to the home directory.

%RELFILEPATH.NAME% - The file name, without the path, relative to the home directory.

%RELFILEPATH.NAME.NAME% - The file name, without the extension, relative to the home directory.

%RELFILEPATH.NAME.EXT% - The file extension, without the path or name, relative to the home directory.

Example

If the Users Home Directory is \\srtserver\users\michael\, and the user goes into a folder 'daily-builds_VF' and uploads a file called 'test.txt':

%RELFILEPATH% will be "\\dailybuilds_vf\test.txt" (note its the full path, but relative to home dir)

%RELFILEPATH.PATH% will be "\\dailybuilds_vf"

%RELFILEPATH.NAME% will be "test.txt"

%RELFILEPATH.NAME.NAME% will be "test"

%RELFILEPATH.NAME.EXT% will be "txt"

%FILENAME% - The complete file name of the last file to be accessed by the server/connection (no path).

%DIRPATH% - The path in which the last server/connection access occurred.

%OLDFILENAME% - The old file name (from a rename).

%ATTRIBUTESCSV% - File attributes, tagged pair of values in CSV format.

%ATTRIBUTESXML% - File attributes, tagged pair of values in XML format.

Server Message Variables

%SERVERNAME% - The name of the server.

%SERVERID% or %SVR.SERVERID% - The internal ID of the server.

%SVR.MACHINENAME% - The name of the box or node where the server is physically located. This is useful in conjunction with the name of the logfile when prefixing the logfile name with the machine name.

%SVR.REPORTSDIR% - Folder name where reports are stored.

%SVR.BACKUPSDIR% - Folder name where backups are stored.

%SVR.DATABASEDIR% - Folder where temporary database files are stored.

%SVR.TEMPDATADIR% - Folder where temporary files (such as zip downloads, etc.) are stored.

%SVR.USERDATADIR% - Root folder where user directories are stored.

%SVR.BASELOGDIR% - Folder where log files are stored.

%SVR.<Attribute>% - Most server attributes are now accessible using variables. To see a list of current server attributes, run the srxCFG.exe utility with the /GETSATTR flag and the name of the server to dump a list of server attributes.

Example:

To get the FTP Send Buffer size, use %SVR.FTPSENDERBUFSIZE%

%SERVERTZ% - The Time Zone configuration value for the server.

%SSUPCNT% - The count of the total number of files that have been successfully uploaded since the server was started.

%SSDNCNT% - The count of the total number of files that have been successfully downloaded since the server was started.

%SSUPKB% - The count of the total kilobytes (KB) of data that has been successfully uploaded to the server since the server was started.

%SSDNKB% - The count of the total kilobytes (KB) of data that has been successfully downloaded from the server since the server was started.

%SSUPTIME% - The count of the total elapsed time that has been spent uploading files to the server since it was started.

%SSDNTIME% - The count of the total elapsed time that has been spent downloading files from the server since it was started.

%SSUPKPS% - The total average bandwidth utilization for uploads, in kilobytes-per-second, since the server was started.

%SSDNKPS% - The total average bandwidth utilization for downloads, in kilobytes-per-second, since the server was started.

%SSTOTCNT% - The count of the total number of files that have been transferred (uploaded and downloaded) since the server was started.

%SSTOTKB% - The count of the total kilobytes (KB) that has been transferred (uploaded and downloaded) since the server was started.

%SSTOTTIME% - The count of the total time that was spent transferring data since the server was started.

%SSTOTKPS% - The total kilobytes-per-second (KPS) value since the server was started. This is the overall bandwidth utilization of the server.

%SSSTARTTIME% - The time that the server started (GMT).

%SSRUNTIME% - The total days, hours, minutes, and seconds that the server has been up and running.

%SSTOTCXN% - The total number of open connections on the server.

%SSTOTUSRS% - The total number of distinct user connections on the server.

User/Connection Message Variables

%USER.USERID% - User ID of the user.

%EXPDATE% - The account expiration date for the logged in user.

%CIP% - The IP address for the client/user.

%FILESIZEKB% - The total number of bytes of the most recent file transfer.

%MAXUPNUM% - The configuration value for the Max Uploads Per Session. Since this is a Server configuration value that can be overridden/customized at the User level, this variable will display the setting that is currently in use. This is useful when the user exceeds the Max Uploads allowed Per session. You can display the maximum setting to the user and inform the user that the value has been exceeded.

%MAXDNNUM% - The configuration value for the Max Downloads Per Session. This is a Server configuration value that can be overridden/customized at the User level, so this variable will display the setting that is currently in use. This is useful when the user exceeds the Max Downloads allowed Per Session. You can display the maximum setting to the user and inform the user that the value has been exceeded.

%MAXUPSIZEKB% - The configuration value for the Max Uploadable File Size. This is a Server configuration value that can be overridden/customized at the User level, so this variable will display the setting that is currently in use. This is useful when the user exceeds the Max Uploadable Size allowed. You can display the maximum setting to the user and inform the user that this value has been exceeded.

%MAXDNSIZEKB% - The configuration value for the Max Downloadable File Size. Since this is a Server configuration value that can be overridden/customized at the User level, this variable will display the setting that is currently in use. This is useful when the user exceeds the Max Downloadable File Size. You can display the maximum setting to the user and inform the user that this value has been exceeded.

%USERNAME% - The user name of the logged in user.

%USEREMAIL% - The e-mail address for the logged in user.

%USERFULLNAME% - The full name of the logged in user.

%USERHOMEDIR% - The home directory for the logged in user.

%USTOTTIME% - The count of the total time that was spent transferring data since the user logged in to the server.

%USTOTKB% - The count of the total kilobytes (KB) transferred (uploaded and downloaded) since the user logged in to the server.

%USTOTCNT% - The count of the total number of files transferred (uploaded and downloaded) since the user logged in to the server.

%USUPKPS% - The total average bandwidth utilization for uploads, in kilobytes-per-second, since the user logged in to the server.

%USDNKPS% - The total average bandwidth utilization for downloads, in kilobytes-per-second, since the user logged in to the server.

%USUPTIME% - The count of the total elapsed time that has been spent uploading files to the server since the user logged in to the server.

%USDNTIME% - The count of the total elapsed time that has been spent downloading files to the server since the user has logged into the server.

%USUPKB% - The count of the total kilobytes (KB) of data that has been successfully uploaded to the server since the user logged in to the server.

%USDNKB% - The count of the total kilobytes (KB) of data that was successfully downloaded from the server since the user logged in to the server.

%USUPCNT% - The count of the total number of files that have been successfully uploaded since the user logged in to the server.

%USDNCNT% - The count of the total number of files that have been successfully downloaded since the user logged in to the server.

%USTOTKPS% - The total kilobytes-per-second (KPS) value since the user logged in to the server. This is the overall bandwidth utilization for the user.

%USTOTCXN% - The total number of connections for the logged in user.

%UUID% - Generates a unique GUID (Universally Unique Identifier) for use by the caller.

Reporting Variables

Dates will output in YYYY-MM-DD format. The .RAW extension variables remove the dash symbols (-) in output.

%DATE.YESTERDAY% - Yesterday's date, YYYY-MM-DD

%DATE.TODAY% - Today's Date, YYYY-MM-DD

%DATE.MONTH.THIS.BOM% - The first day of this month (BOM, beginning of month), YYYY-MM-DD

%DATE.MONTH.THIS.EOM% - The last day of this month (EOM, end of month), YYYY-MM-DD

%DATE.MONTH.LAST.BOM% - The first day of the last month (BOM, beginning of month), YYYY-MM-DD

%DATE.MONTH.LAST.EOM% - The last day of the last month (EOM, end of month), YYYY-MM-DD.

%DATE.MONTH.LAST% - The month number of the last month, MM

%DATE.MONTH.LAST.YEAR% - Year associated with last month, useful for determining last year in January. YYYY

%DATE.MONTH.THIS% - The month number of this month, MM

%DATE.MONTH.THIS.YEAR% - The year number for this month, YYYY

Note: Date variables used to be prefixed with REPORTS. Titan FTP will still recognize these variables, but will automatically change them in the code. They should no longer be implemented.

