TOC

Contents

Overview

Welcome to Titan FTP Server NextGen!

Titan FTP Server provides you with unparalleled features for flexibility and security. NextGen optimizes your experience through new capabilities designed with security and ease-of-use in mind. Please see the Release Notes, provided during your product installation, for details of the newest NextGen features and support.

We've created several useful aides to help you with installing, navigating, and getting to know your product:

- **SRT Quick Reference Guide:** Who to contact, for what… this quick guide points you in the right direction to get what you need.
- **User Guide:** This user guide provides detailed instructions for navigating and using the system, including an end-to-end walk-through of how to use feature capabilities.
- **Upgrading from Titan FTP Server or Legacy ?** Refer to "Upgrade to NextGen from Legacy " on page 14.

Stay "In the Know"

The SRT newsletter keeps you in the know of updates, including upcoming webinars, to take a deeper dive into the full capabilities of your software and to get your questions answered by the Support Team. We're available to help answer any questions you have.

Please note that your quick reference guide includes a detailed list of contacts and portal access links.

Supported Operating Systems

- Windows Server 2016 or later, all 64-bit editions (32-bit is not supported).
- Windows 10 Professional TH1 1507 or later, 64-bit (32-bit is not supported).
- The Web-based Admin Console and the WebUI require the latest versions of Microsoft Edge, Google Chrome, or Mozilla Firefox. Microsoft Internet Explorer (IE) is not supported.

Minimum Hardware Requirements

- 2 GHz Pentium class processor or better is required, multi-core (4-core or more) recommended.
- 8GB RAM is required, 16GB or more is recommended for production systems.
- SVGA (1024x768) resolution display or better is required to run the Administration Console program.

Minimum Software Requirements

- Microsoft .NET Core is required and is included in the installer.
- Microsoft SQL Server/SQL Server Express 2019. SQL Express is included with the installer.
- Microsoft SQL Server Management Studio (SSMS) is not required but recommended. SSMS is available on the Microsoft website.

Limitations

Titan FTP Server is a multi-threaded, dynamic server solution built for the Microsoft Windows operating system. While designed to handle an unlimited number of user connections and configurations, like all software they are limited by the resources of the underlying hardware; most notably, those limitations imposed by memory and the Windows networking subsystems.

Getting Started

Installation

- To install Titan FTP Server, first download it from the link provided in the email after purchase.
- Next, double-click on the **installation/set up file** and follow the installation wizard prompts.
- The installer checks if sufficient permissions are in place. Admin will be required.

Any missing dependencies are added during installation. An Installation Successfully Completed window displays after a successful install. Click **OK** to close the window. When the installation finishes, Titan FTP Server starts up automatically. If Titan FTP Server does not start automatically after installation, please restart Windows. The Welcome window displays. Click **OK** to exit the window and the login window will display.

Upgrade to NextGen from Legacy

If upgrading from a legacy version, you can install NextGen directly over any previous Titan FTP Server installations. Your original installation won't be modified, preserving all of your configuration information during the update. However, your legacy Titan's previous auto-start setting is disabled during NextGen installation to prevent server conflicts.

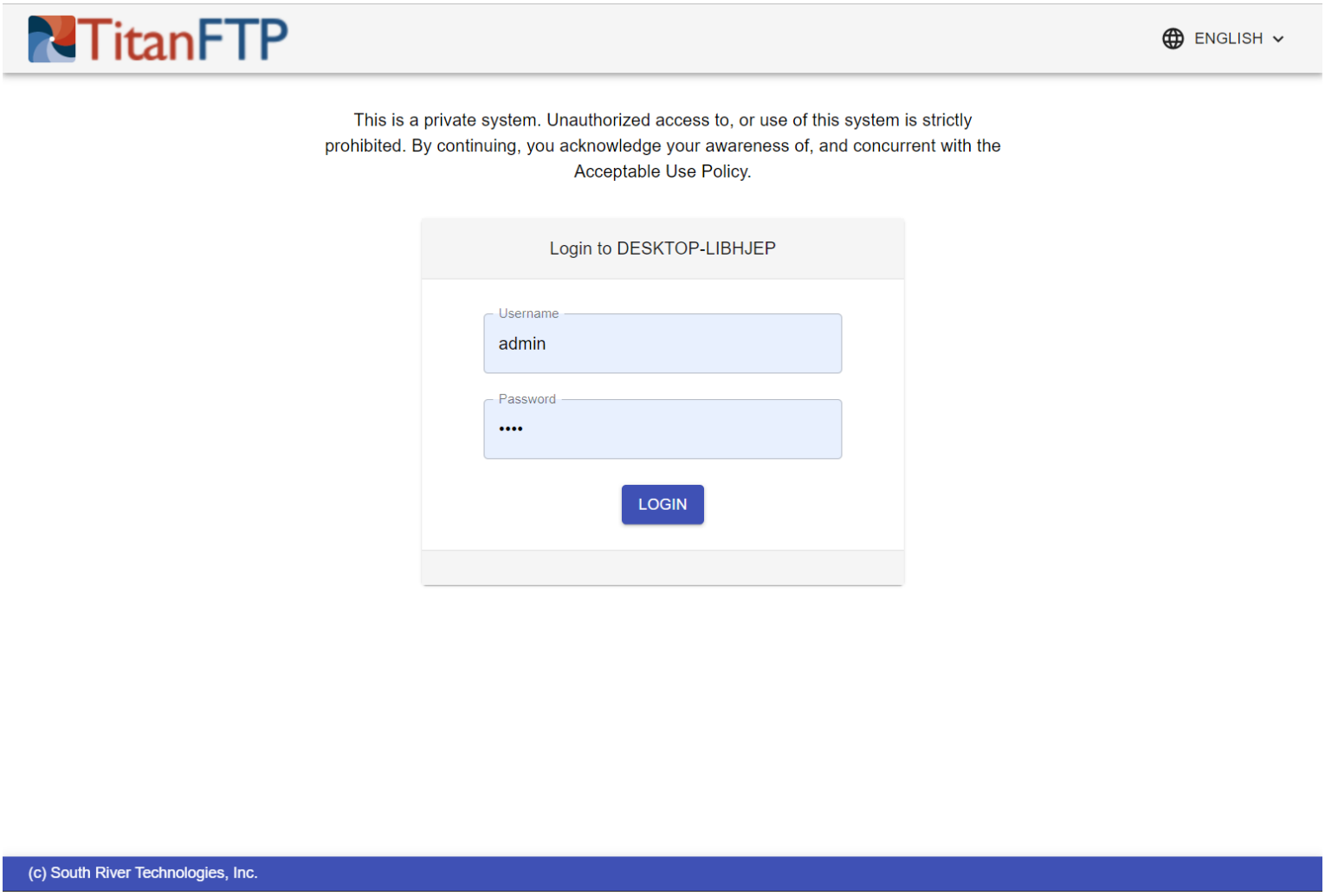
For full instructions on how to perform the upgrade please refer to this KB Article on our helpdesk https://helpdesk.southrivertech.com/

Titan FTP Server is now enabled.

To login, launch the software using the icon on your server desktop and you will receive a prompt to create a set of Admin credentials for the server during first setup. Choose a username and a strong password

and enter these at the login screen to create the initial Admin account. These are the master Admin credentials used to access and configure the server going forward.

Subsequent visits to the Admin login page will result in entering of the Username and Password that was configured at initial launch. Click **Login**. Titan's Administrator Console opens.



Administrator Console Interface

If this is your first visit to the Admin Console, you'll want to begin by activating a license and creating a new server.

Activating a Titan FTP Server License

1. Select the top level **Home** option in the Titan FTP Server Admin Interface.
2. Then, choose the **Product Info** option at the top right.
3. In the Licenses area below, click the **plus** icon to Add a License.
4. Enter your valid Registration/License Code that came with your purchase and click **Add**.
5. Once added, you can click the **plus** icon to the left of the license if you ever want to deactivate this license, or the **trash bin** icon if you want to delete this license.

From the **Product Info** tab, you can choose **Check for Update** to look for any newer versions of Titan FTP Server that may be available by clicking on the **circular arrow** icon in the Product area. Here, you can view the latest Release Notes and download any existing update and then install on the server to update to the most recent version available.

Note: From this same Home tab, you can:

- Configure (or Edit) Local Domain information, such as the Domain Name, Data and Log directory locations, Local Admin Certificate, as well as the IP/URL and Port Number for connection, in addition to enabling Remote Administration of the server.
    - **Enable Remote Admin:** When editing the Domain information, you can select the option to enable **Remote Admin**, which allows for Administration of the server from a remote system using a browser to connect and configure the server. Select the **IP/URL** and **Port Number** of interest, ensure this port is open on any needed firewalls, and then connection remotely is possible.

- **Enable Remote Domain**: On the same page, you can also Configure (or Edit) Remote Domain information, if wanting to manage a remote domain from this Administrator. Provide the URL/Port and authentication information and name the Remote Domain to admin from this environment.
- **Manage Certificates**: Create, View, Import, Export, Update, and Delete certificates for use in your Titan FTP Server environment.
    - **Add a new certificate**: Select **New** to create an official TLS certificate, fill out the required fields, and choose a key size (larger is more secure and also more resource-intensive to utilize). On the second page, choose whether to self-sign the certificate or send to a CSR for signing.
    - **Import a certificate**: Select **Import** to browse and select a **certificate** of interest. If required, enter the Private Key password to finish the import.
    - **Export a certificate**: Select **Export** to the right of the desired certificate in the view to export an existing certificate. Select the **name** and **destination** for the file, as well as whether or not the Private Key should be exported. If so, enter a password for the Private Key.
    - **Update a certificate**: Select **Update** to the right of the desired certificate in the view to browse your system for an updated version of an existing certificate. This is most likely to be used in cases where the certificate was due for renewal and you can simply update the certificate.
    - **Delete a certificate**: Select **Delete** to the right of the desired certificate in the view to delete the certificate from your server environment. This will remove the certificate entirely.

Creating a Server

1. In the Admin Console Interface, click on the **Local Domain** tab (named after the Domain name you provided for the server system).
2. In the Servers area, click on the **plus** icon to begin creating a new server.
3. On the first screen of the wizard, select **New standalone or primary cluster server** and **Next**.
    a. If setting up a cluster of Titan FTP Server to allow for high availability and failover, please see "High Availability and Clustering" on page 59 for more information and details. Click **Next**.

4. Select which type of **database** you prefer to use for the installation. The default recommendation is MS SQL Server. SQL Server Express ships with the installation of Titan FTP Server 2019. IF you have an existing SQL Server database that you would like to use, you can configure to connect to your SQL Server. If you do not have an existing SQL Server database, Titan FTP Server will use a newly created MS SQL Server database. When finished, click **Next**.
    a. You can choose whether to use **Windows Integrated Authentication** or **SQL Server Security**, as appropriate, based on your existing setup or newly created database.
    b. Use the **Test Connection** feature to verify the entered information is correct and Titan FTP Server is able to communicate with an authenticate to the desired database.
5. Choose a name for your Server and provide a helpful Description for its use, if desired.
6. Define any preferred locations for the data and log folders for the server, and whether the server should automatically start whenever the Server Operating System starts. Click **Next**.
    a. If desired, choose to **Manually Configure Directory Locations**. This will create an additional configuration tab that will allow specification of all additional relevant directories used within Titan FTP Server, including: User Data, Temp Data, Database, Backups, Reports, QuickSend Data, and AntiVirus/Quarantine.
7. Define which **Services and Protocols** will be available for use for the Titan FTP Server. Options include FTP, FTPS, SSH/SFTP, and WebUI/HTTP.
    a. These options can be left disabled at time of creation of the server and can be enabled at any time in the future from the Services tab within the server you've created.
8. If **FTP** is enabled, a configuration page will prompt you to select an **IP Address** and **Port Number** to use for communications over FTP. Additionally, if the server is behind a router/firewall, enable the available option and enter the Wireless Access Point (WAP) IP Address for the router/firewall so that Titan FTP Server can communicate successfully over FTP. Click **Next**.
    a. There is an option to choose whether or not to use the Internal IP in any PASV Response to Local Client connections.

9. If **FTPS** is enabled, a configuration page will prompt you to select whether to allow Explicit and/or Implicit FTPS connections over SSL/TLS. When finished with all options, click **Next**.
    a. If Implicit over SSL/TLS is enabled, an additional configuration option will become available to select an **IP Address** and **Port Number** to use for Implicit FTPS communications to/from Titan FTP Server.
    b. Select the **forms** of TLS preferred for support. Options include: TLS 1.1, TLS 1.2, and TLS 1.3.
    c. If wanting to force FTPS connections to use a Certificate to authenticate, enable the option for **Require trusted certificates**. A "Certificate" is another form of authentication that differs from username/password. More information on Certificate Authentication can be found in the "Managing Certificates" on page 78 section.
10. If **SFTP** is enabled, a configuration page will prompt to select which **version** of SFTP to support/prefer, as well as an **IP Address** and **Port Number** to use for communications over SFTP. When finished with all options, click **Next**.
    a. The option to “Kick User on Invalid Host Key” allows for removing a user from attempting to authenticate if the user does not present a valid host key during an attempt to authenticate. A Host Key is used for Public Key Authentication (a form of authentication that differs from username/password). More information on Public Key Authentication can be found in the "SSH and SFTP Configuration " on page 80 section.
11. If **WebUI** is enabled, a configuration page will prompt to enable the Browser Interface (HTTP), as well as an IP Address and Port Number to use for communications over HTTP. This option is NOT required for an accessible browser interface, as the next configuration page is for HTTPS. When finished with all options, click **Next**.
12. If **WebUI** is enabled, a configuration page will prompt to enable the Secured Browser Interface (HTTPS), as well as an IP Address and Port Number to use for communications over HTTPS. When finished with all options, click **Next**.
    a. If wanting to force HTTPS connections to use a Certificate to authenticate, enable the option for **Require trusted certificates**. A Certificate is another form of authentication that differs

from username/password. More information on Certificate Authentication can be found in the"Managing Certificates" on page 78 section.

13. The final configuration page option will be for **Email Server Communications**. This menu allows for configuring an email server for Titan FTP Server to leverage when sending emails and SMS messages.
    a. Email use within Titan FTP Server relates to email notifications.
        A. You will need to enter the relevant credentials and information for Titan FTP Server to be able to connect to your SMTP (Email Server) environment for sending of emails and notifications.
    b. SMS configuration allows for notifications to users' and/or admins' contact numbers, as desired.
        A. You will need to enter the relevant credentials and information for Titan FTP Server to be able to connect to your SMS environment for sending of messages.

This process can be repeated to add additional servers of interest to your Titan FTP Server environment.

Local Domain Tab

From the Local Domain Tab, you can choose to **Manage Certificates** relevant to this Domain. See the Administrator Console Interface section above for any information about the available options.

From the Local Domain tab, you can select the **Edit** option to also Edit Domain information, such as the Domain Name, Data and Log directory locations, and Local Admin Certificate and IP/URL and Port Number for connection.

Enable Remote Admin: From the Local Domain tab, you can select the **Edit** option and enable Remote Admin, which allows for Administration of the server from a remote system using a browser to connect and configure the server. Select the **IP/URL** and **Port Number** of interest, ensure this port is open on any needed firewalls, and then connection remotely is possible.

In the Servers listing, you'll see any available servers. Their current status is indicated by the color of the icon next to the name of the server in the view. A green check box indicates that the server is running. A red X indicates that the server is currently stopped.

The Services that are in use will be listed to the right. If the Service is in dark blue, then the Service is active and running on the server at this time. Hovering the mouse over any Service will provide details on what IP/Port the Service is running.

Using the Menu to the far right of the Servers in the view, you can perform the following:

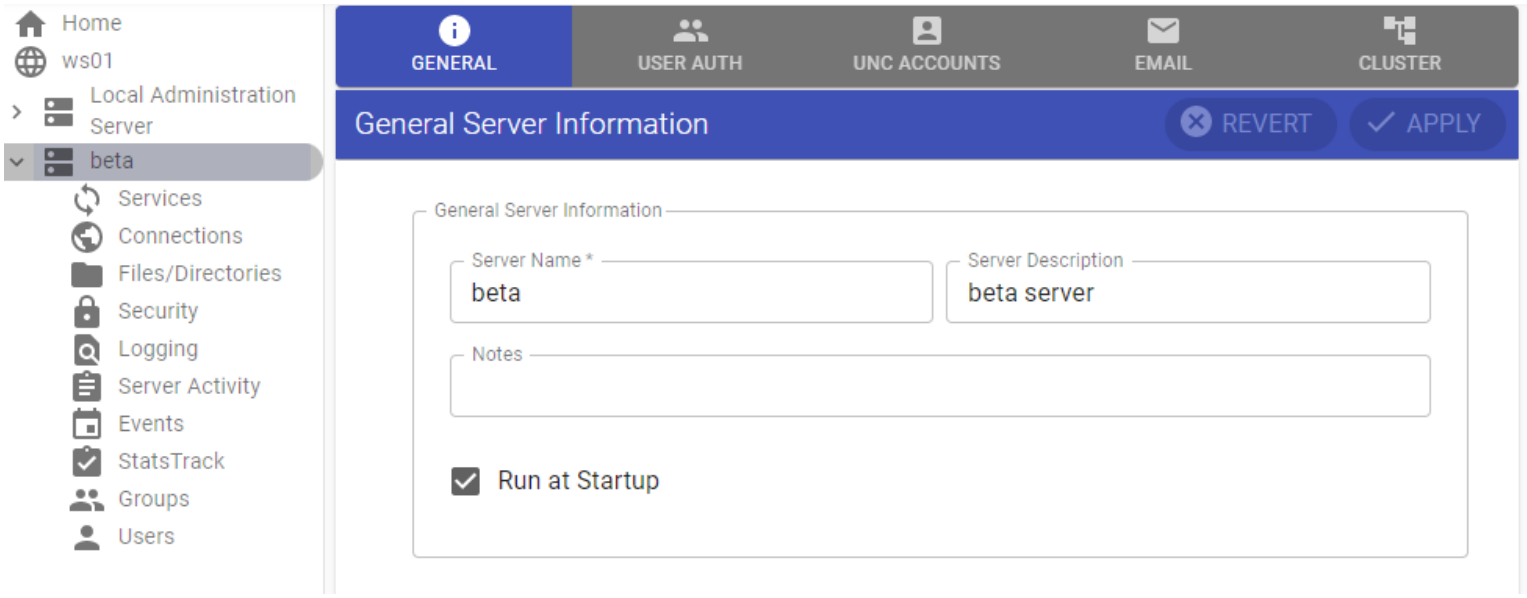
- **Starting a Server**: Use the **Start Server** option to start a server that is currently stopped.
- **Stopping a Server**: Use the **Stop Server** option to stop a server that is currently running.
- **Backing up a Server**: Use the **Backup Server** option to backup the server configuration. This backup will go to the Backups directory (specified in the Data Directories).
- **Restoring a Server**: Use the **Restore Server** option to restore a server from a backed up configuration. By default, existing backups are in the Backups directory (specified in the Data Directories).
- **Deleting a Server**: To remove a server entirely from your environment, go to the tab for your Local Domain (named as the Admin provided for the Domain or System). A list of current Servers will be visible in the Servers area of this page. Click the vertical **...** Actions menu to the right of the server of interest. Choose the **Delete** option, and then **Confirm Delete**.

WARNING: Deleting a Server will remove the server, configuration, and ability to connect to this environment entirely. Ensure this is the desired result before selecting to Confirm Delete.

Viewing and Updating a Server Configuration

From the main drop-down on the left side of the Admin Console, click on the **server** that you want to view or update. Expand the drop-down to see the full list of options available for your system.

These links help you to navigate, update, and manage your Titan FTP Server configurations.



Each link takes you to a distinct area of Titan FTP Server where you can do various tasks. A high-level look at where these different links will land you is below:

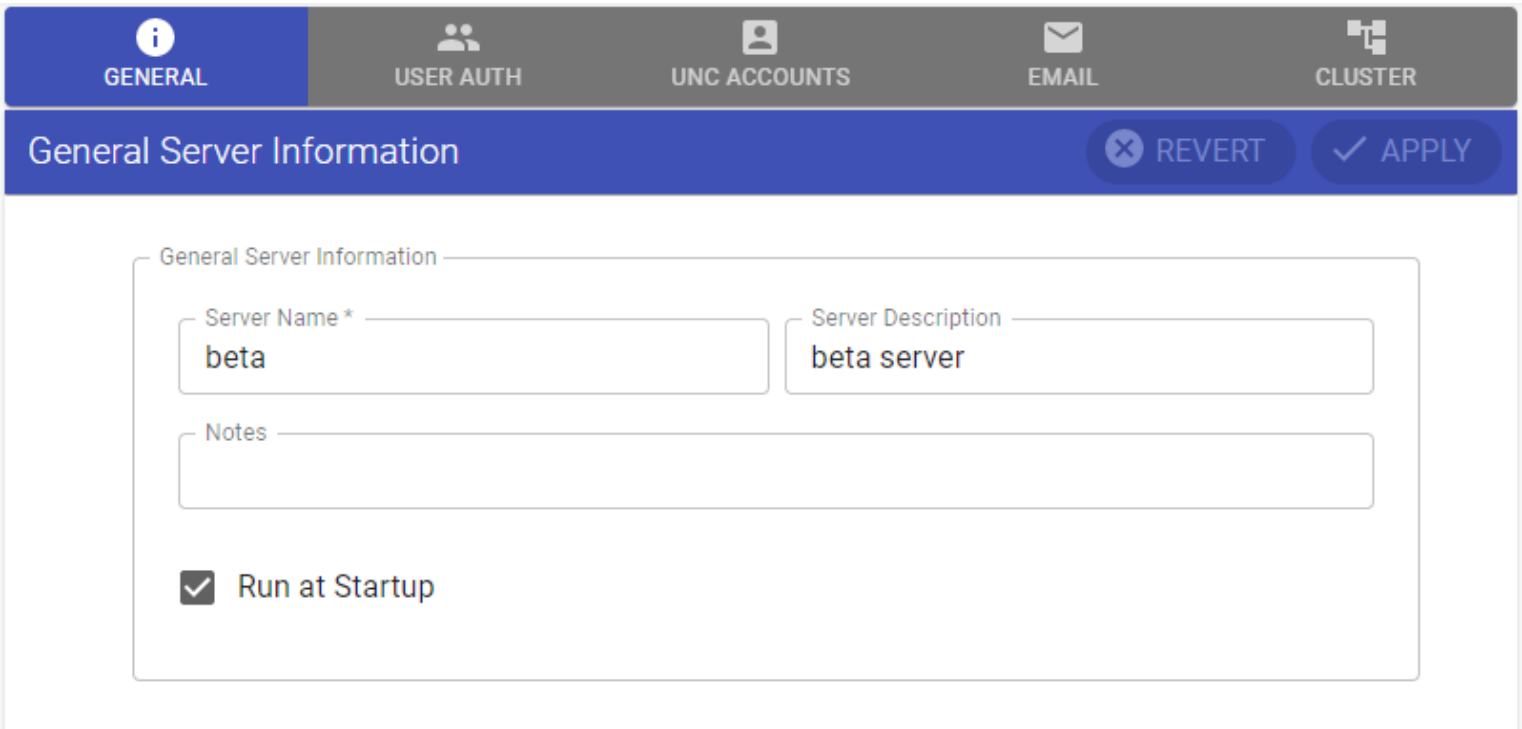
- **Top Navigation:** With the server and the desired page selected on the left navigation, the main window drills down into page-specific options that are labeled according to function (Services, Connections, etc.).
- **Language Preferences:** Titan FTP Server defaults to English. In the top-right corner of the window, click on the **arrow** in the English field to view and select other **language preferences**.
- **View and edit profile information:** Click the **profile** icon on the top far right of the window, and make updates to your profile, update your password, or sign out.
- **Help:** Get assistance from the Titan FTP Server Support.
- **Revert:** Remove recent updates without saving or applying them. This button allows you to revert to the most recently saved setting.
- **Apply:** Clicking this button applies changes to the current page. Click this after making changes to make sure they're updated.

Update Server Information

You can view and update basic server configuration on Titan FTP Server's General Server Information screen.

To get there, select the **server** in your left navigation. The General Server Information page displays your server's name, description, and any related notes.

This page is populated with information that was provided during the new setup wizard. If you skipped entering details or would need to update your information, you can do that on this page.

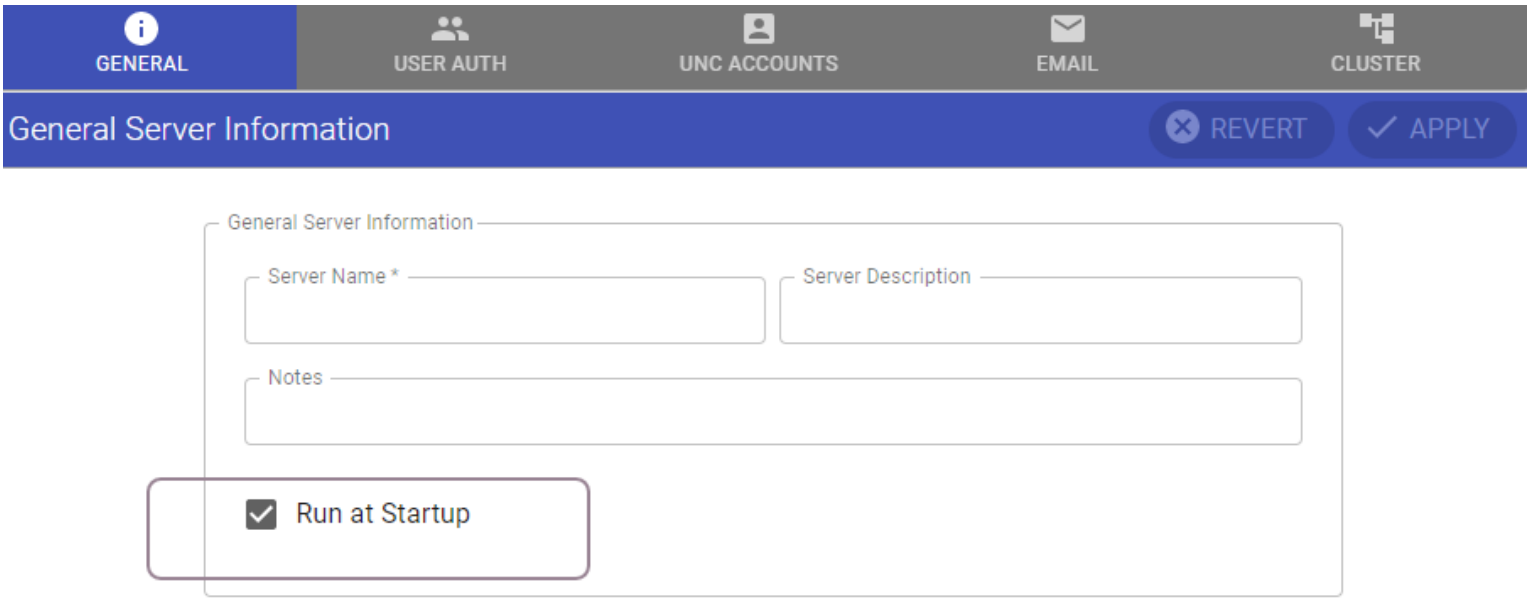


To update the Server Name, Server Description, or add Notes, type the update into the corresponding field and click **Apply** at the top of the window to save the change.

Run at Startup

Titan FTP Server's Run at Setup option allows you to enable the server to automatically start when Titan FTP Server starts by clicking the **Run at Startup** check box and then clicking **Apply**.

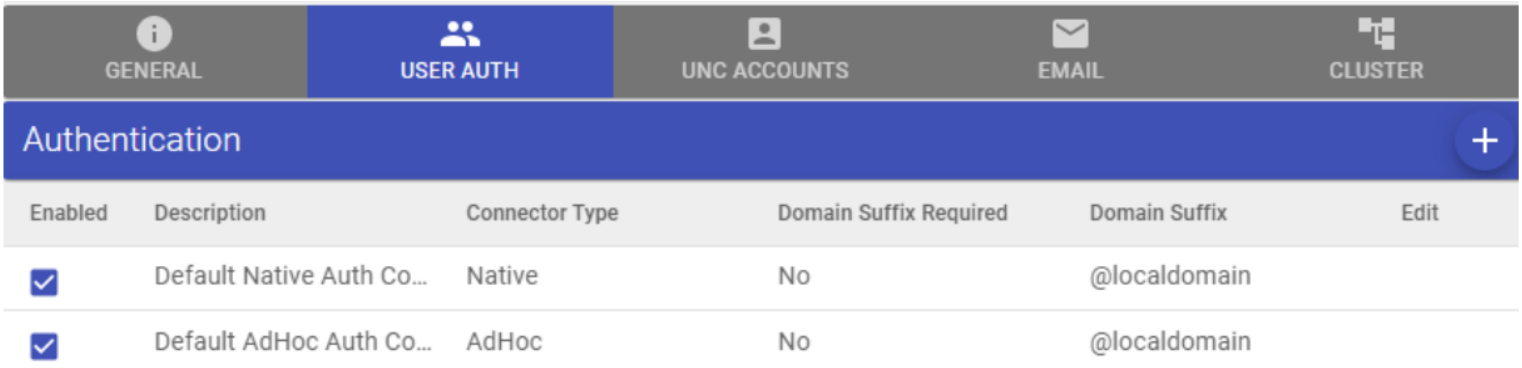
Alternatively, you can disable the server from starting automatically with Titan FTP Server by unchecking the **Run at Startup** check box and then clicking **Apply**.



Authenticate Users

In Titan FTP Server, users are authenticated with databases that display on the User Authentication page. To get there, navigate to the server of interest from the main navigation on the left side, and then click on **User Auth** in your top navigation.

Currently, enabled user authentication databases have a check box in the enabled column on the database listing. Any databases listed without a check box are not currently enabled.



Enable and Disable a User Authentication Database

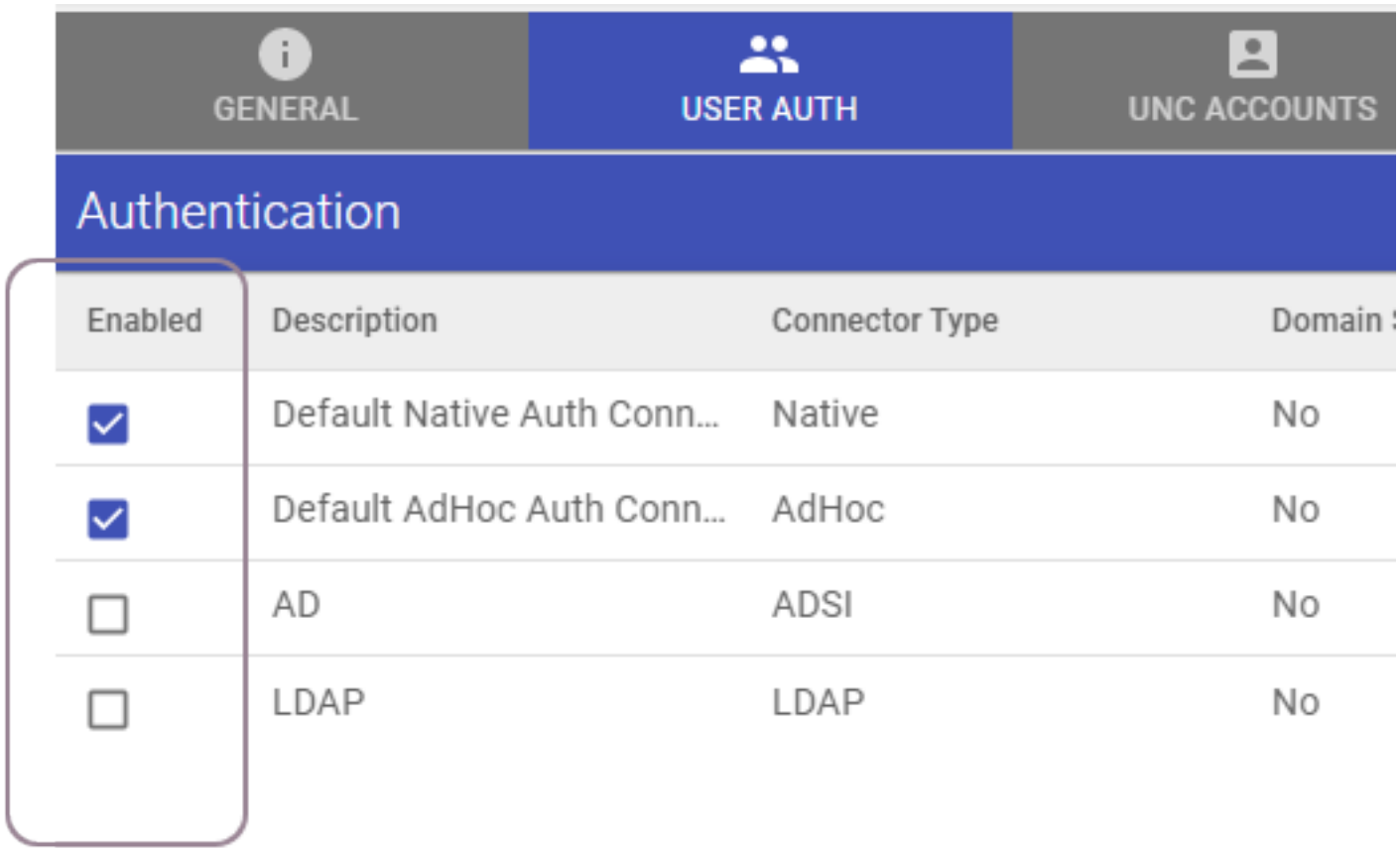
User Authentication Database options include:

- **Default Native Auth Connector:** Allows for the creation and authentication of user accounts using a built-in database support for authentication. This is the default method of authentication for accounts if an Active Directory, NT/SAM, or LDAP connection is not established and enabled. Native Auth allows for creating accounts and directories, setting permissions to directories, and managing users locally within the Titan FTP Server system.
- **Windows NT/SAM User Authentication:** Allows for Titan FTP Server to connect to an existing external authentication database that supports NT/SAM.
    - NT/SAM allows for enabling Windows authentication.

- **Standard LDAP (Lightweight Directory Access Protocol) User Authentication:** Allows for Titan FTP Server to connect to an existing external authentication database that supports LDAP.
    - LDAP provides support for connecting to, searching, and modifying Internet directories.
- **Windows Active Directory (Service Interfaces) or ADSI:** Allows for Titan FTP Server to connect to an existing external authentication database that leverages ADSI for user authentication.
    - ADSI allows a fully robust and feature-supportive option. ADSI allows for admins to automate things like adding users and groups, managing printers and resources, and setting permissions for network resources.

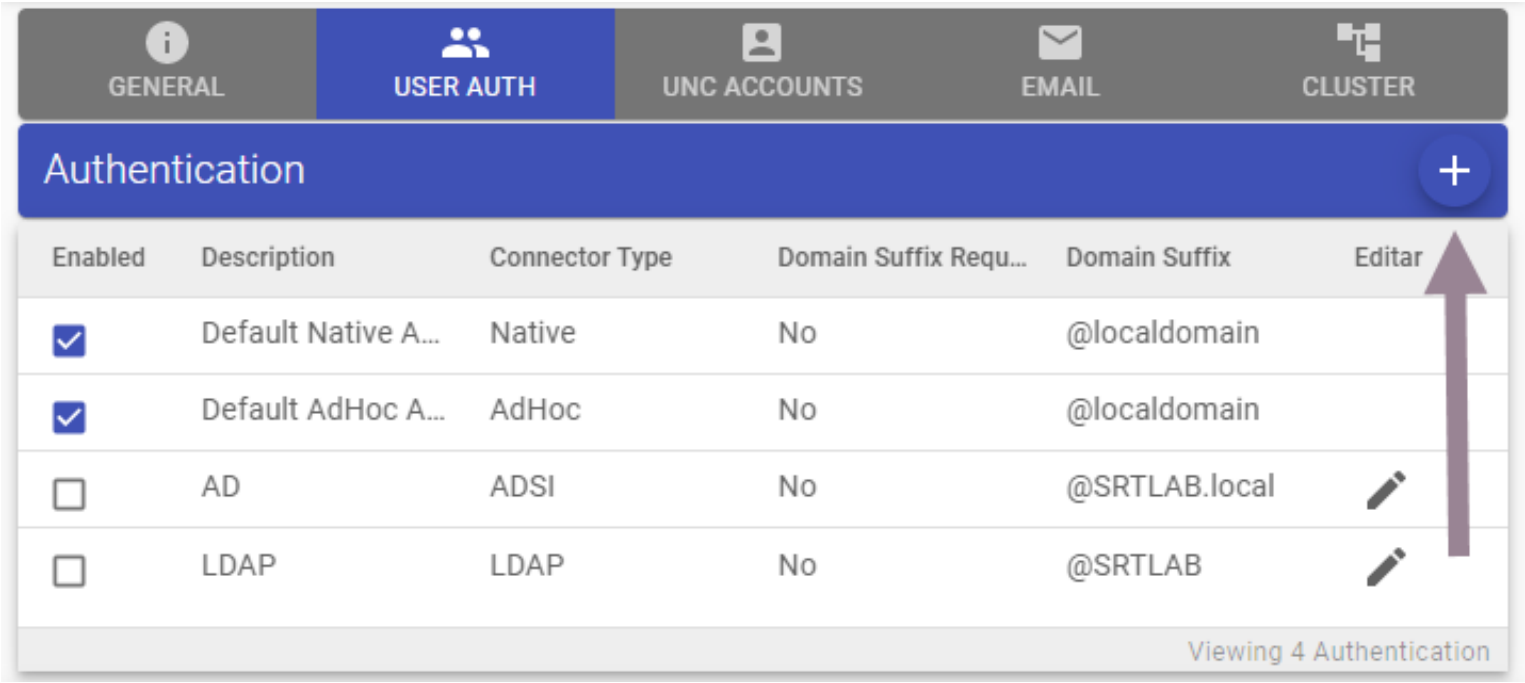
The check boxes in the Enabled column indicate that the database is enabled for authentication. To disable it, click the **check box** next to the database you want to disable.

In this example, the top two databases are enabled for user authentication. The two databases on the bottom are not enabled for user authentication.



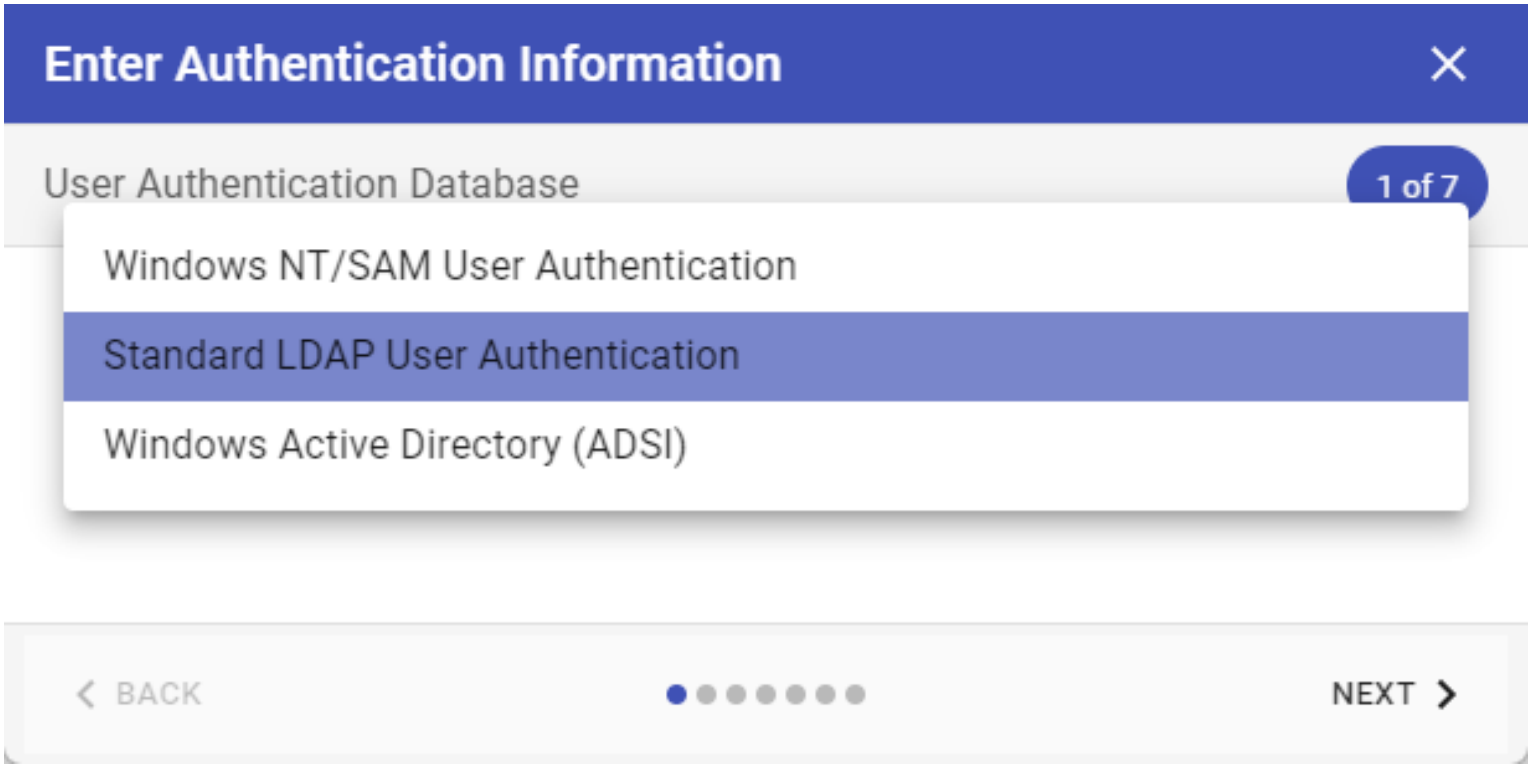
Add a User Authentication Database

To add a User Authentication Database, click the **plus** icon at the top right of the Authentication window.



On the Enter Authentication Information wizard, select the desired **database type** from the drop-down list. Titan FTP Server gives you these options to select from in addition to the two default options:

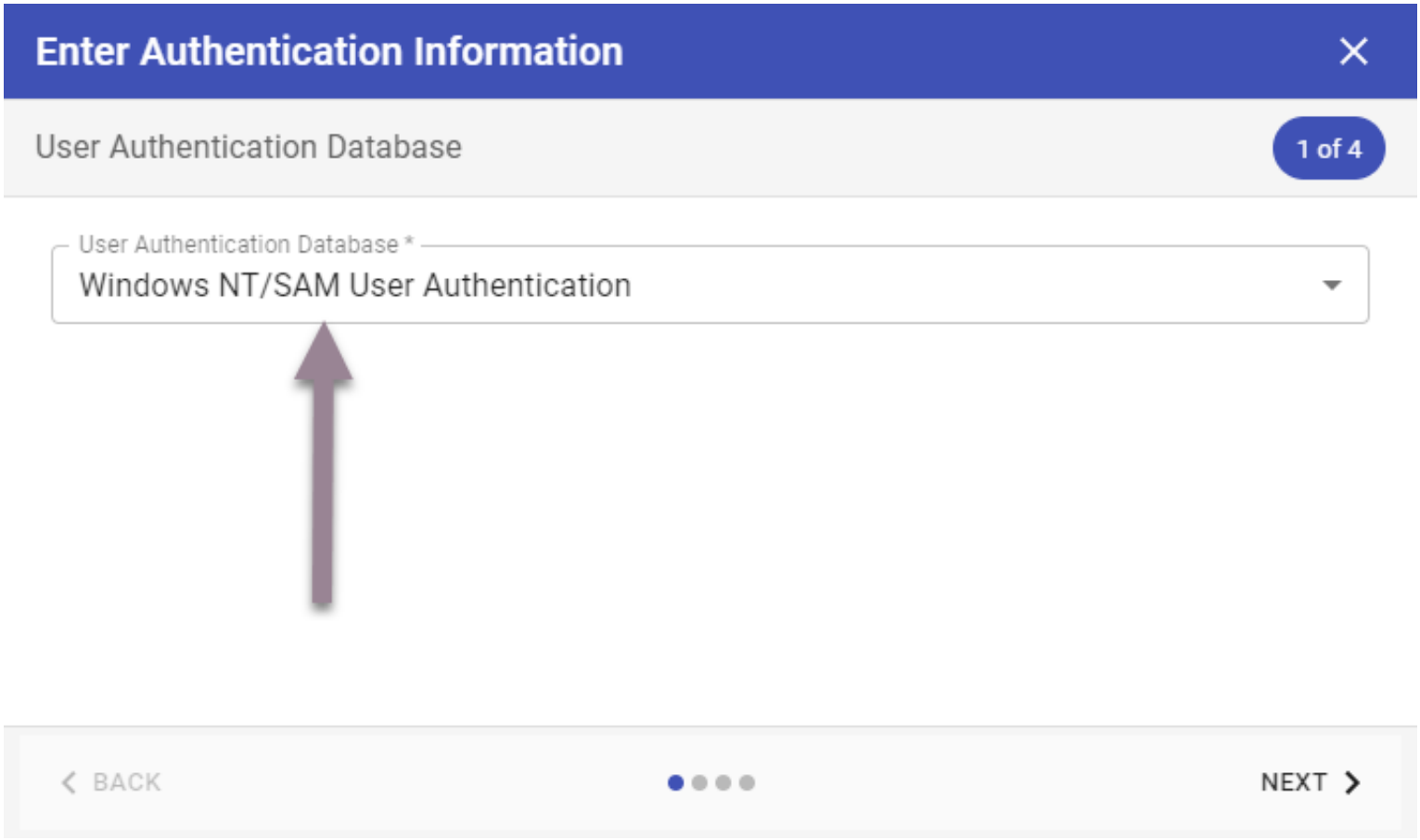
- Windows NT/SAM User Authentication
- Standard LDAP User Authentication
- Windows Active Directory (ADSI)



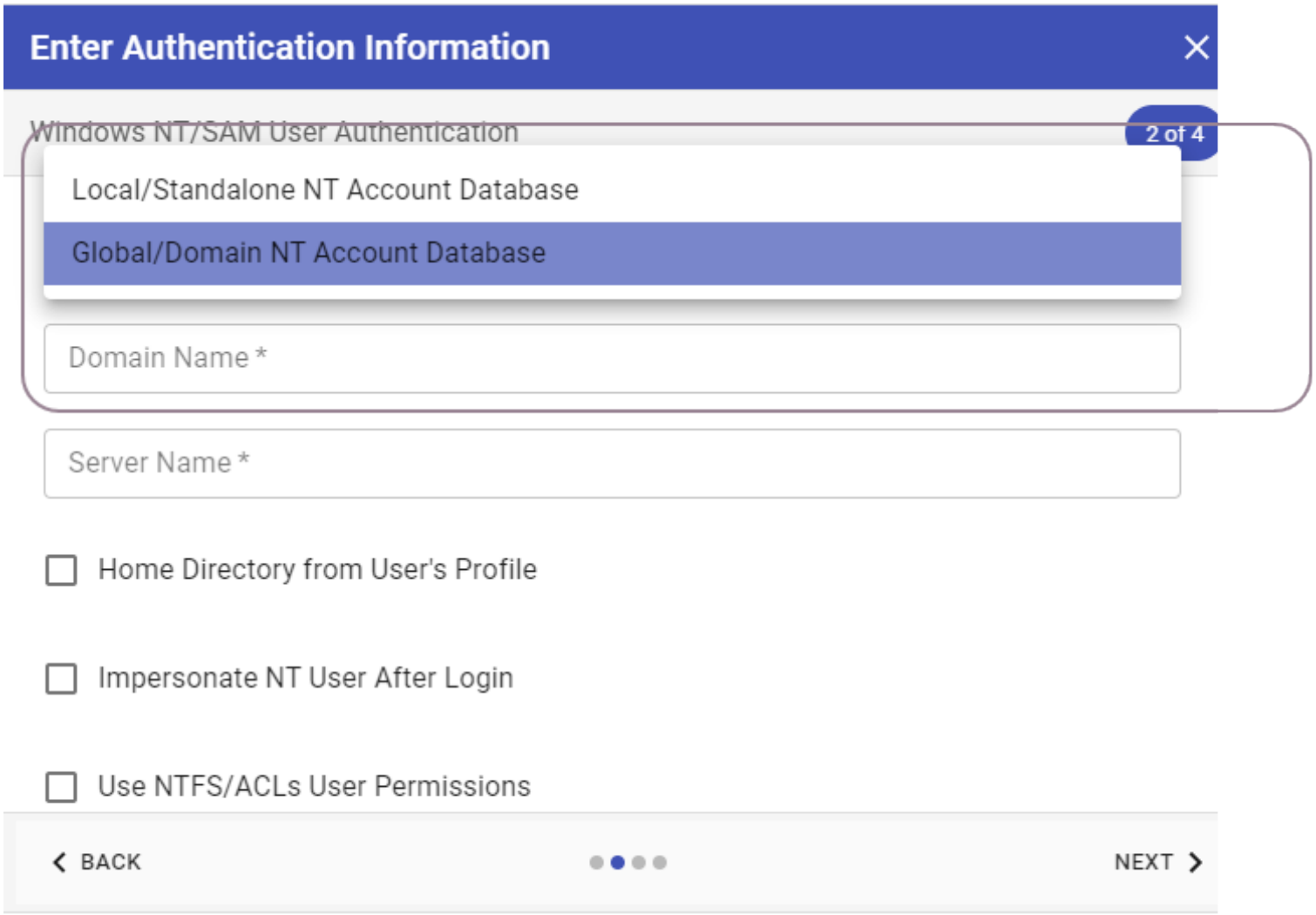
Add a Windows NT/SAM User Authentication Database

To add a Windows NT/SAM User Authentication Database, first navigate to the server in your left navigation. Next, click **User Auth** in your top navigation.

1. Click the **arrow** in the User Authentication Database field and select **Windows NT/SAM User Authentication** in the User Authentication Database field.
2. Then, click **Next** at the bottom right of the window.

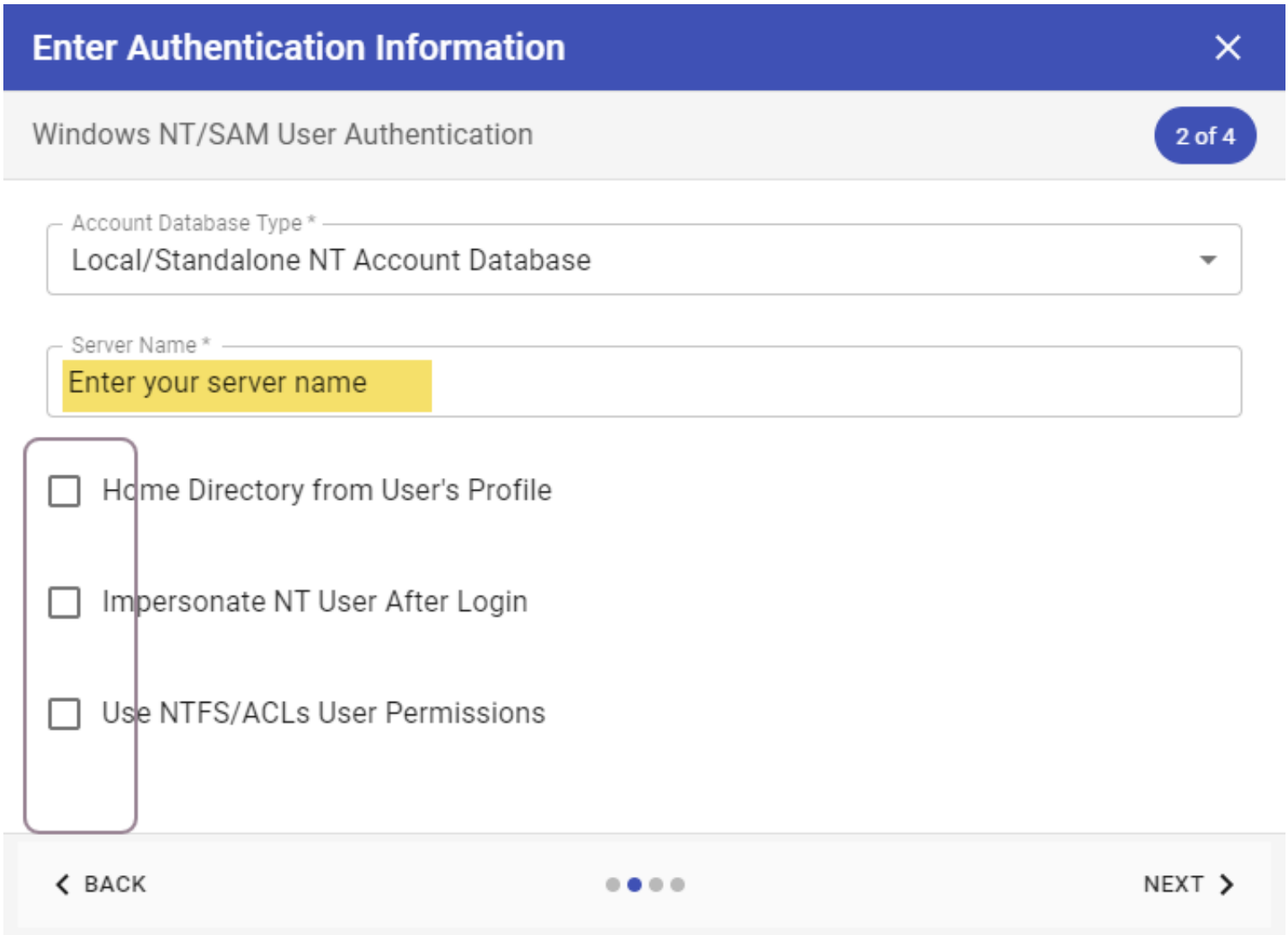


3. Select your **account database type** in the Account Database drop-down list and click **Next**.
4. On the Enter Authentication Information screen, select your **account database type** in the Account Database Type window from the following options:
    a. **Local/Standalone NT Account Database:** Often used with standalone servers and local user account databases (non-networked servers). No Global groups will be visible.
    b. **Global/Domain NT Account Database:** Often used in domain settings incorporating Active Directory as the authentication database.



5. Enter or select the **Domain Name** and **Server Name** and check the **check boxes** to make any applicable selections from the following options:
    a. **Home Directory from User's Profile:** This will have Titan FTP Server use the Home Directory that is associated with a User's Profile from the NT environment.
    b. **Impersonate NT User After Login:** Titan FTP Server will pass the credentials to Active Directory and use them to authenticate to network resources. This allows Titan FTP Server to leverage existing permissions for the user.

c. **Use NTFS/ACLs User Permissions:** Titan FTP Server will use existing Active Directory permissions for a specified resource. This allows Titan FTP Server to leverage existing Active Directory Access Control Entries for the resource.

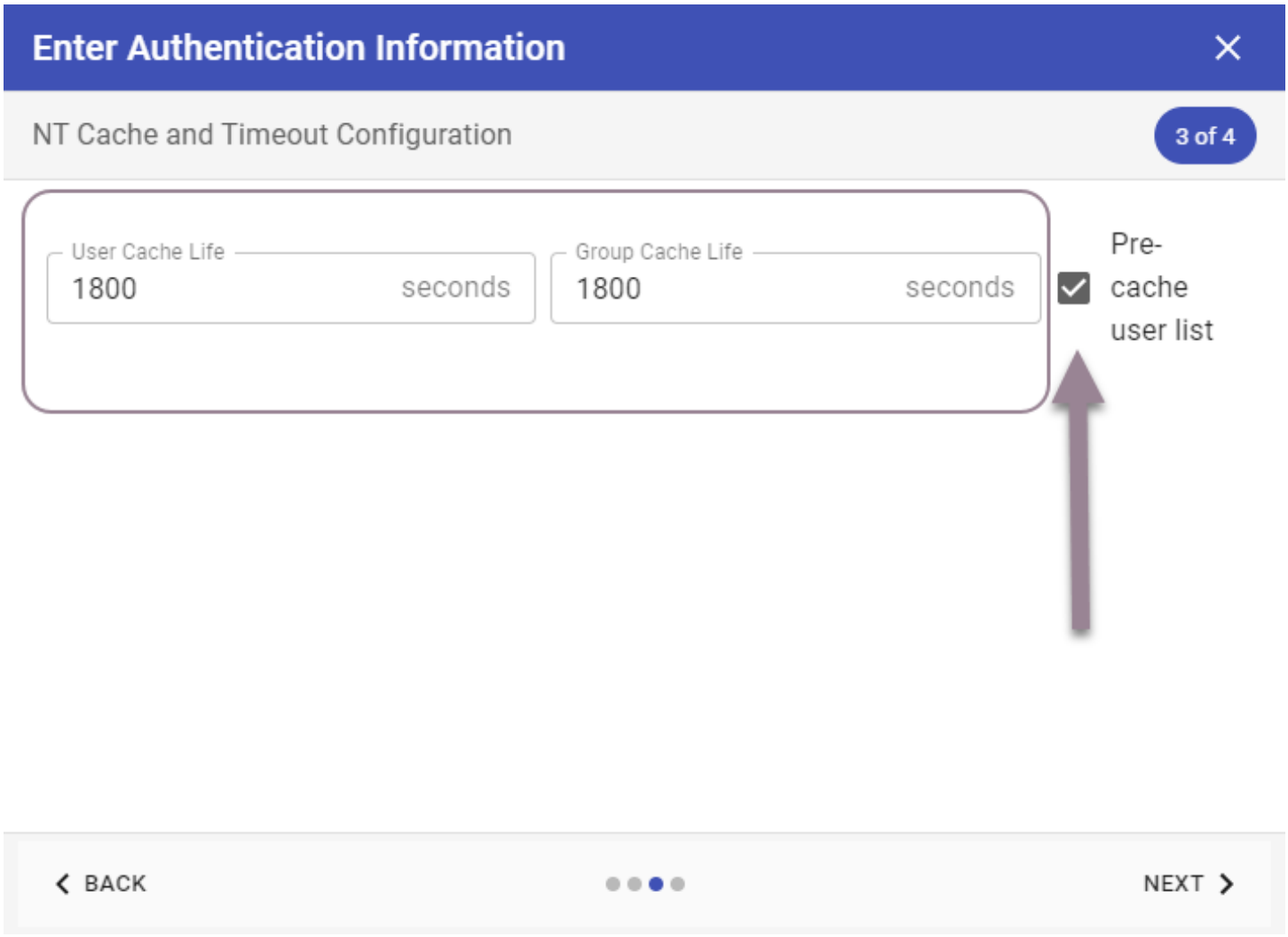


6. Select **Next**.
7. On the NT Cache and Timeout Configuration, view or update the user cache life (in seconds) and the group cache life (also in seconds). To enable the pre-cache user list, click the **check box** in the pre-cache user list field.

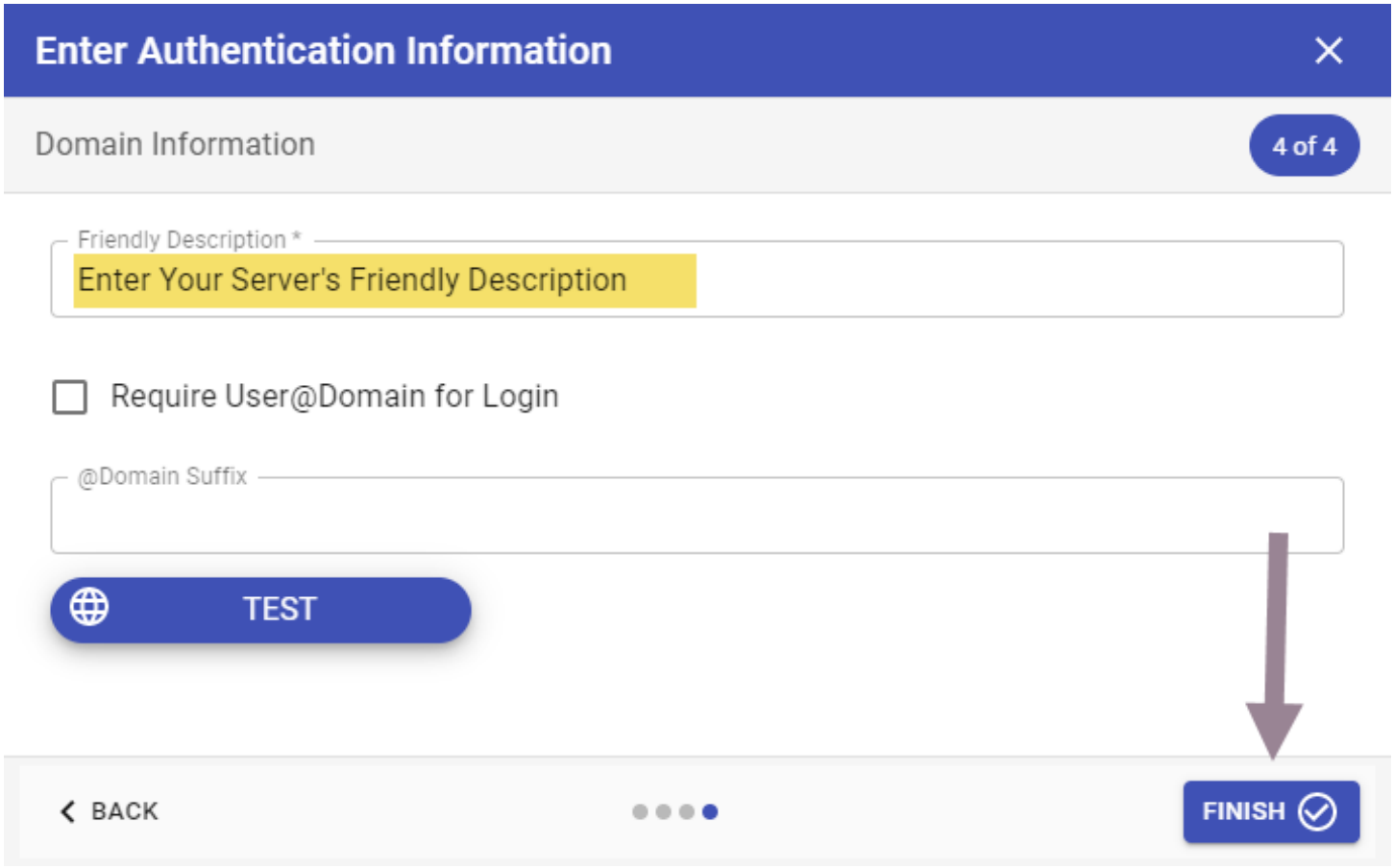
a. **User Cache Life:** The number of seconds the users list will be valid. The longer the period set, the longer the server will take to recognize added or deleted users.

b. **Group Cache Life:** The number of seconds the groups list will be valid. The longer the period set, the longer the server will take to recognize added or deleted groups.

c. **Pre-Cache User List:** Pre-Cache user list allows Titan FTP Server to download and store user information before first connect. This will especially assist the first connection made to the server, as this information would be polled and retrieved at that time.

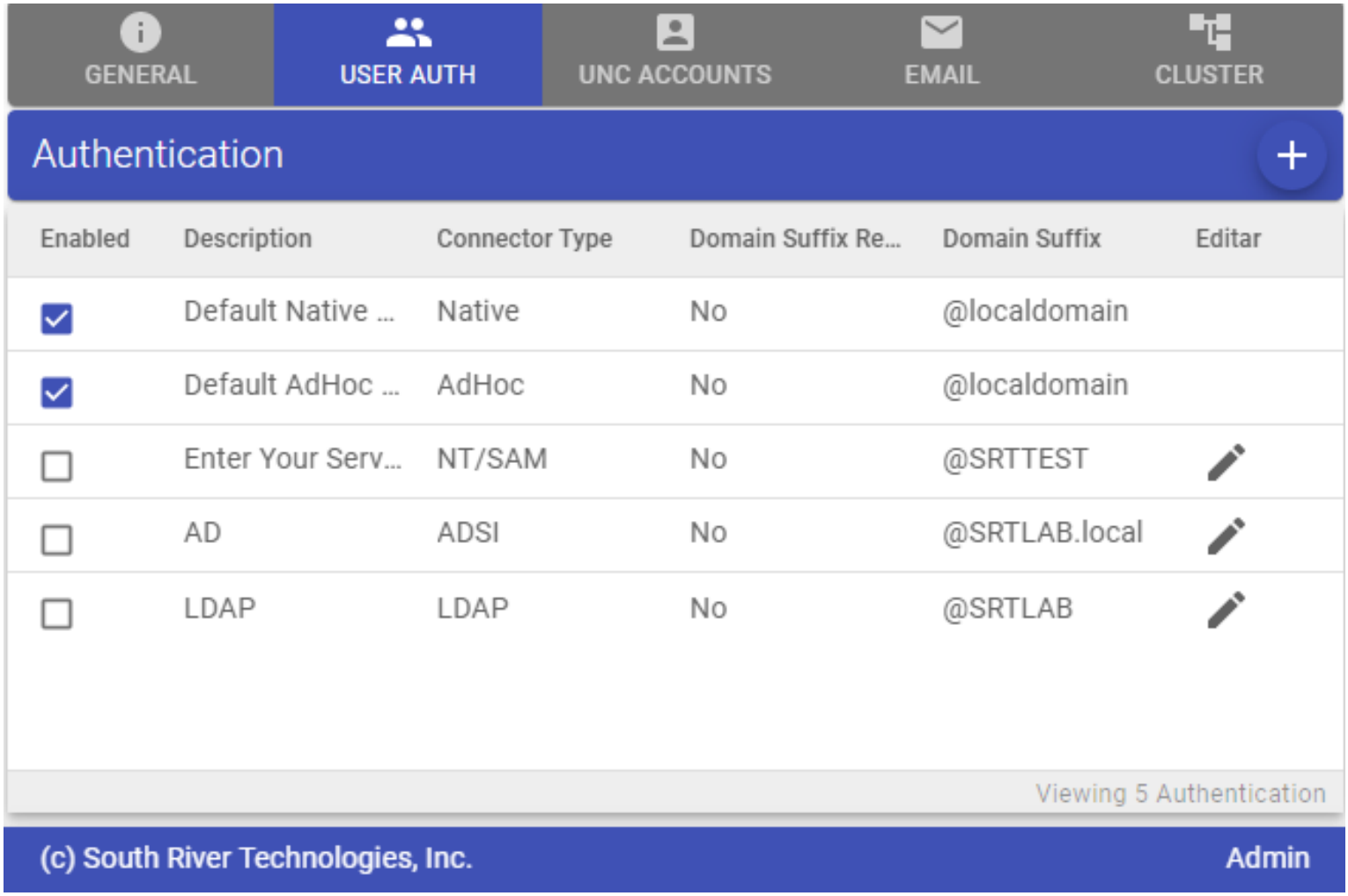


8. Select **Next**.
9. In the Domain Information window, enter a Friendly Description for your domain. Then, click **Finish**.



Titan FTP Server adds the database, and it displays on the User Authentication page along with any other existing authentication databases.

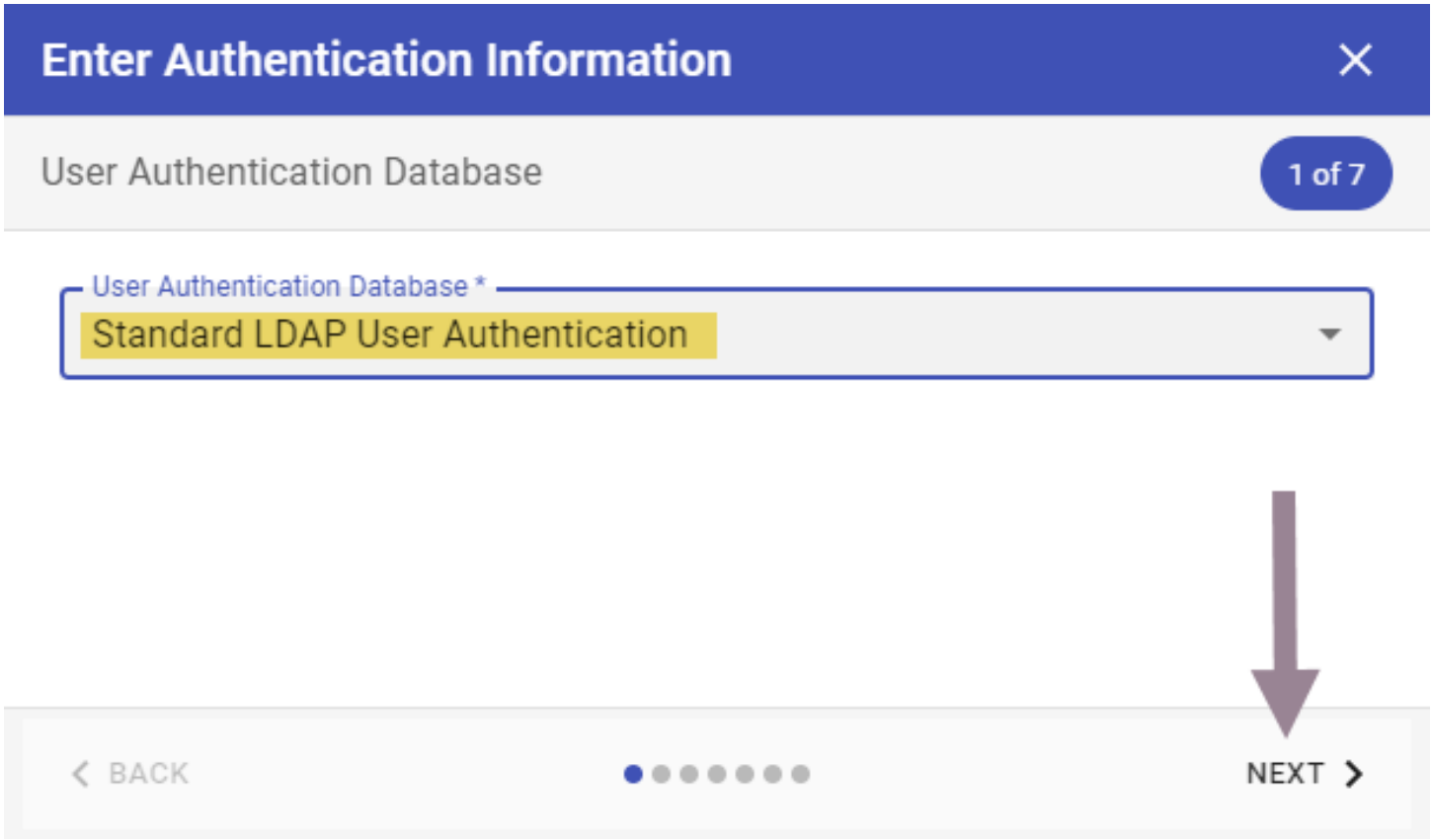
Note: Adding the authentication database does not automatically enable it. To enable the authentication database, find it on the User Authentication screen and click the **check box** in the Enabled column.



Add a Standard LDAP User Authentication

To add a Standard LDAP user authentication database, first navigate to the server in your left navigation. Next, click **User Auth** in your top navigation.

1. Click the **plus** icon in the top right of the window.
2. Select **Standard LDAP User Authentication** from the drop-down menu in the User Authentication Database field. Then, click **Next**.



3. The windows LDAP User Authentication screen displays. Complete the following on this window:
    a. Enter or select the **Domain Name** for your LDAP server.
    b. Enter the Server Name for your LDAP server.
    c. Click the **check box** if using a secure SSL/TLS connection and specify port.
    d. If desired, click the **check box** to have Titan FTP Server use the home directory listed in the user's profile.
    e. If desired, click the **check box** to hide any disabled user accounts from view.
    f. Enter the Administrative Username and Password to the LDAP server.
    g. Select the authentication **Bind** method. Choose from **Simple** or **Negotiate**.

A. Binds are used to authenticate clients (users, applications) to the server.

B. Simple results in the entry (user or application) being identified and then a proof of the identity (usually a password). Simple is only recommended when Secure SSL Connection is enabled, as the password is not further hidden.

   Negotiate allows for a variety of options for authentication, and this is decided between the authentication server and Titan FTP Server based on what is available. The proof of identity in this case is an encoded value, adding further security.

4. Click **Next**.
5. The LDAP Cache and Timeout Configuration window displays. Enter the following:
   a. **User Cache Life in seconds**: The number of seconds the users list will be valid. The longer the period set, the longer the server will take to recognize added or deleted users.
   b. **Group Cache Life in seconds**: The number of seconds the groups list will be valid. The longer the period set, the longer the server will take to recognize added or deleted groups.
   c. **Server Timeout in seconds**: The number of seconds of idle time before a timeout would occur or the server is considered unresponsive.
   d. To pre-cache users, click the **check box** in the **Pre-cache user list**: Pre-Cache user list allows Titan FTP Server to download and store user information before first connect. This will especially assist the first connection made to the server, as this information would be polled and retrieved at that time.

Enter Authentication Information

LDAP Cache and Timeout Configuration

3 of 7

User Cache Life: 1800 seconds

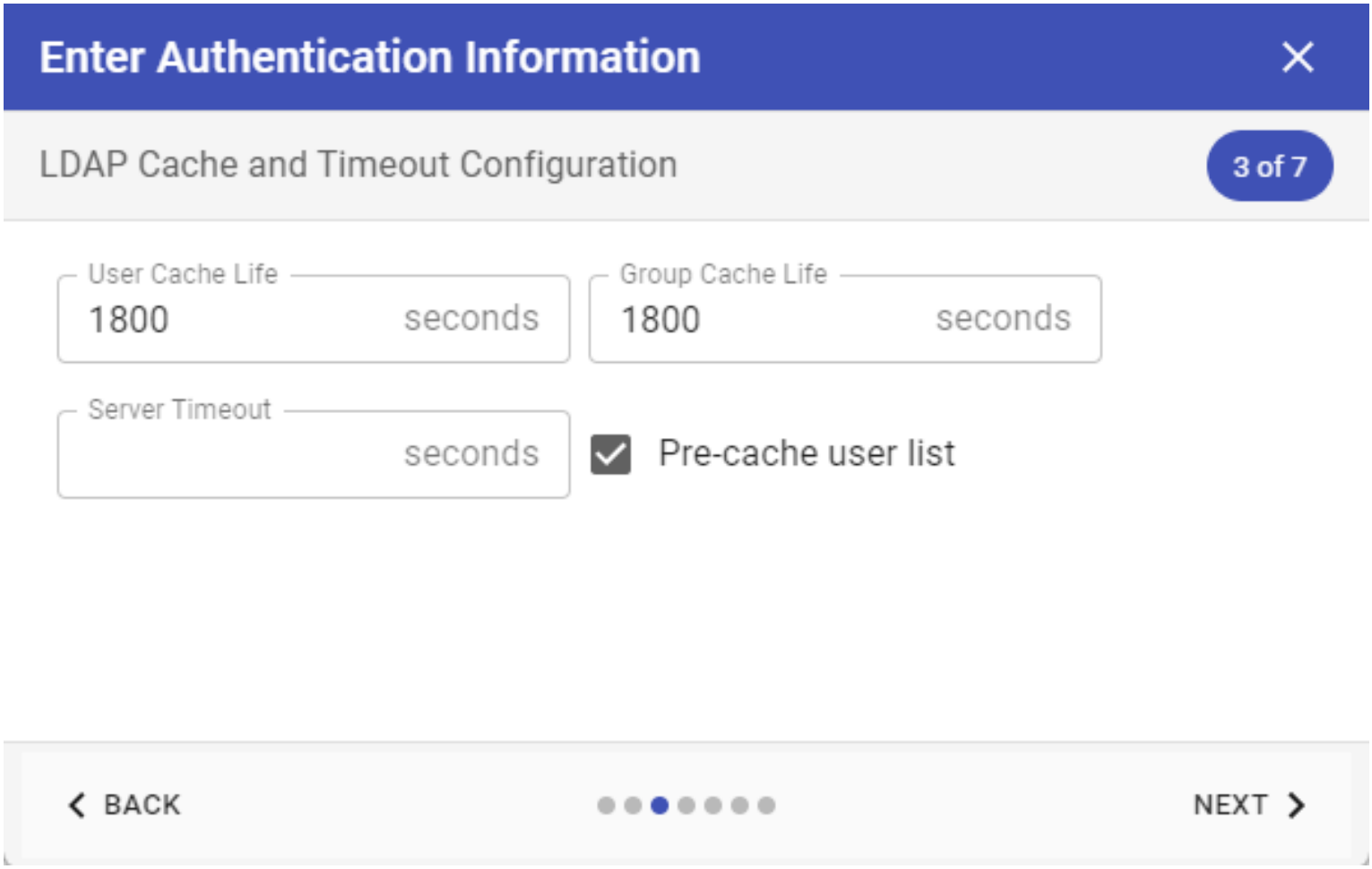
Group Cache Life: 1800 seconds

Server Timeout: seconds

Pre-cache user list

BACK

NEXT



5. View or update the fields on the LDAP User Authentication Configuration window and click **Next**.
    a. **Groups Base DN**: The level of the Active Directory tree from which your search will start searching for groups.
    b. **Group Category Filter:** Any categorical filter you may apply to narrow the search and results for the groups desired to be used in Titan FTP Server.
    c. **Group Class Filter:** Any class filter you may apply to narrow the search and results for the groups desired to be used in Titan FTP Server.
    d. **Search branch and sub-branches:** If deselected, the search will not look in organizational units below the selected DN.

e. **Users Base DN:** The level of the Active Directory tree from which your search will start searching for users.
f. **User Category Filter:** Any categorical filter you may apply to narrow the search and results for the users desired to be used in Titan FTP Server.
g. **User Class Filter:** Any class filter you may apply to narrow the search and results for the users desired to be used in Titan FTP Server.
h. **Search branch and sub-branches:** If deselected, the search will not look in organizational units below the selected DN.

Enter Authentication Information

LDAP User Authentication Configuration

4 of 7

Group Base DN
dc=SRTTEST

Group Category Filter
*

Group Class Filter
group;organizationalUnit;container

☑ Search branch and sub-branches

Users Base DN
dc=SRTTEST

User Category Filter
*

User Class Filter
person;user;

☑ Search branch and sub-branches

BACK

NEXT

6. View or update the following fields on the LDAP User Attributes window and click **Next**. The default values help describe the field for reference. No change may be needed on this page.
    a. User ID
    b. Username
    c. Full Name
    d. Home Directory
    e. Email Address
    f. User DN
    g. Account Enabled
    h. Member of
    i. Primary GroupID

Enter Authentication Information

LDAP User Attributes

5 of 7

User ID
objectSID

Username
sAMAccountName

Full Name
displayName

Home Directory
homeDirectory

Email Address
mail

User DN
distinguishedName

Account Enabled
userAccountControl

Member Of
memberOf

Primary GID
primaryGroupID

BACK

NEXT

7. View or update the following on the LDAP Group Attributes window, and click **Next**:
    a. Group ID
    b. Group Name
    c. Group DN
    d. Group Members
    e. Org Unit Name
8. In the Domain Information window, enter a friendly description for the server in the Friendly Description field.
    a. Click the **check box** to indicate that you require the user to log in from the domain associated with their email address.
9. Click **Finish**.

The database displays on the User Authentication page. Adding the database does not automatically enable it. To enable it, find the database on the page and click on the **check box** in the Enabled column. A check displays when enabled.

Add a Windows Active Directory (ADSI) User Authentication Database

To add a Windows Active Directory (ADSI) User Authentication Database, first navigate to the server in your left navigation. Next, click **User Auth** in your top navigation.

1. Click the **arrow** in the User Authentication Database field and select **Windows Active Directory (ADSI)** in the User Authentication Database field.
2. Then, click **Next** at the bottom right of the window.
3. Enter or select the **Domain Name** and **Server Name** and check the check boxes to make any applicable selections from the following options:

a. **Use SSL for Connection:**

b. **Home Directory from User's Profile:** This will have Titan FTP Server use the Home Directory that is associated with a User's Profile from the NT environment.

c. **Impersonate NT User After Login:**Titan FTP Server will pass the credentials to Active Directory and use them to authenticate to network resources. This allows Titan FTP Server to leverage existing permissions for the user.

d. **Use NTFS/ACLs User Permissions:** Titan FTP Server will use existing Active Directory permissions for a specified resource. This allows Titan FTP Server to leverage existing Active Directory Access Control Entries for the resource.

4. Then, select **Next**.
5. **Enter the Administrative Username and Password** to the AD server and click **Next**.
6. **The ADSI Cache and Timeout Configuration** window displays. Enter the following:
    a. **User Cache Life in seconds:** The number of seconds the users list will be valid. The longer the period set, the longer the server will take to recognize added or deleted users.

    b. **Group Cache Life in seconds:** The number of seconds the groups list will be valid. The longer the period set, the longer the server will take to recognize added or deleted groups.

    c. **Server Timeout in seconds:** The number of seconds of idle time before a timeout would occur or the server is considered unresponsive.

    d. To pre-cache users, click the **check box** in the **Pre-cache user list:** Pre-Cache user list allows Titan FTP Server to download and store user information before first connect. This will especially assist the first connection made to the server, as this information would be polled and retrieved at that time.
7. View/Update the fields on the ADSI User Authentication Configuration window and click **Next**.
    a. **Groups Base DN:** The level of the Active Directory tree from which your search will start searching for groups.

b. **Group Category Filter:** Any categorical filter you may apply to narrow the search and results for the groups desired to be used in Titan FTP Server.

c. **Group Class Filter:** Any class filter you may apply to narrow the search and results for the groups desired to be used in Titan FTP Server.

d. **Search branch and sub-branches:** If deselected, the search will not look in organizational units below the selected DN.

e. **Users Base DN:** The level of the Active Directory tree from which your search will start searching for users.

f. **User Category Filter:** Any categorical filter you may apply to narrow the search and results for the users desired to be used in Titan FTP Server.

g. **User Class Filter:** Any class filter you may apply to narrow the search and results for the users desired to be used in Titan FTP Server.

h. **Search branch and sub-branches:** If deselected, the search will not look in organizational units below the selected DN.

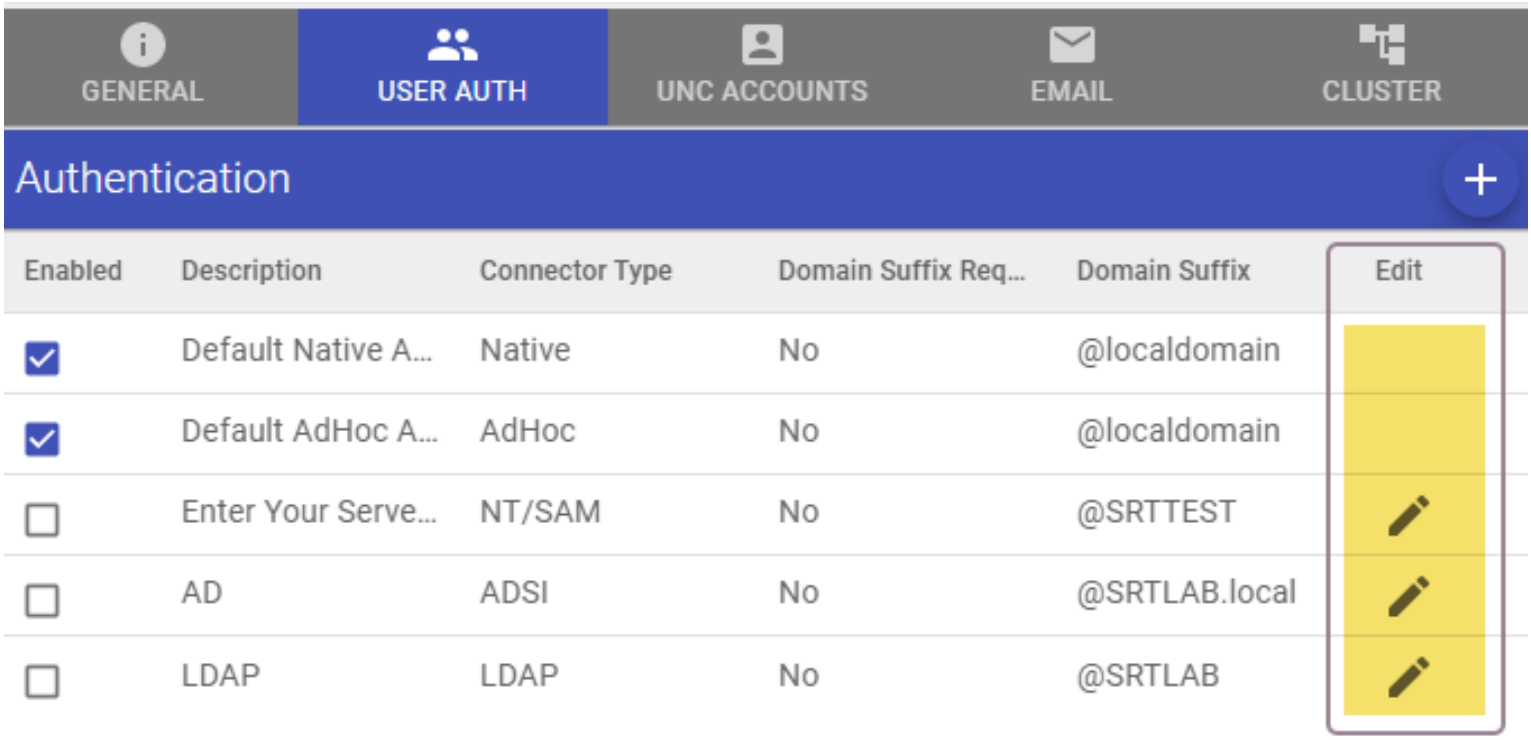
8. In the Domain Information window, enter a friendly description for the server in the Friendly Description field.
    a. If desired, click the **check box** to require the user login to include username@domain .
    b. If desired, click **Test** to ensure the credentials and information supplied allow a successful connection from Titan FTP Server to the ADSI server.
9. Click **Finish**.

The database displays on the User Authentication page. Adding the database does not automatically enable it. To enable it, find the database on the page and click on the **check box** in the Enabled column. A check displays when enabled.

Update User Authentication Database

You can update the details and settings of a user authentication database by first selecting the **server** in your left navigation. Next, click on **User Auth** in the top navigation.

1. Find the database that you want to update on the list and click on the **pencil** icon.



The User Authentication database information screen displays.

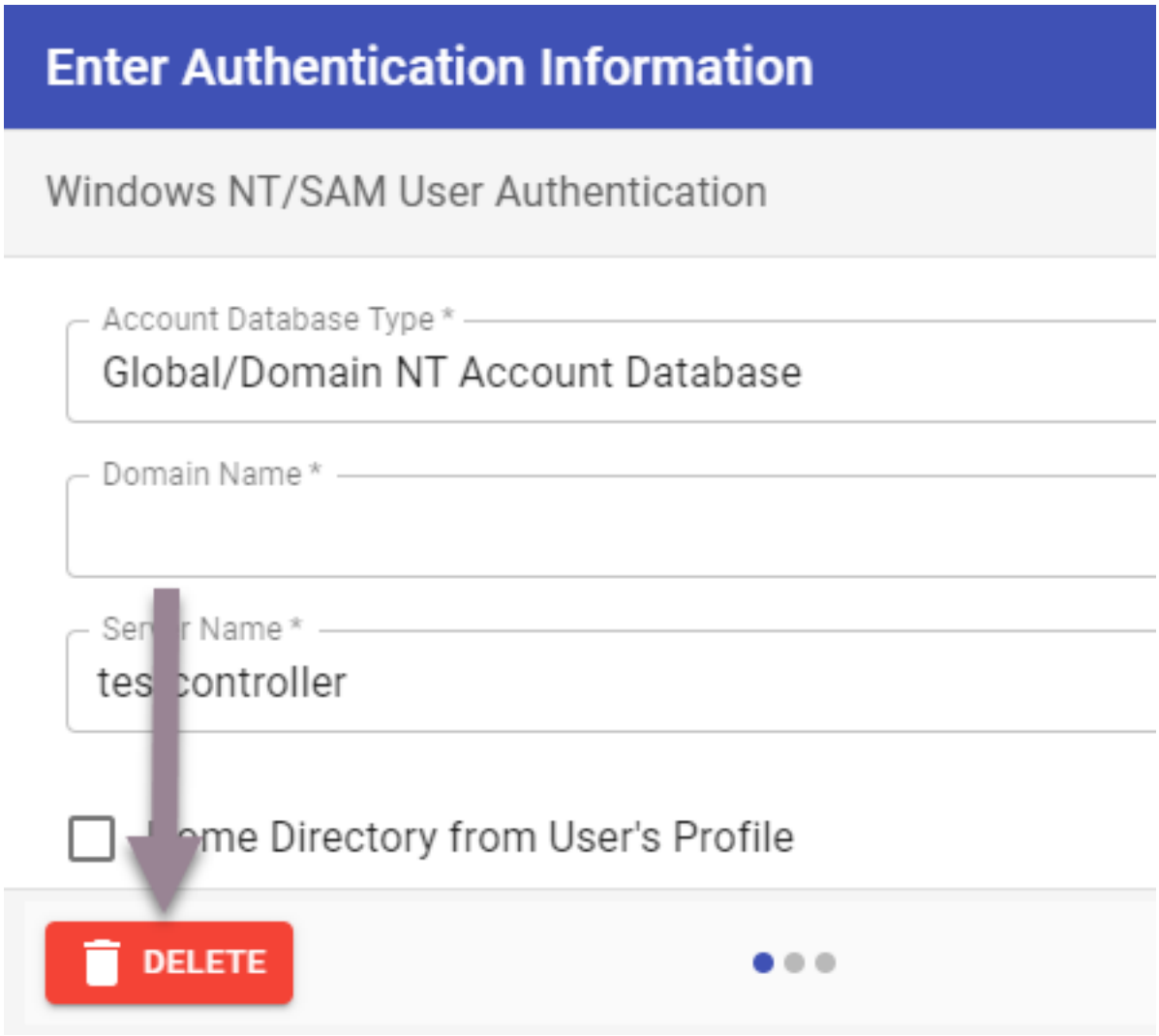
2. Make desired changes to fields in the User Authentication wizard, clicking **Next** to move through the three screens of the wizard and making appropriate changes.
3. Next, click **Finish** to save your changes. Titan FTP Server returns to the User Authorization screen and saves your updates.