Events Overview

What is an Event?

A server **Event** is any action performed by or on the server, whether it be a user logging in or out, a command issued by a user, files uploaded or downloaded, or any other action. You can also elect to run an event at any time by selecting it and clicking the Run Now button on the Event Handlers tab.

Where is it?

Within the administrator, select your server in the left-hand panel, then select Events. The Event Handlers tab should be open by default.

Events are organized into a relational hierarchy in order to handle events from a more general level to a more specific level. For example, **all events** can be used as a basis to handle every server event. More events may be added to Titan FTP in the future to address protocol enhancements.

Event Handlers are used to trigger customized actions based on specific events and conditions. Events can be fired whenever anything of importance occurs on the server, such as a user logging in or a file being uploaded. You can find examples of specific event handlers and how to set them up in our QuickStarts. Titan FTP also provides pre-configured event handlers, which are listed on the Event Handlers tab.

For a detailed list of the available events, see our topic on [Events Options](#).

Additional Event Handler Options

Other ways you can configure your Event Handlers to use your server efficiently:

- Constrain certain users/groups to a limited command set.
- Create a directory log for each shared folder, so that whenever anything happens in that folder, an entry is added.
- Create command logs for every command entered.
- Kick any lower-class users (members of a less privileged group) if the number of connections to the server reaches a certain threshold.
- Compress or decompress a file after it has been uploaded (requires third party compression software).
- Encrypt or decrypt a file after it has been uploaded (requires third party encryption software).

- Scan a file for viruses after it has been uploaded (requires third party virus scanning software).
- Send an email to the administrator every hour showing the current status of the server.

Inheritance

Titan FTP supports the ability to set Shared Attributes at the Server, Group, or User level.

If an attribute is set at the Server level, every Group can inherit the value.

If an attribute is set at the Group level, every user who is a member of that group can inherit the value.

Inheritance at the Group and User level is controlled by the Use Inherited Setting check box. For certain attributes, such as directory permissions and virtual folders, the Server and Group level values are always inherited.

Advantages of Using Inherited Settings

Setting attribute values at the Server or Group level and then enabling Use Inherited settings at the Group or User level provides several advantages, including organization and simplification.

Rather than setting values for each user, you can set these values at the Server or Group level and minimize the amount of work required when you add new users or update attribute values.

Server Log Tab

The Server Log tab is used to view the Server Log in real-time. To access the Server Log tab, in the tree pane expand the Server, click Logging, and select the Server Log tab.

Auto-refresh list every X seconds: Enable this option schedules the logfile viewer to automatically refresh the screen after the specified interval has elapsed. For efficiency, the most recent entries are listed. For a complete listing of the entire logfile, click View Entire Logfile.

Refresh: Click Refresh to force an immediate refresh of the log viewer.

View Entire Logfile: Opens the complete logfile in a text editor.

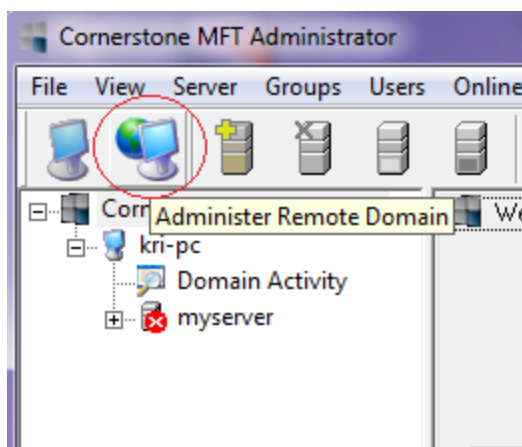
Clear Log Window: Clears the Log Window. To view the erased text, click View Entire Logfile.

Remote Administration

Your Titan FTP Service can be configured to allow for Remote Administration. If Remote Administration is enabled, you can launch the Administrator program and connect to your Titan FTP Service over the Internet.

To administer a Titan FTP server remotely:

Launch the Titan FTP Administrator and select Administer Remote Domain from the File menu.



When prompted, you will need to type the IP address and PORT number the remote Titan FTP server is listening on.

Remote Administration provides most of the same functionality available during Local Administration with the exception of certain directory traversal and security functions.

If you attempt to administer a server remotely and the configuration options are disabled, you are most likely not logged on locally.

Routers and Firewalls

How It Works

Most corporate and home networks today rely on a router and/or firewall to protect the internal computers or LAN (Local Area Network) from unauthorized access by outside users. An open port allows TCP/IP traffic to travel inbound or outbound through the router. Firewalls are designed to block inbound TCP/IP access on any ports not designated as open. A closed port blocks traffic from traveling through that port.

Firewalls provide a high level of security by preventing most inbound traffic while allowing most outbound traffic. However, they prevent any computers located outside the LAN (outside the firewall) from accessing any server installed on your internal LAN (inside the firewall).

When installing a server on the internal LAN, additional steps are necessary to allow users to gain access to the server without creating risk to other computers on the internal LAN. This can be accomplished by applying port forwarding to the firewall, which directs TCP/IP traffic to the proper computer. Port forwarding is used by most router/ firewalls. While using port forwarding, data arriving on a specific port is redirected to the same port on a different computer.

How Titan FTP Helps

When using Titan FTP with a router, cable-modem, DSL modem, or firewall, you can configure Titan FTP to recognize the IP address of the router. When the Titan FTP server goes in to [Passive](#) mode, it returns the proper global IP address to the client.

If you would like more information about configuring Titan FTP with a router/firewall, see the [Configuring Cornerstone with a Router/Firewall Quick Start Guide](#).

SFTP Support

Titan FTP provides support for SFTP (SSH's Secure File Transfer Protocol). When using SFTP and an SFTP-enabled client (such as [WebDrive](#)), data can be securely transferred over the Internet.

Titan FTP currently supports SFTP v.3 through SFTP v.6. Versions 5 and 6 support is still in a preliminary stage since many clients do not yet support these versions. If you experience any problems with SFTP, try setting the version back to 3 or 4.

Host Key Support

Titan FTP supports SSH host key authentication for secure connections. SSH host keys are similar to SSL Certificates in that there is a public key and a private key. The client keeps the private key secure on a local computer and distributes the public key to be imported into the Titan FTP system. Titan FTP will associate this public key portion with a user's account and will use it to verify that the client is using the correct key pair.

Titan FTP currently supports two host key encryption algorithms: RSA and DSA. Predefined key lengths of 512, 1024, 2048, and 4096 are supported as well as custom key lengths. Smaller key lengths are slightly faster but less secure. Larger/longer key lengths are stronger but slower.

For more information, see the [Cornerstone MFT FTPS/SSL QuickStart Guide](#).

Shared Attributes

Shared Attributes are variables that can be set at the Server, Group, or User level. These variables are common to all three levels and can be Inherited. Shared Attributes are located under the Connections and Files/Directories nodes for Servers, Groups, and Users.

Whenever possible, **set these values at the Server or Group level.**

List of Shared Attributes

Attribute	Description
AcctDisabledMsg	Message to display if a disabled user attempts to log in to the server. For multi-line messages, separate each line with a ' '.
AcctExpiredMsg	Message to display if an expired user attempts to log in to the server. For multi-line messages, separate each line with a ' '.
AllowMDTM	Allow users to modify file date/time settings via MDTM command. 0 - No, 1 - Yes.
AllowPASV	Allow Passive (PASV) mode connections. 0 - No, 1 - Yes.
BadPass	Disable Users account after BadPassCnt number of invalid password attempts. 0 - Do not disable the account, 1 - Yes disable the account.
BadPassCnt	Number of bad password attempts allowed before disconnecting the user. This value is ignored unless BadPass is enabled.
BadPassVal	Reserved.
BanFileTypes	Controls the use of banned file types. 0 - Disabled, 1 - Enabled.
BannedFileTypeMsg	Message to be displayed when the user attempts to upload a file that is banned. For multi-line messages, separate each line with a ' '.
BannedFileTypes	A semicolon separated list of file types to ban. For example: *.exe;*.txt;
BannedMsg	Message to display to users who are banned from the server. For multi-line messages, separate each line with a ' '.
BannerMsg	Message returned to the client upon initial connection to the server. For multi-line messages, separate each line with a ' '.