Delete User Authentication Database

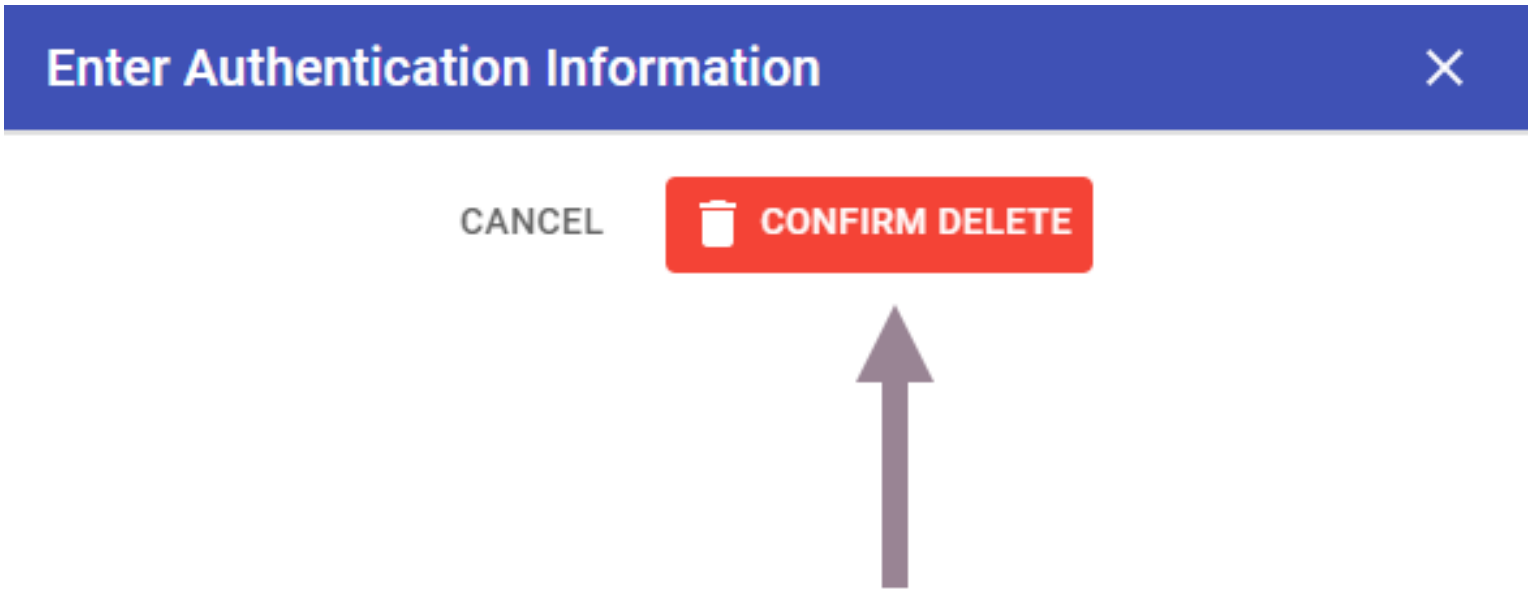
To delete a user authentication database, first navigate to the server in your left navigation. Next, click **User Auth** in your top navigation .

The screen displays the databases, enabled, and not enabled, that authenticate your users.

1. To delete a database, locate it on the User Authorization screen and click the **pencil** icon in the Edit column.
2. Click **Delete** in the bottom left of the User Authentication Database window.



3. Next, click **Confirm Delete**.



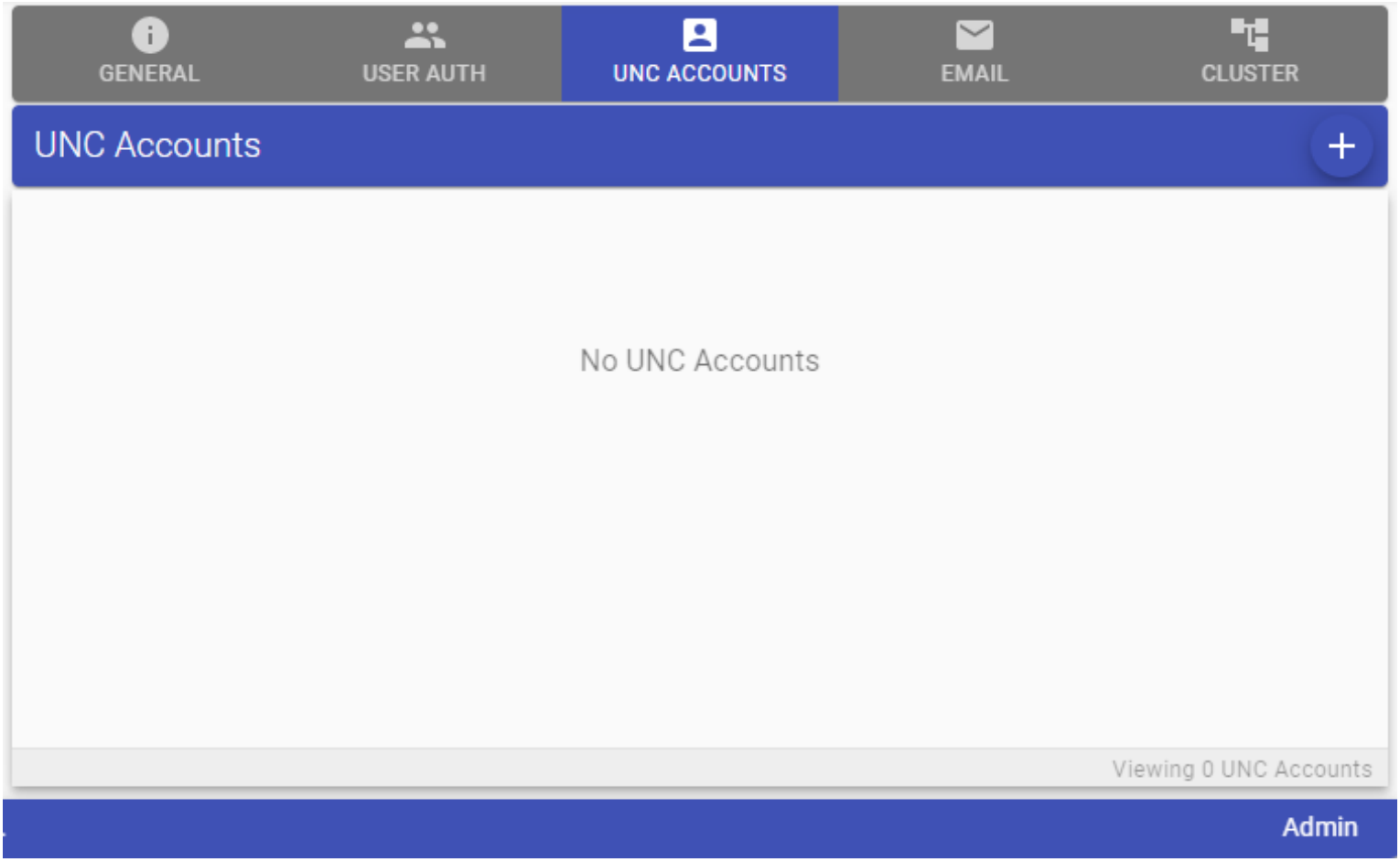
Titan FTP Server removes the database. The User Authentication page no longer displays the database after it is deleted.

UNC Account Authentication

Titan FTP Server allows you to use UNC Accounts to authenticate users who access the server and allow access to network shares. This would be useful in allowing users to access UNC locations (network shares) by leveraging an account with the proper permissions. The UNC Account must have access to the desired shares.

You can view, add, and delete special accounts to access file shares on the UNC Accounts screen. To get there, first navigate to the server in your left navigation. Then, click **UNC Accounts** in the top navigation.

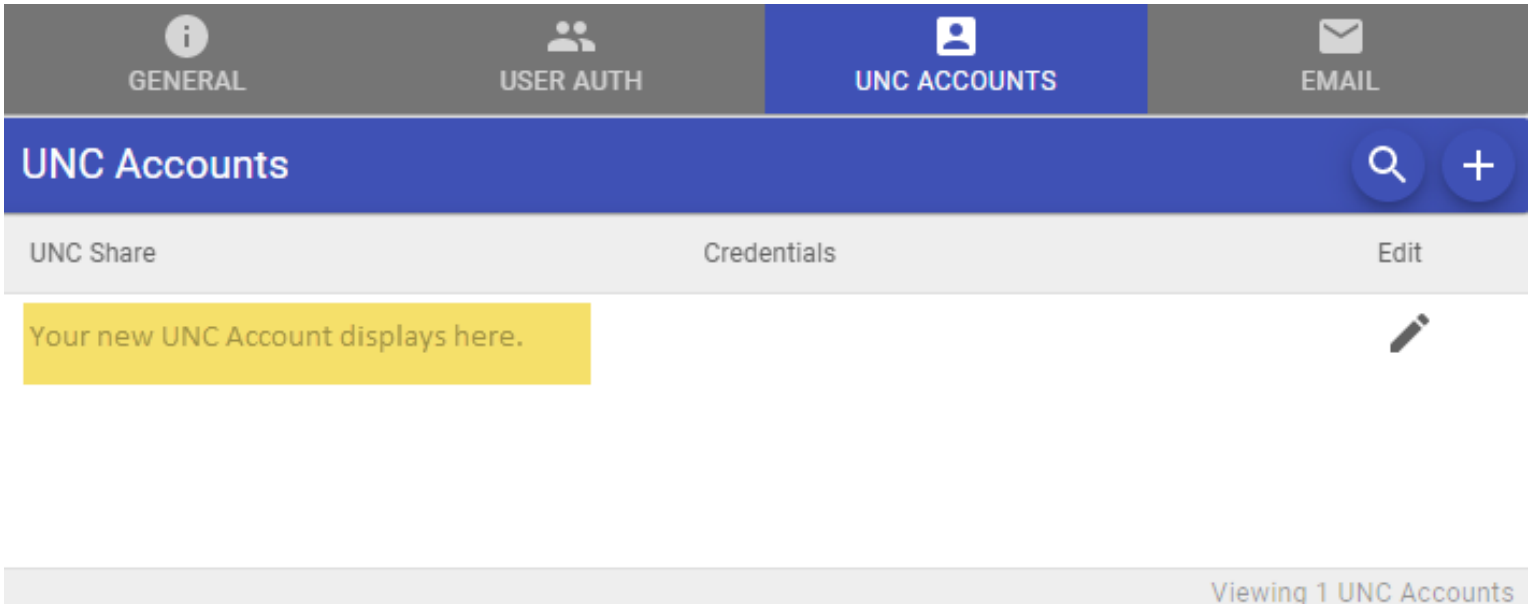
Your UNC Accounts are listed here. If you haven’t added any accounts yet, the screen displays "No UNC Accounts".



Add a UNC Accounts

To add a UNC Account:

1. Click on the **plus** icon to add a UNC Account.
2. In the UNC Account window, enter the desired UNC share path for the folder/directory of interest and then supply the proper UNC Account username and password.
3. Click **Add** at the bottom right of the screen. The account displays on the UNC Accounts screen:

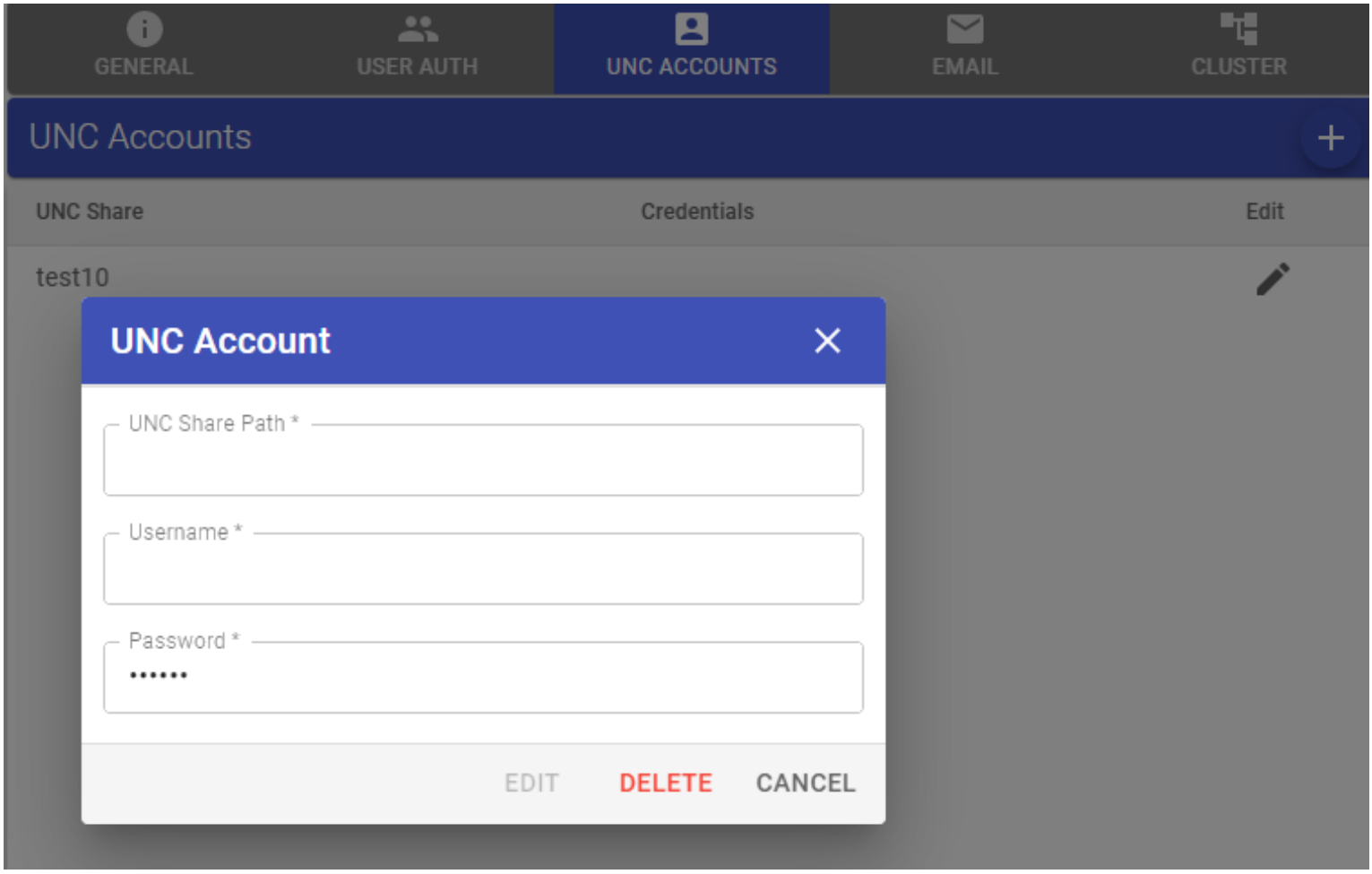


Editing UNC Accounts

To edit a UNC Account:

1. Click on the **pencil** icon next to the account you want to edit on the UNC Accounts screen. The account details display for UNC Share Path, Username, and Password.

2. Make updates by entering the text in the respective fields.
3. Select **Edit** when finished.

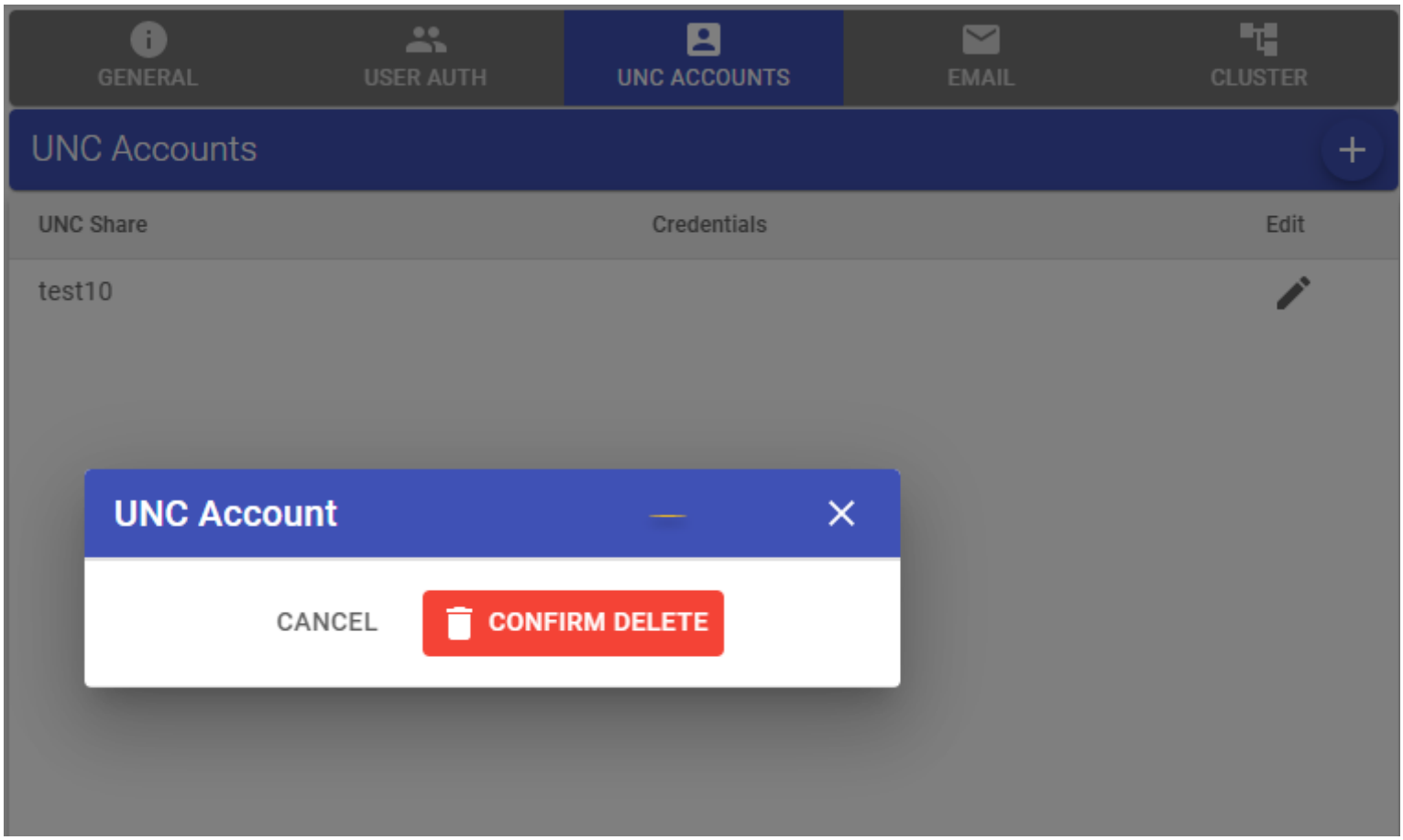


Deleting UNC Accounts

To delete the UNC Account:

1. Click on the **pencil** icon next to the account you want to delete on the UNC Accounts screen.
2. Click **Delete** on the UNC Account window.

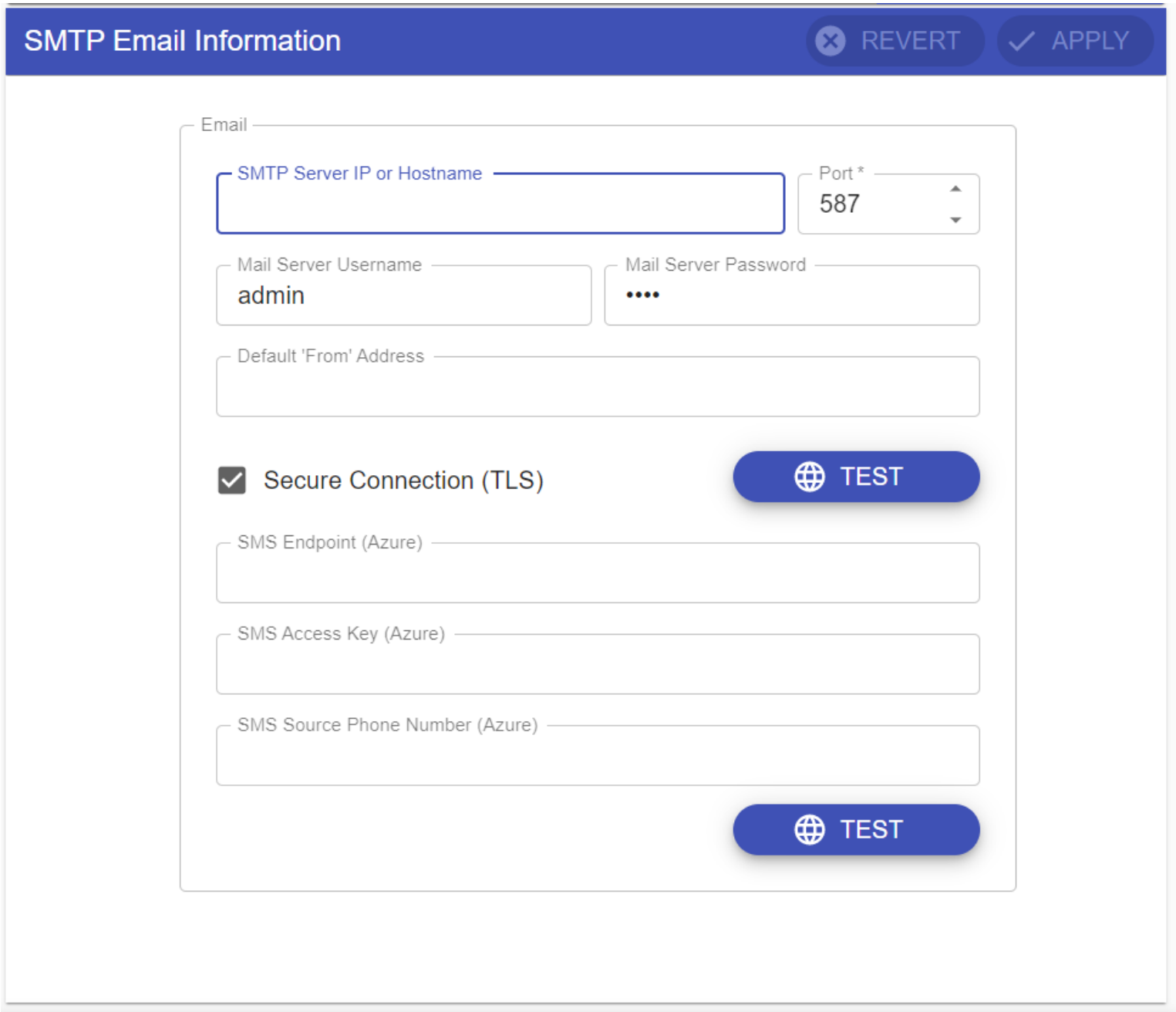
3. Then, choose to **Confirm Delete**.



Email Settings

You can configure and update email server settings, as well as test email and SMS server connections, on the Email Information screen. To access this screen, click on **Email** in the top navigation.

This menu allows for configuring an email server for Titan FTP Server to leverage when sending emails. Email use within Titan FTP Server relates to email notifications.



- **Update email information:** Make updates to the following field(s) by entering text in the respective field. Click **Apply** to save your updates.
- You can also make changes to the following:

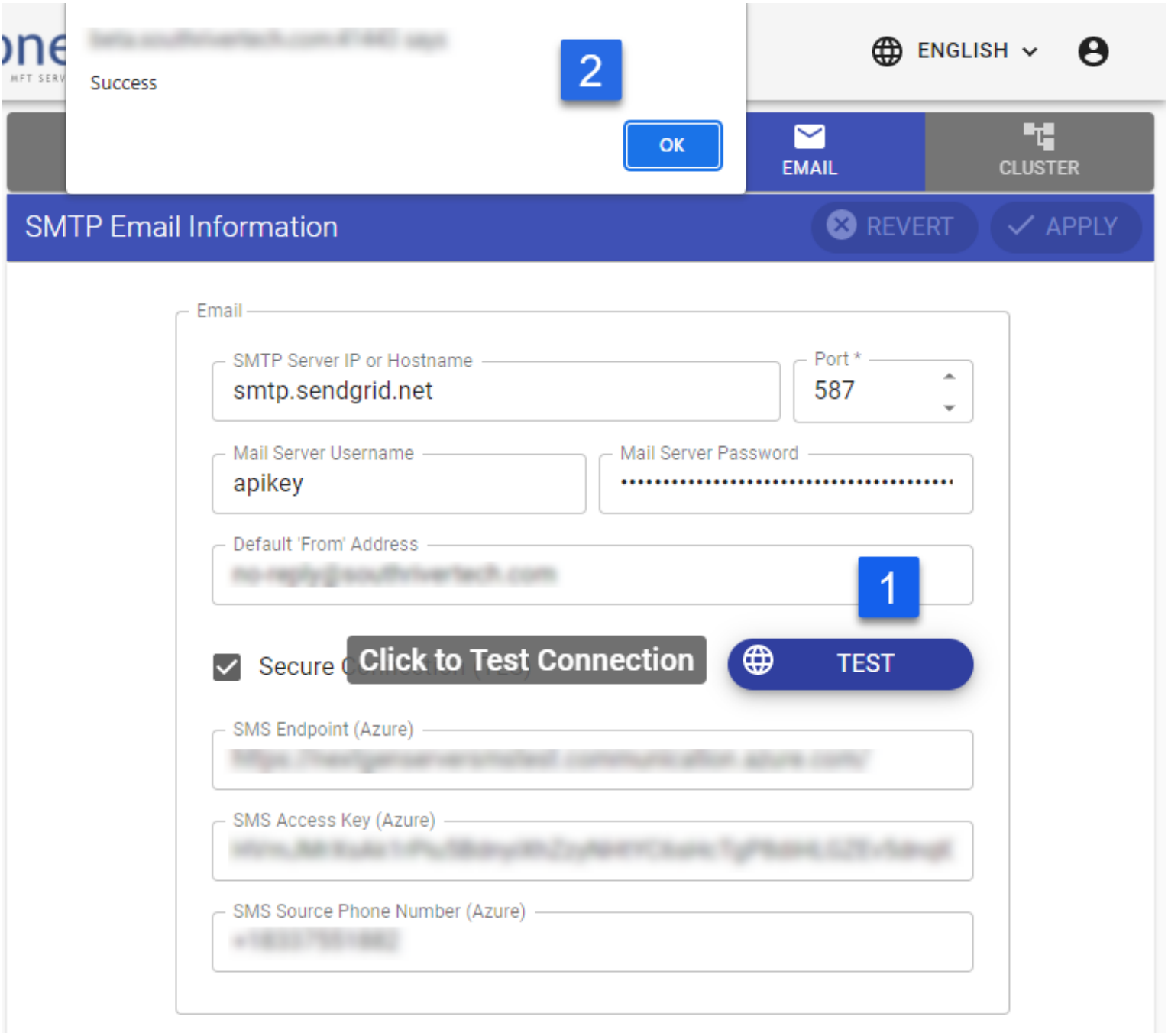
- **SMTP Server IP or Hostname:** Enter the IP Address or Hostname that Titan FTP Server should connect to in order to leverage an existing Mail Server.
- **Port:** Enter the port number to use for connecting to the Mail Server.
- **Mail Server Username:** Username for Titan FTP Server to use to connect and authenticate to the Mail Server.
- **Mail Server Password:** Password associated with the Username to use to connect and authenticate to the Mail Server.
- **Default "from email address":** Emails sent out by Titan FTP Server will use this FROM address by default.
- **Enable or disable Secure TLS Connection:** Option to choose whether the connection should be made over TLS (securely) or not.
- **SMS Endpoint (Azure):** Enter the endpoint of the SMS Server Titan should connect to. Currently, this is through Azure Communication Services (e.g. https://mysmsurl.-communication.azure.com).
- **SMS Access Key (Azure):** Enter the Access Key for Titan FTP Server to use to authenticate to the SMS Endpoint.
- **SMS Source Phone Number (Azure):** The Mobile Number from which to send the SMS messages through Titan FTP Server to recipients.

- **Enable secure connection:** Check the **Secure Connection (TLS)** check box.
- **Send a test email:** Click **Test** to send a test email.
- **Send a test SMS:** Click **Test SMS** to send a test SMS.

Testing Email Connections

To test your email connections, click **Email** from your top navigation. The SMTP Email Information screen displays.

Click **TEST**.



If this test fails, verify the account information and credentials, as well as ensuring there are no beginning or ending spaces added to the proper entries (common when copying + pasting).

High Availability and Clustering

Titan FTP Server can be deployed to be highly available and cluster multiple nodes to provide the services your end users need.

To achieve this, you can have two or more Titan FTP Servers point to the same central SQL server, which can house the server configuration. This way, all nodes in the cluster will share the configuration and will always be up to date with any changes allowing to share the load of all incoming connections, load balance any automations, and allow for regular server maintenance without any downtime.

If used with a load balancer, traffic to the clusters can be routed evenly throughout the clusters to avoid interruption of service. If one server goes offline, traffic will route to the other server.

The User Accounts will also be available like in the case of Active Directory/LDAP-based user authentication, on an external server, which is accessible from multiple nodes. Employing an external database to store configuration and user account information creates a fully scalable system, where multiple nodes share the workload and allow system maintenance, without creating user access limitations.

Important Recommendations for Setting up Clustering with Titan FTP Server

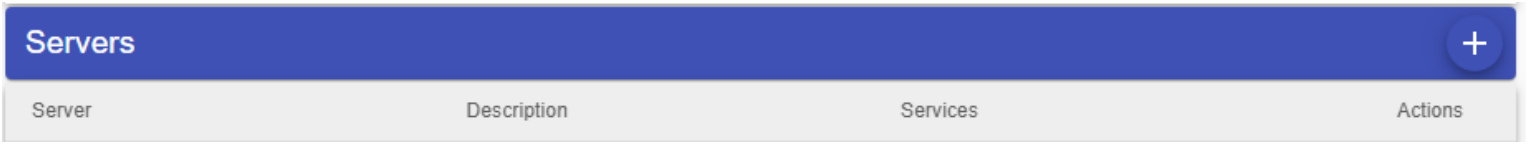
- Dedicate a separate machine to be used as your SQL Database server. This will allow multiple Titan FTP Server nodes to gain access to the server configuration.
- Make sure network and firewall policies allow communication with your SQL server from your Titan FTP Server. For example, default port 1433 should be open to connect to SQL server.
- Store your user data out on a network drive, accessible through a UNC, and make sure all of your Titan FTP Server nodes have proper access.

- Store your log files and any TLS certificates out on a UNC for shared access across the clustered nodes.

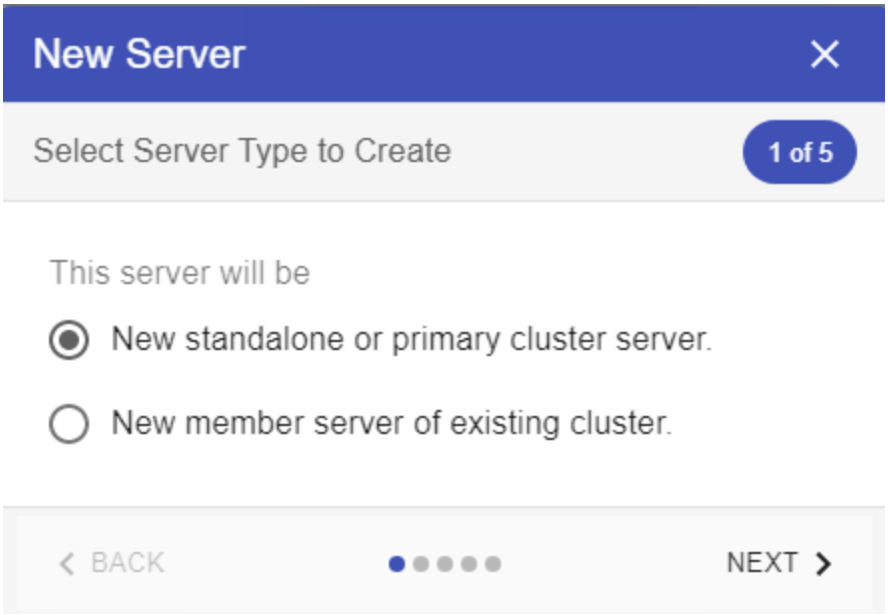
Once the multiple servers have been configured, they will all share the same server, user, and group configuration settings.

Create a Primary Titan FTP Server

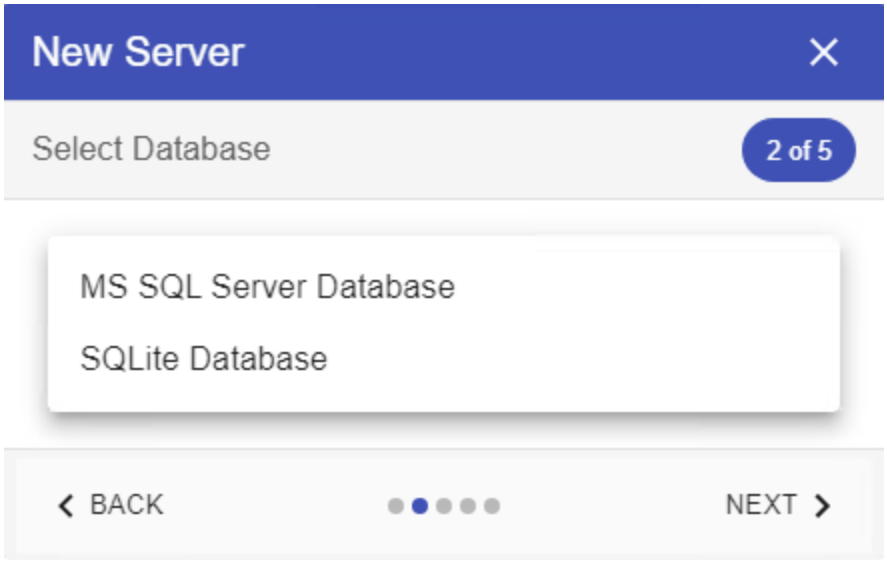
1. Login to the Titan FTP Server admin portal and select the **plus** icon under Servers.



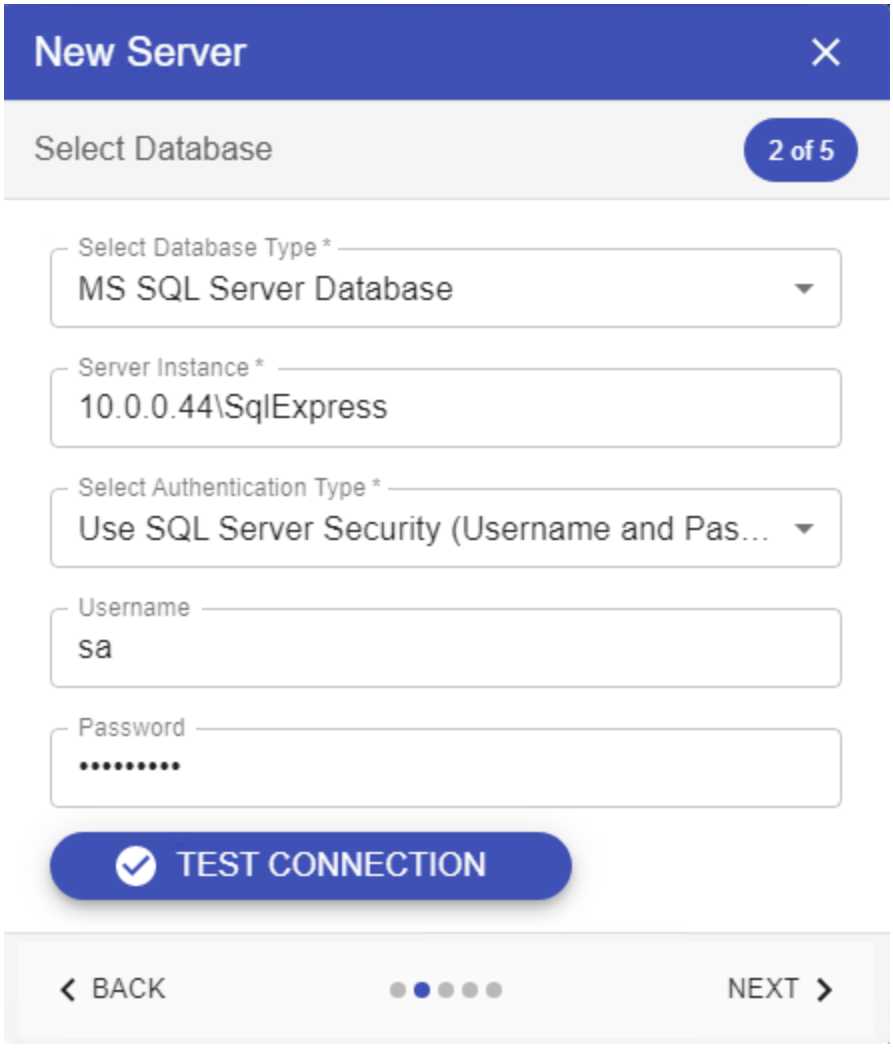
2. Select the **New standalone or primary cluster server** option and click **Next**.



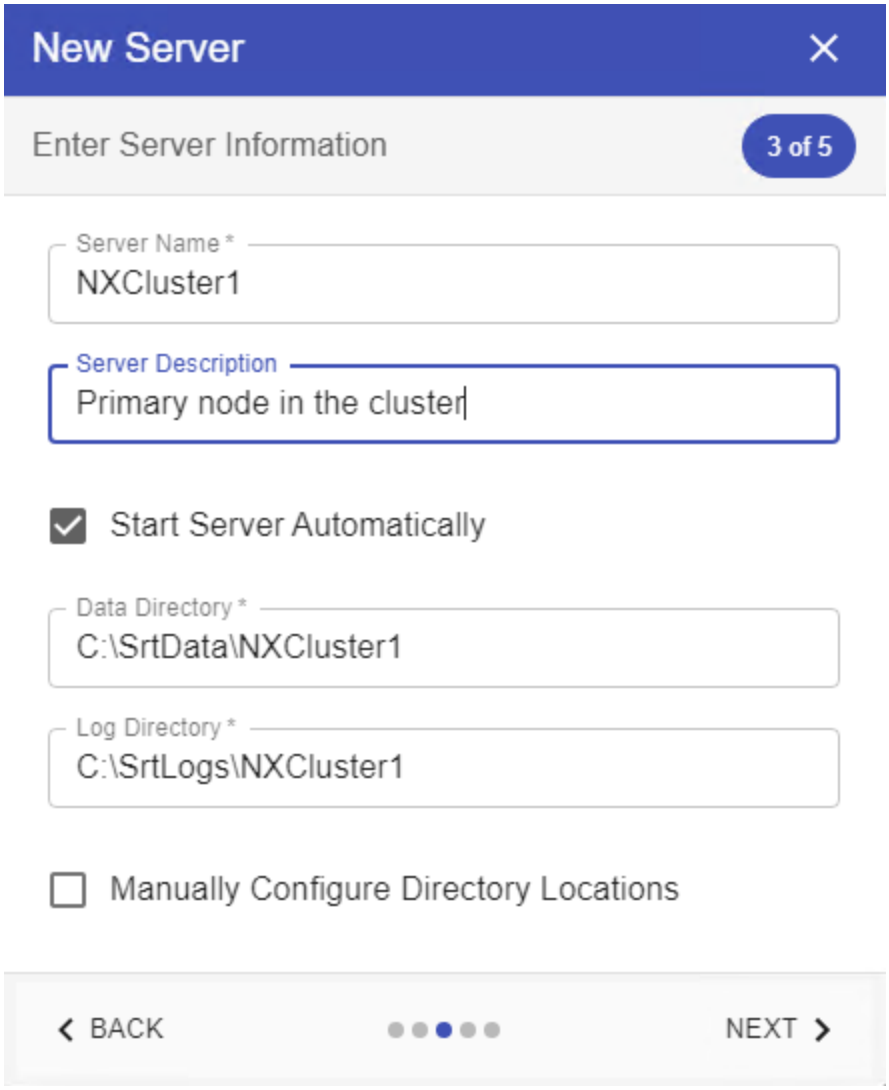
3. Select the **database type**. For clustering, we recommend having a central SQL server, so we will select the **MS SQL Server Database** option.



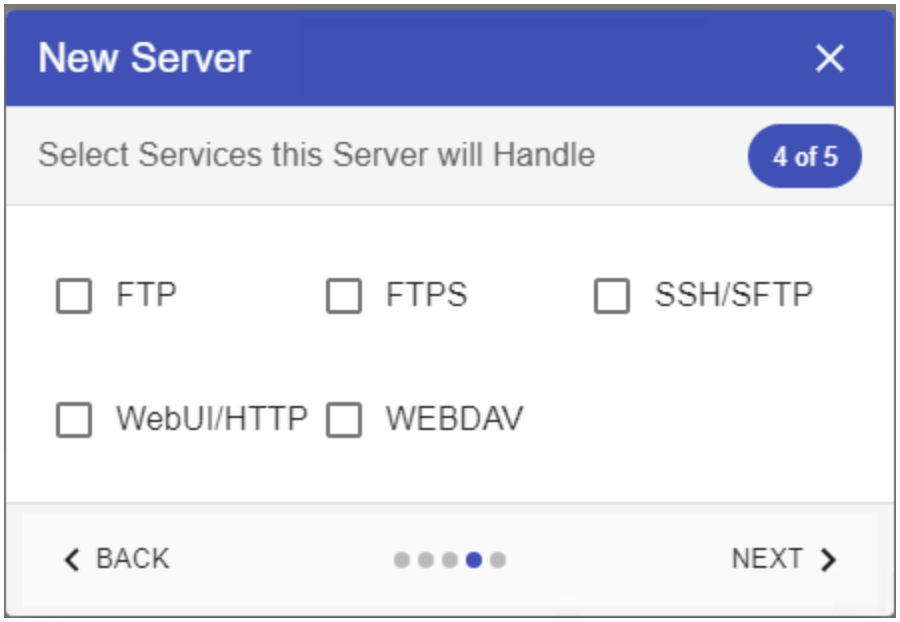
4. Input all of the connection parameters for your SQL server. You can select **Test Connection** to ensure you have access before proceeding.



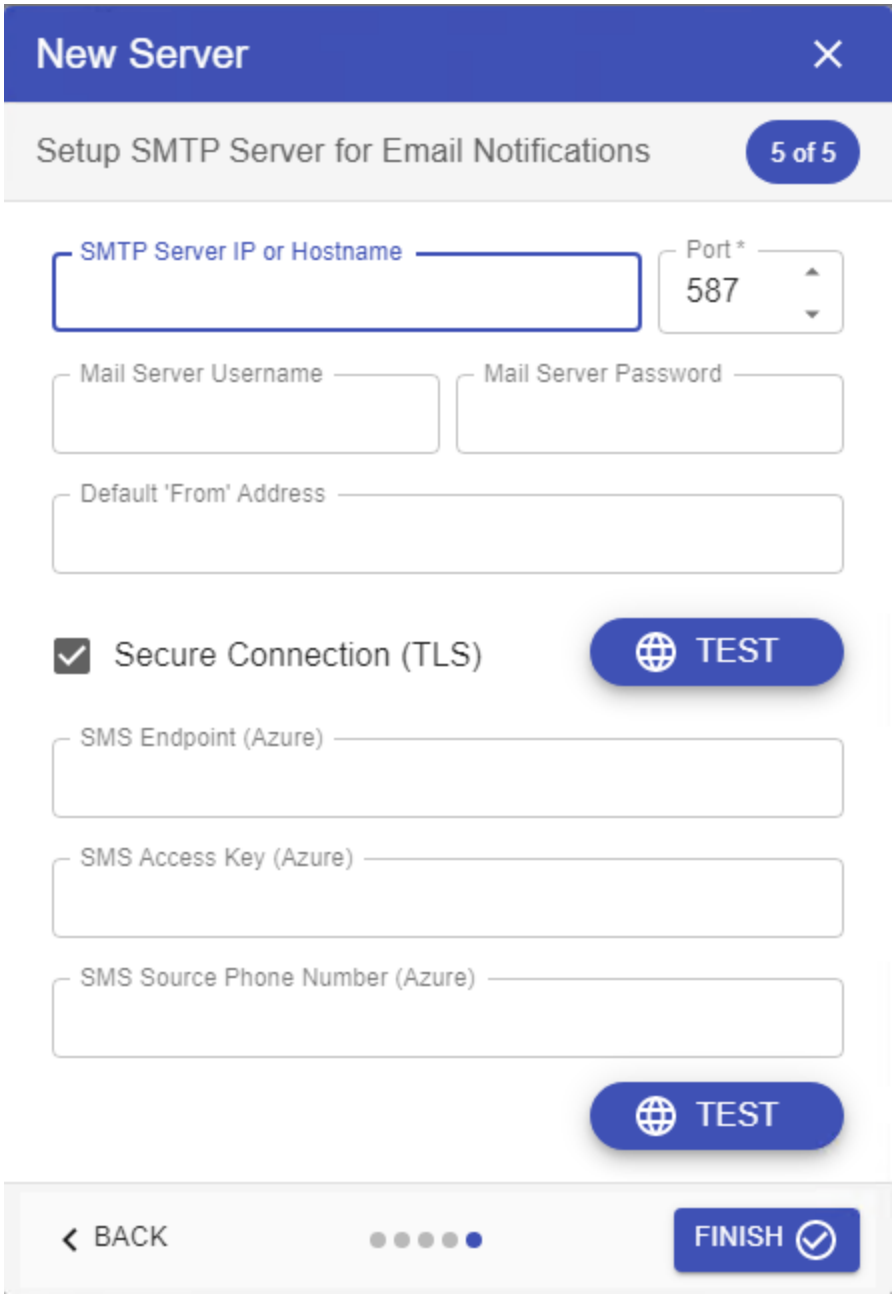
5. Provide the new Server Name and Description.



6. Enable any protocols. If you do enable a protocol, the server creation wizard will add steps to allow you to configure each protocol. In this example, we will leave all of the protocols disabled so we can enable them afterward.



7. Configure your SMTP settings for notifications. This can also be done after creation, as well.

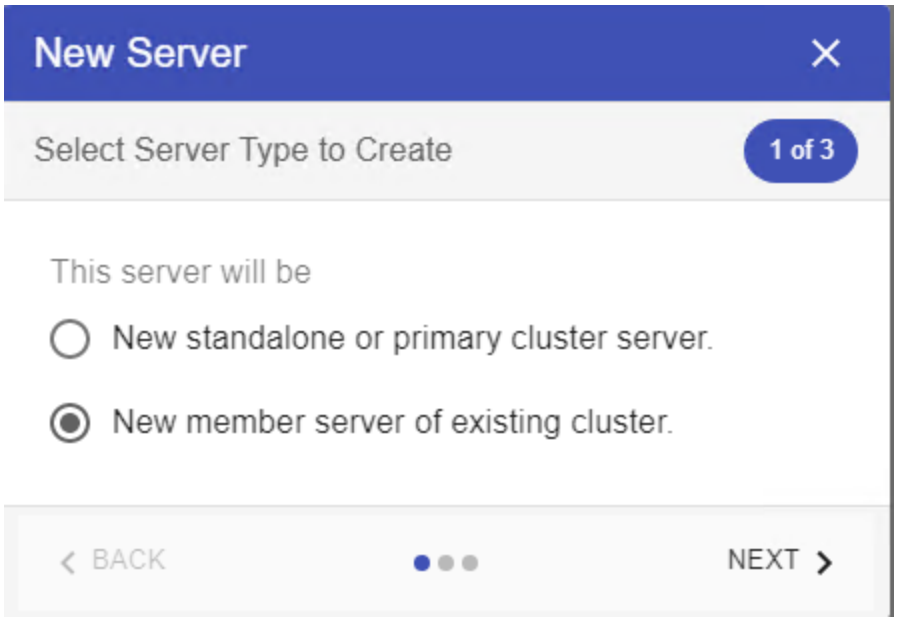


8. Select **Finish**.

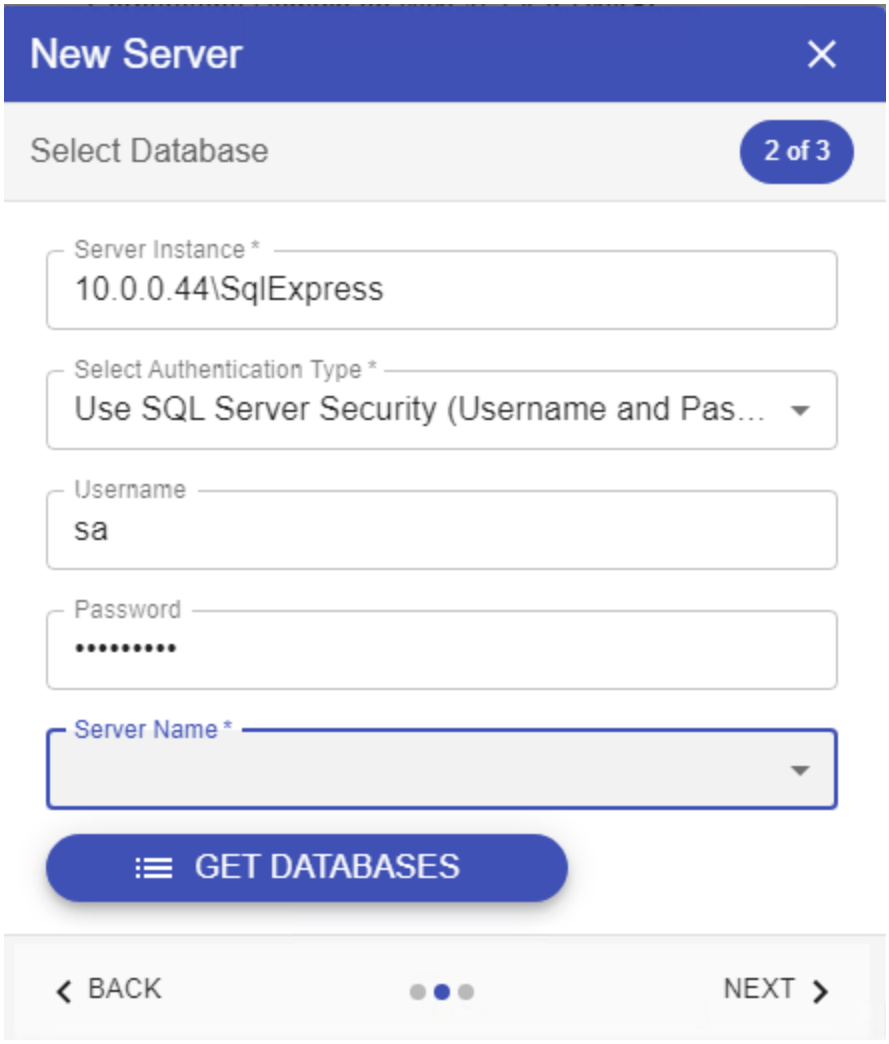
Now, your newly created server will appear in your admin portal under Servers.

Create a Member/Secondary Clustered Server

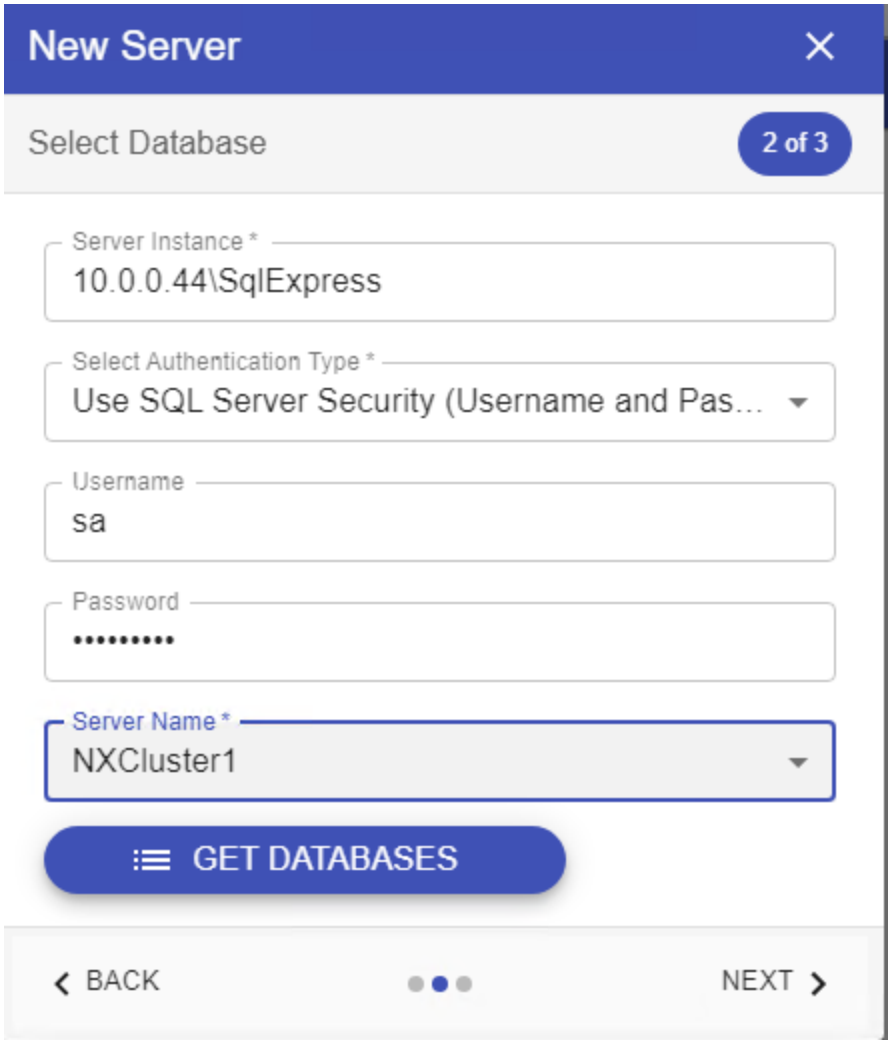
1. On your second Titan server, access the admin portal and select the **plus** icon under Servers.
2. Select the **New member server of existing cluster** option and click **Next**.



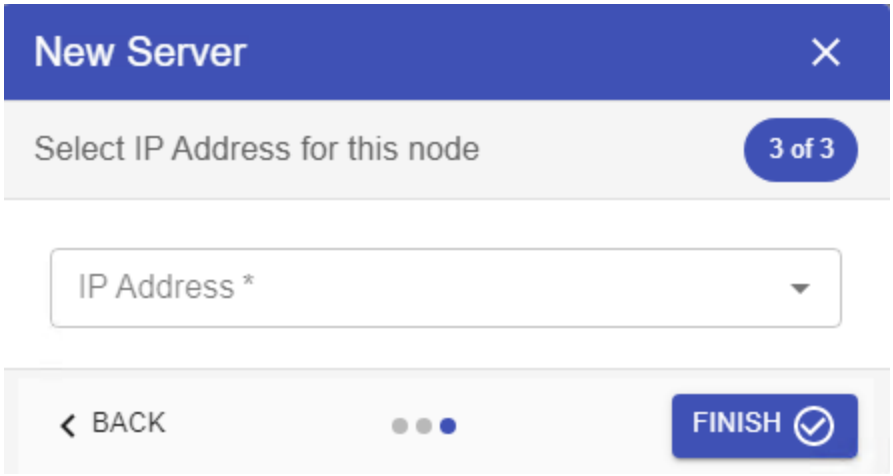
3. Input the connection parameters to the same SQL server you used to create the primary server in the cluster.



4. Select **Get Databases** and any supported databases will populate in the drop-down list.
5. Then, select the **server** you created as primary so this node can also access and share its configuration and click **Next**.



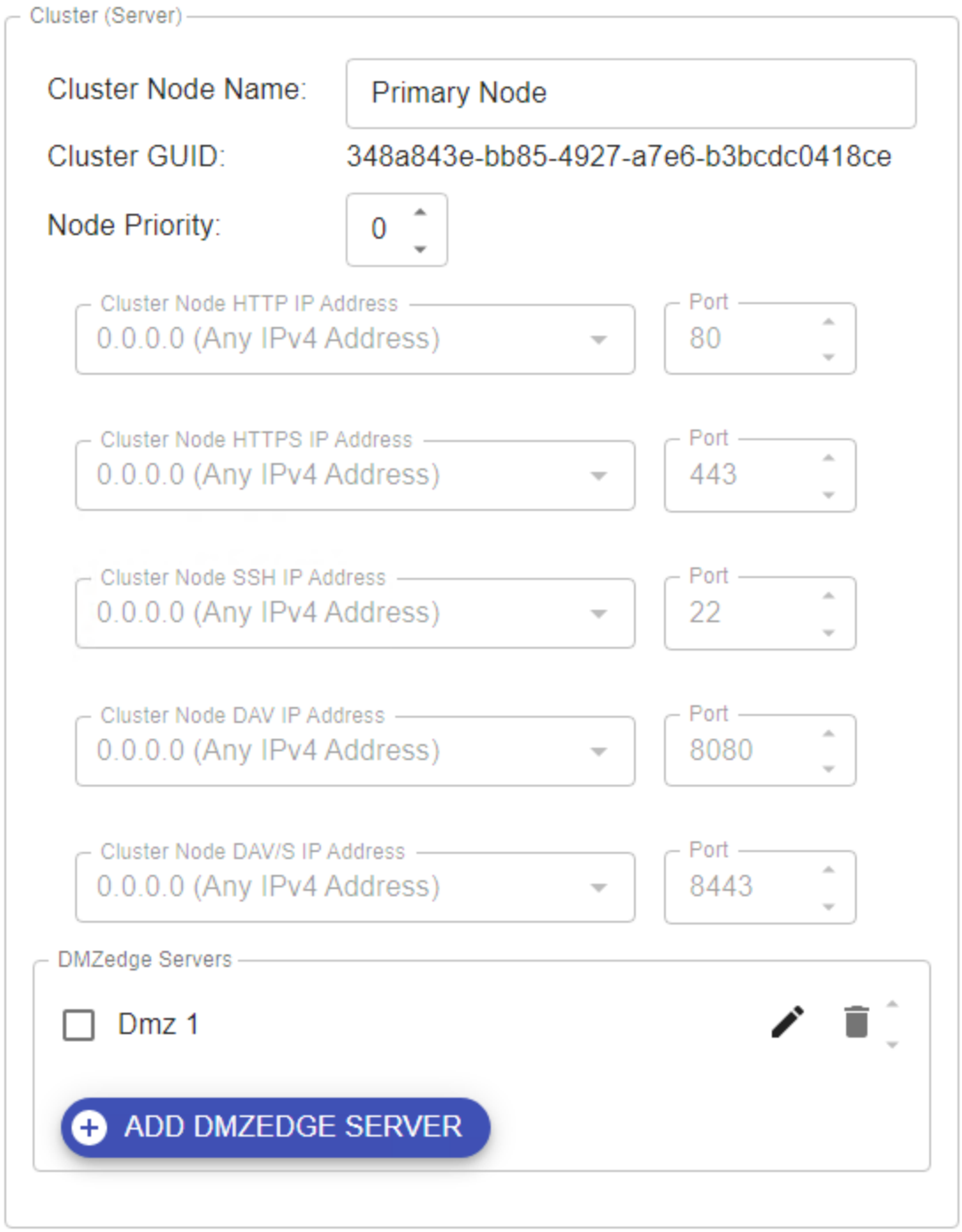
6. Select an **IP Address** for this node and click **Finish**.



Now, you can see the server in the admin portal of this second Titan FTP Server under Servers.

Cluster Tab

Once you have created your cluster, you can navigate to the **Cluster** tab to view additional settings.



- **Cluster Node Name**: This option allows you to give this particular node a specific name.
- **Cluster GUID**: This is a unique identifier this cluster uses in the back-end to be able to sync to the correct cluster configuration shared among member nodes.

- **Node Priority**: This setting allows you to give this particular node a priority for traffic if using DMZ Edge. In that scenario, DMZ Edge will look at the priority settings of all member nodes and will select the highest priority (highest number) to send traffic to first.
- **Cluster Node HTTP IP Address/Port**: This field is for display purposes only to show which IP/port this server is configured to listen on for HTTP.
- **Cluster Node HTTPS IP Address/Port**: This field is for display purposes only to show which IP/-port this server is configured to listen on for HTTPS.
- **Cluster Node SSH IP Address/Port**: This field is for display purposes only to show which IP/port this server is configured to listen on for SFTP.
- **Cluster Node DAV/S IP Address/Port**: This field is for display purposes only to show which IP/port this server is configured to listen on for DAV/S.

Server Configuration

In Titan FTP Server, you can configure multiple server instances under a single domain or physical computer. Configure servers to store data in a separate directory, on your local hard drive, or on a shared network drive.

Titan FTP Server supports standard DOS path syntax and UNC paths. Please use a UNC path instead of a mapped drive (or a path that points to a mapped drive), as these are not accessible by the system.

To view and update general and advanced configuration settings and options, navigate to the **Services** page on your left navigation.

NX Configuration Utility

[Placeholder for engineering – screen shots when NextGen is complete/ready]

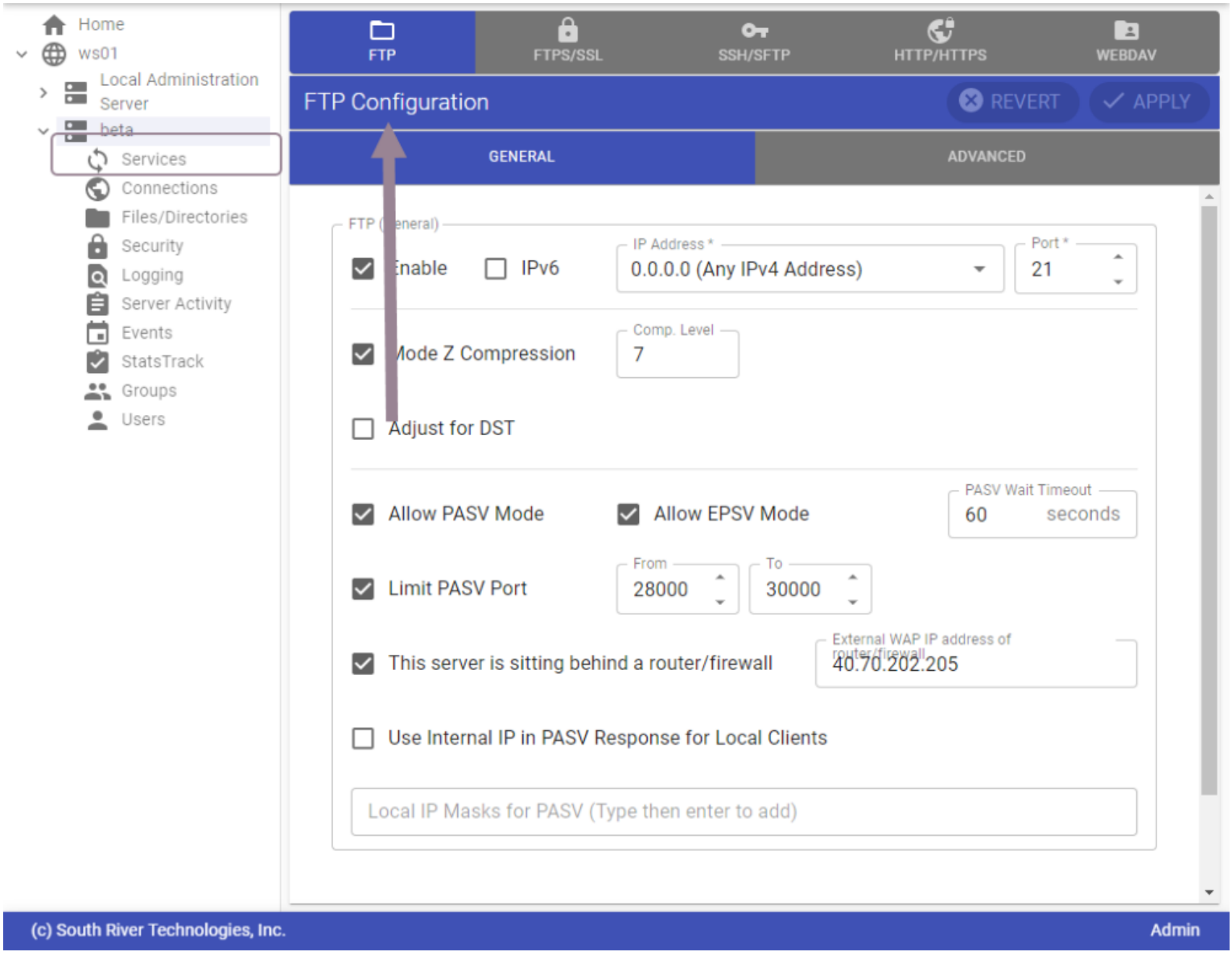
File Transfer Protocol (FTP) Configuration

File Transfer Protocol (FTP) is a means of transferring files between computers. FTP is transmitted in clear text and therefore is unsecure. The use of this protocol should be limited to internal transfers only as it is not encrypted.

To set your desired configuration settings, click on **Services** in your left navigation. Next, select **FTP** from your top navigation.

To do this..	Do this
Enable or disable a user's ability to connect to the server using FTP	Click the **Enable** check box
Avoid data collision	If your computer has multiple IP addresses, we recommend you select a single **IP address**. Enter a specific IP address in the IP Address field.
Choose the port the server will use to accept FTP connections. The default port is 21.	Select the **port** in the FTP Port field.

You can update and set your configuration settings on this screen:



General FTP Configuration:

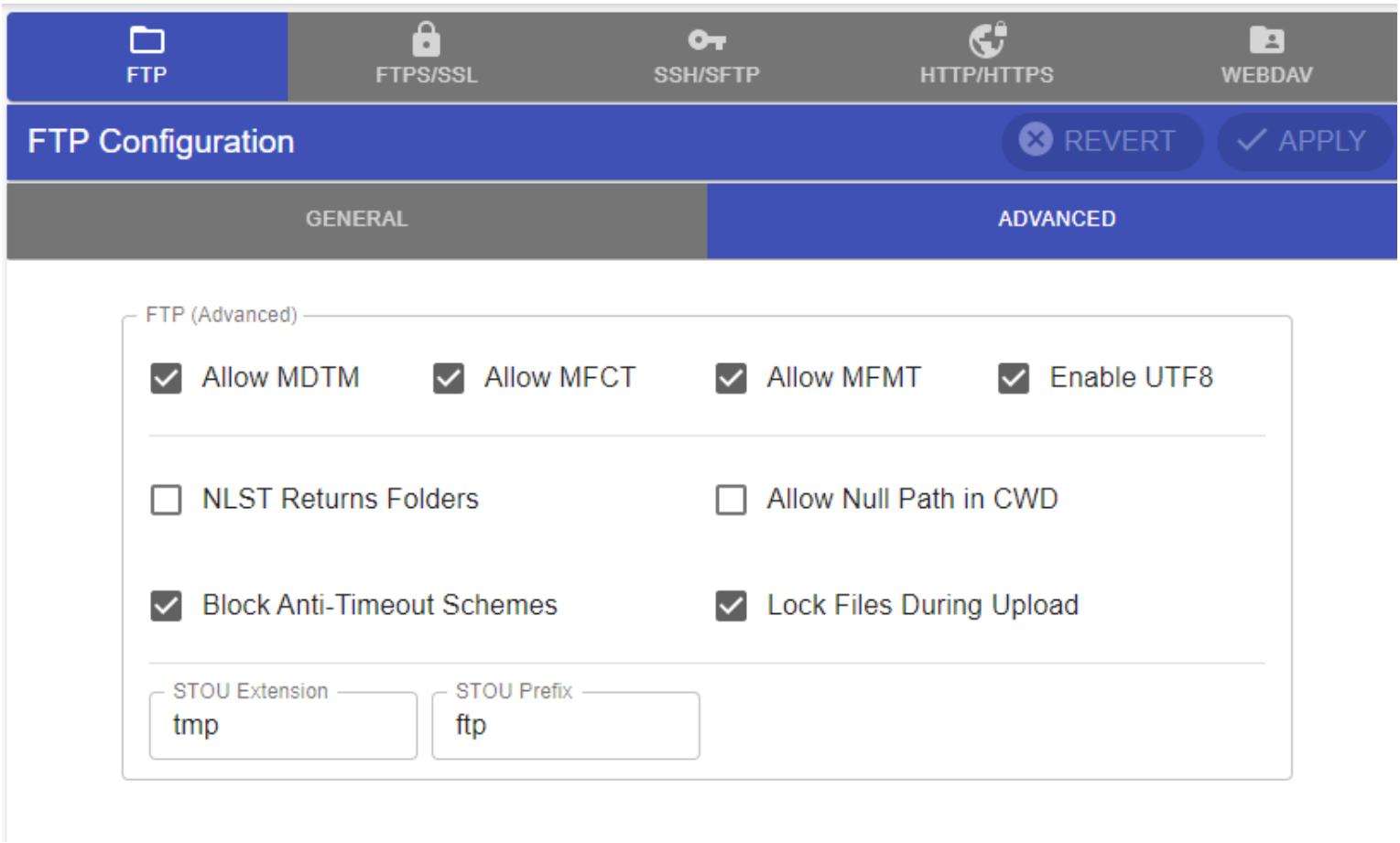
- **IP Address:** This refers to the IP address this Titan FTP Server will be listening on. It is important to note that if you have more than one server, each server should have its own IP address if using the same port numbers to avoid port conflicts.
- **Port:** Select a **port** on which FTP will be listening on and end-users will use to connect. Default port is 21 for the command channel.

- **Mode Z Compression:** You can enable this option to compress files being sent and received which saves you bandwidth and improves transfer time.
- **Adjust for DST:** This will account for “Daylight savings time” on the time stamp for file transfers on the server.
- **Allow PASV Mode:** When sending a file, a client will send the commands via the command channel on default port 21 but data will be sent via the data channel on a different port. The client issues the PASV command which will ask the server to provide a port so they can transmit data over. This is more secure than PORT mode where the client tells the server which port to use because it allows the administrator to open only the specified ports on the firewall.
- **Allow EPSV Mode:** This option allows extended passive mode to be enabled which also supports IPV6 addresses.
- **PASV Wait Timeout:** Give a specific time frame in seconds to wait for the PASV or EPSV.
- **Limit PASV Port Range:** This will let Titan FTP Server send a port within the specified range to the client to use for data transfer once the PASV command is issued. This is recommended as it will allow you to configure your firewall accordingly and not have to open a large range of ports.
- **This server is sitting behind a router/firewall:** This helps in the routing of traffic from the internet by providing Titan FTP Server with the WAN or external IP address.
- **Use internal IP in PASV response to local clients:** This will allow Titan FTP Server to use its internal IP address when responding to PASV commands for the data channel when an internal user is connecting, making the transfer occur internally instead of going outside through the internet.

Advanced FTP Configuration

For advanced FTP configuration options, click on the **Services** option on your left navigation. Next, click on the **FTP** option on the top navigation. The FTP Configuration screen displays.

Click on the **Advanced** tab. The Advanced configuration options for FTP display below.



Enable the option clicking the **check box** next to it. Advanced FTP Configuration allow you to:

- **Allow MDTM:** This command stands for Modified Time and will preserve the last modified time and day.
- **Allow MFCT:** This command is used to modify a file or folder's creation date and time information. When a file or folder is uploaded to an FTP server, the creation date and time of the file or folder is set to the transfer date and time.
- **Allow MFMT:** This command is used to modify a file or folder last modified date and time information. MFMT duplicates similar functionality implemented by the MDTM command.
- **Enable UTF8:** UTF-8 is an encoding system for Unicode. It can translate any Unicode character to a matching unique binary string, and can also translate the binary string back to a Unicode character.

This is the meaning of “UTF”, or “Unicode Transformation Format.”

- **NLST Returns folders:** The NLST command is used to retrieve a list of files from the server over a previously established data connection. Unlike the LIST command, the server will send only the list of files and no other information on those files.
- **Block Anti-Timeout Schemes:** This option will ignore any keep alive commands to maintain any idle session alive which will keep consuming a port and resources. An example of such commands in FTP is NOOP.
- **Lock Files During Upload:** Allow Titan FTP Server to have an exclusive lock on files during upload.
- **STOU Extension:** Existing files will not be overwritten, instead it will have the specified extension.
- **STOU Prefix:** Existing files will not be overwritten, instead it will have the specified prefix.

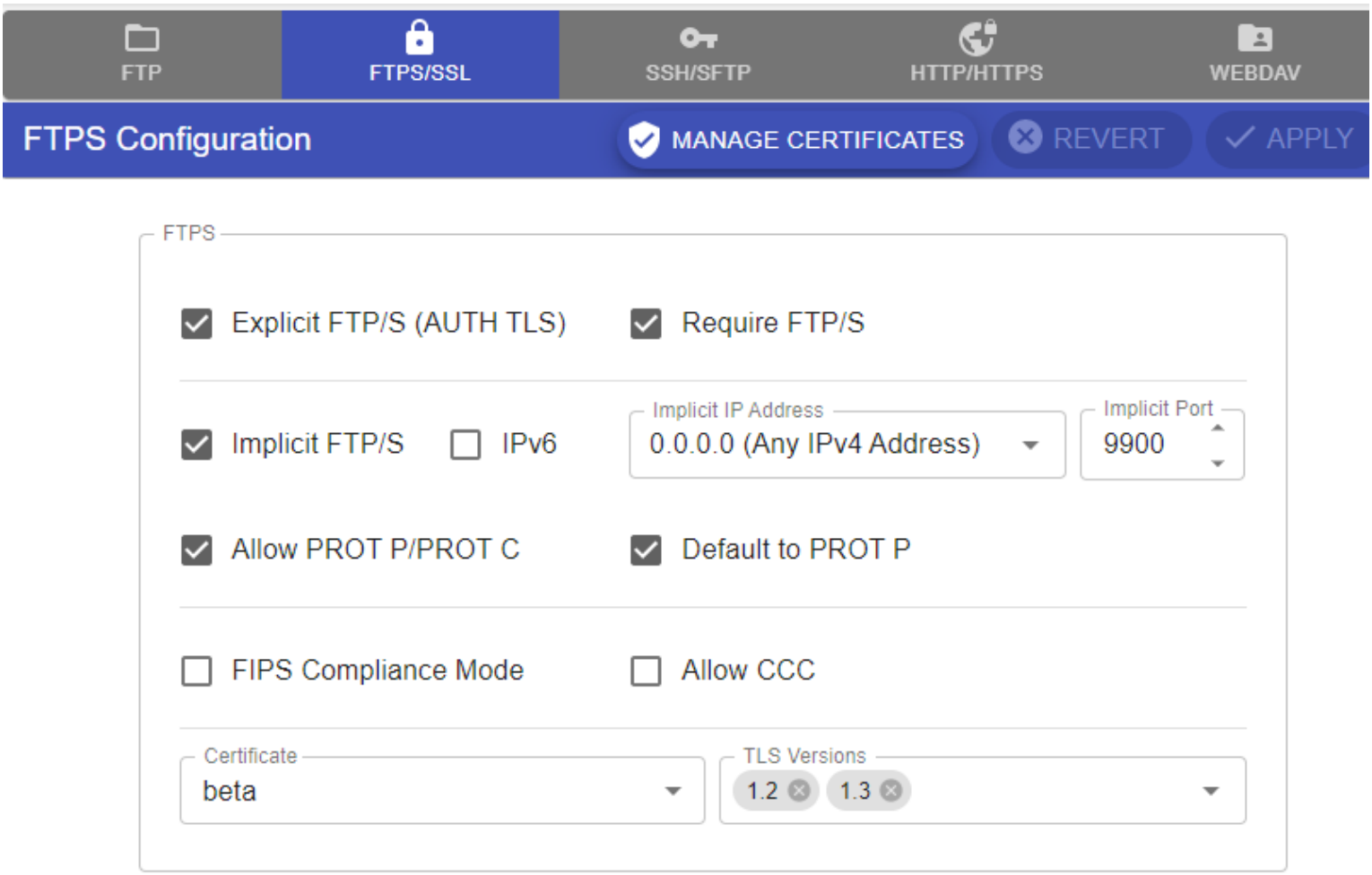
Click **Apply** at the top right window to keep your changes or **Revert** to remove them without saving.

FTPS Configuration

FTPS refers to File Transfer Protocol but over TLS. This allows the connections to be secure and encrypted using an TLS certificate. You can use this to send and receive files from external users as it is a secure connection.

To access FTPS configuration options, first navigate to the server and click **Services** in the left navigation.

Next, click **FTPS/SSL** in the top navigation. The FTPS Configuration screen displays.



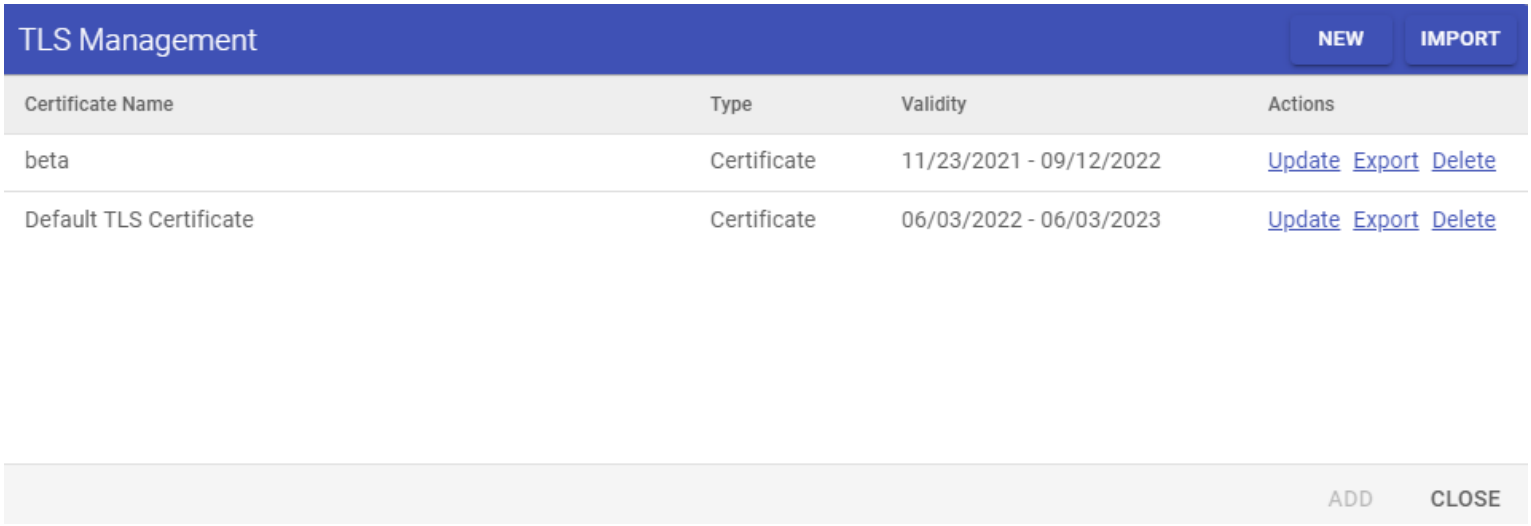
Make sure that your firewall allows for the selected port. If you have more than one server and the IP Address field is set to “Any IPv4 Address” you might have issues connected with the intended server; if you have more than one server, be sure to select the correct one in the **IP address** drop-down list.

Managing Certificates

To manage certificates, navigate to the server in your left navigation and click **Services**.

- Click **New** to add a new certificate.
- Click **Import** to import a certificate.

- Update, export or delete a certificate on the list by clicking on the appropriate **link** next to the certificate.



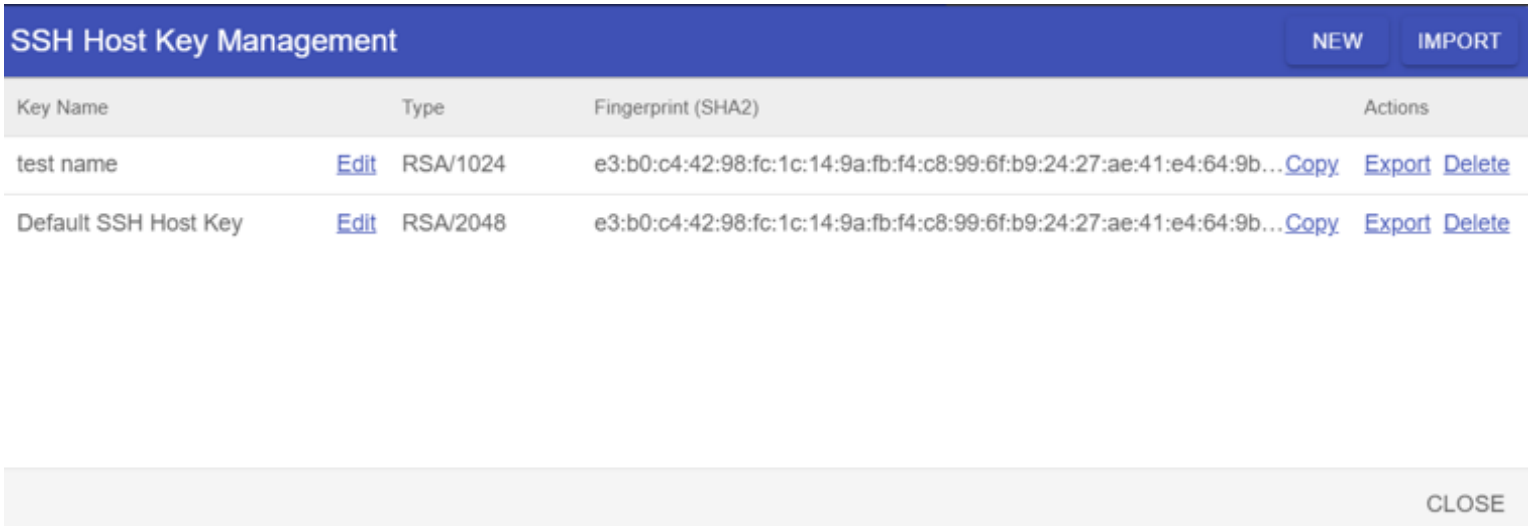
- **Explicit FTP/S(AUTH TLS):** This option allows TLS authentication for a secure connection.
- **Implicit FTP/S:** This option enforces TLS authentication for a secure connection.
- **IPv6:** This option allows IPv6 addresses.
- **Implicit IP Address:** Select the **IP address** that this server will be listening on for implicit connections.
- **Implicit Port:** Select the **port** for implicit connections. Default port is 990 for implicit connection.
- **Allow PROT P/PROT C:** This refers to the data transfers. P is protected and encrypted while C is clear and unencrypted.
- **Allow CCC:** This option allows a clear command channel. Once the server authenticates securely it can revert back to clear plain text.
- **Certificate:** Select one available **certificate**.
- **TLS Versions:** Select which **security protocols** you will allow on the server.

SSH and SFTP Configuration

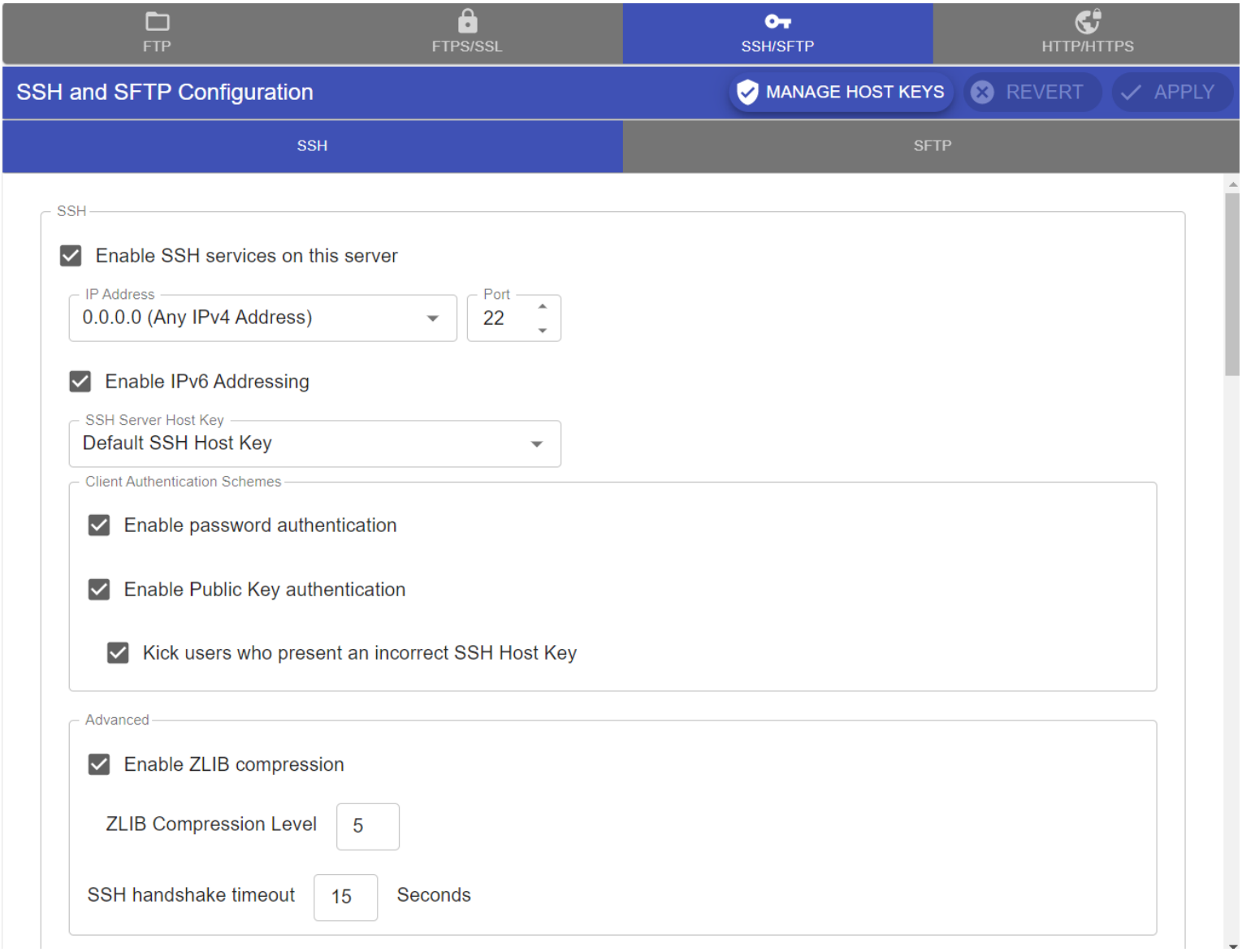
SFTP is another file transfer protocol which uses FTP over SSH. This is a secure protocol which uses a host key to encrypt the traffic and a private key to decrypt traffic. This can be used with internal or external users since it is a secure connection.

In this tab, you will find all of the settings to configure SFTP protocol for your server.

You can click on **Host Key Management** and create, copy, delete, import, or export SFTP keys.



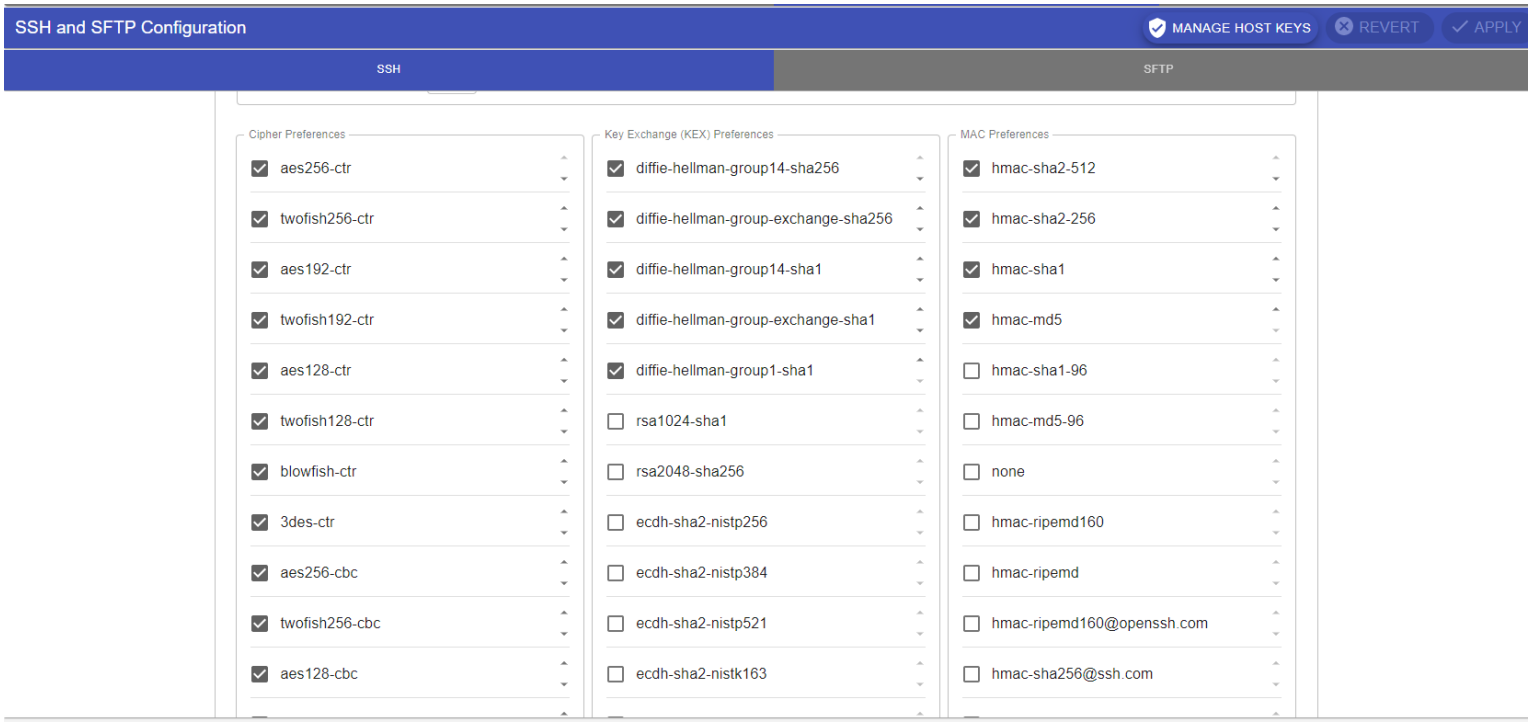
On the SSH tab, you will find the following settings:



- **Enable SSH services on this server:** Enables SFTP protocol on this server.
- **IP Address/Port:** Specify the IP address and port this server will be listening on for SFTP connections.
- **Enable IPv6 Addressing:** Allows IPv6 support.
- **SSH Server Host Key:** Specify the host key for this server.
- **Enable password authentication:** Allow users to authenticate via a password.