BaseLogDir	The fully qualified path to store the server log files.
BlockAntiTimeout	Block anti-timeout schemes. 0 - Disabled, 1 - Enabled.
BlockFXP	Block site-to-site/FXP file transfer attempts. 0 - Disabled, 1 - Enabled.
BlockFXPMsg	Message to display to the user when a site-to-site/FXP transfer is detected. For multi-line messages, separate each line with a ' '.
CanChangePwd	Allow the user to change their own password. 0 - Disabled, 1 - Enabled.
DelPartFiles	Delete partially uploaded files. 0 - Disabled, 1 - Enabled.
DenyAccessByDefault	When enabled, the default setting is to deny access to all IP addresses except those listed in the IPAccessList attribute. Ignored unless EnableIPAccess is enabled. 0 - Disabled, 1 - Enabled.
DiskQuota	Control disk quota usage. 0 - Disabled, 1 - Enabled.
DiskQuotaCnt	Disk quota, in KB. Ignored unless DiskQuota is enabled.
EnableIPAccess	Controls access checking by IP Address. If enabled, DenyAccessByDefault and IPAccessList will be used to determine who can access the server. 0 - Disabled, 1 - Enabled.
EnableRatios	Controls upload/download ratios. 0 - Disabled, 1 - Enabled.
ExceededQuotaMsg	Message displayed to the user if the user's disk quota has been exceeded. For multi-line messages, separate each line with a ' '.
IdleTimeout	Controls the monitoring of the IdleTimeoutCnt. 0 - Disabled, 1 - Enabled.
IdleTimeoutCnt	Number of minutes to elapse before kicking an idle user off the system. This value is ignored unless IdleTimeout is enabled.
IPAccessList	<p>List of IP addresses and masks that are used in conjunction with the DenyAccessByDefault and EnableIPAccess attributes to determine who can access the server. Each entry in the list is composed of a pair of values. The first value is whether to Deny (0) or Permit (1) access from the address. The second value is the address mask.</p> <p>Example1: 1 1.2.3.4 1 12.*.23.34 1 192.168.1.100-255 </p> <p>Example2: 1 127.0.0.1 0 63.*.* </p>
KickedMsg	Message displayed to the user when they are kicked off the server. For multi-

	line messages, separate each line with a ' '.
KickUser	Controls whether or not to kick users off the server after a certain number of consecutive bad commands. 0 - Disabled, 1 - Enabled.
KickUserBanIP	If enabled, the IP will be banned once the user has been kicked. This value is ignored unless KickUser is enabled. 0 - Disabled, 1 - Enabled.
KickUserCnt	The number of consecutive invalid commands to allow before kicking the user off the system.
KickUserDisable	If enabled, the user account will be disabled once the user has been kicked off the server. This value is ignored unless KickUser is enabled. 0 - Disabled, 1 - Enabled.
LimitPASVPORT	Controls the use of the range of ports available for use by the PASV command. 0 - Disabled (use all ports), 1 - Enabled (use only those ports in PasvPortStart and PasvPortEnd).
LockHome	Lock the user in their home directory. The user home directory is treated like the root of a drive, and the user will not be able to traverse up the directory structure.
MaxConnects	Controls the Maximum Number of Connections. 0 - Disabled, 1 - Enabled.
MaxConnectsCnt	If MaxConnects is enabled, this value determines the maximum number of simultaneous connections permitted.
MaxConnectsIP	Controls the Maximum Number of Connections Per IP. 0 - Disabled, 1 - Enabled.
MaxConnectsIPCnt	If MaxConnectsIP is enabled, this value determines the maximum number of simultaneous connections per IP.
MaxConnectsIPMsg	Message to display to a user if the MaxConnectsIPCnt value has been exceeded. For multi-line messages, separate each line with a ' '.
MaxConnectsMsg	Message to display to a User if the MaxConnectsCnt value has been exceeded. For multi-line messages, separate each line with a ' '.
MaxDownloadKPS	Controls the Maximum Download KB Per Second. 0 - Disabled, 1 - Enabled.
MaxDownloadKPSCnt	If MaxDownloadKPS is enabled, this value determines the maximum band-

	width allowed for downloading on the server (in KPS). This value will be divided up evenly among all sessions logged in. If this value is 10KPS and there are 5 active sessions, each session will max out at 2KPS during downloads
MaxDownloadNum	Controls the Maximum Number of Files Downloaded Per Session. 0 - Disabled, 1 - Enabled.
MaxDownloadNumCnt	If MaxDownloadNum is enabled, this value is the maximum number of files that a User is permitted to download during a session.
MaxDownloadNumMsg	Message to display to the user once they have exceeded their MaxDownloadNum for the session. For multi-line messages, separate each line with a ' '.
MaxDownloadSize	Controls the Maximum Download File Size. 0 - Disabled, 1 - Enabled.
MaxDownloadSizeCnt	If MaxDownloadSize is enabled, this value contains the maximum file size in KB that can be downloaded.
MaxDownloadSizeMsg	Message to display to the user when they attempt to download a file larger than MaxDownloadSizeCnt. For multi-line messages, separate each line with a ' '.
MaxUploadKPS	Controls the Maximum Upload KB Per Second. 0 - Disabled, 1 - Enabled.
MaxUploadKPSCnt	If MaxUploadKPS is enabled, this value determines the maximum bandwidth allowed for uploading on the server (in KPS). This value will be divided up evenly among all sessions logged in to the server. If this value is 10KPS and there are 5 active sessions, each session will max out at 2KPS during uploads.
MaxUploadNum	Controls the Maximum Number of Files Uploaded Per Session. 0 - Disabled, 1 - Enabled.
MaxUploadNumCnt	If MaxUploadNum is enabled, this value is the maximum number of files that a user can upload during any given session.
MaxUploadNumMsg	Message to display to the user once they have exceeded MaxUploadNum for the session. For multi-line messages, separate each line with a ' '.
MaxUploadSize	Controls the Maximum Upload File Size. 0 - Disabled, 1 - Enabled.

MaxUploadSizeCnt	If MaxUploadSize is enabled, this value contains the maximum file size in KB that can be uploaded.
MaxUploadSizeMsg	Message to display to the user when they attempt to upload a file larger than MaxUploadSizeCnt. For multi-line messages, separate each line with a ' '.
Notes	Comments about this Server/Group/User.
PASVPortEnd	If LimitPasvPort is enabled, this value is the ending value for the allowable passive port range.
PASVPortStart	If LimitPasvPort is enabled, this value is the starting value for the allowable passive port range.
QuitMsg	Message to display to the user in response to the QUIT command. For multi-line messages, separate each line with a ' '.
QuotaFreeFileList	If DiskQuota is enabled, this value specifies a list of file types (*.exe;*.txt;*.doc) that are considered free and will not count against the disk quota.
RatioDLCnt	If EnableRatios is enabled, this value represents the number of downloads.
RatioFreeFileList	If EnableRatios is enabled, this value specifies a list of file types that are considered free and will not count against the ratios.
RatioType	If EnableRatios is enabled, this value determines the type of ratios to use. 0 - Count number of files per each individual session. 1 - Count number of KB per each individual session. 2 - Count number of files across all sessions for a user. 3 - Count number of KB across all sessions for a user.
RatioULCnt	If EnableRatios is enabled, this value represents the number of uploads required before a download can occur.
ShowHiddenFiles	Controls the display of hidden files in directory listings. If this feature is enabled, files marked as Hidden in the local file system will show up during a generic directory request from a client. If this feature is not enabled, the client will need to explicitly specify the -H flag during a LIST command. 0 - Disabled, 1 - Enabled.
SSLAllowFXPS	If SSLEnabled is enabled, this flag determines if secure Site-To-Site FXPS