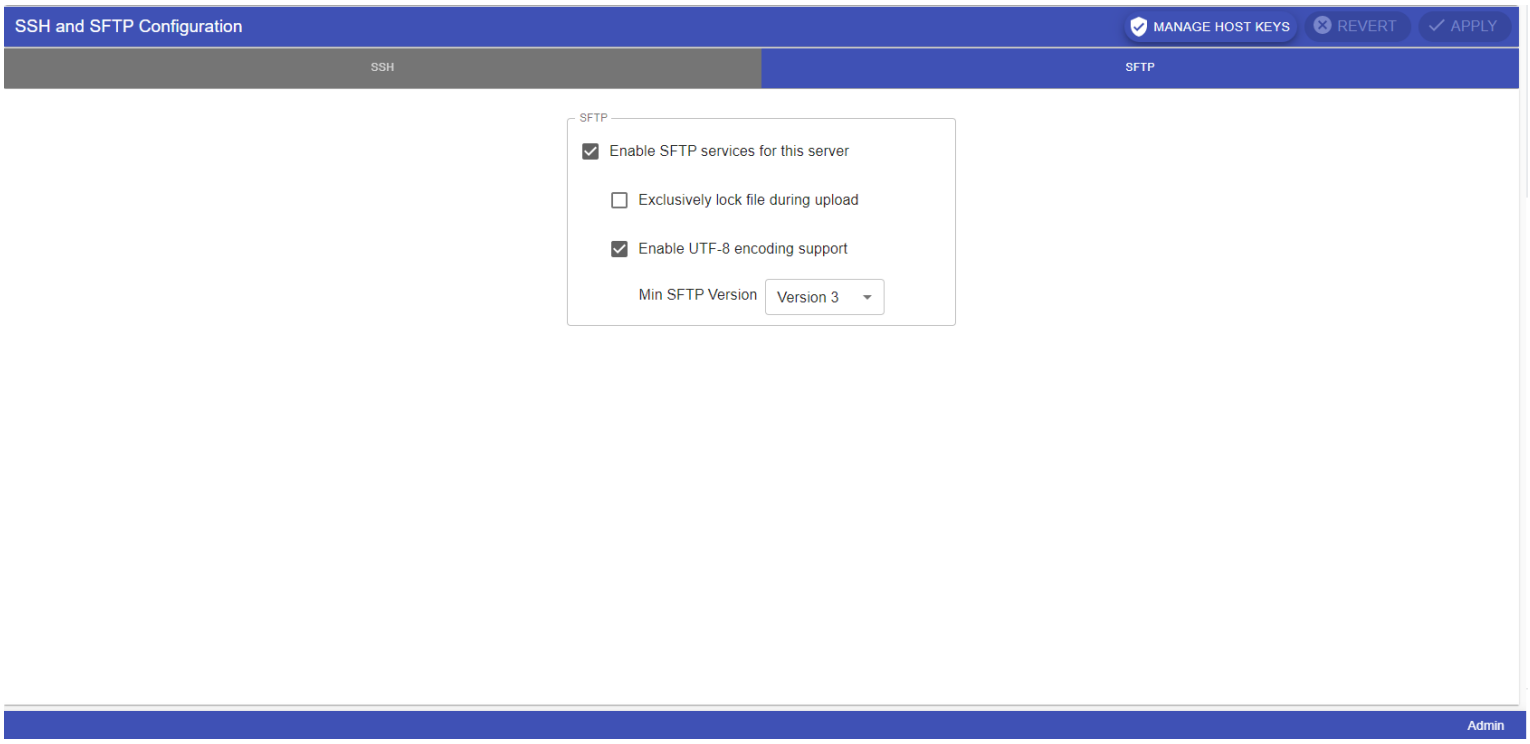
- **Enable Public Key Authentication:** Allows users to authenticate via a public key.
- **Kick users who present an incorrect SSH Host Key:** This option will check to see if a user connecting to the server presents an incorrect password and it will reject their connection.
- **Enable ZLIB compression:** Enables the use of the ZLIB library for compression or decompression of files.
- **SSH handshake timeout:** Specify the amount of time in seconds that the server will wait until it times out the handshake.

The following section allows you to set your Cipher Preferences, Key Exchange (KEX) Preferences, and MAC Preferences to make your server more secure.



When a user tries to connect, the SSH handshake will complete only if both the server and client have at least one of each of the above sections in common. If one of the above enabled settings are not supported by one of the two parties, then the SSH handshake will terminate and the connection will not be completed.

Under the **SFTP** tab, you will find the following settings:



- **Enable SFTP services for this server:** Allows you to enable the SFTP protocol on this server.
- **Exclusively lock file during upload:** Allows the server to have an exclusive lock on the file during upload.
- **Enable UTF-8 encoding support:** UTF-8 is an encoding system for Unicode. It can translate any Unicode character to a matching unique binary string, and can also translate the binary string back to a Unicode character. This is the meaning of “UTF”, or “Unicode Transformation Format.”
- **Min SFTP Version:** You can specify which version the server will support. Different versions of SFTP will support different requirements for initialization, attributes, etc.

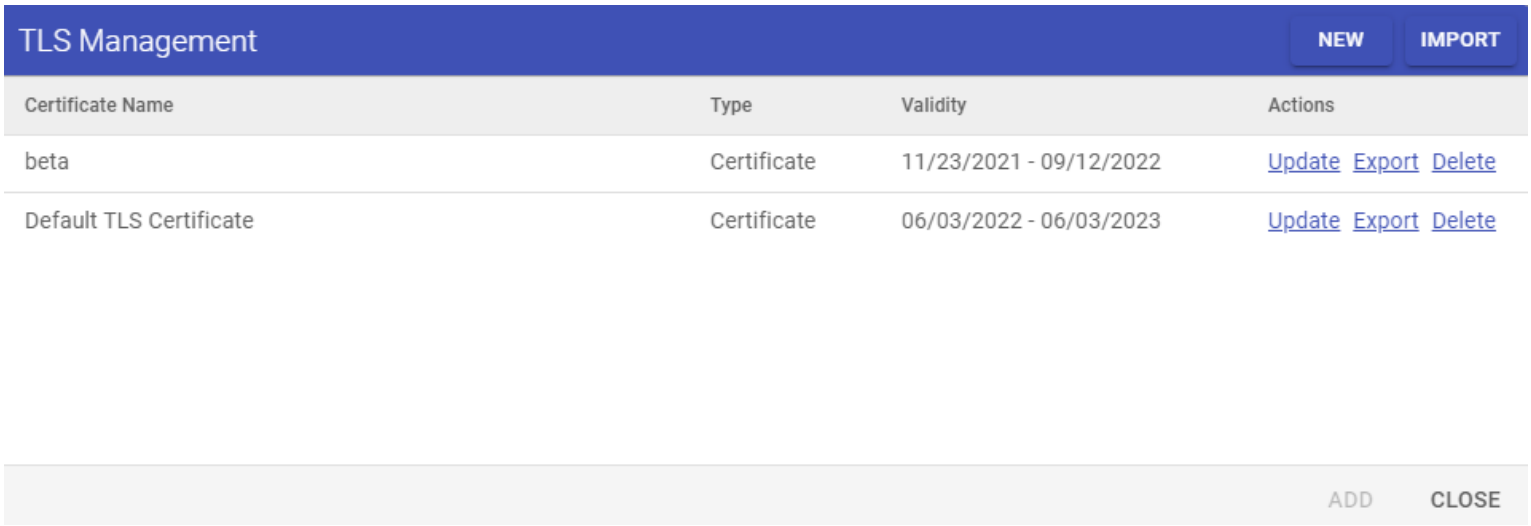
Hyper Text Transfer Protocol (HTTP) and HTTPS Configuration

You can access the server via a Web browser using an unsecure connection via HTTP or using a secure connection via HTTPS, which is encrypted. It is okay to use HTTP if internal users are accessing the WEBUI, but if external users are going to connect to the server, HTTPS should be used to ensure a secure connection.

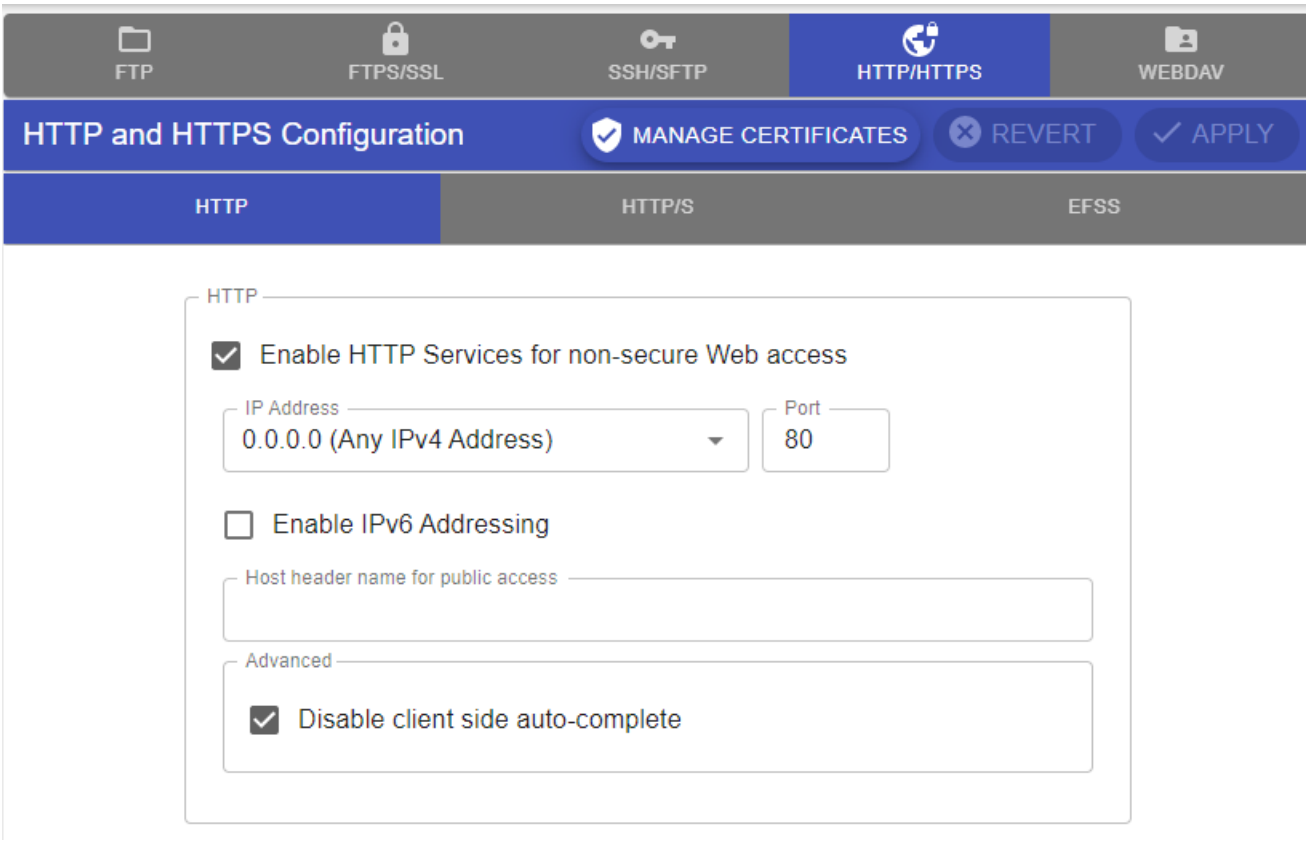
On this tab, you will be able to enable HTTP and HTTPS protocol to be able to access this server via Web browser.

To manage certificates, navigate to the server in your left navigation and click **Services**.

- Click **New** to add a new certificate.
- Click **Import** to import a certificate.
- Update, export, or delete a certificate in the list by clicking on the appropriate **link** next to the certificate.

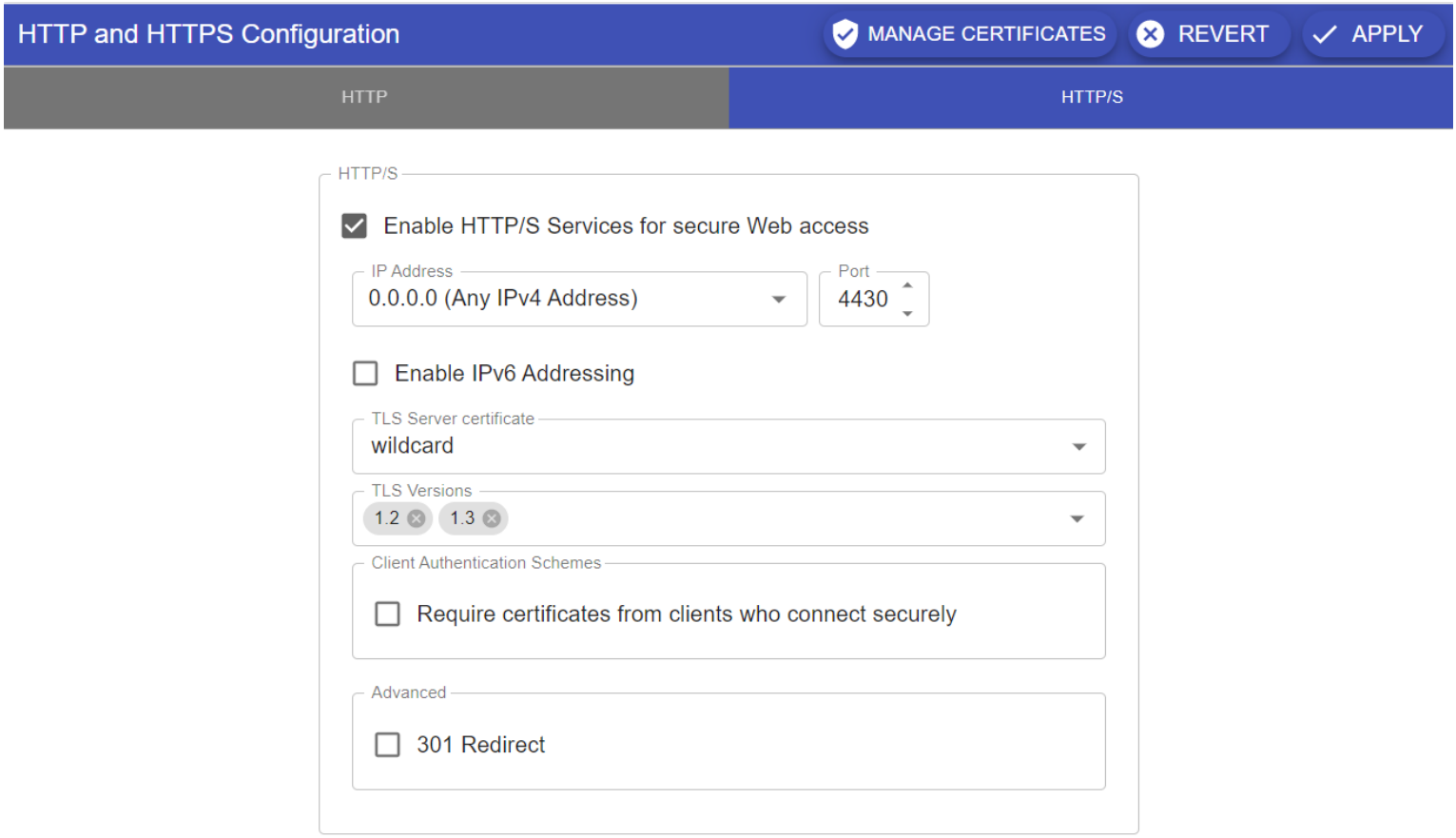


To configure HTTP on this server, you have the following settings:



- **Enable HTTP Services for non-secure Web access:** This option turns on the HTTP protocol on this server.
- **IP Address/Port:** Specify the IP address and port this server will listen on for HTTP connections.
- **Enable IPv6 Addressing:** Allows support for IPv6 addresses.
- **Host header name for public access:** Provide the WAN name for public access to this server.
- **Disable client side auto-complete**

To configure HTTPS on this server, you have the following settings:

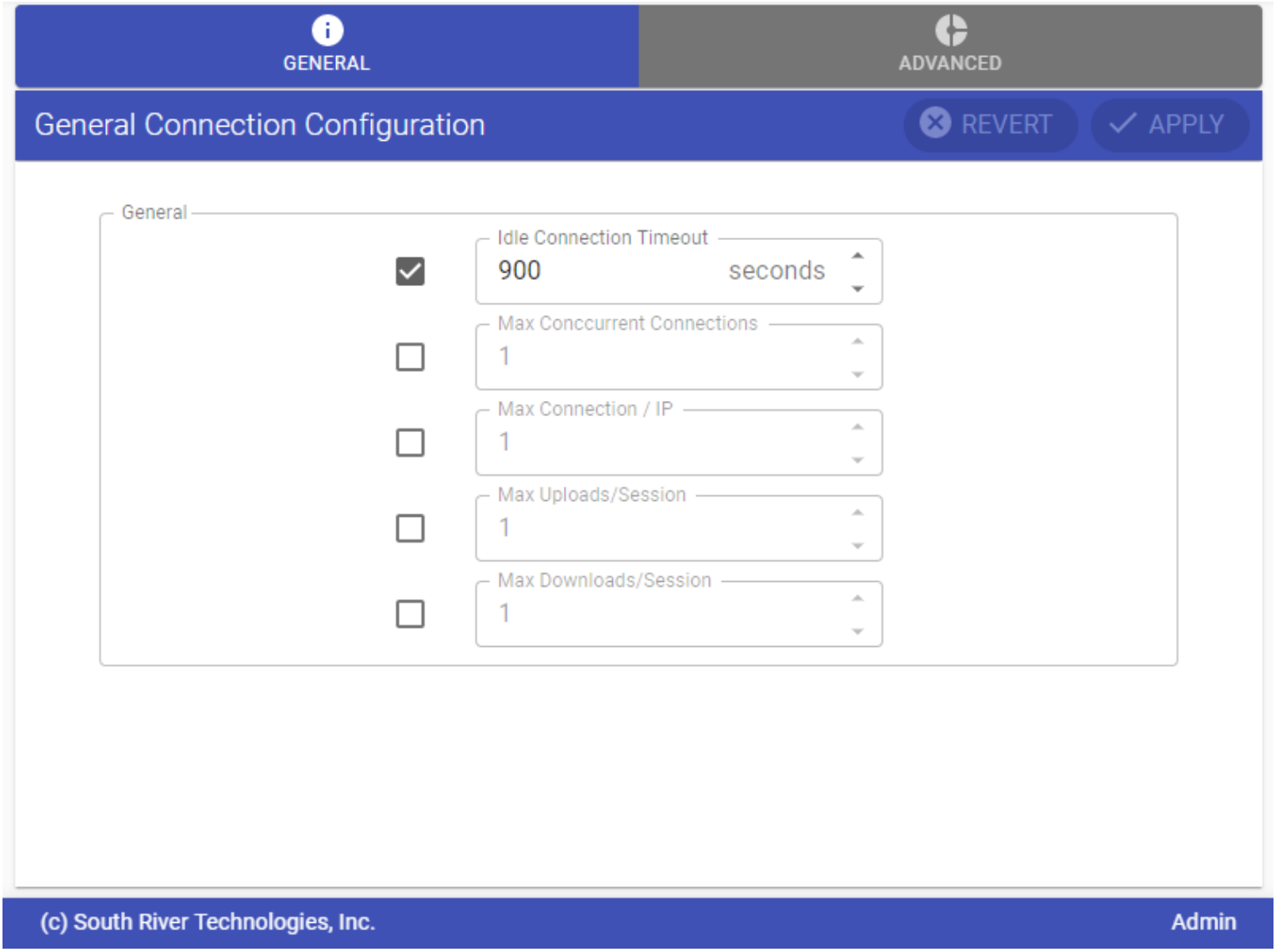


- **Enable HTTPS Services for secure Web access:** This option turns on HTTPS protocol on this server.
- **IP Address/Port:** Specify the IP address and port this server will listen on for HTTPS connections.
- **Enable IPv6 Addressing:** Allow support for IPv6 addresses.
- **TLS Server certificate:** Select the **SSL certificate** that will be applied to this server to make the connection secure.
- **TLS Versions:** Select the **security protocols** you will allow on this server.
- **Require certificates from clients who connect securely:** This option will ensure any clients connecting have to present a valid certificate in order to authenticate with this server.
- **301 Redirect:** Redirect connections coming in from HTTP to HTTPS to ensure a secure connection.

Connection Settings

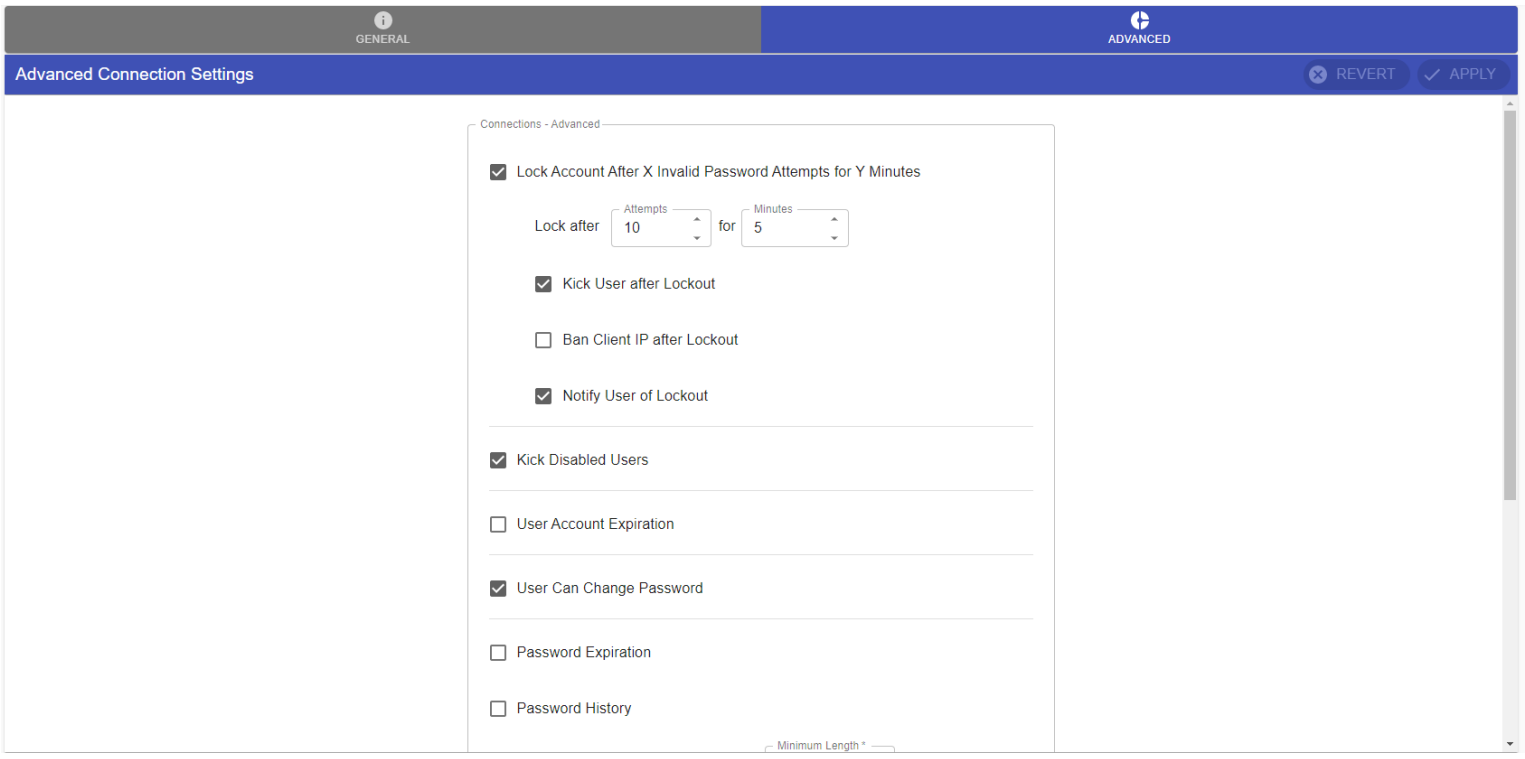
You can configure general connection settings on the Connections page. In this section, you will see several different settings which will allow you to apply limits to user connections that can help you maintain your server health and performance.

Under the General tab, you will find the following settings:



- **Idle Connection Time-out:** The maximum amount of time, in minutes, the server will wait before dropping a user due to inactivity.
- **Max Concurrent Connections:** The total number of concurrent sessions that may be established by a single user at one time.
- **Max Connections/IP:** The total number of concurrent connections a user can establish from any given IP address at the same time.
- **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.

Under the Advanced tab, you will find the following settings:



- **Lock account after X invalid password attempts for Y minutes:** When enabled, the user account will be disabled after the specified number of consecutive incorrect password attempts for the specified number of minutes
- **Kick user after lockout:** This option will kick the user out of their current session once it is locked out.
- **Ban Client IP after Lockout:** This option will place the client IP address in the IP Ban list and will reject any further connections coming from that IP address.
- **Notify user of Lockout:** Will send out an email notification to the user's email address if specified under the user account letting them know that their account has been locked.
- **Kick disabled users:** Will kick any connection from a user account which is in a disabled state in Titan FTP Server.
- **User Account Expiration:** Enable feature that will expire user accounts after the specified time frame.
- **User can change password:** This allows the users the ability to change their own passwords.
- **Password Expiration:** Password will expire after a specified time period.
- **Password History:** This option will not allow users to re-use passwords for added security.
- **Force Complex Passwords:** Enable the ability for the administrator to enforce password complexity requirements for all users.
- **Prevent username use:** This will not allow a user to try and set their password to their username.
- **Require Uppercase character:** Require a user to include an uppercase character in their password.
- **Require lowercase character:** Require a user to include a lowercase character in their password.
- **Require a numeric digit 0..9:** Require a user to include a numeric digit from 0 to 9 in their password.

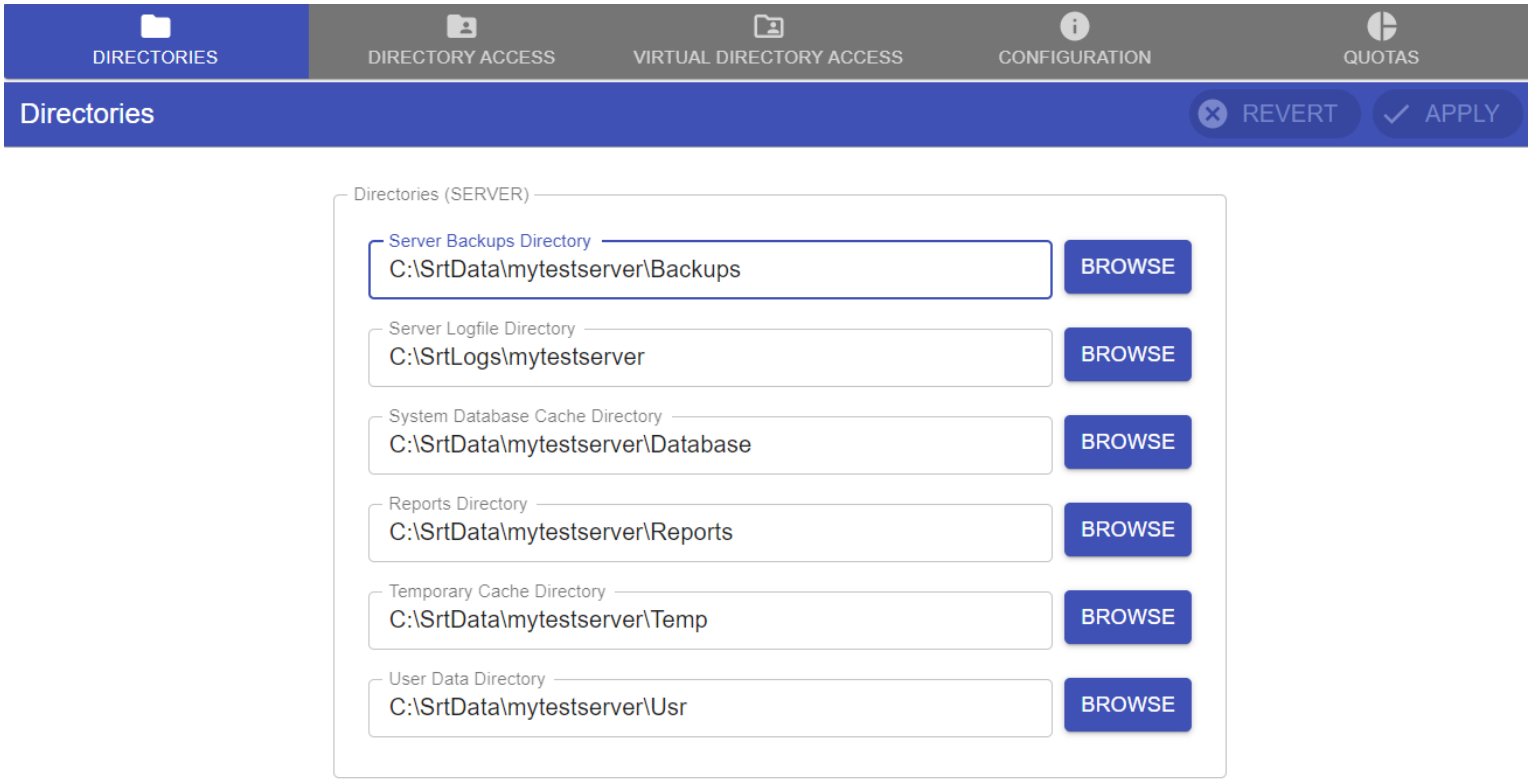
- **Require a special character:** Require a user to include a special character specified under the Special Characters field.

Files and Directories

In this section of the server administration, you will find the directory paths for all of the important server data, directory access, virtual folders, and other settings.

Under the **Directories** tab, you will find the default locations of the different server data. You can modify any of the below directories to point toward your location of choice by simply changing the path, or clicking **Browse** and then **Apply**.

If changing to a UNC file share, make sure Titan FTP Server has access to the desired location.

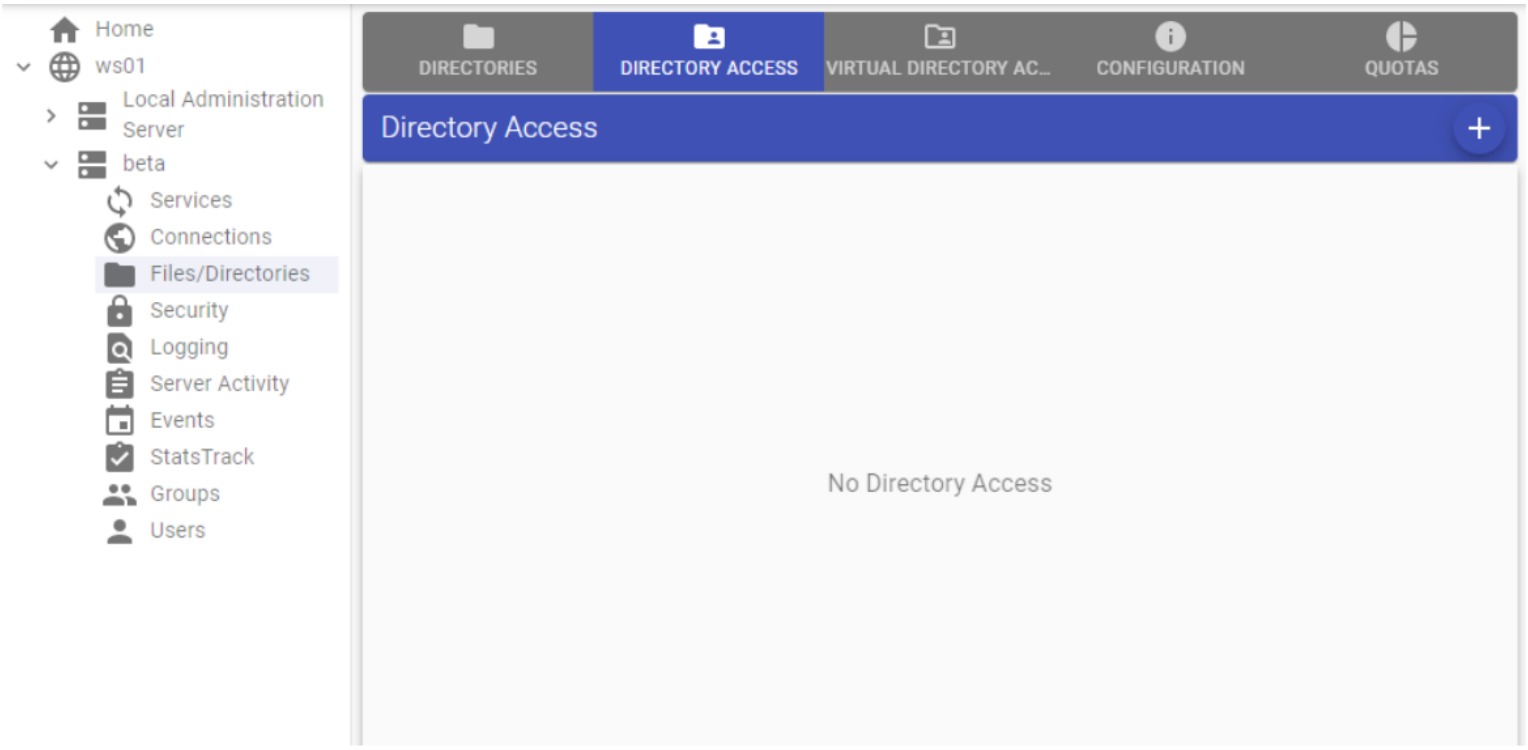


- **Server Backups Directory:** This is where the server backups are stored.
- **Server Logfile Directory:** This is where the server log files are stored.

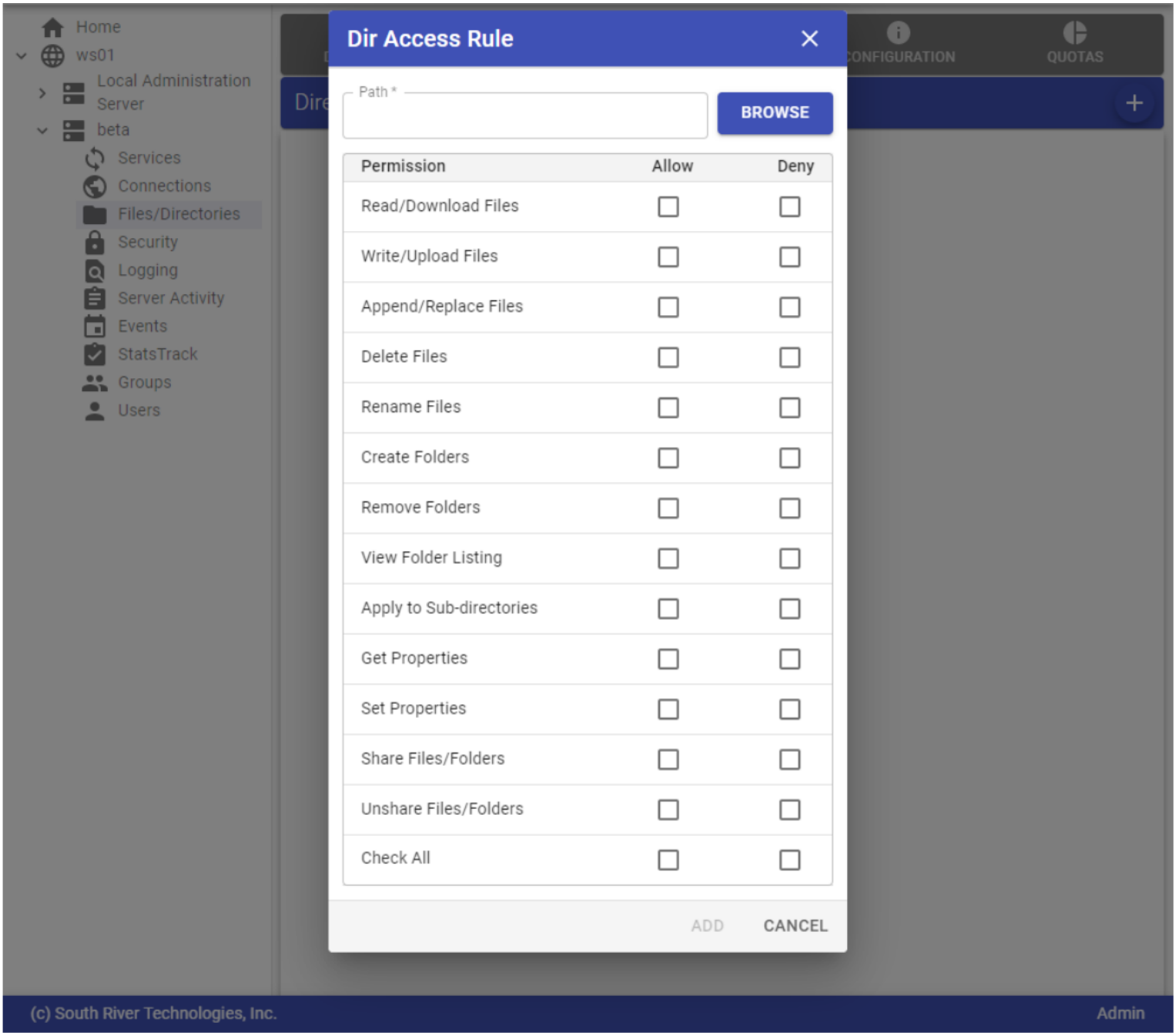
- **System Database Cache Directory:** This is where temporary files are stored as cache to improve response time and performance.
- **Reports Directory:** This is where the default reports included in Titan FTP Server are stored to be able to query the database and pull the desired information.
- **Temporary Cache Directory:** This is where temporary files are stored as cache to improve response time and performance.
- **User Data Directory:** This is where all of the user data is stored. This includes all of the user home folders and where all users will upload and download files from.

Directory Access

Use the **Directory Access** tab to grant or deny access to folders on the server. If you want to configure the different directories to point to paths that are not accessible by default, you can add them here on this tab to make sure Titan FTP Server can access them as needed.



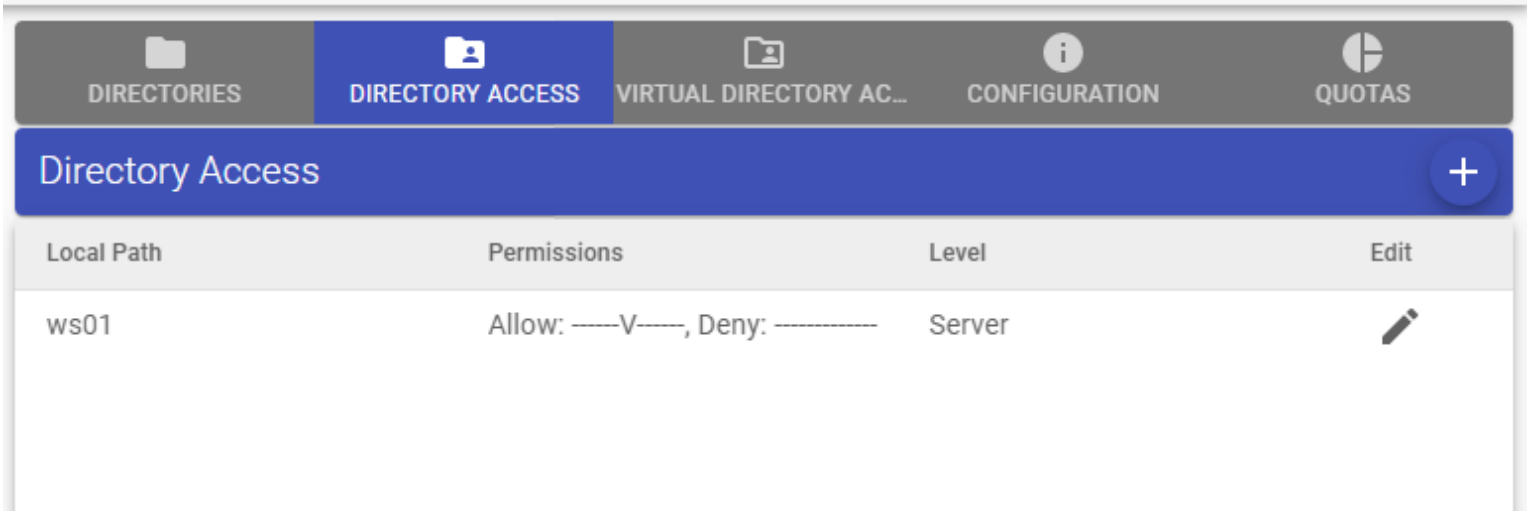
You can also configure the permissions to any of the directories added above, as seen below:



The permissions available for configuration are as follows:

- **Read/Download Files:** Allow or deny users to read/download files from this directory.
- **Write/Upload Files:** Allow or deny users to write/upload files to this directory.

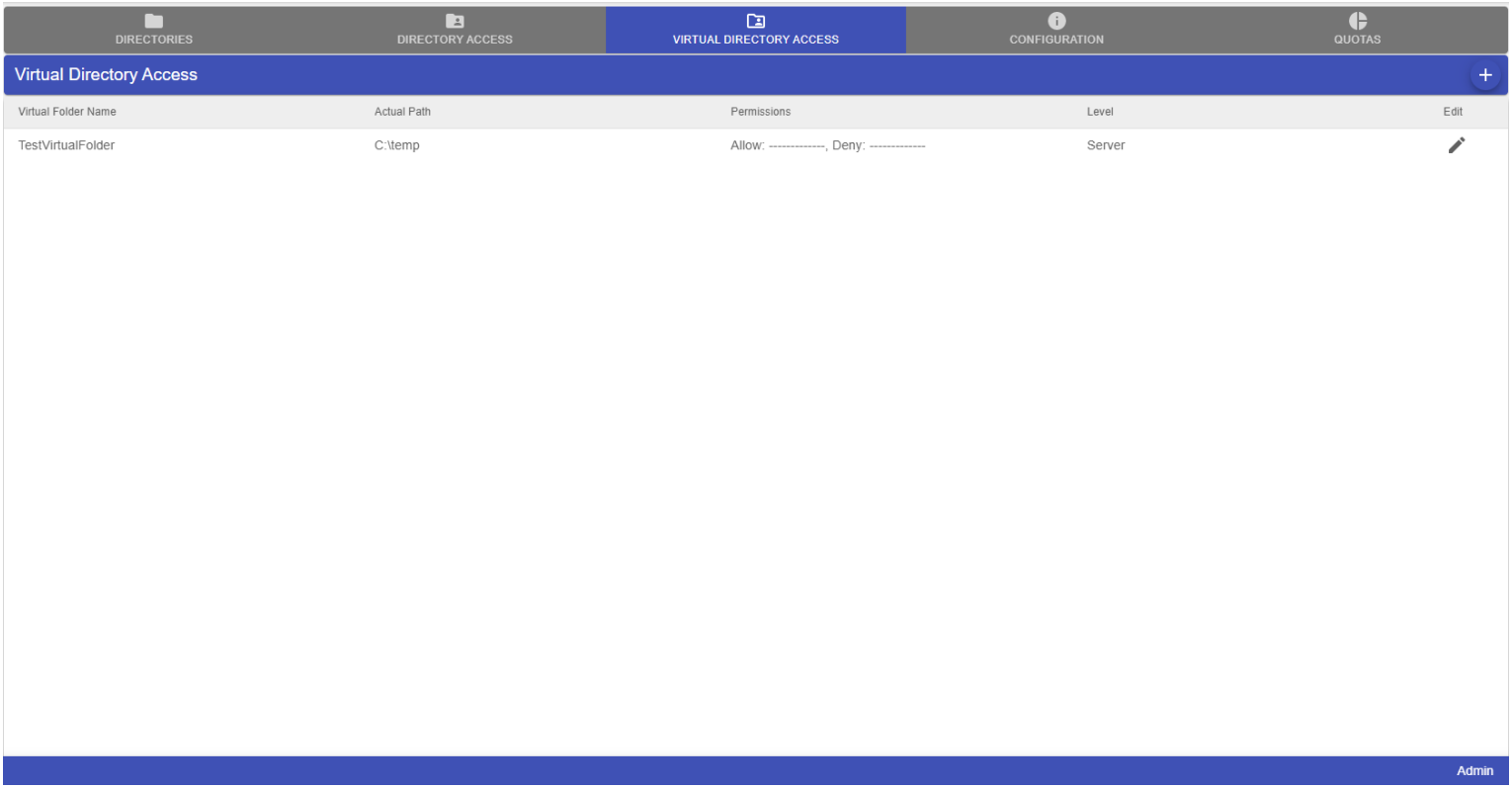
- **Append/Replace Files:** Allow or deny users to append/replace files in this directory.
- **Delete Files:** Allow or deny users to delete files in this directory.
- **Rename Files:** Allow or deny users to be able to rename a file in this directory.
- **Create Folders:** Allow or deny the ability for users to create folders in this directory.
- **Remove Folders:** Allow or deny the ability for users to remove folders in this directory.
- **View Folder Listing:** Allow or deny users to be able to view the contents of this folder.
- **Apply to Sub-directories:** Allow or deny these settings on sub-directories of this parent folder.
- **Get Properties:** Allow or deny users to be able to get properties from files in this folder.
- **Set Properties:** Allow or deny users to be able to set properties to files in this folder.
- **Share Files/Folders:** Allow or deny the ability for users to share files or folders from this directory.
- **Unshare Files/Folders:** Allow or deny the ability for users to be able to unshare files/folders in this directory.
- **Check All:** Will either allow all of the above permissions or deny all.



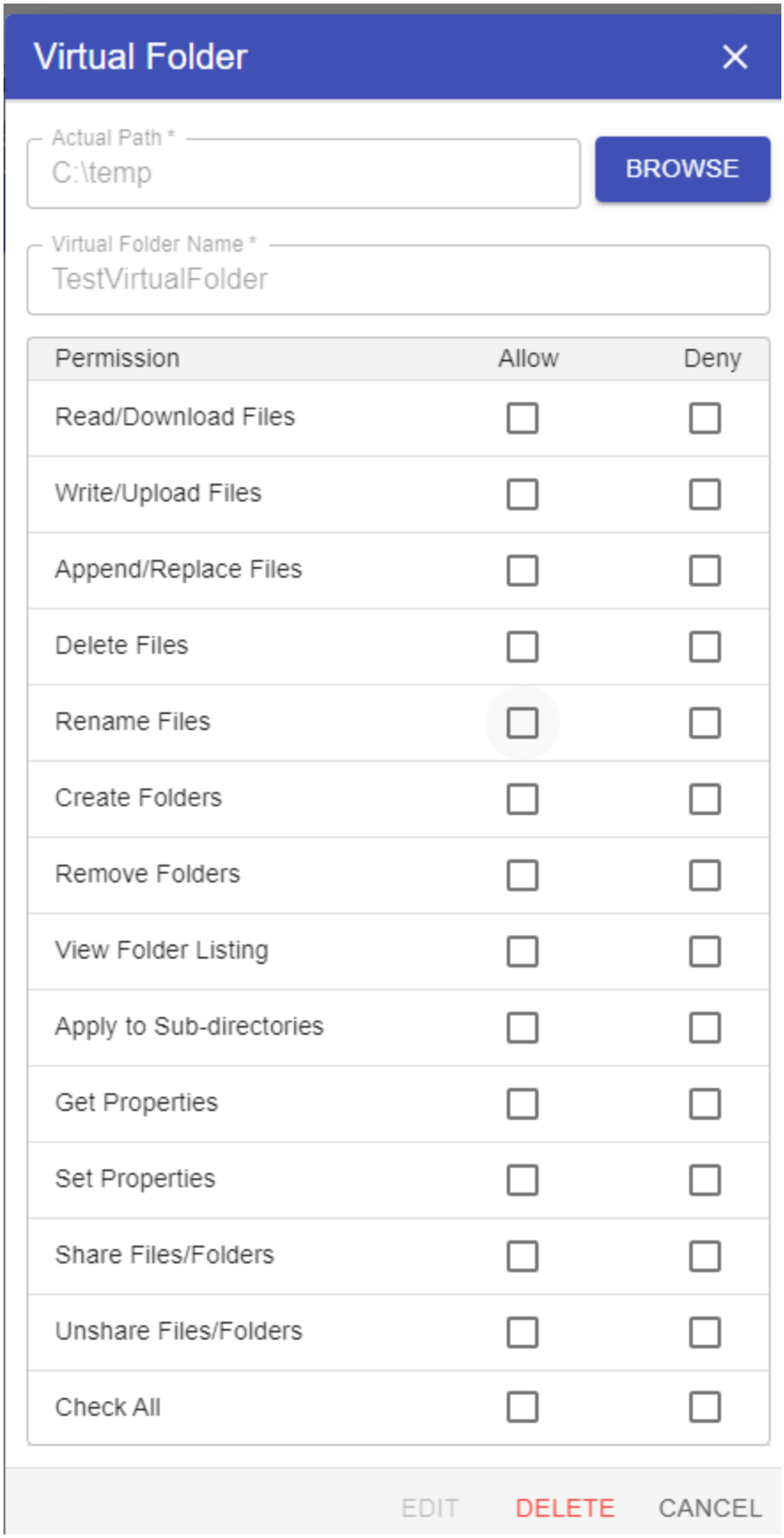
Virtual Directory Access

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 like symbolic links. Virtual Folders are commonly used to give users access to network shares or folders from different file servers and display them in their home folder as just another subfolder.

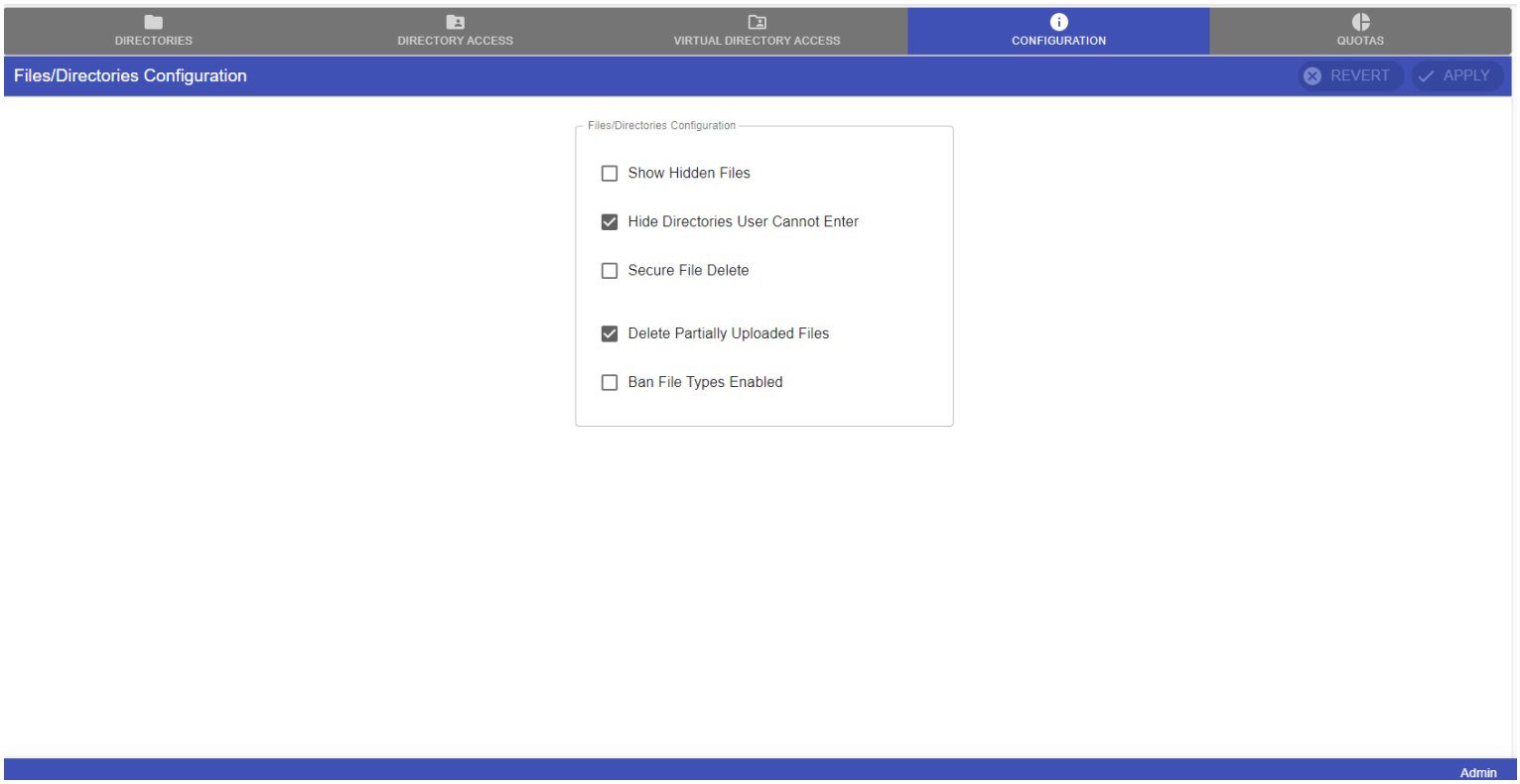


The permissions available for configuration are as follows:


Virtual Folder
Actual Path *
C:\temp
BROWSE
Virtual Folder Name *
TestVirtualFolder
Permission
Allow
Deny
Read/Download Files
Write/Upload Files
Append/Replace Files
Delete Files
Rename Files
Create Folders
Remove Folders
View Folder Listing
Apply to Sub-directories
Get Properties
Set Properties
Share Files/Folders
Unshare Files/Folders
Check All
EDIT
DELETE
CANCEL

- **Read/Download Files:** Allow or deny users to read/download files from this directory.
- **Write/Upload Files:** Allow or deny users to write/upload files to this directory.
- **Append/Replace Files:** Allow or deny users to append/replace files in this directory.
- **Delete Files:** Allow or deny users to delete files in this directory.
- **Rename Files:** Allow or deny users to be able to rename a file in this directory.
- **Create Folders:** Allow or deny the ability for users to create folders in this directory.
- **Remove Folders:** Allow or deny the ability for users to remove folders in this directory.
- **View Folder Listing:** Allow or deny users to be able to view the contents of this folder.
- **Apply to Sub-directories:** Allow or deny these settings on sub-directories of this parent folder.
- **Get Properties:** Allow or deny users to be able to get properties from files in this folder.
- **Set Properties:** Allow or deny users to be able to set properties to files in this folder.
- **Share Files/Folders:** Allow or deny the ability for users to share files or folders from this directory.
- **Unshare Files/Folders:** Allow or deny the ability for users to be able to unshare files/folders in this directory.
- **Check All:** Will either allow all of the above permissions or deny all.

Under the **Configuration** tab, you will find the following settings:

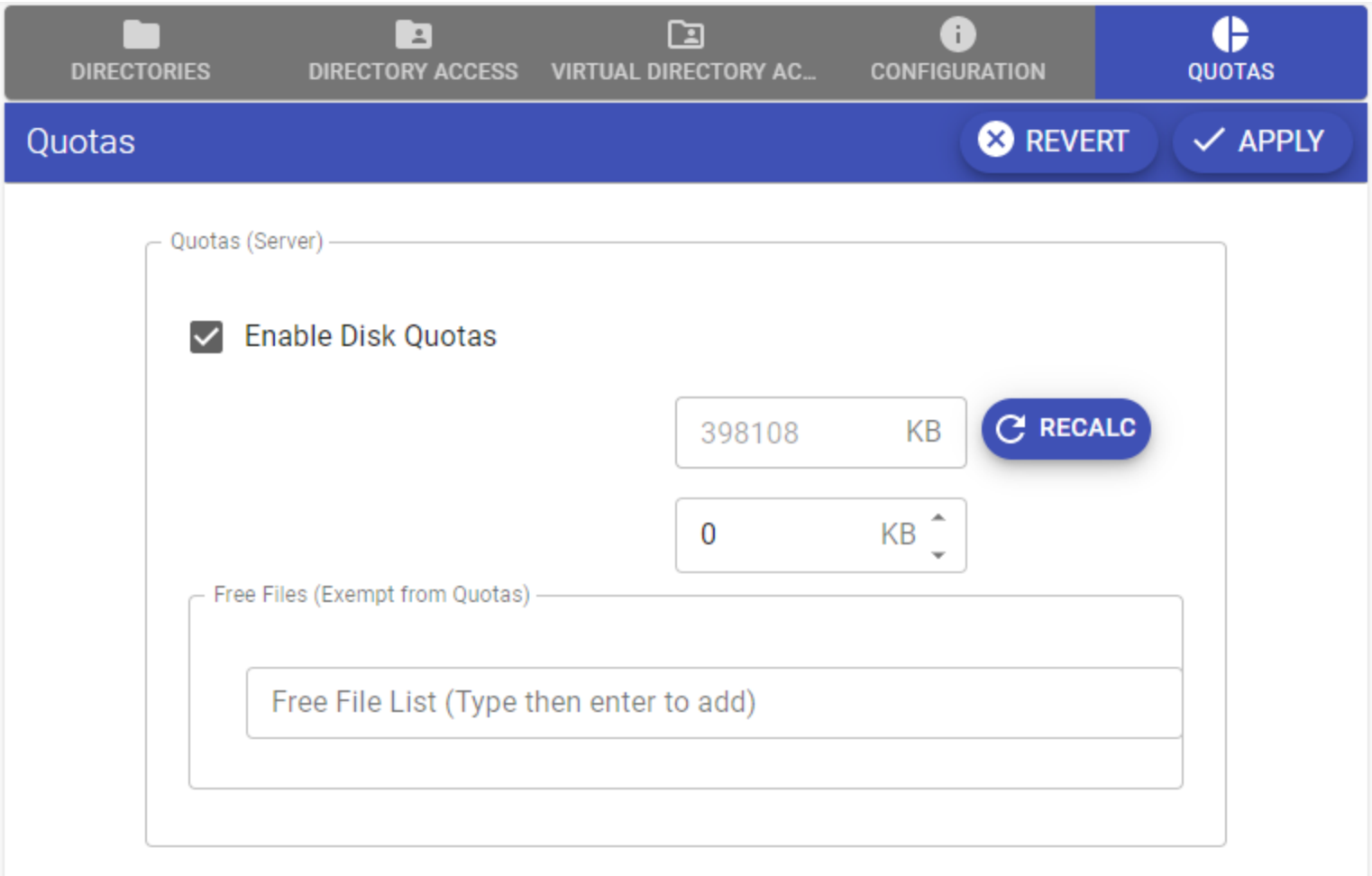


- **Show Hidden Files:** Allow users to see files that are hidden.
- **Hide Directories User Cannot Enter:** Hide any directories that the user does not have access to.
- **Secure File Delete:** Enable the secure deletion of files.
- **Delete Partially Uploaded Files:** Any files that are not uploaded in their entirety will be deleted if this option is enabled.
- **Ban File Types Enabled:** This option will deny upload of files with the extension specified in the Ban File Types field.
- Write Cache Enabled

Quotas:

Titan MFT Server's File Quotas allow you to set limits on the amount of disk space that you want your users to use. This helps in avoiding users sending large files that occupy most or all your disk space. Prevent this by setting the limits you prefer in Titan FTP Server.

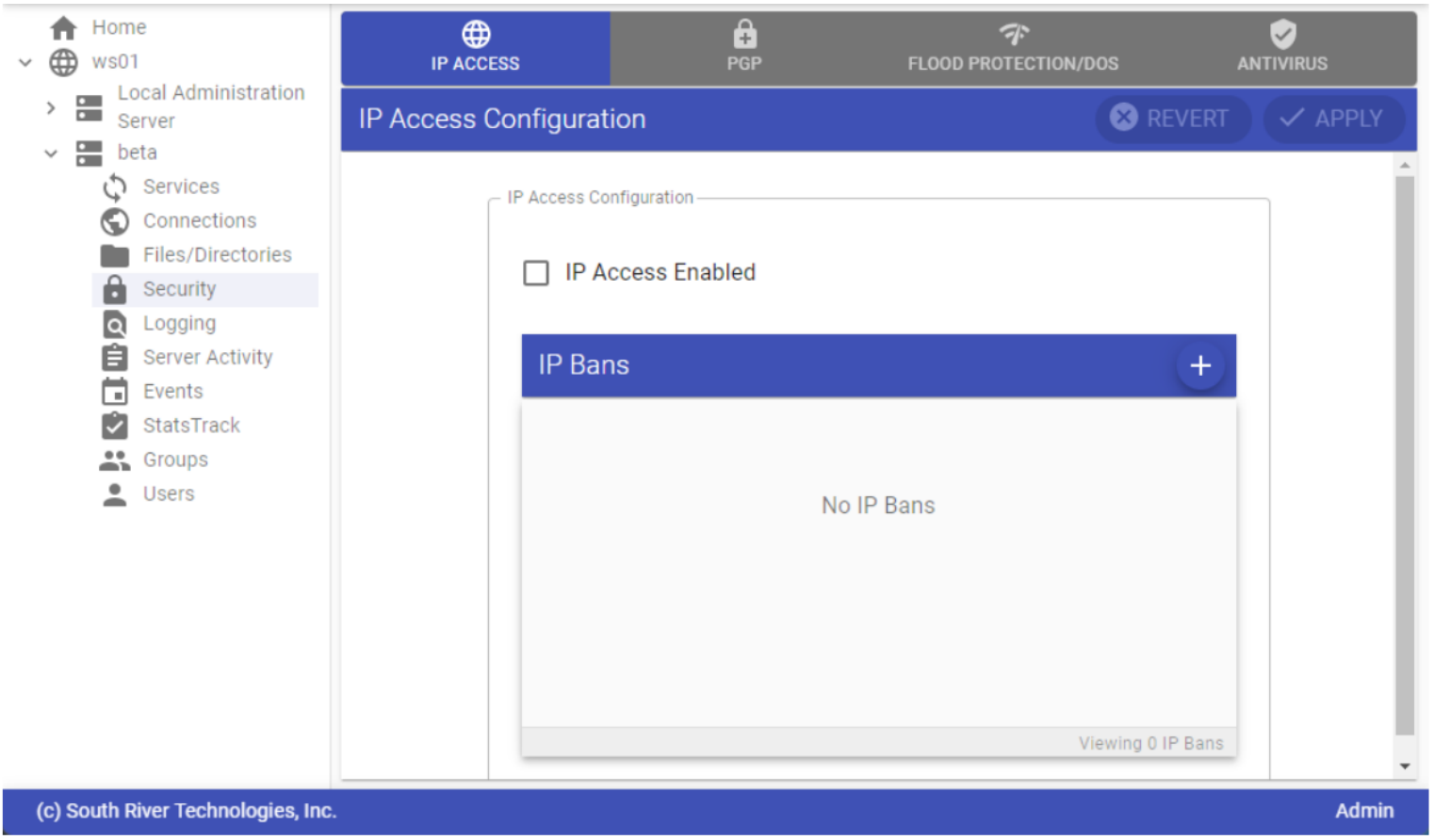
To do this, navigate to the server in your left navigation and click **Files and Directories**. Next, click **Quotas**.



- **Enable Disk Quotas:** This will enable the feature to set disk space limits on the server level.
    - The first field will specify the total disk space limit, while the second field will display the current disk space used.
- **Free Files:** Titan FTP Server allows you to exempt certain files from counting against your maximum file limits, applying to all other documents only.

Security

This section focuses on the configuration settings that will help secure access to the server, maintain integrity of uploaded files, and thwart Denial of Service attacks.



IP Access

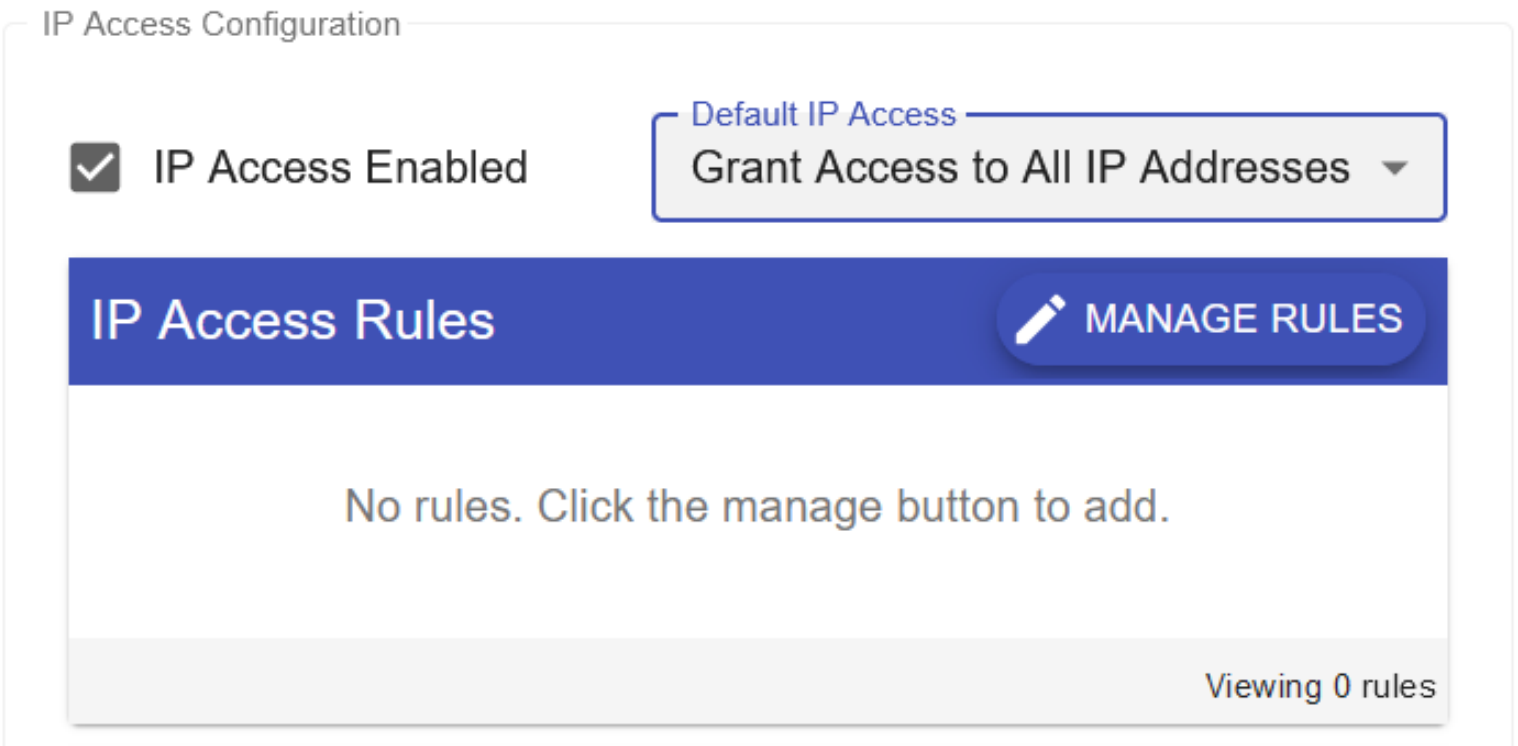
The IP Access setting provides an administrator a second layer of security by allowing them to control the source IP address(es) that authorized users can connect from. The Administrator can either lock down access to the server by certain source IP addresses or allow access from anywhere. By default, this set-

ting is disabled and is set to allow All IP addresses to access the server. The administrator has the option to either allow (whitelist) or deny (blacklist) certain IP addresses.

Alternatively, an administrator can choose to manually ban IP addresses for a certain amount of time, or indefinitely, using the IP Bans feature.

Controlling Access using IP Access: To prevent access to the server and only allow certain entities or all to access the server, the IP Access configuration must be turned on by enabling the IP Access Enabled setting, defining the Default IP Access policy (Grant all or Deny all), and defining optional IP Access Rules.

1. Enable the **IP Access Enabled** setting.
2. Select the **Default IP Access policy** that conforms to your needs:
    a. The Grant Access to All IP Addresses allows everyone to access your server and attempt authentication from anywhere. This type of open access allows the administrator to ensure unhindered access to all authorized end users from anywhere.
    b. Deny Access to All IP Addresses prevents anyone from accessing or authenticating against your server unless explicitly specified using an IP Access rule. This type of locked-down access allows the administrator to ensure access to the server by authorized users from confirmed IP addresses only. All others will be denied access.
3. Optionally, you can create IP Access Rule(s) to complement the selected Default IP Access policy.



Creating IP Access Rules

To create an IP Access Rule:

1. Click on **Managed Rules** and the **plus** icon in the subsequent screen.
2. Fill in the following fields:
    a. **Protocols:** The protocol(s) end users can or cannot use to access the server based on the Allow Access setting. If Allow Access is enabled, then the selected protocol(s) can be used by end users to access the server to transfer files. If Allow Access is disabled, then the selected protocol(s) cannot be used by end users to access the server to transfer files.
    b. **Start IP:** The starting IP address from a range of source IP addresses that is being granted or denied server access. For example, if granting or denying access to all IP addresses ranging

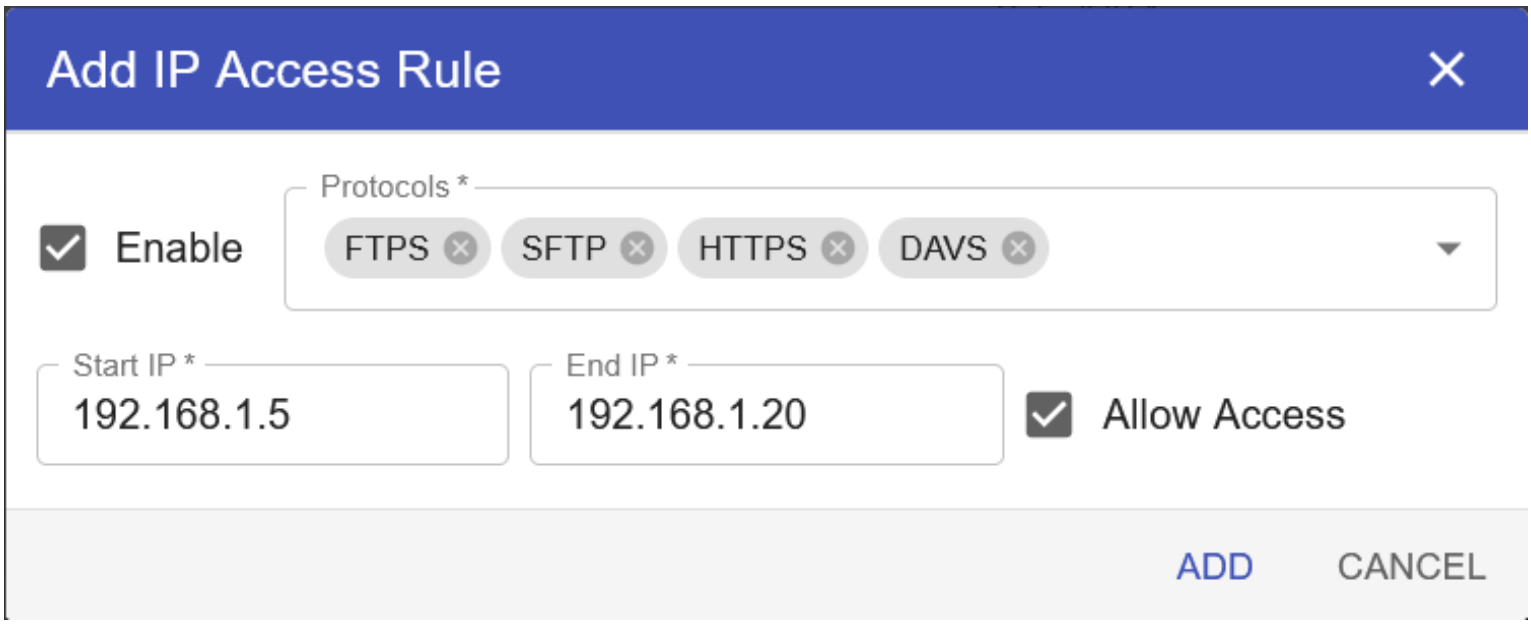
from 192.168.1.5 - 192.168.1.20, the start IP would be 192.168.1.5. If only specifying a single IP address, the Start IP and the End IP can be the same.

c. **End IP:** The ending IP address from a range of source IP addresses that is being granted or denied server access. For example, if granting or denying access to all IP addresses ranging from 192.168.1.5 - 192.168.1.20, the end IP would be 192.168.1.20. If only specifying a single IP address, the Start IP and the End IP can be the same.

d. **Allow Access:** Set IP Access Rule to Grant access (enabled) or Deny access (disabled). If this setting is enabled, then the specified IP address (Start IP & End IP) is granted access to the server using the specified protocol(s). If this setting is disabled (unchecked) then the specified IP address(es) are denied access to the server using the specified protocol(s).

e. **Enabled:** To enable (checked) or disable (unchecked) this specific IP Access rule.

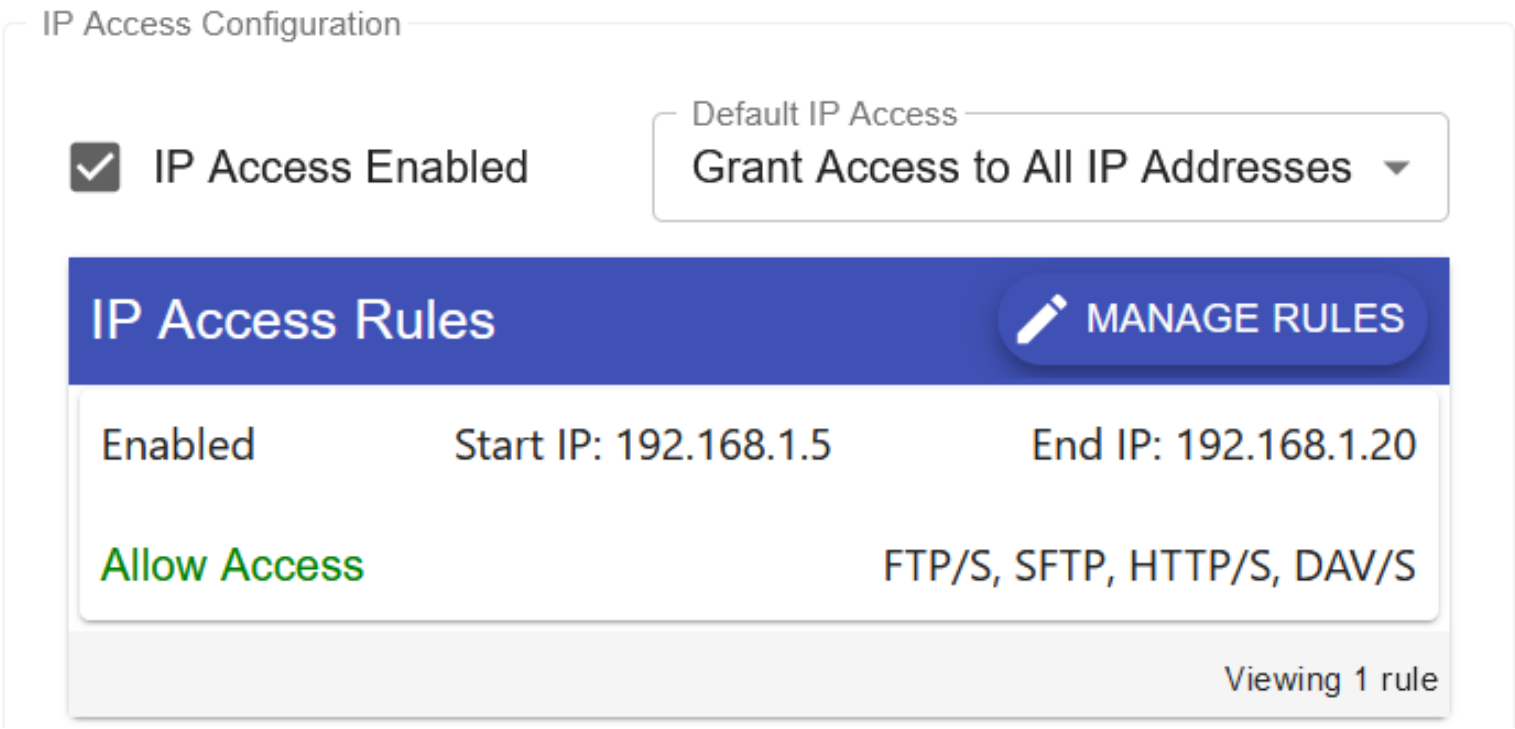
3. Click **Add** to complete setup of new IP Access Rule.



Editing, Disabling or Deleting IP Access Rules

To edit, disable or delete existing IP Access Rules:

1. Confirm the IP Access Enabled setting is enabled (checked).
2. Click on the **Manage Rules** and the **pencil** icon in the subsequent screen.
3. Edit the Protocols, Start IP, End IP, Allow Access, and Enable settings as needed.
4. To disable (turn off) an IP Access Rule, uncheck the **Enable** check box for the rule and click **Close**.
5. To delete an IP Access Rule, click **Delete** and **Confirm Delete** in subsequent screen.



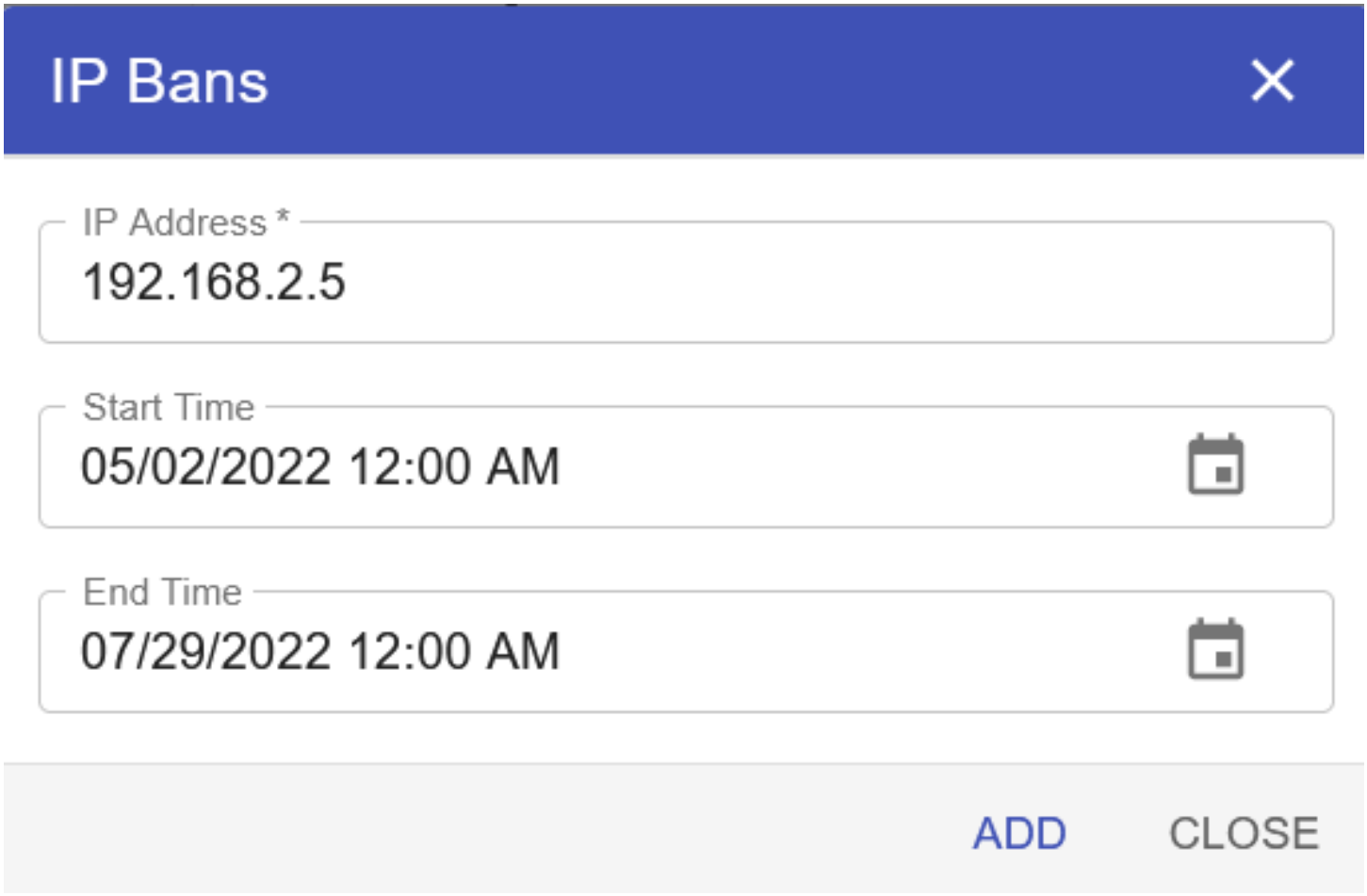
Controlling Access Using IP Bans: An administrator can manually ban an IP address from being able to connect to their server temporarily or indefinitely. Titan FTP Server also automates the adding of an IP address to the IP Ban list based on the status and configuration of the following settings:

- Lock Account settings under Advanced Connection
- Flood Protection/DOS settings

Adding IP Addresses to Ban List

To manually add an IP address to the IP Bans list:

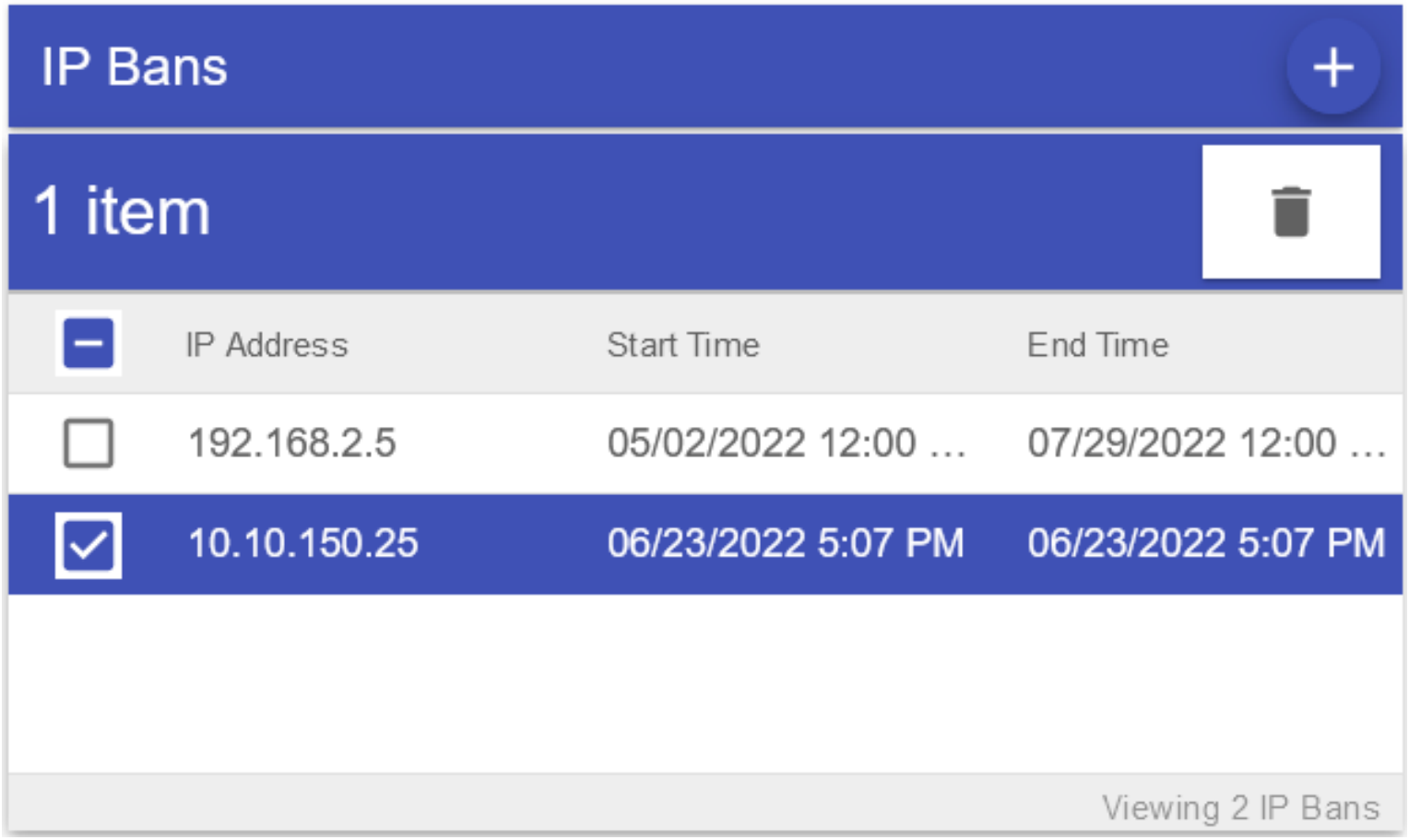
1. Click on the **plus** icon located to the right of the IP Bans table.
2. Fill in the following fields:
    a. **IP Address:** The source IP address of the entity that you want to deny/ban server access.
    b. **Start Time:** The start date and time of when to deny/ban access to the source IP Address.
    c. **End Time:** The date and time of when to end the ban and allow the source IP address to access the server.
3. Click **Add** followed by the **Apply** button located in the top-right corner of the main screen.



Deleting/Removing Banned IP Addresses

To delete or remove IP addresses in the IP Ban list:

1. Click on the **IP address(es)** you want to delete from the list.
2. Click the **trash bin** icon followed by the **Apply** button in the top-right corner of the main screen.



Flood Protection/DoS

The Flood Protection/DoS settings allow an administrator to limit a hacker's ability to flood the server with multiple connections over a short period of time. If left uncontrolled, these types of unwanted connections can produce a Denial of Service (DoS) attack, which can cripple the server and render it unable to properly service existing or new connections.

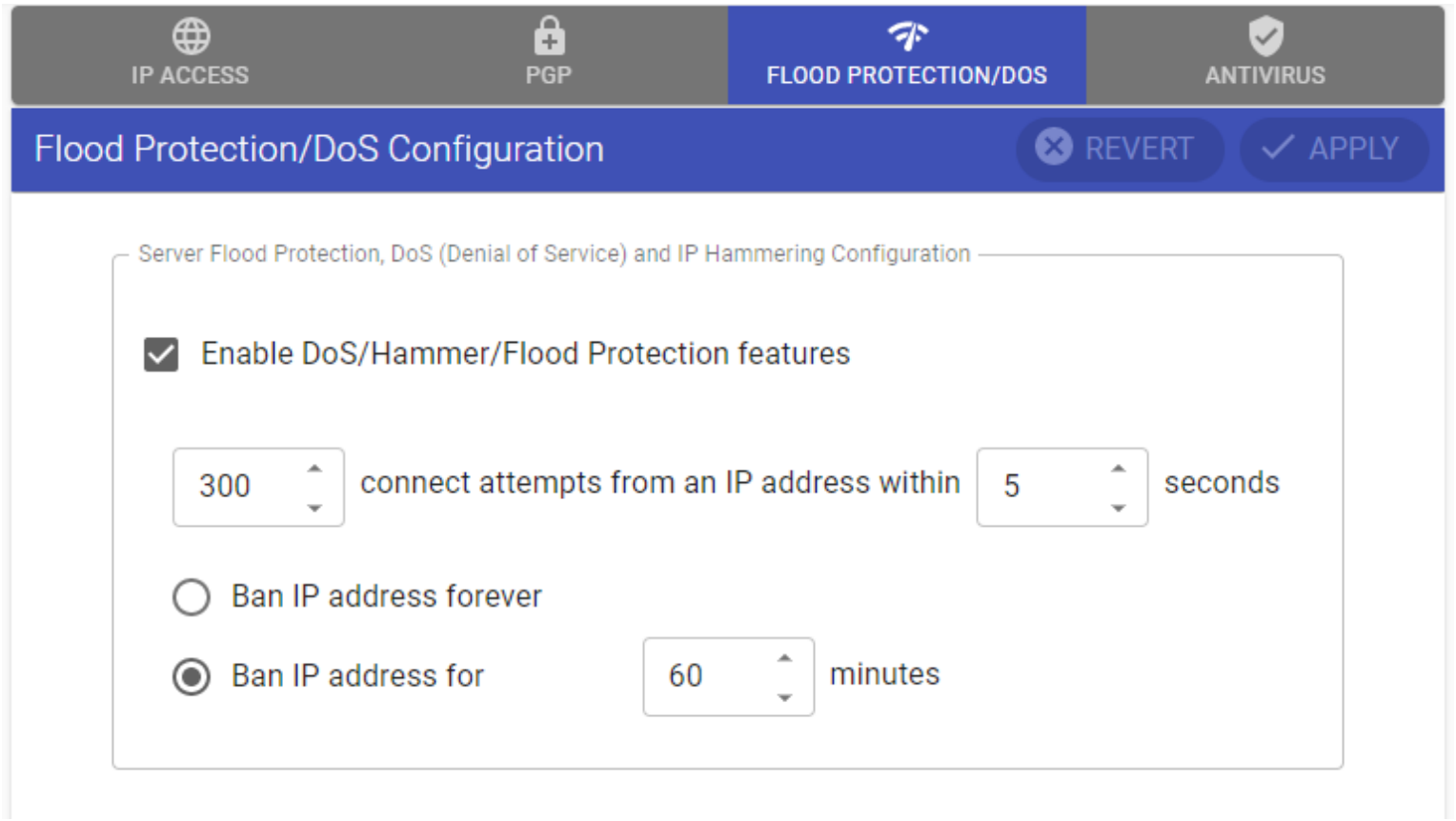
Using the Flood Protection/DoS setting, Titan FTP Server has the ability to track incoming connections based on IP address and time since last connection. If Titan FTP Server finds that a client IP address has

attempted to connect to the Titan server more than X number of times in Y seconds, Titan FTP Server 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. It does this by either temporarily or permanently banning the IP address based on how the Flood Protection/DoS setting was configured.

Note: There are some critical things to consider when configuring the Flood Protection/DoS setting. Accessing the Titan server through the WebUI (HTTP or HTTPS) will generate a much higher ratio of connections/second, due to the client browser using multiple HTTP or HTTPS connections in parallel, per login session, to load and render the contents to the browser. SFTP on the other hand, uses one connection for the life of the login session. Setting a threshold of five connections/second is not likely to trigger a ban over SFTP, but will most likely trigger a ban over HTTP/S. Once an IP is banned, it will be visible in the IP Bans tab of the Admin console.

You can configure the following settings per your needs:

- **Enable DoS/Hammer/Flood Protection features:** Enable this feature to have Titan FTP Server track incoming connections and look for flooding/DoS attacks.
- **X connect attempts 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: 300 connections received from an IP address within five seconds.
- **Ban IP Address Forever:** If this option is selected, Titan FTP Server will add the client IP address to the list of IP addresses that are banned from accessing the server. To view the list, go to the IP Access tab under Security.
- **Ban IP Address for X Minutes:** If this option is selected, connections from the client IP address will be prevented server access 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 60 minutes.



[Placeholder for SRT's AV Server – info and screenshots prior to release in Q3 of 2022]

Logging

This section focuses on the different log settings of the server, along with how to view and manage current and historical logs.