	<p>transfers are permitted.</p> <p>0 - No, do not allow FXPS.</p> <p>1 - Yes, allow FXPS.</p>
SSLBannerMsg	Message to display to the user when they connect to the server over the SSLImplicitPort. For multi-line messages, separate each line with a ' '.
SSLCertName	Name of the SSL certificate to be used at this level.
SSLCertPassword	Password for the SSL certificate. For security reasons, this attribute can only be set, not retrieved.
SSLDisabledMsg	Message to display to the user if they attempt to initiate an SSL connection and SSLEnabled is disabled. For multi-line messages, separate each line with a ' '.
SSLEnabled	Controls if SSL is enabled. 0 - Disabled, 1 - Enabled.
SSLProtData	This flag controls the default protection mode of the data connection in SSL. If the client does not specify a PROT P or PROT C, this flag will be used to determine if the data connection is encrypted.
SSLRequired	1 - Require any FTP connection to use SSL. 0 - Allow FTP connections that are not secured with SSL.
SSLRequiredMsg	Message to display to the user if they attempt to initiate an FTP connection without SSL and SSLRequired is enabled. For multi-line messages, separate each line with a ' '.
STOUPrefix	Prefix to be used during the generation of a unique file name used in the STOU command.
STOUExtension	File extension to be used during the generation of a unique file name used in the STOU command.
WelcomeMsg	Message to display to a user once they have successfully logged in. For multi-line messages, separate each line with a ' '.
SFTPEnabled	1 - Enables SFTP support. 0 - Disables SFTP support.
SFTPHostKeyName	The name of the Host Key file, stored in the Host Key Folder, used by Titan FTP during SFTP handshaking.

SFTPHostKeyPassword	Password for the SFTP Host Key. For security reasons, this attribute can only be set, not retrieved.
SFTPUseCompression	1 - Titan FTP will use zlib compression if also supported by the client.
SFTPCipherList	A list of encryption ciphers, in order, that Titan FTP will present to the SFTP client during the handshaking/negotiation phase of the connection.
SFTPMACList	<p>A list of MAC algorithms, in order, that Titan FTP will present to the SFTP client during the handshaking/negotiation phase of the connection. The following MAC algorithms are currently supported:</p> <ul style="list-style-type: none"> md5 sha1 ripemd160 ripemd160@openssh.com sha1-96 md5-96

SSL Support

Titan FTP provides support for the industry standard Secure Sockets Layer (SSL). When using SSL and an SSL-enabled client (such as WebDrive), data can be securely transferred over the Internet.

Titan FTP supports two methods of SSL enabling: Implicit and Explicit SSL.

Explicit SSL: Allows the client to initiate an SSL connection explicitly using the AUTH SSL command. See [RFC 2228](#) for more information.

Implicit SSL: Using Implicit SSL, Titan FTP will open a specific port that will only be used for SSL connections. By default, this is port 990; however, any port can be used.

Notes on SSL

Titan FTP does not support the [PBSZ](#) FTP command as defined in RFC 2228. When a client issues the [PBSZ](#) command, Titan FTP will return a 200 OK, PBSZ=0 message. See [PBSZ](#) for more information. [PROT](#) P, [PROT](#) S, and [PROT](#) E are all treated as equal. Issuing any of these commands will result in the data channel being encrypted. To disable encryption of the data channel, issue the [PROT](#) C command. See [PROT](#) for more information.

UNC Accounts

Titan FTP can utilize **UNC** accounts to authenticate users who access the server. Titan FTP will check the users in the list one at a time until it authenticates against the UNC share.

To modify the UNC settings in the Titan FTP Administrator, see the topic on [Server UNC Accounts Tab](#).

This list is not intended to be a list of your users. You will likely only need to add one username to the UNC Accounts tab. The UNC account should have all of the permissions any of your users will need on the UNC share. The permissions of the UNC user can be further restricted by Titan FTP, but Titan FTP cannot elevate the permissions of the UNC user. For example, a user may have write access in Titan FTP, but if the UNC user does not have write access, the user will not be able to write to files.

See methods for using UNC pathways with different forms of Titan FTP [User Authentication](#).

NT Impersonation with UNC

If you are using Window NT Impersonation, the UNC Accounts tab will be disabled. When you use Windows Impersonation, the access rights of individual users will be used to authenticate UNC shared documents. UNC accounts are not used in conjunction with Windows Impersonation.

For more information on configuring Titan FTP using UNC paths for data storage and scalability, see theTitan FTP [Using UNC Paths for Data Storage & Scalability QuickStart Guide](#).

User Authentication

Titan FTP supports Native Authentication and NT/SAM Authentication:

[Titan FTP Native Authentication](#)

When using native Titan FTP authentication, the server administrator creates, manages, and deletes user accounts from within the Titan FTP Administrator. The user accounts created in the Administrator are used to access the server for which they are defined. These user accounts will not permit users to access other areas of your network.

[Windows NT/SAM Authentication](#)

When using Windows NT/SAM authentication, the server administrator creates and deletes user accounts using the Windows NT User Manager, found in the Windows Control Panel. The Administrator can then be configured to include one or more NT Groups from the Windows SAM database. All NT user accounts from the selected NT group or groups will then appear in the valid user list for Titan FTP. This has the benefit of providing your NT users with a single username/password they can use to access both the NT domain and the Titan FTP. When using Windows NT/SAM Authentication, Titan FTP can be configured to access a local Windows workstation or a Windows Domain Controller.

See our topic on the [Windows NT/SAM Authentication](#).

Virtual Folders

Virtual folders are folders that can be mapped into a server's data directory. They are used to link, or map, external folders into a user's directory space. The virtual folder appears to be on your computer; however, the data is actually stored somewhere else.

If you are a Windows user, you can think of a virtual folder as a Windows Shortcut. The link appears in one location and the data lives in another location. For UNIX users, virtual folders are very similar to Symbolic Links.

These values can be set at the Server, Group, and User level. See [Inheritance](#) and [Shared Attributes](#) for more information.

- Group level virtual folders allow data to be shared with all users of a given group. All users can share the same data and have Directory Access Rights to that data. Virtual folders can be made accessible to all users in the group, depending on the Directory Access Permissions set for that group.
- Virtual folders added at the User Level are limited to a specific user. When you add a virtual folder to a Titan FTP configuration, the default Directory Access Permissions will be set to Read Only, which means users are allowed to browse the folder and download information, but cannot modify the contents or upload files. You can modify the standard Directory Access Permissions after the virtual folder has been added to the configuration.

For more information on group and user virtual folder options, see our topic on the [Where is it?](#).

UNC Support

One of the benefits of virtual folders is that you can access network shares from the Titan FTP server through the use of virtual folders. Titan FTP supports the ability to add a UNC path into the name space.

For example, if you have a share on your network called \\MyServer\\My Music\\ you can use virtual folder support to map that into your server data directory as /pub/My Music/ or /usr/joe/My Music/.

If you attempt to create a virtual folder for a mapped network drive, Titan FTP will replace the drive mapping with the actual UNC name. The Titan FTP Service does not have access to mapped drives, only to UNC shares. Titan FTP runs as a Windows Service that, by default, does not have access to shared network resources because shared network resources are based on the authorized Windows user. If you are mapping a UNC share, you must make sure that the account under which the Titan FTP Service is running has access to the UNC. Otherwise, you will need to enter the appropriate username and password under the [UNC Accounts](#) tab.

Default Permissions for Virtual Folders

When you add a virtual folder to a Titan FTP configuration, the default Directory Access Permissions will be set to Read Only. Users will be able to browse the folder and download information, but will not be able to modify the contents or upload files.

You can modify the standard Directory Access Permissions once the virtual folder has been added to the configuration.

For more information about configuring group level virtual folders, please see the [Titan FTP Using Group Level Virtual Folders QuickStart Guide](#).

Wildcards

Titan FTP's powerful events configuration options allow for the use of **wildcards**, or short commands which blanket-call variables. Titan FTP uses standard pattern-matching syntax for computers. Here are a few examples of wildcards to use for event creation:

Specifying **A*** in a list of variables would cause the condition to be satisfied if the server command used started with an A.

Specifying **4*** in the list would cause any 400-level return codes to satisfy the condition.

Specifying ***z*** in the list would cause the condition to be satisfied for any username that contains a z.

Specifying **grp*** in the list would cause the condition to be satisfied for any group names that begin with grp.

Specifying ***.txt** in the list would cause the condition to be satisfied for any filename with a .txt extension.

Specifying ***f*** in the list would cause the condition to be satisfied for any directory name that contains an f.

Specifying **123.*.*** in the list would cause the condition to be satisfied for any IP address that starts with 123.

FAQ

Can I upgrade over my existing version of Titan FTP?

When upgrading to a new release of Titan FTP, you can install the new version directly over your existing version. All current configuration settings will be retained.

When installing an update, it is highly recommended that you restart the OS after installing the update even if the installer program does not require you to do so.

It is also recommended that you backup your data directories, as well as export (using regedit) any registry keys under HKLM\Software\South River Technologies\%program name% (where program name is replaced by Titan or Cornerstone). This process is considered a "best practice" and simply assures that any information lost during an upgrade can be restored if necessary.

What characters can't be used in a file name?

You can't use any of the following characters in a file name: \ / ? : * " > < |

Can I configure the MFT server to listen for standard FTP and explicit SSL on multiple ports?

Titan FTP can listen for FTP on one port and SSL/FTPS on another port. If you want to have SSL/FTPS listening on multiple ports, you must configure another server under the domain and set up the other SSL/FTPS ports.

When a user is created, why does Titan FTP automatically give them full access to the home directory, but when you delete the access from the user, it puts it back?

When a user account is created, Titan FTP will give the account full rights to its home directory. To change/limit access to the home directory, you can alter the Directory Access Rule for the user's home directory. If you delete the rule, Titan FTP will restore it to the default permissions. If you want the user to have no access to their home directory, you need to leave an empty rule in the list.

Why doesn't the server I configured start automatically when the computer is booting up?

- Make sure you have enabled Start Titan FTP Service when Windows boots in your Titan FTP Domain Configuration.
- Make sure you have enabled Start this server when Titan FTP Service starts in your Titan FTP Server Configuration.
- Make sure Titan FTP service is set to Automatic so the service starts automatically under your Windows service administration.
- Please check the Titan FTP log files for any errors. The log files will display an error if the server is unable to start.

- You may have a NIC card that does not come online with a valid IP address before the Titan FTP service starts, or you could have another service that is trying to use port 21.
 - To check if other services may be using port 21, run a netstat -a -n -p tcb -b from a command line interface before you start your Titan FTP servers and check to see if another program may be using FTP port 21.
- You may have to change the binding order of your NICs.
- Make sure the FTP Publishing Service is set to automatic or turned on, as it will affect Titan FTP. (Microsoft updates may automatically install this service.)

Can I use IE7 with Titan FTP?

If you are using IE7 and need to access a Titan FTP server, you should consider using the Lock User In Home Directory feature; otherwise IE7 will issue a CWD/ immediately after connecting to the Server. If Lock User In Home Directory is not enabled, a CWD/ command usually results in Titan FTP trying to do a CWD c:\srFTPData\ which users do not have access to for security reasons. If you are not able to use the Lock User in Home Directory feature, you will need to change your root directory level Directory Access to at least View Directory/List for your IE7 users, or they will have problems accessing your Titan FTP server.

Does Cornerstone MFT provide an API?

Yes, there is a COM interface called srxCOM, and there is a command line utility called srxCFG.exe.

What Ports does Titan FTP use when integrating with Active Directory?

AD Ports used by Titan FTP:

- TCP %localmachine%:microsoft-ds %localmachine%.srt:0 LISTENING 4
- [System] - Directory Services
- TCP %localmachine%:1045 %localmachine%.srt:0 LISTENING 416
- [Isass.exe] - Local Security Authority Subsystem Service
- TCP %localmachine%:1050 %localmachine%.srt:0 LISTENING 1744
- [dsamain.exe] - if using ADAM
- TCP %localmachine%: netbios-ssn %localmachine%.srt:0 LISTENING 4
- [System] - Netbios session
- UDP %localmachine%: isakmp *: * 416
- [Isass.exe] - Local Security Authority Subsystem Service

- UDP %localmachine%: ipsec-msft *.* 416
- [lsass.exe] - Local Security Authority Subsystem Service
- UDP %localmachine%:microsoft-ds *.* 4
- [System] - Directory Service
- UDP %localmachine%:1052 *.* 356
- [winlogon.exe] - Windows login manager

[Why do I receive an error upon startup of Titan FTP Administrator stating that my IP may be incorrect or the port may be in use?](#)

Java has made a recent change that takes over port 31000. Please run a **netstat -a -n -p tcp -b**. If the Java service (or any other than Titan FTP) is running on port 31000, you will need to change your Administration port in Titan FTP to a non-used port (for example, 31010 or other not well-known port that is not currently in use).

[Why do I receive the error code “425 Cannot open data connection”?](#)

The 425 error indicates that the client is running in Active/PORT mode and you have a firewall in front of your client PC.

You should contact the user and have them configure their client to run in PASV/Passive mode instead.

[How do I configure Public Key authentication with Titan FTP?](#)

If you plan to use public key authentication with Titan FTP, Titan FTP must have a copy of each client's public key before the client can connect. To do this, run the Titan FTP Administrator utility and use the left-hand tree pane to navigate to the Username who will be using public key authentication with the server. Click Security in the tree pane, then select the SFTP/SSH tab and use the Host Key Management utility to Import the public key for that user. Once the key is imported, return to the main user's SFTP tab and select their public key from the list of public keys in the dropdown list box. This will assign that public host key to the user.

Also, on the main SFTP tab for the Server, make sure you have enabled the **Allow Trusted Host Keys When Accessing this Server** option. This option tells Titan FTP to send public key as an authentication type (along with password). If you enable the Require Trusted Host Keys option, then Titan FTP will only send Public Key as the authentication method.

For more details on how to use public key authentication with Titan FTP, please review the [SFTP SSH Host Key Authentication QuickStart](#).

[Why do I receive the “Error 1610” message while importing SSHKEYGEN host keys in Titan FTP for](#)

SFTP?

There are two options to fix this issue. This problem most commonly occurs when you are using Linux.

Option #1, Performed on the client:

1. Download and run Puttygen.
2. Select Conversions > Import Key.
3. Select the Private Key and click Open.
4. Type the password for the Public Key and click Save Public Key.
5. Send the public key file to the Server Administrator to import into Titan FTP Server.

Option #2, Performed on the client:

If you have created an OpenSSH key pair with the ssh-keygen command, you can use the following command to create a usable public key:

```
ssh-keygen -e -f <private_key_name> > <public_key_name>
```

For example:

```
ssh-keygen -e -f $HOME/.ssh/id_dsa > $HOME/.ssh/SSH_dsa.pub
```

This command will read the private key and generate a public key that can be used by Titan FTP Server.

[What should I do if I receive the "Error 1610" message while trying to import Public Keys created by MFT Clients that are not SSHKEYGEN created?](#)

1. Generate Key(s) in Puttygen.
2. Type in password for key and change conversion option to Export ssh.com key.
Note: You must add the *.pub extension to the filename.
3. Export the private key from puttykeygen (you do not have to change file extensions on this file).
4. You should now have two key files. Import the *.pub key into the Titan FTP user's account via the SFTP tab under the user's configuration options.
5. You must replace the older putty generated public key with the one you are importing into Titan FTP, so click Yes when prompted.
6. Click Close once the import is finished, then attach the public key to the user via the SFTP tab on the user's configuration.
7. Open MFT client software and import the private key into user's configuration.

8. Browse to the private keyfile, type the keyfile password, and click OK.

To test this, make sure that the Titan FTP server is configured to Require trusted host keys when accessing this server at the server level. Have your test user try to connect using SFTP.

For more information about using Titan FTP with Host Keys, see the [Titan FTP Host Key Quick-Start Guide](#).

How do I configure an SFTP Server and create a HOSTKEY Pair in Titan FTP?

You can run the standard Titan FTP wizard to configure a standard server. Once the server has been created, click the SFTP/SSH tab for the server and enable SFTP/SSH. You will then create a hostkey pair for use by the server. Once this has been completed, you must open port 22 for standard SFTP/SSH.