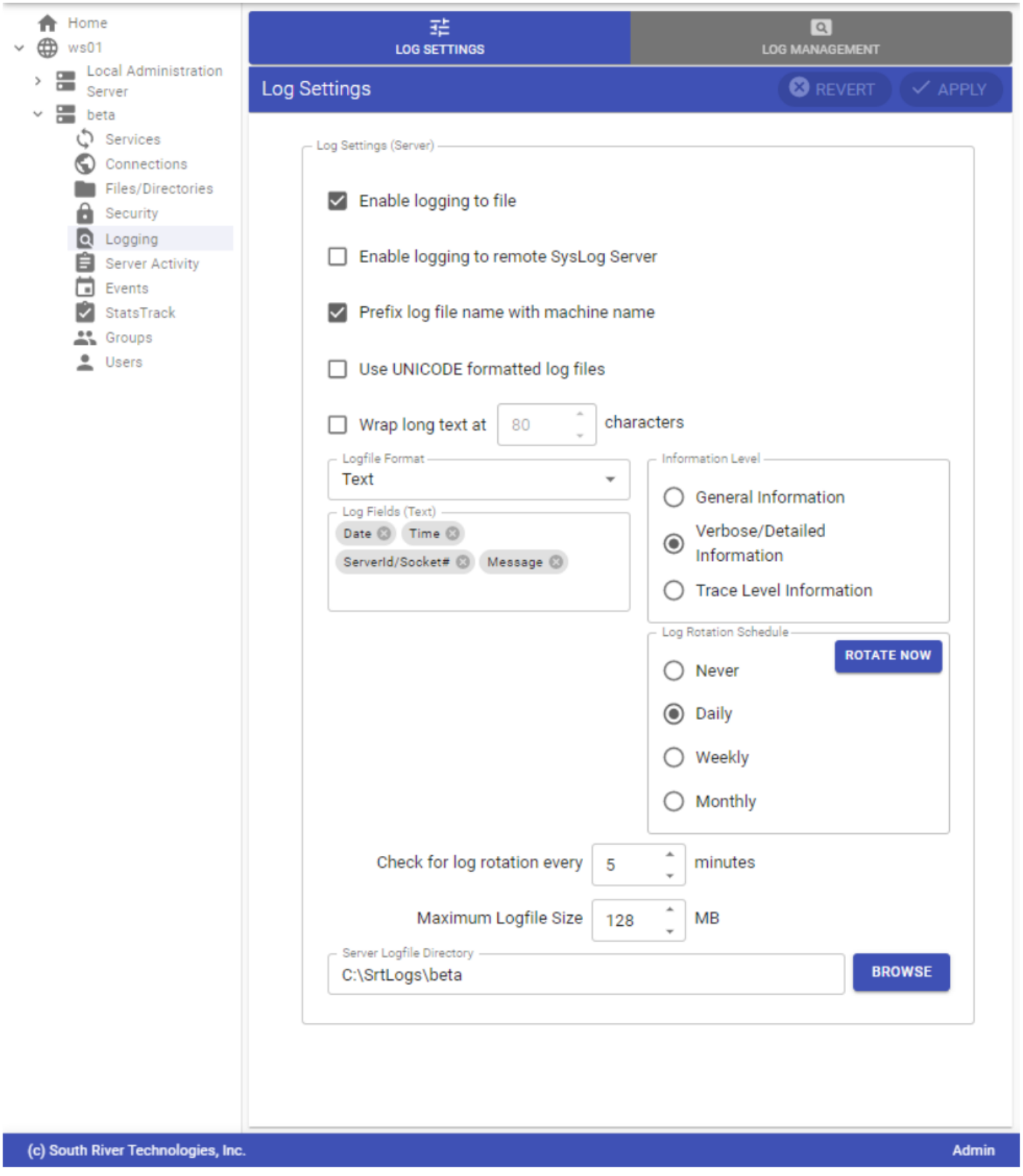
Log Settings

The Log Settings tab is used by an administrator to configure the logging options for the server. Titan FTP Server's Logging allows an administrator to gain valuable insight into their organization's file transfers. It allows an administrator to record and store detailed bits of information related to file server activity and events processed through its Event Management System in a local file or a remote SysLog server.

You can configure the following settings per your needs:

- **Enable logging to file:** This enables logging to a disk file local to the server.
- **Enable logging to remote SysLog Server:** Intensive logging can bog down Titan FTP Server's memory and slow critical file transfer processes. To ease the burden on Titan FTP Server, export files to another database using the SysLog protocol. When this option is enabled, Titan FTP Server will use the SysLog protocol to send formatted log messages to an external logging server, which can then compile these logs in report-generation software or simply store them to a database. Refer to RFC 5424 for more information on the SysLog protocol.
    - **External SysLog Server IP:** Enter the hostname or IP address of your SysLog server.
    - **External SysLog Server Port Number:** Defaults to port 514, but can be changed to another port number if your SysLog server listens on a different port.
- **Prefix log file name with machine name:** If enabled, Titan FTP Server will name log files with both the name of the computer on which the logs are stored and the date. This gives the log files a unique name if the files are merged into a single location at a later date.

- **Use UNICODE formatted log files:** If enabled, file characters will be saved using Unicode, which allows for a greater variety of characters, especially international alphabets.
- **Wrap long text at X characters:** When enabled, each line in the log file is limited to the specified number of characters.
- **Logfile Format:** Use the drop-down arrow to select the **output format** for the server log file. The options are **Text** or **W3C** format. The W3C format records all times in GMT (Greenwich Mean Time).
- **Log Fields:** Select the **log fields** to be included in each log entry (Date, Time, ServerID/Socket#, Message).
- **Information Level:** Choose the **level** (General, Verbose, or Trace) of information to be recorded in the log file.
- **Log Rotation Schedule:** 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 LogFile.log. The rotated file's filename becomes YYYYMMDD.number.log. 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 Server service, it is highly recommended that the anti-virus software be configured so that it does not actively scan the Titan FTP Server log file subdirectories. Contention between the anti-virus software actively scanning the Titan FTP Server log files and service attempting to write to those files could cause performance issues with the Titan server.
- **Check for log rotation every X minutes:** Specify the number of minutes between checks to see if it is time to rotate the logs, which will create a new file.
- **Maximum Logfile Size (In MBs):** 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 Logfile Directory:** Specifies the location of where log files will be stored.


Home
ws01
Local Administration Server
beta
Services
Connections
Files/Directories
Security
Logging
Server Activity
Events
StatsTrack
Groups
Users
LOG SETTINGS
LOG MANAGEMENT
Log Settings
REVERT
APPLY
Log Settings (Server)
Enable logging to file
Enable logging to remote SysLog Server
Prefix log file name with machine name
Use UNICODE formatted log files
Wrap long text at
80
characters
Logfile Format
Text
Log Fields (Text)
Date
Time
ServerId/Socket#
Message
Information Level
General Information
Verbose/Detailed Information
Trace Level Information
Log Rotation Schedule
ROTATE NOW
Never
Daily
Weekly
Monthly
Check for log rotation every
5
minutes
Maximum Logfile Size
128
MB
Server Logfile Directory
C:\SrtLogs\beta
BROWSE
(c) South River Technologies, Inc.
Admin

Log Management

Log Management is a repository of all logs captured by the server, per the settings defined in the Log Settings section of the Titan server. It allows administrators a quick view of the captured logs, their file size, date and time of when they were created, and the ability to either download or delete them from the server.

Downloading or Deleting Log Files:

1. Sort the files by name by clicking on the **Name** column.
2. Click the **check box(es)** to the left of the file(s) you want to either download or delete. A download and trash bin icon will appear on the top right-hand side of the screen under the refresh icon.
3. Click the **download** icon and the file will be downloaded to your Downloads folder. If you select multiple log files to download, then it will be zipped up and downloaded with a filename of Files.zip.
4. To delete log files, you can follow steps 1 - 3 above and click the **trash bin** icon when the download and trash bin icon appears. Please note that this will delete the selected files from the actual server.

LOG SETTINGS | LOG MANAGEMENT

Log Files

Name	Size	Type	Date	Actions
20220531.0001.log	16.0 KB	File	05/31/2...	
20220531.0002.log	6.0 KB	File	05/31/2...	
20220531.0003.log	6.0 KB	File	05/31/2...	
20220531.0004.log	7.0 KB	File	05/31/2...	
20220531.0005.log	6.0 KB	File	05/31/2...	
20220601.0001.log	257.0 KB	File	06/01/2...	
20220601.0002.log	7.0 KB	File	06/01/2...	
20220601.0003.log	5.0 KB	File	06/01/2...	
20220601.0004.log	5.0 KB	File	06/01/2...	
20220601.0005.log	12.0 KB	File	06/01/2...	
20220601.0006.log	5.0 KB	File	06/01/2...	
20220601.0007.log	5.0 KB	File	06/01/2...	
20220601.0008.log	13.0 KB	File	06/01/2...	
20220601.0009.log	13.0 KB	File	06/01/2...	
20220601.0010.log	5.0 KB	File	06/01/2...	
20220602.0000.log	738.0 KB	File	06/01/2...	

Admin

Server Activity

The Server Activity can be used by administrators to view the real-time status of any logged in users. By default, the information on the activity page is refreshed every second, but can be modified for a longer refresh time if needed using the **settings** button located next to the refresh icon.

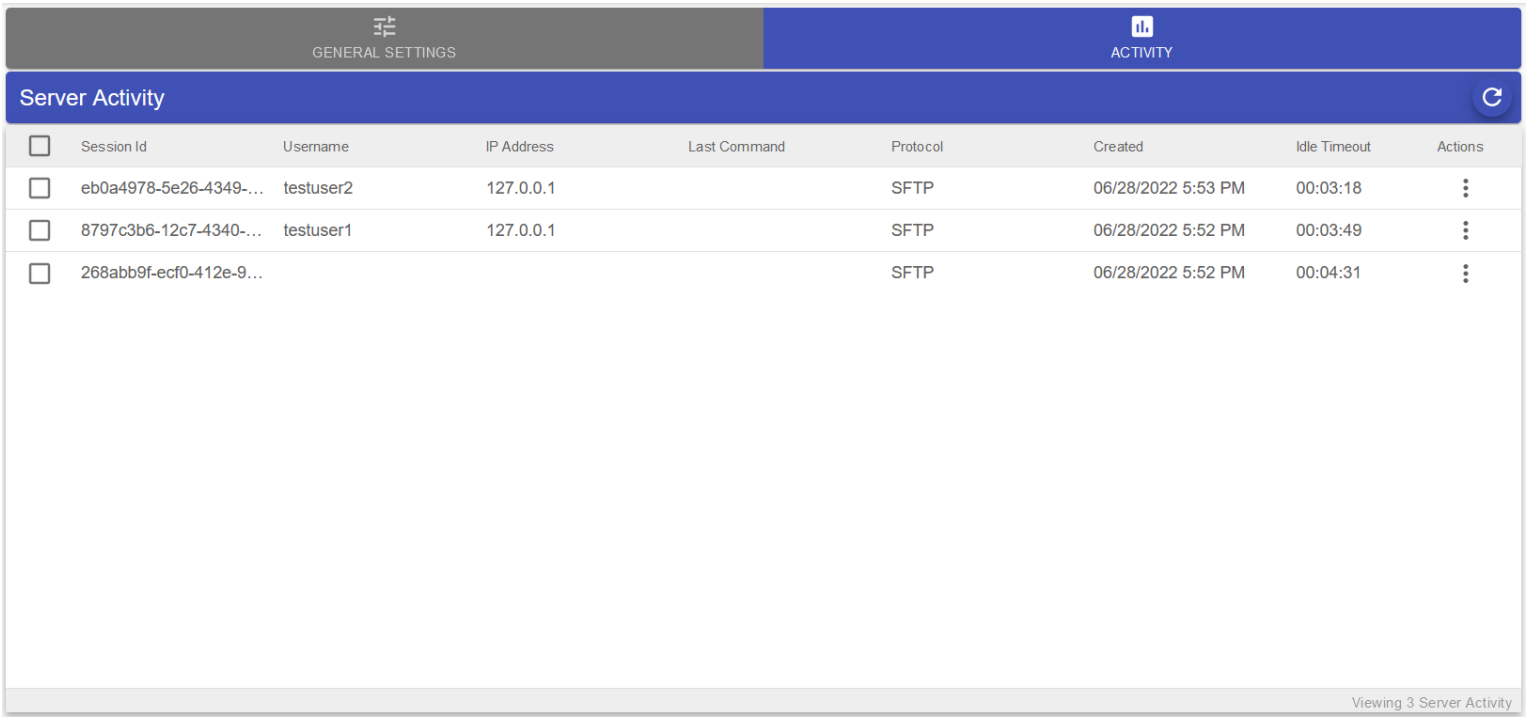
Once configured, it provides the administrator with the following bits of information under the Activity tab of Server Activity:

- the username of who is connected to the server
- the source IP address of the user
- the protocol (FTP/S, HTTP/S, or SFTP the user used to connect to the server
- the last command (STOR, GET, LIST, DELE, etc.) used by the user
- when the user connected
- how long the user's session has been idle (no activity)

The Activity tab also provides an administrator with the following quick actions in case the administrator does not recognize a username or if there is suspicious activity being performed on the server:

- **Kick User:** This option will log the selected user off of the server. All current sessions for this user will be disconnected, but the user can re-authenticate and launch subsequent session(s).
- **Kick User & Disable User Account:** This option will log the selected user off of the server. All current sessions for the selected user will be disconnected, and their account will be disabled to prevent any further activity with the server from the user account.
- **Kick User & Ban IP:** This option will log the selected user off of the server. All current sessions for the selected user will be disconnected, and the source IP address will be banned to prevent any further activity with the server from the source IP.

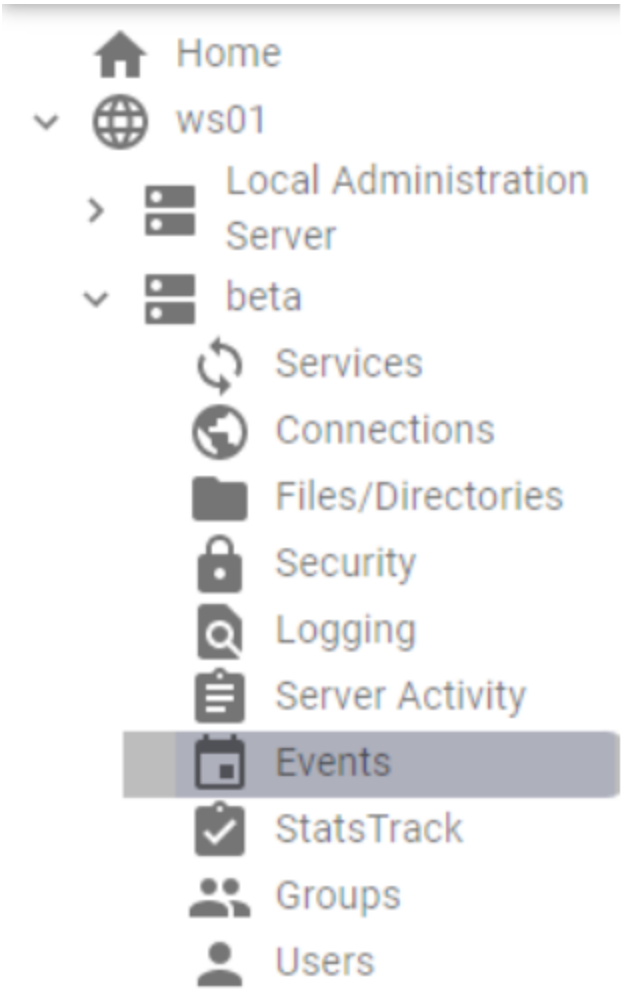
- **Kick Session(s):** This option will terminate the currently selected user session only. If the user is connected multiple times and has multiple sessions open, the remaining sessions will still remain active.



Event Management System

In Titan FTP Server, Administrators can leverage the power of automation by creating Events within the Events Management System. The Events Management System allows an administrator to automate certain file transfer tasks either post or prior to end user file transfers. Through its Event Management System, Titan FTP Server also allows Administrators to automate certain cumbersome day to day tasks which are performed manually.

Let’s start with managing events by navigating to the **Events** option in the left navigation pane.



The Events Management System consists of Events, Conditions, and Actions to allow Administrators 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. It can also be triggered on a scheduled basis to perform certain tasks. Please see the list of all the Events, Conditions, and Actions within Titan FTP Server.

Events

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.

- **Scheduled Standard Event:** Use this Event to set up a one-time or repeatable Event that will run based on the current time. This Event type must have a corresponding Scheduled time elapsed condition.
- **System Events:** Use this Event to set up system-specific events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
    - **Client Hammering Ban IP Permanent:** This Event will fire when an IP address is banned forever because it was hammering/flooding the server.
    - **Client Hammering Ban IP Temporary:** This Event will fire when a temporary ban occurs on an IP address hammering/flooding the server.
    - **Client Hacking Ban IP Permanent:** This Event will fire when an IP is banned forever because it was hacking a username.
    - **Client Hacking Ban IP Temporary:** This Event will fire when the IP is only banned temporarily for hacking a username.
    - **Real-Time Virus Scanning:** This Event will fire when a file has been uploaded to the server or data is being appended to an existing file.
    - **Calculate Disk Usage:** This Event will fire when an administrator performs a manual recalculation of disk quota.

- **Domain Startup**: This Event will fire when the domain first starts.
- **Configuration Backup:** This Event will fire when an administrator performs a manual backup of the server's configuration.
- **Reset User Credentials:** This Event will fire when a user has reset their password.
- **PCI Scan:** This Event will fire when a PCI scan is complete.

- **Server Events:** Use this Event to set up server-specific events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
  - **Server instance startup successful:** The Event will trigger if the server instance was started up successfully
  - **Server instance startup failed:** The Event will trigger if the server instance failed to start up successfully
    - **Server instance startup failed - Stats services:** This Event will be triggered if the server failed to start correctly because the Stats tracking subsystem failed to initialize.
    - **Server instance startup failed - FTP services:** The Event will be triggered if the server failed to start correctly because the FTP subsystem failed to initialize. This often indicates a port conflict.
    - **Server instance startup failed - FTP/S services:** The Event will be triggered if the server failed to start correctly because the FTP/S subsystem failed to initialize. This often indicates a port conflict.
    - **Server instance startup failed - SFTP services:** The Event will be triggered if the server failed to start correctly because the SFTP subsystem failed to initialize. This often indicates a port conflict.
    - **Server instance startup failed - HTTP services:** The Event will be triggered if the server failed to start correctly because the HTTP subsystem failed to initialize. This often indicates a port conflict.

        - **Server instance startup failed - HTTPS services:** The Event will be triggered if the server failed to start correctly because the HTTPS subsystem failed to initialize. This often indicates a port conflict.
    - **Server Stopped:** This Event is triggered if the server is stopped or if the server is restarted (in which case, a server start Event would immediately follow).
    - **Server Log Rotated:** This Event occurs every time the server starts, any time the log rotation period expires, or any time the administrator manually rotates the log.
    - **Before Command Processed:** Occurs any time a command is sent from the client to the server. By handling this Event, you can block unwanted commands or simply keep track of commands issued, among other things. See the list of FTP and SFTP commands.
    - **Return Code Sent To Client:** Occurs after the server has processed a client command and is about to return a status code. See the list of FTP and SFTP commands.
    - **Connection Attempt Succeeded:** This Event is triggered if a client connection attempt has succeeded. This Event is fired before any username/password verification, so it is still possible that the connection will be closed afterward.
    - **Connection Attempt Failed:** This Event is triggered if a client connection attempt has failed.
        - **Ban IP Address:** This Event is triggered if a client connection attempt has failed because the IP address is banned at the server level.
        - **Server Hammering:** This Event is triggered if a client connection attempt has failed because the IP address is banned at the server level due to DoS/Hammering.
        - **Server Hacking Attempt:** This Event is triggered if a user attempts to connect with random usernames and passwords until one works. If these attempts happen in rapid order, the system detects a hacking attempt and triggers the Event.
    - **Disconnection:** This Event is triggered if a client connection has been closed.
        - **User Quit:** This Event is triggered if a client connection has been closed because the user has quit.

        - **User Kicked:** This Event is triggered if a client connection has been closed because the user has been logged out by the server.
        - **Timeout:** This Event is triggered if a client connection has been closed because it has exceeded the idle timeout limit.
        - **Server Stopped:** This Event is triggered if a client connection has been closed because the server is stopping.
        - **Connection Closed:** This Event is triggered if a client connection has been closed because the server connection has been closed.
- **User Events:** Use this Event to set up user-specific events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
    - **User Login Attempt Successful:** When a user has successfully logged in.
    - **User Login Attempt Failed:** When a user login attempt has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
        - **Bad Username:** The username specified does not exist.
        - **Banned IP Address:** A user login attempt failed because the IP address is banned for the specified username. The password specified does not match the correct password for the supplied username.
        - **Banned IP Address:** A user login attempt failed because the IP address is banned for the specified username.
        - **Banned IP Address:** A user login attempt failed because the IP address is banned for the specified username.
        - **Max Connections:** A user login attempt failed because the maximum number of connections has been reached.
        - **Max Connections/IP:** A user login attempt failed because the maximum number of connections for that IP address has been reached.

- **Password Expired:** A user login attempt failed because the user's password is expired.
- **FTPS Login Failed:** A user's FTPS login attempt failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
    - **User Not Using FTPS:** A user's FTPS login attempt failed because the user is not using FTPS.
    - **FTPS Not Permitted For this User:** A user's FTPS login attempt failed because the specified username is not permitted FTPS access on the server.
    - **Cert Load Failed:** A user's FTPS login attempt failed because the user's certificate cannot be loaded by the server.
    - **Cert Not Supplied:** A user's FTPS login attempt failed because the user did not supply a certificate.
    - **Cert Did Not Match:** A user's FTPS login attempt failed because the user-supplied certificate does not match the certificate on the server.
- **SFTP Login Failed:** User's SFTP login attempt failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
    - **User Not Using SFTP:** A user's SFTP login attempt failed because the user is not using SFTP.
    - **SFTP Not Permitted For This User:** A user's SFTP login attempt failed because the specified username is not permitted SFTP access.
    - **Host Key Load Failed:** A user's SFTP login attempt failed because the user's host key cannot be loaded by the server.
    - **Host Key Not Supplied:** A user's SFTP login attempt failed because the user did not supply a host key.
    - **Host Key Did Not Match:** A user's SFTP login attempt failed because the user-supplied host key does not match the host key on the server.
- **Bad Username:** The username specified does not exist.

        - **Bad Password:** The password specified does not match the correct password for the supplied username.
    - **Bad Command Issued:** A user has issued a bad command. The command was either unrecognized, the syntax was incorrect, or the command was invalid based on the connection state.
    - **User IP Address Auto-Banned:** An IP address has been automatically banned by the server due to excessive bad commands.
    - **User Account Auto-Disabled:** A user account has been automatically disabled by the server due to excessive bad commands.
    - **User Account Created:** A user account has been created.
    - **User Account Deleted:** A user account has been deleted.
    - **User Changed Password:** The user has changed their account password.
- **File Events:** Use this Event to set up file-specific events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
    - **File Download/Read:** This is the parent Event for any file download/read events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
        - **Before Download/Read:** Occurs before the downloading of a file begins. By handling this Event, you can block unwanted downloads.
        - **Download/Read Successful:** A file has been successfully downloaded.
        - **Download/Read Failed:** A file download has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
            - **Bad Filename:** A file download has failed because the specified filename is a reserved name.

- **Insufficient Permissions:** A file download has failed because the user has insufficient access rights.
- **File Not Found:** A file download has failed because the specified file was not found.
- **Insufficient Upload/Download Ratios:** A file download has failed because the user has insufficient upload/download ratios. The user must first upload or download enough files/bytes to satisfy the ratio.
- **Max Session Downloads:** A file download has failed because the user has downloaded the maximum number of files allowed in a session.
- **Max Download Size:** A file download has failed because the file is larger than the maximum download size.

- **File Upload/Write:** This is the parent Event for any file upload/write events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
  - **Before Upload/Write:** Occurs before the uploading of a file begins. By handling this Event, you can block unwanted uploads.
  - **Upload/Write Successful:** A file has been successfully uploaded.
  - **Upload/Write Failed:** A file upload has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
    - **Bad Filename:** A file upload has failed because the specified filename is a reserved name.
    - **Insufficient Permissions:** A file upload has failed because the user has insufficient access rights.
    - **Banned File:** A file upload has failed because the specified filename matches one in the banned file list.

- **Disk Quota Limit:** A file upload has failed because the disk quota limit has been exceeded.
- **Max Session Uploads:** A file upload has failed because the user has uploaded the maximum number of files allowed in a session.
- **Max Upload Size:** A file upload has failed because the file is larger than the maximum upload size.
- **File Append:** This is the parent Event for any file append events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:

◦ **File Append:** This is the parent Event for any file append events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:

- **Before Append:** Occurs before appending to a file begins. By handling this Event, you can block unwanted appends.
- **Append Successful:** A file has been appended successfully.
- **Append Failed:** A file append has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
  - **Bad Filename:** A file append has failed because the specified filename is a reserved name.
  - **Insufficient Permissions:** A file append has failed because the user has insufficient access rights.
  - **Banned File:** A file append has failed because the specified filename matches one in the banned file list.
  - **Disk Quota Limit:** A file append has failed because the disk quota limit has been exceeded.

            - **Max Session Uploads:** A file append has failed because the user has uploaded the maximum number of files allowed in a session. This only occurs when an upload is masquerading as an append.
            - **Max Upload Size:** A file append has failed because the file is larger than the maximum upload size.
    - **File Delete:** This is the parent Event for any file delete events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
        - **Before Delete:** Occurs before deleting a file. By handling this Event, you can prevent unwanted deletes or back up files to another location.
        - **Delete Successful:** A file has been successfully deleted.
        - **Delete Failed:** A file delete has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
            - **Bad Filename:** A file delete has failed because the specified filename is a reserved name.
            - **Insufficient Permissions:** A file delete has failed because the user has insufficient access rights.
            - **File Not Found:** A file delete failed because the specified file did not exist.
    - **File Rename:** This is the parent Event for any file rename events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
        - **Before Rename:** Occurs before renaming a file. By handling this Event, you can block unwanted renaming.
        - **Rename Successful:** A file has been successfully renamed.
        - **Rename Failed:** A file rename has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:

            - **Bad Filename:** A file rename has failed because the specified filename is a reserved name.
            - **Insufficient Permissions:** A file rename has failed because the user has insufficient access rights.
            - **Banned File:** A file rename has failed because the specified filename matches one in the banned file list.
            - **Source File Not Found:** A file rename failed because the specified source file was not found.
            - **Dest File Already Exists:** A file rename has failed because the specified destination file already exists.
    - **Partially Uploaded File Deleted:** A partially uploaded file has been deleted by the server.
    - **Directory Events:** This is the parent Event for any directory-specific events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
        - **Directory Created:** This is the parent Event for any directory created events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
            - **Before Directory Create:** Occurs before creating a directory. By handling this Event, you can block unwanted directory creation.
            - **Directory Create Successful:** A directory has been successfully created.
            - **Directory Create Failed:** A directory create has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
                - **Bad Directory Name:** A directory create has failed because the specified directory name is a reserved name.

        - **Insufficient Permissions:** A directory create has failed because the user has insufficient access rights.
        - **Directory Already Exists:** A directory create has failed because the directory already exists.

- **Directory Removed:** This is the parent Event for any directory removed events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
    - **Before Directory Remove:** Occurs before removing a directory. By handling this Event, you can block unwanted directory removal.
    - **Directory Remove Successful:** A directory has been successfully removed.
    - **Directory Remove Failed:** A directory remove has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
        - **Insufficient Permissions:** A directory removal has failed because the user has insufficient access rights.
        - **Directory Not Found:** A directory remove has failed because the directory was not found.
- **Directory Content Listed:** This is the parent Event for any directory list events. FTP commands LIST, NLST, MLST, or MLSD will trigger an Event on all of the following:
    - **Before Directory List:** Occurs before a directory listing. By handling this Event, you can block unwanted directory listings.
    - **Directory List Successful:** A directory listing has been successful.
    - **Directory List Failed:** A directory listing has failed. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:

- **Bad Directory Name:** A directory listing has failed because the specified directory name is a reserved name.
- **Insufficient Permissions:** A directory listing has failed because the user has insufficient access rights.

- **Limit Events:** This is the parent Event for any limit-specific events. Selecting this will trigger an Event on all below events or you can alternatively select one or more from the following:
  - **Timeout Limit Hit:** The idle timeout limit has been reached.
  - **Connection Limit Hit:** The maximum number of connections limit has been reached.
  - **Connections/IP Limit Hit:** The maximum number of connections per IP address limit has been reached.
  - **Session Upload Limit Hit:** The session upload limit has been reached.
  - **Session Download Limit Hit:** The session download limit has been reached.
  - **Upload Size Limit Hit:** The file upload size limit has been reached.
  - **Download Size Limit Hit:** The file download size limit has been reached.
  - **Max Upload Speed Limit Hit:** The maximum file upload speed limit has been reached.
  - **Max Download Speed Limit Hit:** The maximum file download speed limit has been reached.
  - **Upload/Download Ratio Limit Hit:** The upload/download ratio limit has been reached. No more downloads will be allowed until more uploads occur.
  - **Bad Command Limit Hit:** The bad command limit has been reached.
  - **Disk Quota Limit Hit:** The disk quota limit has been reached.

Event Conditions

Conditions can be created to fine-tune Event definitions to handle specific cases. They allow you to add “if/then” situations or specifics that you can add to the Event. You can choose under what conditions the action will fire. Events must meet all conditions for the action to fire. The primary reason that actions don’t fire is because the conditions weren’t all met. Please also know that different conditions apply to each Event type, and it is important to be careful not to create conditions that are never satisfied.

Use wildcards on conditions to narrow or expand the condition criteria. Titan FTP Server recognizes the standard set of wildcards.

- **Server Conditions:**
  - **Command In List:** Use this condition to specify one or more server commands. When you select this condition, note that there are both FTP and SFTP commands listed. If any of the specified server commands match the current server command, the condition will be satisfied. Wildcards can be used.
  - **Return Code In List:** Use this condition to specify one or more server return codes. When you select this condition, note that there are both FTP and SFTP commands listed. If any of the specified server return codes match the current server return code, the condition will be satisfied. Wildcards can be used.
  - **Scheduled Time Elapsed:** Use this condition in conjunction with the *Scheduled Event*.
    - For a *one-time scheduled Event*, simply specify the date/time you wish the Event to occur. This one-time condition is satisfied if the current system time is beyond the First occurrence time.
    - For a *repeatable scheduled Event*, specify the date/time of the first occurrence, and the repeat interval. The repeatable condition is satisfied if the current system time is beyond the First occurrence time and has been at least the Repeat Interval units of time since the condition was last satisfied. The repeatable condition will keep track of the last time the

condition was satisfied so it will not repeat more than once in any Repeat Interval units of time.

- **IP Address:** Use this condition to *specify one or more IP addresses*. If any of the specified IP addresses match the IP address of the account that caused the Event to be triggered, the condition will be satisfied. Wildcards can be used.
- **Connection Type:** Use this condition to specify one or more connection types (protocols). By default, all supported protocols are included in the list of connection types.
- **Connection Time:** Use this condition to specify a time span for the connection. The time range can be either less or greater than a set number of days/hours/minutes/seconds. If the connection that caused the Event to be triggered has a connection time that is within the specified range, the condition will be satisfied. For example, specifying More than 1 days means that the condition will be satisfied if the connection has been alive for more than 1 day.
- **Connection Idle Time:** Use this condition to specify a time range for the connection idle time (time since the last command was received). The time range can be either less than or greater than a set number of days/hours/minutes/seconds. If the connection that caused the Event to be triggered has a connection idle time that is within the specified range, the condition will be satisfied. For example, specifying More than 1 hour means that the condition will be satisfied if the connection has been idle for more than 1 hour.

- **User Conditions:**
  - **User Enabled:** Use this condition to specify whether an account is enabled or disabled. If the account that caused the Event to be triggered matches this specified value, the condition is satisfied.
  - **User Group Membership:** Use this condition to specify one or more groups. If any of the specified groups match the group membership of the account that caused the Event to be triggered, the condition will be satisfied. Wildcards can be used.
  - **Username:** Use this condition to specify one or more usernames. If any of the specified usernames match the username of the account that caused the Event to be triggered, the condition

will be satisfied. Wildcards can be used.

- **User Account Expiration Date:** Use this condition to specify a time range for account expiration date values. The time range can be either less or greater than a set number of days/hours/minutes/seconds. If the account that caused the Event to be triggered has a valid expiration date within the specified range, the condition will be satisfied. For example, if you specify less than 20 days, the condition will be satisfied if the user account is expiring within the next 20 days. This condition is very useful for reminding users and administrators that an account will soon be expiring.

- **File Conditions:**
  - **Directory Name:** Use this condition to *specify one or more directory names*. If any of the specified directory names match the directory name being accessed, the condition will be satisfied. Wildcards can be used.
  - **File Name:** Use this condition to *specify one or more file names*. If any of the specified file names match the current file name being accessed, the condition will be satisfied. Wildcards can be used.
  - **File Size:** Use this condition to specify the size limit of a file. If any of the files match the file size being accessed, the condition will be satisfied.

Event Actions

Actions are server responses that can be configured to trigger for specific events. Depending on the actions you select, different Action Properties windows will appear on the right side of the screen to allow you to add Custom Message Variables to fine-tune your Event. Available actions are outlined below:

- **Break - Do Not Process Further Actions:** This action stops the processing of subsequent actions. The Event will be considered complete and no further actions will be performed. It can also be used for any Event actions that fail for any reason. Any actions that would normally have followed will be

canceled (will not execute) to prevent errors.

- **Send Email:** Sends an email, provided you have a SMTP mail server that will handle the request. SMTP mail server configuration will need to be configured under the Email Server tab at the server level for the email to be sent out to the recipient.
    - **Wait for Action to Complete:** If enabled (true), the action will wait for the operation to complete before returning.
    - **Wait Timeout in Seconds:** When enabled, this value indicates the number of seconds to wait for the operation to complete. -1 will wait indefinitely.
    - **To:** Specifies the email address to which the email will be sent. This can also accept Custom Message Variables. For example, you could specify the %USEREMAIL% variable in the case where a user-triggered Event has occurred, and you wish to notify that user. You can send the email to more than one person by separating addresses with a semicolon. *Example*: bob@-abc.com; joe@abc.com
    - **From:** Specifies the email address from which the email will be sent.
    - **CC:** Carbon copy email to other recipient(s). Separate names with ';'.
    - **BCC:** Blind copy to one or more recipient(s). Separate with ';'.
    - **Subject:** Specifies the text that will go into the email subject line.
    - **Email Message Body:** Specifies the text that will go into the body of the email.
    - **Attachments:** Specify one or more files to attach. This can also accept Custom Message Variables.
- **Flag for review:** Causes a notification to be sent to the user.
- **Spawn process to run job:** Ability to launch a file/script with optional command line parameters. Bear in mind that if the script launches an action in a third-party service (such as RoboCopy) the action will appear under the context of the Titan FTP Server service, even if Titan FTP Server itself does not perform the action and only instructs another program to do so. Therefore, if an action fires several batch files in rapid succession, spawning many instances of another program, this will

consume a great deal of memory, which will be attributed to Titan FTP Server, though the third-party program is actually using the memory.

    - **Attachments:** Specifies the location of the file/script to be run.
    - **Parameters:** Specifies any command line arguments to the file. Add each parameter to the parameter list in the order in which they should be passed to the file/script.
    - **Params:** The list of specified parameters, which can be prioritized using the Up and Down buttons. They can also be removed using the Trash Bin icon.
    - **Add Quotes to Parameters:** Adds double quotation marks around all parameters in the list. Any parameters that contain a space should always be wrapped in double quotes.
        - *Examples:*
            - C:\long file name.txt"
            - "% FILEPATH%"
    - **Dump Script Command Line Info to Log File:** Writes information pertaining to the script to the log file.
    - **Wait for Script to Complete Before Continuing:** Used to queue running scripts and execute them one at a time. Disabling this will allow scripts to run in tandem.
    - **Seconds:** The value of Seconds determines the acceptable run time for the specified script.
    - **Abort Scripts That Run Too Long:** Aborts a script that runs longer than the value of Seconds.
- **Write to custom log or file:** Writes a message to a logfile.
    - **Log Text:** Specifies the message that will be written to the logfile.
    - **Log Filename:** Specifies the location of the file that the message will be written to.
    - **Write file in ASCII Format:** The option to write log text messages in ASCII format.
- **Ban remote client IP address:** Bans specified IP address. This can also accept Custom Message Variables. For example, you could specify the %CIP% variable in the case where a user-triggered

Event has occurred, and you wish to ban that user's IP address.

- **Kick current user from the system:** Logs specified user off of the server. This can also accept Custom Message Variables. For example, you could specify the %USERNAME% variable in the case where a user-triggered Event has occurred, and you wish to kick that user from the system.
- **Disable user account:** Disables specified user account. This can also accept Custom Message Variables. For example, you could specify the %USERNAME% variable in the case where a user-triggered Event has occurred, and you wish to disable that user account.
- **Backup Configuration:** When used with Scheduled Events, Titan FTP Server will back up configuration information on a schedule.
    - **Backup Set Name:** The name of the backup configuration file so it can help easily identify it from other backup configuration files. This can also accept Custom Message Variables. For example, you could specify the %SVR.SERVERNAME%.%UUID% variable to help specify a unique name for the configuration file.
    - **Backup Set Description:** A description of the Backup set.
    - **Backup Set Location:** The file path of where the Backup set will be written to and saved.
- **Push to remote Internet site:** This action will upload the specified files to a remote server using PowerShell scripts in the \Program Files\South River Technologies\SrxServer\Scripts folder.
    - **WebDrive Connection Profile:** The file path of the WebDrive Connection profile (*.wdexport) that will need to be exported from WebDrive. This file will contain the connection details (hostname/IP address, port, username, password) in an encrypted format.
    - **Source Directory:** The file path (directory) of the file to upload. The %FILEPATH% variable can be used in the case where a file-triggered Event has occurred.
    - **Source Filename:** The file name of the file to upload.
    - **Destination Directory:** The file path (directory) on the destination of where the file will be uploaded. The %FILEPATH.PATH% variable can be used in the case where a file-triggered Event has occurred.

- **Destination Filename:** The name of the file on the destination.
- **Recurse Subdirectories:** Enable this option to consider the files in the source directory and any subdirectories.
- **Disconnect from remote connection after transfer:** Enable this option if you would like to immediately end your session with the remote server once the file(s) have been successfully transferred.
- **Delete source after transfer:** Enable this option if you would like to delete the source file(s) after they have been successfully transferred.
- **Wait For Script to Complete Before Continuing:** Used to queue the PowerShell scripts running in the background and execute them one at a time. Disabling this will allow scripts to run in tandem.
- **Seconds:** The value of Seconds determines the acceptable run time for the default PowerShell script.
- **Abort Scripts That Run Too Long:** Aborts the PowerShell script that runs longer than the value of Seconds.

- **Pull from remote Internet site:** This action will download the specified files from a remote server using PowerShell scripts in the \Program Files\South River Technologies\SrxServer\Scripts folder.
  - **WebDrive Connection Profile:** The file path of the WebDrive Connection profile (*.wdexport) that will need to be exported from WebDrive. This file will contain the connection details (hostname/IP address, port, username, password) in an encrypted format.
  - **Source Directory:** The file path (directory) of the file to download from a remote server.
  - **Source Filename:** The file name of the file to download from a remote server.
  - **Destination Directory:** The file path (directory) on the destination server of where the file will be downloaded.
  - **Destination Filename:** The name of the file on the destination server.

- **Recurse Subdirectories:** Enable this option to consider the files in the source directory and any subdirectories.
- **Disconnect from remote connection after transfer:** Enable this option if you would like to immediately end your session with the remote server once the file(s) have been successfully transferred.
- **Delete source after transfer:** Enable this option if you would like to delete the source file(s) after they have been successfully transferred.
- **Wait For Script to Complete Before Continuing:** Used to queue running scripts and execute them one at a time. Disabling this will allow scripts to run in tandem.
- **Seconds:** The value of Seconds determines the acceptable run time for the specified script.
- **Abort Scripts That Run Too Long:** Aborts a script that runs longer than the value of Seconds.

- **PCI Compliance Scan:** This action will run a scan of your Titan FTP Server configuration to check for PCI-DSS compliance. This will run a scan to review configuration settings that directly relate to PCI-DSS standards in your server and store them in the database, where the data can later be used to generate reports on your personal PCI-DSS compliance status.
- **Run Report:** This action will generate a customized report according to the settings you input in the Advanced Properties window. You can give your report a name, specify the file path for the output, and specify up to 6 parameters. Select from the Report Name drop-down to select a report.
  - **Report Name:** From the list of reports, select a report you would like to generate.
  - **Report Output File:** Specify the file path of where you would like to have the report outputted to.
  - **Report Parameter 1 - 6:** Enter the param=value for each parameter. The name of Parameters can be found by opening the report of choice and noting the parameters needed to run the report.

        - *Examples:*
            - Report Parameter 1: StartDate=%DATE.TODAY.BOY% or 01/01/2022
            - Report Parameter 2: EndDate=%DATE.TODAY% or actual date
    - **Wait for Action to Complete:** If enabled (true), the action will wait for the operation to complete before returning.
    - **Wait Timeout in Seconds:** When enabled, this value indicates the number of seconds to wait for the operation to complete. -1 will wait indefinitely.
- **Zip file or folder:** Upon successful completion of a file transfer, zip the files for storage. This can also be used to zip files before transferring them, to speed transfer times.
    - **Source File to Zip:** The file path of the file to zip. This can also accept Custom Message Variables. For example, you could specify the %FILEPATH% variable in the case where a file-triggered Event has occurred, and you wish to zip the file.
    - **Destination Path:** By default, the zipped file will be placed in the same path as the source file. You can change this to have the zip file created in a different location.
    - **Wait for Action to Complete:** If enabled (true), the action will wait for the operation to complete before returning.
    - **Wait Timeout in Seconds:** When enabled, this value indicates the number of seconds to wait for the operation to complete. -1 will wait indefinitely.
    - **Overwrite Existing Files:** Enable this feature if you wish to overwrite any existing file during the zip. Disabling this feature will force the zip process to fail if the file already exists.
    - **Preserve Path:** Enable this feature to preserve the file path during the zip.
    - **Compression Level:** Select a compression level. Higher compression will result in a slower Zip process but may generate a smaller file. Lower compression will run faster but the file may be larger.

    - **Recurse Subdirectories:** If zipping a folder, this flag indicates if subdirectories will also be included in the zip process.
    - **Zip File Comment:** Add an optional comment to be written into the zip file.
- **Unzip file or folder:** Unzip successfully transferred files.
    - **Source File to Unzip:** The file path of the zipped files. This can also accept Custom Message Variables. For example, you could specify the %FILEPATH% variable in the case where a file-triggered Event has occurred, and you wish to unzip the file.
    - **Destination Path:** By default, the unzipped file(s) will be placed in the same path as the source file. You can change this to have the unzipped file(s) created in a different location.
    - **Wait for Action to Complete:** If enabled (true), the action will wait for the operation to complete before returning.
    - **Wait Timeout in Seconds:** When enabled, this value indicates the number of seconds to wait for the operation to complete. -1 will wait indefinitely.
    - **Overwrite Existing Files:** Enable this feature if you wish to overwrite any existing file during the unzip. Disabling this feature will force the unzip process to fail if the file already exists.
    - **Preserve Path:** Enable this feature to preserve the file path during the unzip.
- **Recalc Disk Usage:** This Action will calculate the current disk usage. This information is provided per user, or for all users in a group, based on the user home directory. This information is written to the disk usage table and can be displayed through a Disk Usage report.
    - **Is Group:** If true, the ID supplied is a GroupID, not a UserID.
    - **User Group ID:** Specify the GroupID or UserID to generate. The Everyone Group is 101.
    - **Path:** Specify the path to check. Usually this will be %USERHOMEDIR% in the case where a user-triggered Event has occurred, and you wish to calculate the current disk usage for that user.

    - **Wait for Action to Complete:** If enabled, the action will block and wait for the file to be completed. Note that if the file is very large, this could take time and delay other operations.
    - **Wait Timeout in Seconds:** When enabled, this value indicates the number of seconds to wait for the operation to complete. -1 will wait indefinitely.
- **File system - Move Files:** This is a command-line move action alternative to using a third-party software to move individual or groups of files, such as in workflow environments where files are moved to a back-end processing folder once they have been uploaded. This helps to keep memory drain to a minimum when initiating frequent move actions.
    - **Source Path and Filename:** The fully qualified path and filename for the source object. Wild cards are permitted.
    - **Destination Path and Filename:** The fully qualified path and filename for the target object. The filename can be omitted if moving multiple files.
    - **Overwrite if Exists:** If enabled and the file exists on the destination, the action will overwrite the destination object. Otherwise, it will fail if the file exists on the destination.
    - **Wait for Action to Complete:** If enabled, the action will block and wait for the file to be completed. Note that if the file is very large, this could take time and delay other operations.
    - **Wait Timeout in Seconds:** The number of seconds to wait for the MOVE operation to complete.
    - **Abort if Timed Out:** Enable this feature to abort the MOVE if "Wait for Action to complete" is enabled and the action does not complete within the Wait Timeout.
    - **Create Path:** Enable this option to force the creation of the destination path if it does not exist. If the destination path does not exist, and this option is not enabled, the move will fail. The move will also fail if the destination path cannot be created and this flag is enabled.
    - **Success Script:** Options Powershell/DOS script to execute on success.
    - **Failure Script:** Options Powershell/DOS script to execute on failure.
- **File system - Delete Files:** Permanently and securely delete files from the server.

- **Source Path and Filename:** The fully qualified path and filename for the source object(s) to delete.
- **Wait for Action to Complete:** If enabled, the action will block and wait for the file to be completed. Note that if the file is very large, this could take time and delay other operations.
- **Wait Timeout in Seconds:** The number of seconds to wait for the DELETE operation to complete.
- **Abort if Timed Out:** Enable this feature to abort the DELETE if "Wait for Action to complete" is enabled and the action does not complete within the Wait Timeout.