How to create a Hostkey pair:

On your server, you must create a Host Key Pair that will be used/assigned to the SFTP server. Use the Host Key Management utility in the Titan FTP Admin console to generate the key pair and to assign it to the server. You might not need to send it to the client; however, you can if you want to. Just Export the Public Key and send that .pub file to the client.

If the client intends to use Public Key Authentication instead of the default Password Authentication, you must configure Titan FTP for Public Key Authentication and the SFTP/SSH client Administrator must export the client's Public Host Key and send it to you so that you can import it into Titan FTP.

This process is outlined in detail in our SFTP/Host Key Quick Start Guide on our Web site.

Troubleshooting - set logging level to debug

If you are experiencing problems with your server, please set your logging level to Debug (change your rotation schedule to Daily so the log files won't grow too large) and send a copy of your log files attached to a new support ticket. This will allow SRT to troubleshoot your support ticket more quickly and efficiently.

For more information on using logging for troubleshooting, see our topic on [Logging](#).

Report Issues

Reporting Problems

To report a problem, visit the Titan FTP [support page](#). If the answers aren't in the product help, explore the Knowledge Base and submit a ticket if necessary.

Please furnish our Support Engineers with the following information:

- The Windows platform that you are running
- The Titan FTP version you are using
- The URL of the server that you were using when the problem occurred
- A detailed description of the problem

Include file name and complete sub-directory name if applicable. Attach a copy of the log file to your e-mail.

To find pertinent information specific to your version of this product, go to the License Information tab under App Settings, General Settings and click Copy Program Info to Clipboard.

See our topic on [Server Log Tab](#).

Configuring a New Server

We have provided a sequence of topics which cover configuring a server from start to finish. This tutorial is designed to give you detailed, step-by-step instructions for creating a new server, including helpful tips and general information about servers which will help you get the most out of your Titan FTP software.

Choosing IP Address and Port

Note: Servers will compete for ports if identical port numbers are used on multiple servers. If you plan to create more than one server using the same protocols, designate different port numbers to prevent complications.

Before you create a new server, you must decide which IP address and port number your server will use. Most computers have a single IP address that can be accessed by other users. If you do not know the IP address of your computer, open a command prompt (DOS box) and type the command `IPCONFIG`. This command displays the IP address of your computer.

This IP address can be used for your server. You should also make sure that you have a static IP address for your computer.

NOTE: If you access the Internet through a dial-up account, you most likely have a dynamic IP address. If you have a dynamic IP address: during the setup process when you are prompted for the IP address, select Any Available IP Address.

For each IP address, there are many ports that can be used to access the computer.

If you think of the IP address as your house, a port is similar to a door that can be used to gain access to your home. TCP/IP defines standard port numbers for various protocols. For example, when you connect to a Web site using your browser, you usually connect over port 80, which is the port reserved for HTTP access. For FTP access, the default port is port 21. If you are setting up an FTP server, you will usually use port 21.

Before you set up an FTP server, check if any other program is currently using port 21 on your computer. To check which ports are being used on your computer, open a command prompt and enter the command:

```
netstat -a -n -p TCP
```

This command will dump out a list of IP addresses and ports that are currently in use on your computer. If ipconfig revealed that your IP address was 192.168.1.100, then the netstat command may print information such as:

Proto	Local Address/Port	Foreign Address	State
TCP	192.168.1.100:80	0.0.0.0:0	Listening
TCP	192.168.1.100:990	0.0.0.0:0	Listening

Under the Local Address/Port column is a list of IP/ports that are currently in use. If you see an entry that has ':21' after the IP address in the Local Address/Port column, then your default FTP port is currently being used by another application. If you do not see ':21', then the FTP port is available for use. If port 21 is currently in use, it may be that another FTP server is active on your computer. You can either choose another port, such as port 2100, or you can make port 21 available by closing the application that is using port 21.

There are over 32000 ports per IP address on your computer, and you can use any port that is available for your Server. TCP/IP usually reserves ports 1 through 1024 for special uses (such as 21 for FTP and 80 for HTTP), so if you do not use port 21, you should use a port number above 1024 for your server.

Choose a Location for Your Data

Your server will serve files to users who connect using a client. When users connect to your server, they will usually want to download existing files or upload new files. The files that your server serve are stored either on your local disk drive or on a network UNC that has been shared for you to use.

Typically, you will not want to provide users with the ability to access all of your files. You should choose a location that will house the files that you want users to be able to access (for example, an individual subdirectory). This directory, along with all subdirectories and files within those subdirectories, is known as the namespace for the server. By default, Titan FTP will create a base directory on your computer named C:\srFTPData, which is the primary namespace where Titan FTP will store all of the data for all servers that you configure. If you create an server name MyFirstServer, then Titan FTP will create a directory named C:\srFTPData\MyFirstServer\ that will be used as the primary namespace for all files accessible to users connecting to MyFirstServer.

Note: During the process of creating the new server, you will have an opportunity to customize the directory name for the server.

Once you have chosen an IP address, a Port number, and a Data Directory location for your new server, you are ready to create your new server. You can use the Titan FTP Server Administrator New Server Wizard to create your new server.

New User Wizard

A separate **New User Wizard** window will appear to help you through the steps of creating a new User for your server. This wizard should be simple to navigate, but here is some extra information on your initial configuration options.

Most of these settings can be changed after the user is created.

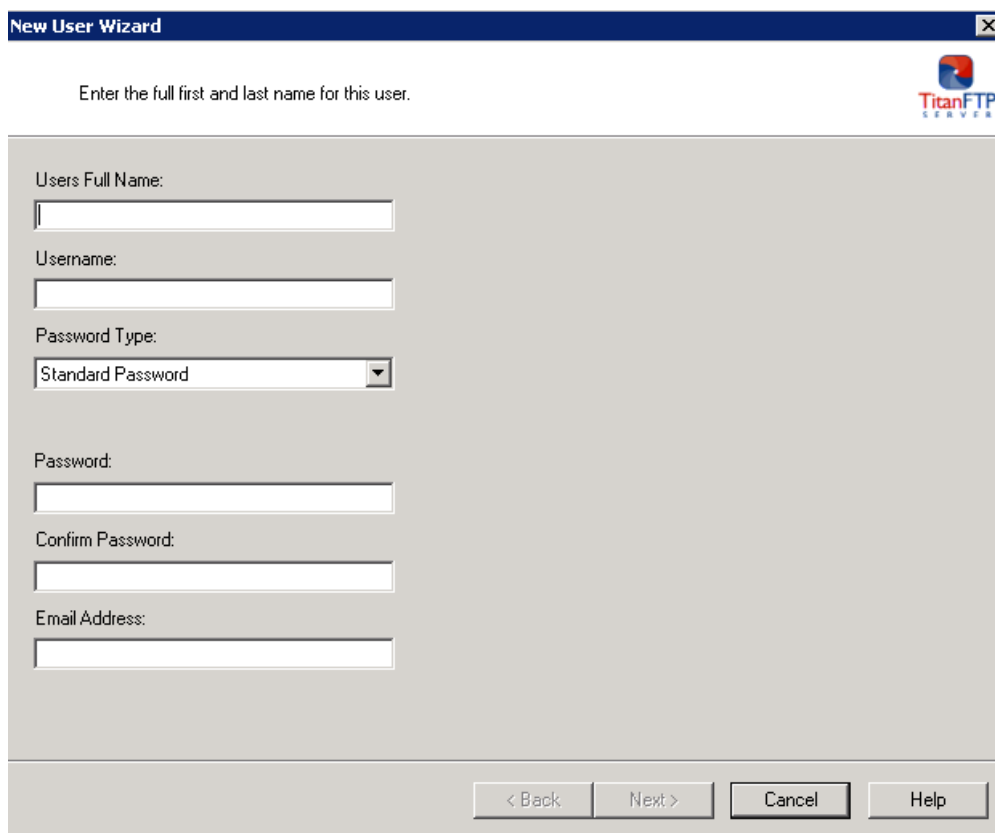
See our topic on the .

Where is it?

Launch the New User Wizard by navigating to Groups in your left-hand tree-pane, expanding the appropriate group, and selecting Users. Click the New User button on the User tab.

Wizard Steps

Step 1



The screenshot shows the 'New User Wizard' window, titled 'New User Wizard' with a close button (X) in the top right corner. The window has a dark blue header bar. Below the header, there is a instruction: 'Enter the full first and last name for this user.' and the TitanFTP logo. The main area contains several input fields: 'Users Full Name:' with a text box, 'Username:' with a text box, 'Password Type:' with a dropdown menu showing 'Standard Password', 'Password:' with a text box, 'Confirm Password:' with a text box, and 'Email Address:' with a text box. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Users Full Name: Enter a full name for the user. This is for metadata purposes or to identify between multiple users with similar usernames. This does not need to be unique.

Username: A unique name used to log into the Titan FTP server.

Password Type: Specify the type of encryption you would like to use for your password. Standard alphanumeric passwords are supported as well as One Time Passwords using S/Key.

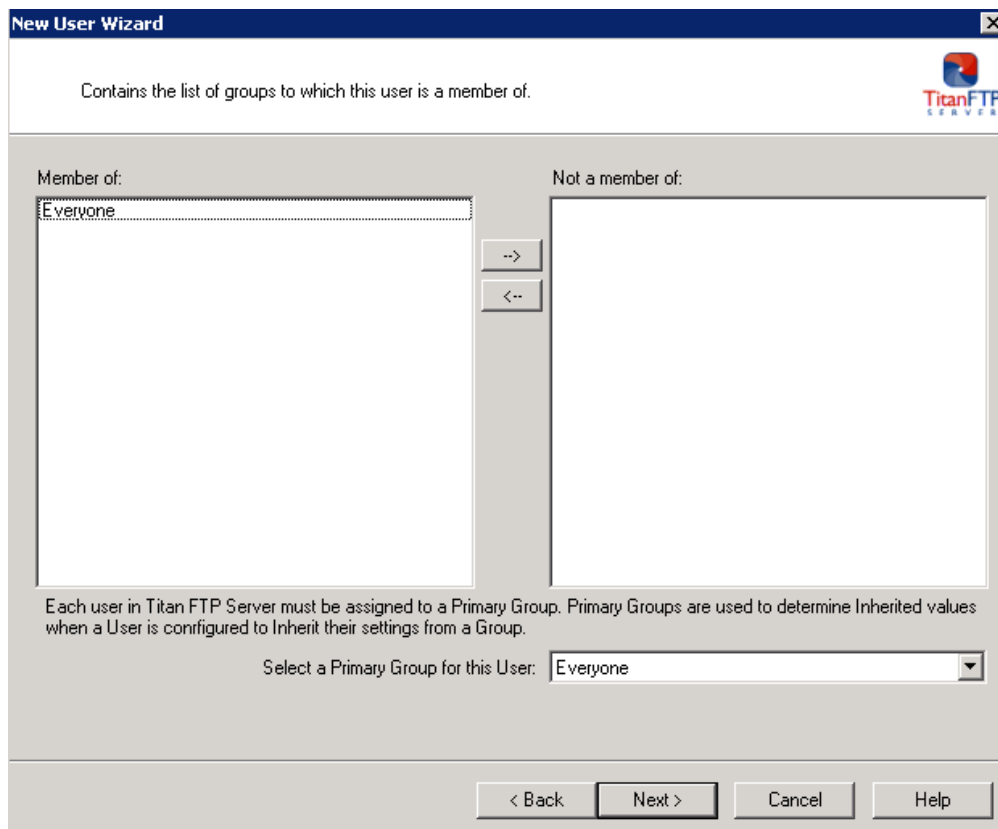
Force Complex Password Rules: When enabled, this feature will require users to use a password with a minimum of 8 characters.

Password: Specify the password.

Confirm Password: Retype/confirm the password.

Email Address: The email address will default to username@server instance name. The address may need to be manually entered to reflect the correct email account.

Step 2



New User Wizard

Contains the list of groups to which this user is a member of.

Member of:

Everyone

Not a member of:

-->

<--

Each user in Titan FTP Server must be assigned to a Primary Group. Primary Groups are used to determine Inherited values when a User is configured to Inherit their settings from a Group.

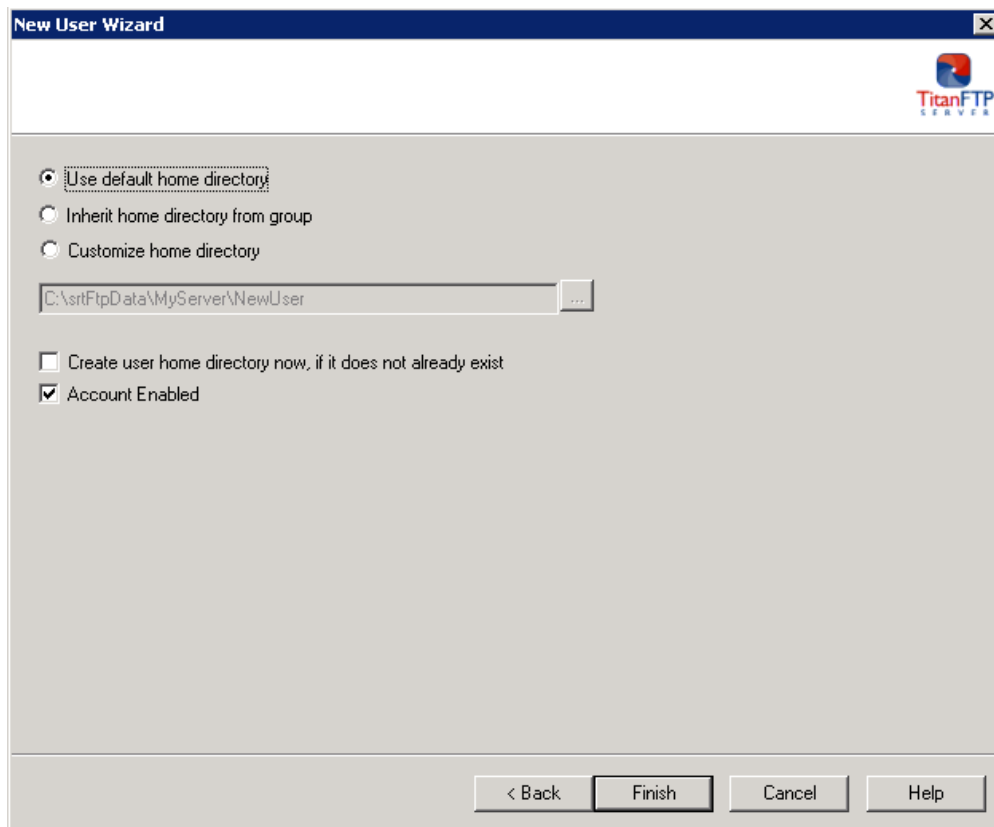
Select a Primary Group for this User: Everyone

< Back Next > Cancel Help

Members of: Lists the groups this user is a part of. To add groups, select a group in the Not a member of list and use the arrows to shunt the group back and forth until the member is a part of the appropriate groups. Click Apply when you have completed your changes.

Not a member of: Lists all groups this member is not currently a member of. To add members to a group, select a group from the list and use the arrow buttons to shunt the user to the Members list. Click Apply when you have completed your changes.

Step 3



The screenshot shows the 'New User Wizard' dialog box from the TitanFTP Server application. The window has a title bar with the text 'New User Wizard' and a close button. In the top right corner, there is a logo for 'TitanFTP SERVER'. The main area of the dialog contains three radio button options for home directory settings: 'Use default home directory' (which is selected), 'Inherit home directory from group', and 'Customize home directory'. Below these options is a text field containing the path 'C:\srtFtpData\MyServer\NewUser' and a browse button ('...'). At the bottom of the main area, there are two checkboxes: 'Create user home directory now, if it does not already exist' (unchecked) and 'Account Enabled' (checked). The bottom of the dialog features four buttons: '< Back', 'Finish' (highlighted with a black border), 'Cancel', and 'Help'.

Directory Options:

Use default home directory: The default home directory will be a subdirectory of the default server directory. In this case, the server data folder is C:\srtMFTData\newserver and each user's home directory will be placed under that folder.

Inherit home directory from group: Use this setting if the user is a member of a group from which you want him to inherit his user directory. The user must be added to the desired group and the group must be set as his primary group in order for inheritance to work.

Customize home directory: Use this setting to define the user's home directory to be outside the default folder structure (either locally on the same server, or as a UNC pointing to a network resource).

Create user home directory now, if it does not already exist: This will create the folder you specify if it is not already created. This is particularly useful if you are creating a folder outside the default server directory structure.

Account Enabled: The user account is enabled by default, but the administrator can choose to create it in a disabled state.

New Group Wizard

A separate **New Group Wizard** window will appear to help you through the steps of creating a new Group for your server. This wizard should be simple to navigate, but here is some extra information on your initial configuration options.

Most of these settings can be changed after the group is created.

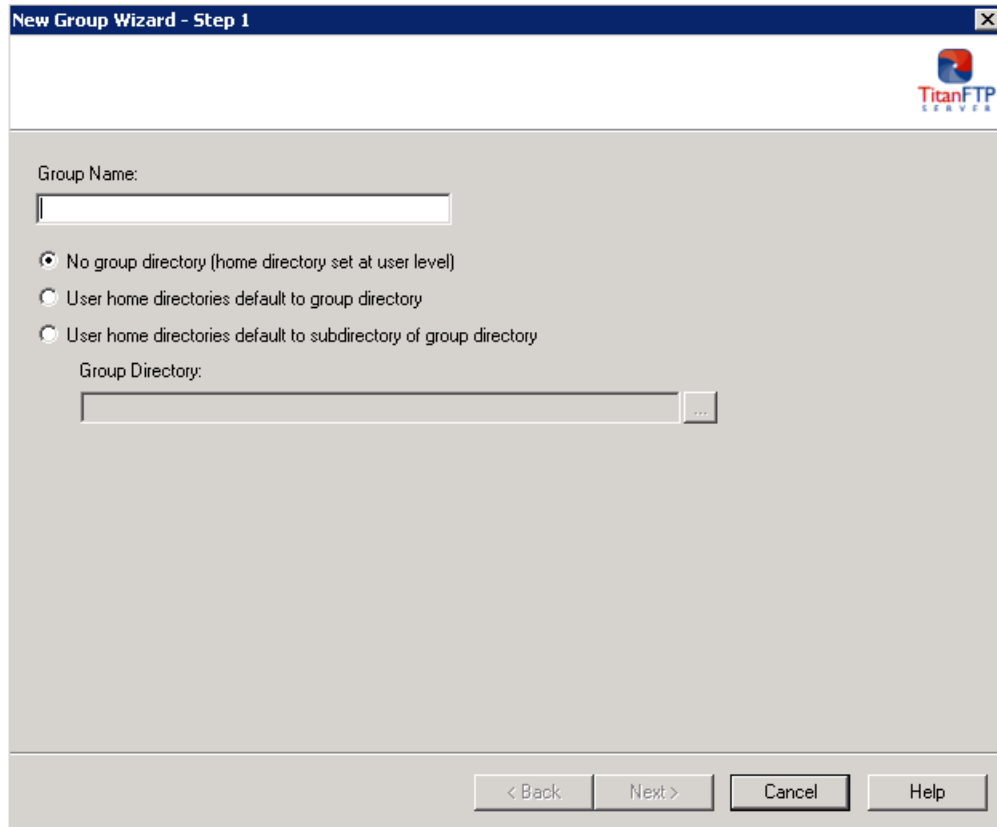
See our topic on the [Group General Tab](#).

Where is it?

Launch the New Group Wizard by navigating to Groups in your left-hand tree-pane, selecting the appropriate group, and clicking the New Group button on the Groups tab.

Wizard Steps

Step 1



New Group Wizard - Step 1

TitanFTP

Group Name:

☒ No group directory (home directory set at user level)

☐ User home directories default to group directory

☐ User home directories default to subdirectory of group directory

Group Directory:

...

< Back Next > Cancel Help

Group Name: Displays the Group Name. Use this text box to change the group name. You cannot change the group name for the Everyone group.

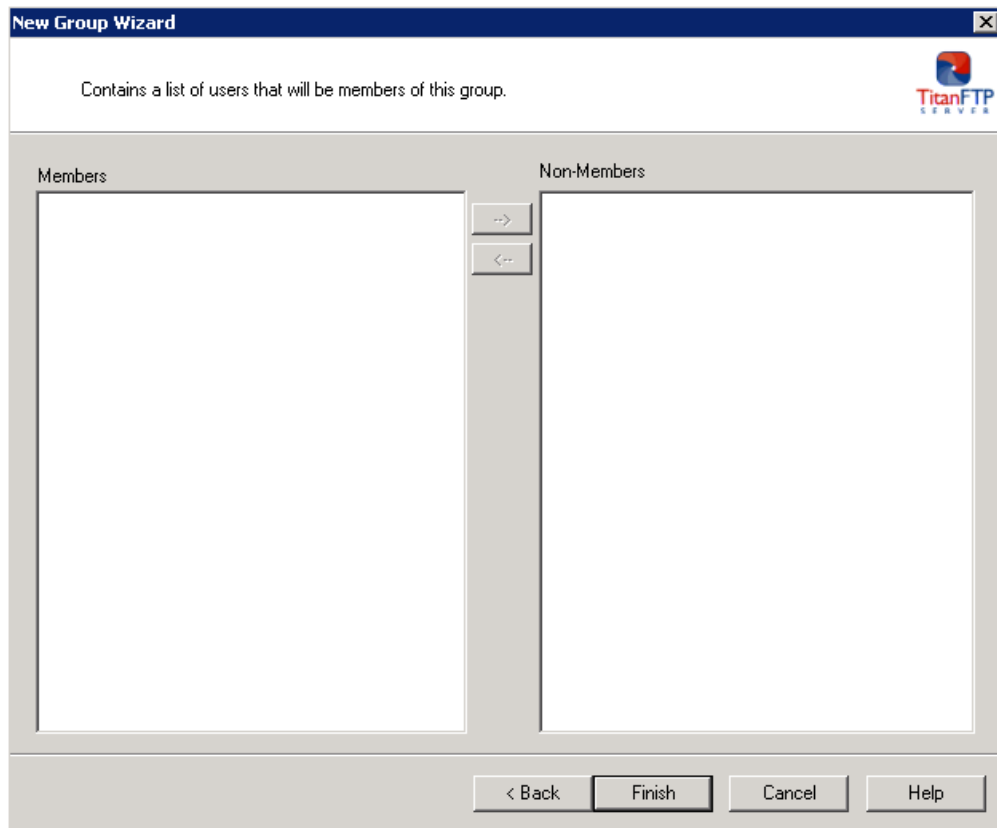
Group Home Directory: These options specify the kind of group home directory to be used. The Group home directory can be used to ensure that group members are organized according to Group settings, rather than having to set these values at the individual User level. Care must be taken to ensure that users that are members of multiple groups have the correct home directory.

- **No group directory (home directory set at user level):** This group does not have a home directory. Home directories will default to the Server home directory. The home directory can be changed on an individual user level.
- **User home directories default to group directory:** Select this value to cause any users that are members of this group to use the Group Home Directory as their home directory.

- **User home directories default to subdirectory of group directory:** Select this value to cause any users that are members of this group to have their own subdirectory created under the Group Home Directory.

Group Directory: If the group is defined to have user home directories based on a group directory, this is where the base group directory will be set.

Step 2



Members of: Lists the groups this user is a part of. To add groups, select a group in the Not a member of list and use the arrows to shunt the group back and forth until the member is a part of the appropriate groups. Click Apply when you have completed your changes.

Not a member of: Lists all groups this member is not currently a member of. To add members to a group, select a group from the list and use the arrow buttons to shunt the user to the Members list. Click Apply when you have completed your changes.