- **File System - Copy Files:** This is a command-line copy action alternative to using a third-party software to copy individual or groups of files, such as in workflow environments where files are copied to a back-end processing folder once they have been uploaded. This helps to keep memory drain to a minimum when initiating frequent move actions.
  - **Source Path and Filename:** The fully qualified path and filename for the source object. Wild cards are permitted.
  - **Destination Path and Filename:** The fully qualified path and filename for the target object. The filename can be omitted if copying multiple files.
  - **Overwrite if Exists:** If enabled and the file exists on the destination, the action will overwrite the destination object. Otherwise, it will fail if the file exists on the destination.
  - **Wait for Action to Complete:** If enabled, the action will block and wait for the file to be completed. Note that if the file is very large, this could take time and delay other operations.
  - **Wait Timeout in Seconds:** The number of seconds to wait for the COPY operation to complete.
  - **Abort if Timed Out:** Enable this feature to abort the COPY if "Wait for Action to complete" is enabled and the action does not complete within the Wait Timeout.
  - **Create Path:** Enable this option to force the creation of the destination path if it does not exist. If the destination path does not exist, and this option is not enabled, the copy will fail. The copy

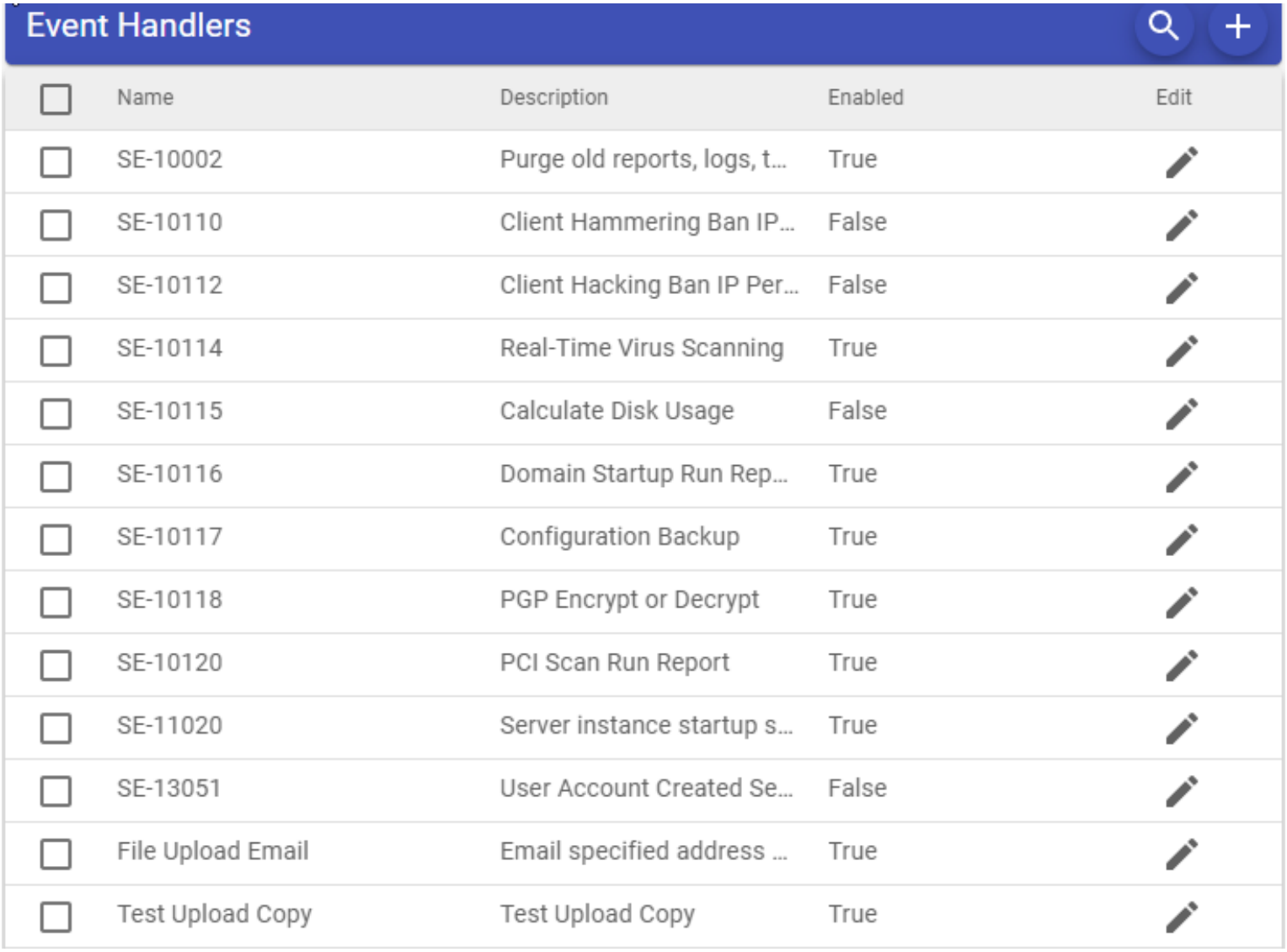
will also fail if the destination path cannot be created and this flag is enabled.

- **Success Script:** Options Powershell/DOS script to execute on success.
- **Failure Script:** Options Powershell/DOS script to execute on failure.

System Events

Although you may not have created any Events, Titan FTP Server does come with some predefined Events (some in an enabled and others in a disabled state) that perform certain tasks. These are advanced events and should not be modified, enabled, or disabled unless instructed to do so by SRT Support representatives.

System Events are hidden by default but can be viewed by clicking the **filter** icon in the top-right corner of the Event Handlers screen, enabling the **Show System Events** setting, and clicking **Add**. They are preceded with “SE” in their name to help identify them as System Events.



Adding Events

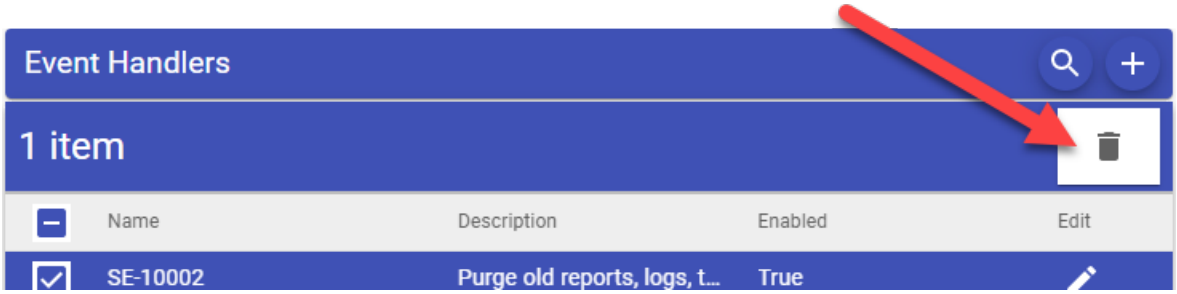
1. To add an Event, click on the **plus** icon at the top-right corner of the Event Handlers screen. The New Event handler screen displays.
2. Click **Add Event**. The Add Event screen displays.

3. The initial Add Event screen displays the top-level Event categories. Click on the **>** icon to expand the Event types to view additional options for each Event category.
4. Select an **Event type** from the list and click **Okay** at the bottom of the Add Event window.
5. Now that we have an Event selected, click on the **>** icon of the Event to expand it to see Conditions.
6. Select **Conditions** and click the **Add Condition** button at the bottom of the screen to reveal a list of conditions associated with the selected Event.
7. Select the **Condition(s)** that fits your need, or, select **All Conditions** and click the **Okay** button. Please be sure to fill in the fields associated with the selected Conditions. You can repeat this step to add more conditions, if needed.
8. Now that we have the Event and Condition(s) specified, select **Actions** followed by the **Add Action** button.
9. In the subsequent Add Action screen, there will be a list of actions to select from. Please select the **Action(s)** that are needed, fill in the fields associated with each Action, and click the **Okay** button.
10. In the New Event Handler screen, please confirm that your Event shows the selected Condition(s) and Action(s). If so, click **Next**.
11. In the subsequent New Event Handler screen, please specify a Name for the Event along with a description to help you understand the purpose of the Event.
12. Select the Enabled **check box** to enable the Event. Uncheck the Enabled **check box** if you do not want to enable the Event.
13. Click on the **Create** button. The Event will now display in the Event Handlers window.

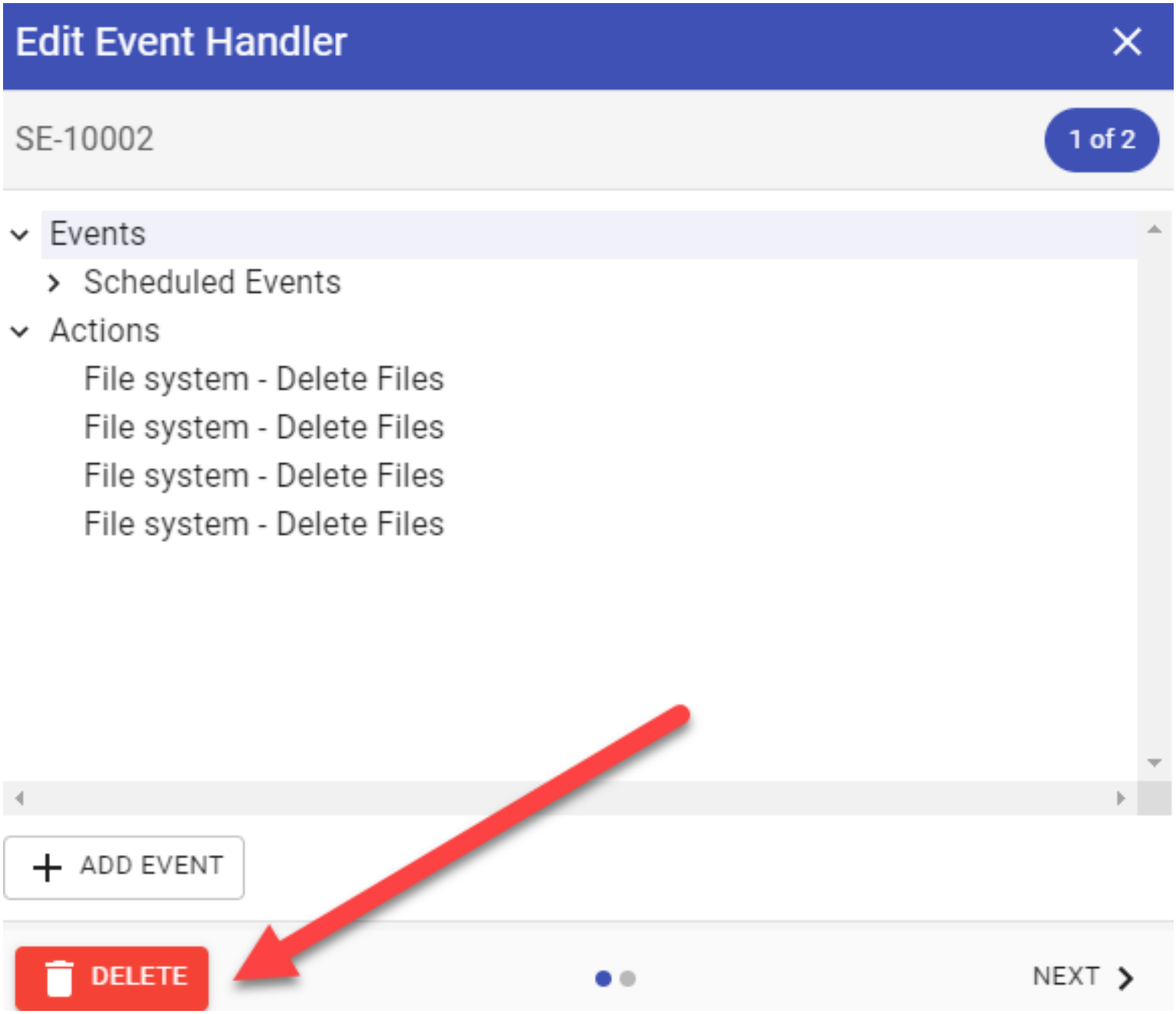
Deleting Events

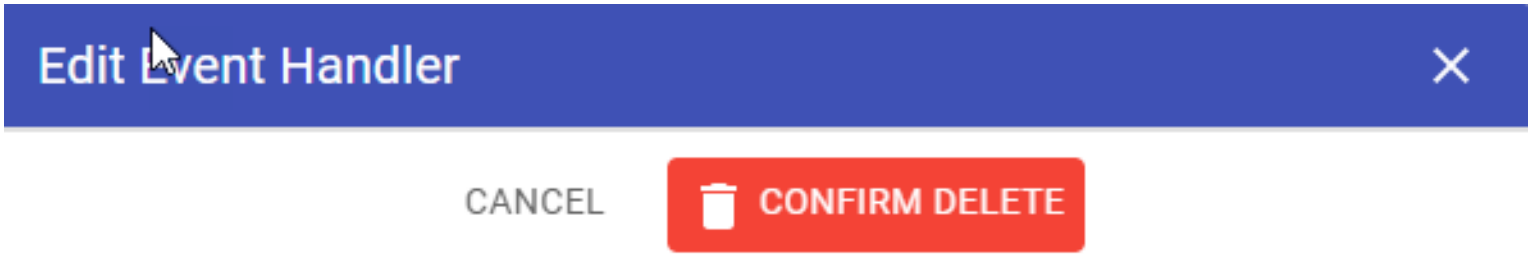
To delete an Event, navigate to the Events option on your left navigation. The Event Handlers screen displays. You can delete an Event in two ways:

1. You can delete an Event using the trash bin icon:
    a. Select the **check box** next to the Event that you want to delete. The trash bin icon displays at the top right of the window.
    b. Click the **trash bin** icon. The Event is deleted and no longer displays in the Event Handlers list.



2. You can also delete an Event on the Event Handlers screen:
    a. Click on the **pencil** icon next to the Event that you want to delete. The Edit Event Handler window displays.
    b. Select **Delete** at the bottom of the window, followed by **Confirm Delete** in the subsequent screen. The system deletes the Event and no longer displays in the Event Handlers list.


Edit Event Handler
SE-10002
1 of 2
Events
Scheduled Events
Actions
File system - Delete Files
File system - Delete Files
File system - Delete Files
File system - Delete Files
ADD EVENT
DELETE
NEXT

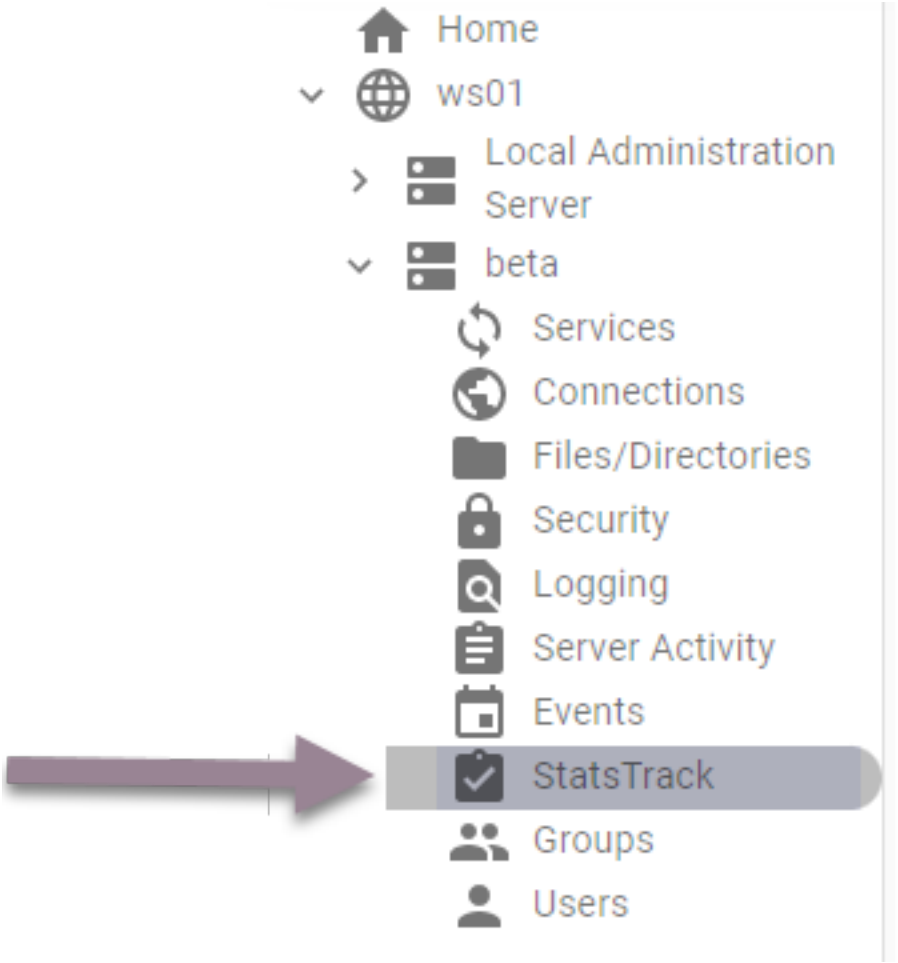

Edit Event Handler
CANCEL
CONFIRM DELETE

Statistics and Reporting (StatsTrack)

The StatsTrack feature of Titan FTP Server provides an administrator with access to important system information through our advanced reporting module. It allows for the generation of reports related to file transfer activity, user statics, and server configuration. The reports can be run as needed for quick viewing or scheduled through our Events Management System to share with management via email as an attachment or save on a network share.

The StatsTrack feature also allows an administrator to archive and purge data from the database to ensure optimal performance and adhere to data retention policies.

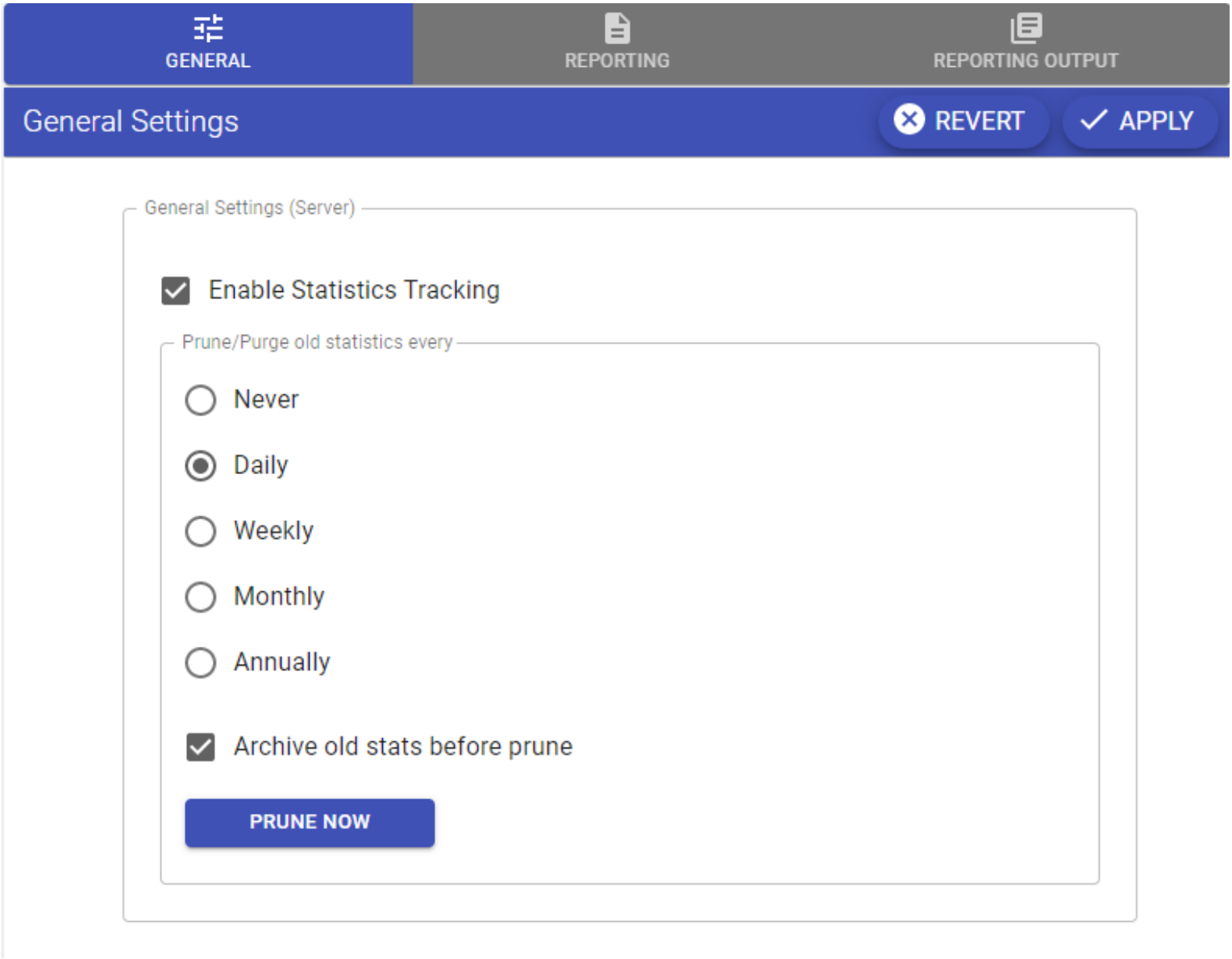
For statistics tracking and reporting, click on the **Stats Track** option in Titan FTP Server's left navigation.



To get started, it will be important to enable the StatsTrack feature so it can monitor and log server activity and transactions. It is also recommended to configure the archiving of historical data and a purge interval to help ensure optimal performance and adherence to any data retention policies.

Enabling StatsTrack:

1. Click on the check box next to **Enable Statistics Tracking**.
2. In the **Prune/Purge old statistics every** field, select your preferred **cadence** for pruning and purging old statistics. You can choose to prune/purge **Never**, **Daily**, **Weekly**, **Monthly**, or **Annually**.
3. To preserve and archive old statistics prior to pruning, enable the **Archive old stats before prune** option.
4. Click the **Prune Now** button to start an initial prune followed by **Apply** to commit your settings.



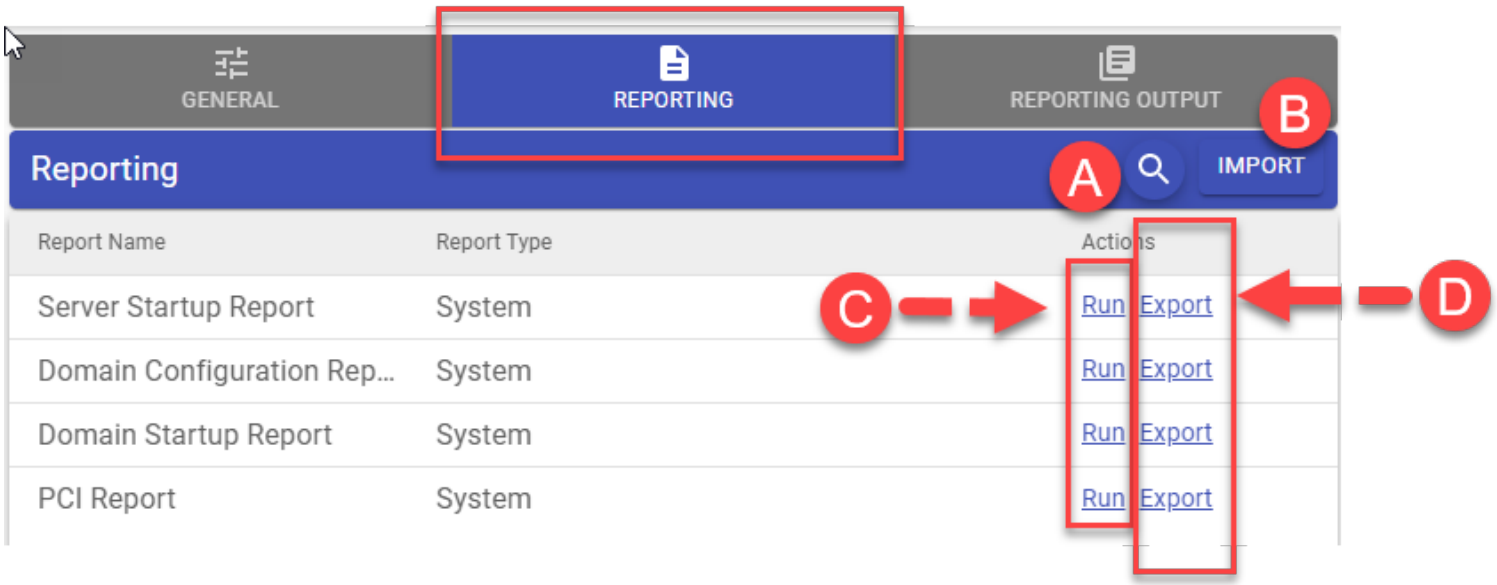
Reporting

The StatsTrack module comes with pre-configured reports that give you the ability to track server transactions, services, commands, connections, file operations, and user activity. The Report Viewer is included with the StatsTrack module and can be used to view and print reports.

- **Domain Startup Report:** This report lists the status of the domain(s) upon startup.
- **Domain Configuration Report**
- **Server Startup Report**
- **Server Configuration Report**
- **Server List Report**
- **Group List Report**
- **User List Report**
- **Group Configuration Report**
- **User Configuration Report**
- **PCI Compliance Report:** This report lists in detail the PCI DSS conditions your server passed or failed.

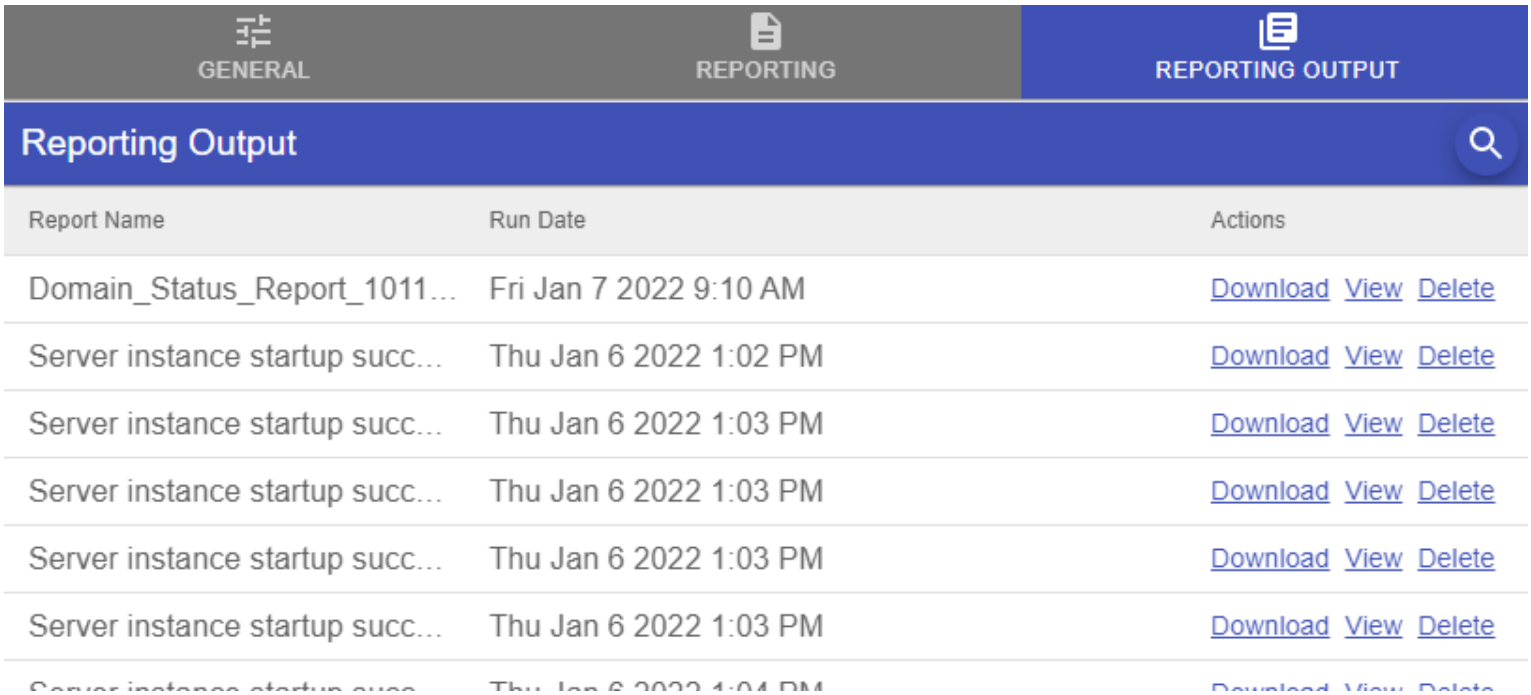
The screen displays the available reports, indicated by Report Name and Report Type. Below are some of the settings that can be used with Reporting:

- **Magnifying Glass:** This button can be used to search for a specific report. (A)
- **Import:** This button can be used to Browse your PC to import a report. (B)
- **Run:** This button can be used to run a report and receive a PDF download to your PC. (C)
- **Export:** This button can be used to export the report. (D)



Reporting Output

The Reporting Output contains a list of all reports run by an administrator. Once an administrator clicks on the **Run** link next to the report in the Reporting tab, it is saved under the Reporting tab to download, view, or delete.

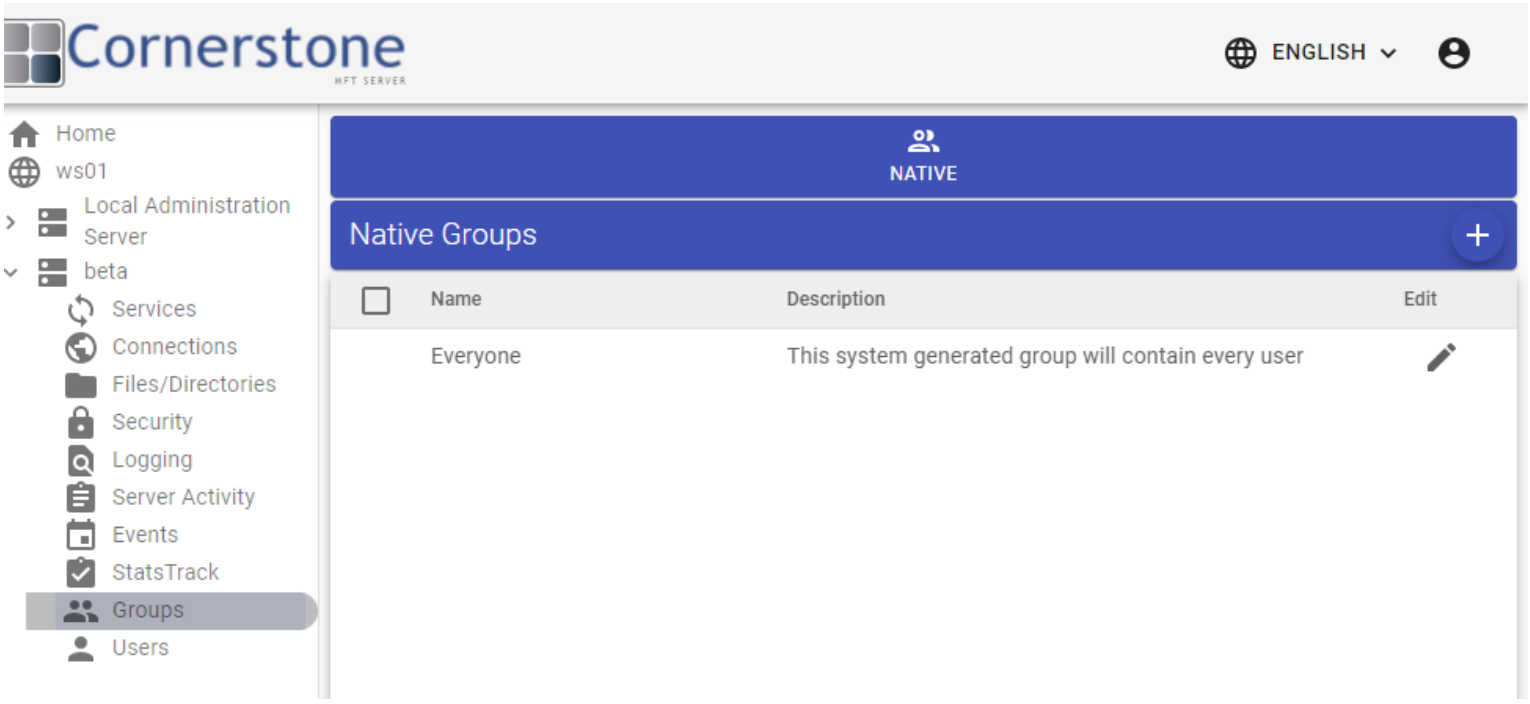


Groups

Groups can be used in Titan FTP Server to allow administrators to control access and set limits to the server and its files and folders. Groups allow an administrator to categorize members and consolidate their privileges. Group members have all rights granted to the group, unless overridden at the User level. By default, Titan FTP Server creates an Everyone group for every Native User Auth server instance.

Administrators can create new groups but should first consider their security and access needs. Once defined, they can create the needed group based on those needs and add users to the group.

To access Groups, click on the **Groups** option in your left navigation pane.



Creating Groups

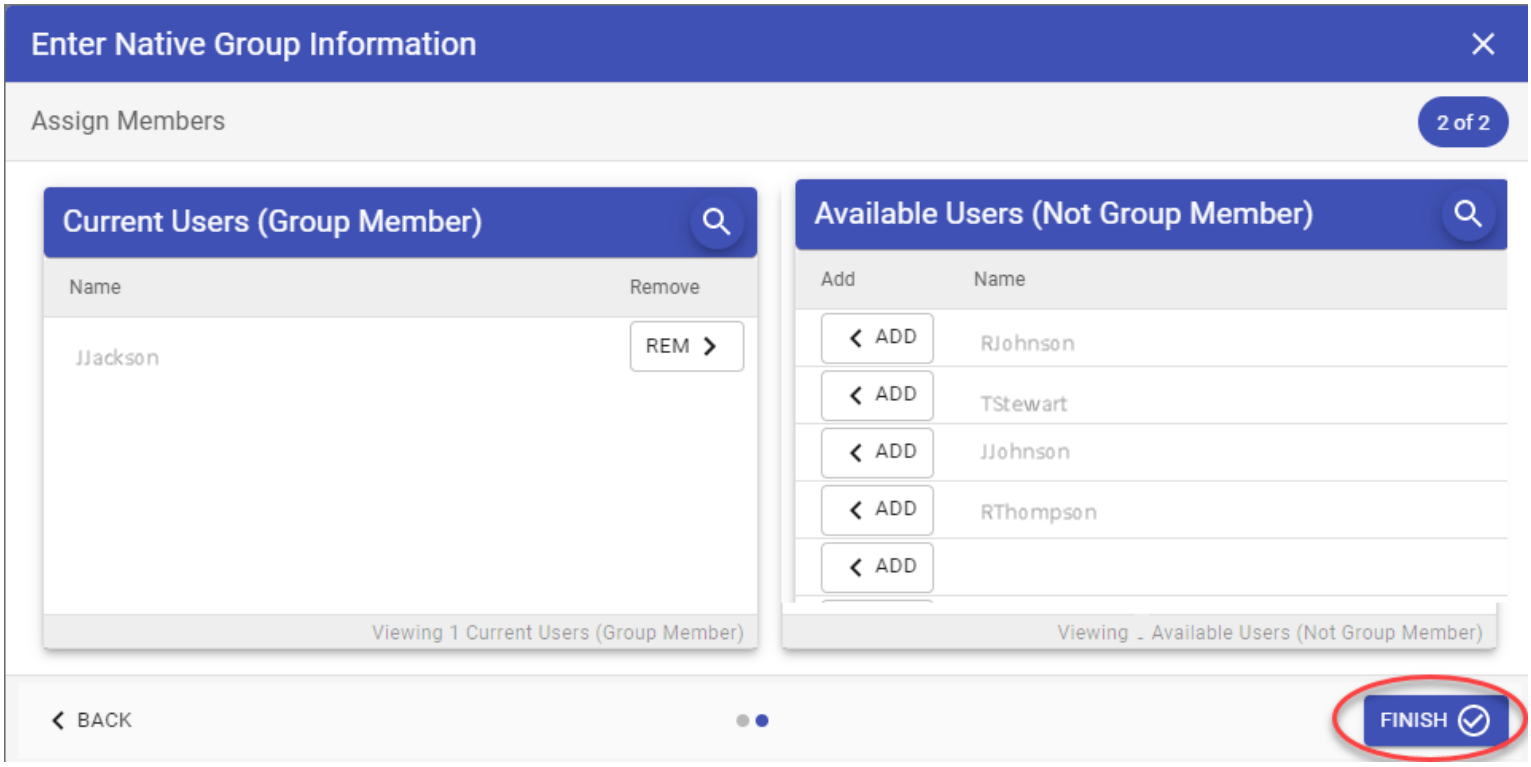
An administrator can create groups in Titan FTP Server and designate access and permissions to the users that are added as members of those groups.

To create a Group:

1. Click on the **plus** icon at the top right of the Native Groups window. The Enter Native Group information window appears.
2. Enter your preferred group name in the Group Name field.
3. Enter a description of the group in the Group Description field.
4. Select your desired **home directory** in the Home Directory field and click **Next**. The drop-down arrow in the Home Directory field will have the following three options to select from:
    a. **No home directory:** 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.
    b. **User home directories default to group directory:** Select this option to cause any users that are members of this group to use the Group Home Directory as their home directory.
    c. **User home directories default to group sub-directory:** Select this option to cause any users that are members of this group to have their own sub-directory created under the Group Home Directory.

5. The Assign Members window displays. Add the user(s) to the group by locating the name in the Available Users (Not Group Member) pane on the right side of the Assign Members window. Click the **Add** button next to the name(s) you want to add. The name displays in the Current Users (Group

Member) pane on the left side of the Assign Members window. Click the **Finish** button if all looks okay.



Adding Groups from an AD or LDAP Connector

An administrator can add AD or LDAP groups into Titan FTP Server and designate access and permissions to the users that are members of those groups.

To add a group from AD or LDAP:

1. Navigate to the **ADSI** or **LDAP** tabs located under Group. If you do not see an ADSI or LDAP tab, you will need to configure the ADSI and/or LDAP connector under the User Auth tab at the Server level.

2. Click on the **plus** icon and select the **Authentication domain** and the **Group(s)** you would like to add from your AD or LDAP server in the subsequent screen. Multiple Groups can be selected and added to your Titan FTP Server instance.
3. Once you have selected the group(s) you want added to Titan FTP Server, please click **Add**.

The new Group(s) should now appear in the list.

Editing Group Properties

To edit a Group, do the following:

1. Select the **pencil** icon next to the group that you want to edit.
    a. For **Edit Group & Assigned Users:**
        i. The Enter Group Information screen displays. You can update the following on this screen:
            1. **Group Name:** Displays the Group Name. Use this text box to change the group name. **Note:** You cannot change the group name for the Everyone group.
            2. **Group Description:** A descriptor of the group name to help easily identify its purpose.
            3. **Home Directory:** The defined home directory for users in the group.
            4. **Current Users (Group Member):** A list of users currently associated with the group.
            5. **Available Users (Not Group Member):** A list of users available to add to the group.

b. **For Group Services:** These *Server access (FTP/S, SFTP, & HTTP/S)* values within the Group Services are inherited (see Inheritance table below) from the Services setting set at the Server level. These settings can be overridden to restrict control and/or access to the users assigned to the group. For more information on these settings, please see "File Transfer Protocol (FTP) Configuration" on page 73.

c. **For Group Connections:** These *General & Advanced Connection* values within the Group Connections are inherited (see Inheritance table below) from the Connections setting set at the Server level. These settings can be overridden to enforce or ease end-user connections for the users assigned to the group. For more information on these settings, please see "Connection Settings" on page 88.

d. **For Group Files & Directories:** These *Files & Directories* values within the Group Files & Directories are inherited (see Inheritance table below) from the Files & Directories setting set at the Server level. These settings can be overridden to add additional directories, virtual folders, file restrictions, or quotas for the users assigned to the group. For more information on these settings, please see "Files and Directories" on page 92.

e. **For Group Security:** These *Security* values within the Group Security are inherited (see Inheritance table below) from the Security settings set at the Server level. These settings can be overridden to fine tune the IP Access to the users assigned to the group. For more information on these settings, please see "Security" on page 103.

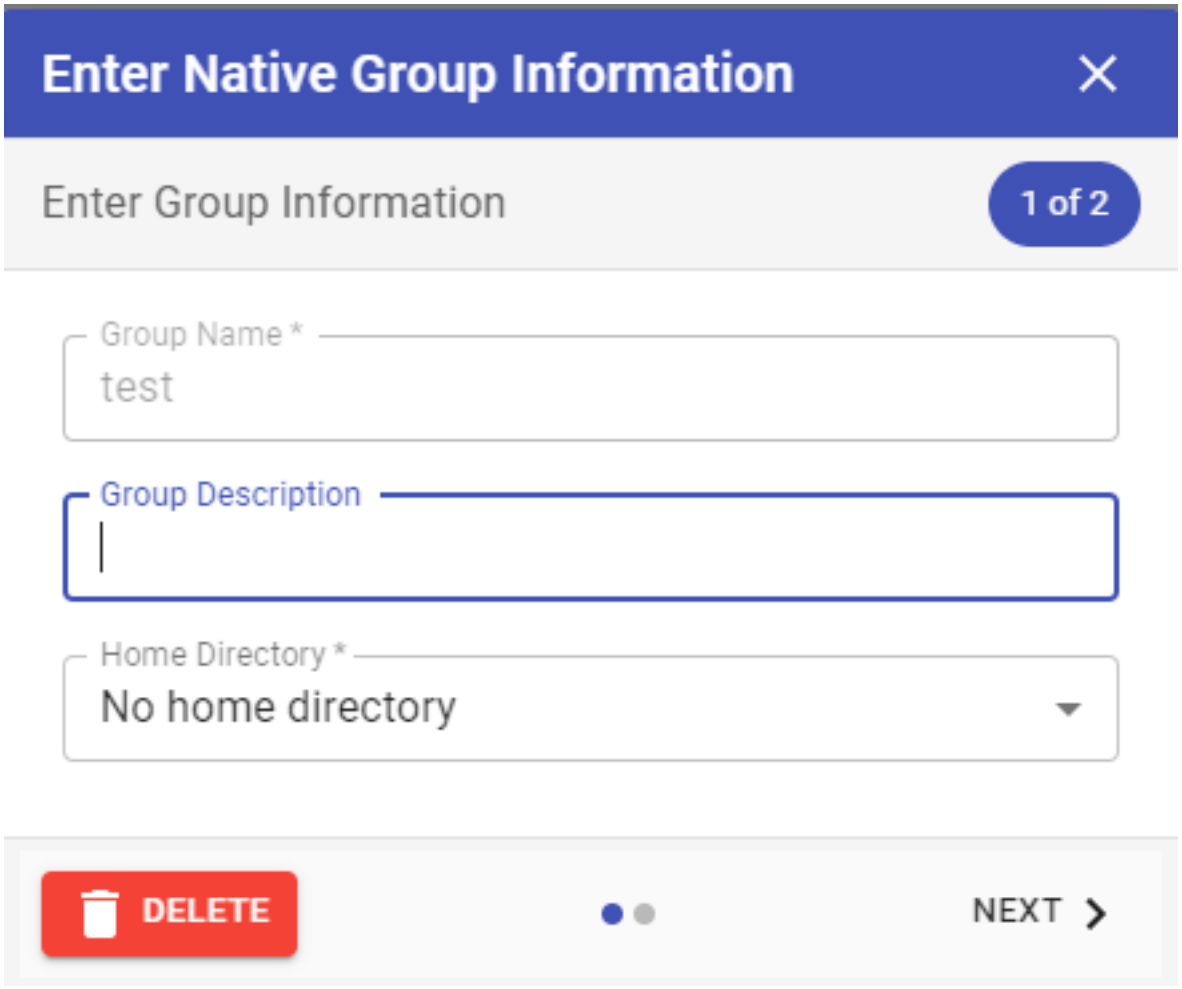
Inheritance Value	Meaning
	Setting is inherited from Parent
	Setting overridden from Parent
	Setting is disabled

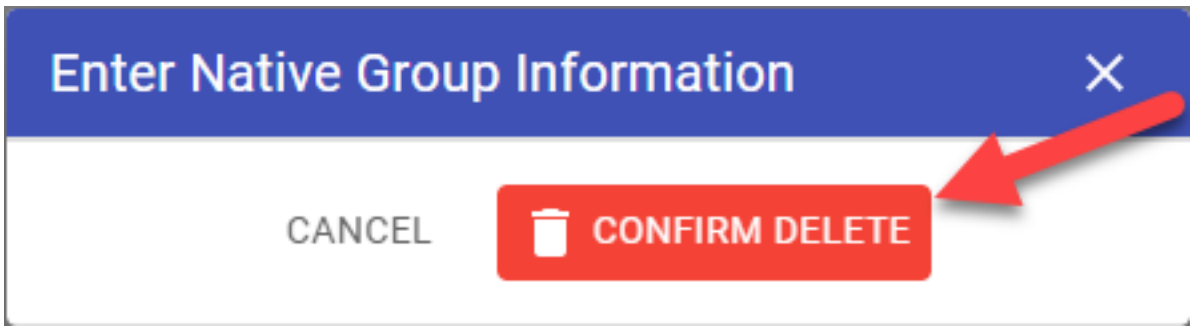
2. Click the **Finish** button.

Delete a Group

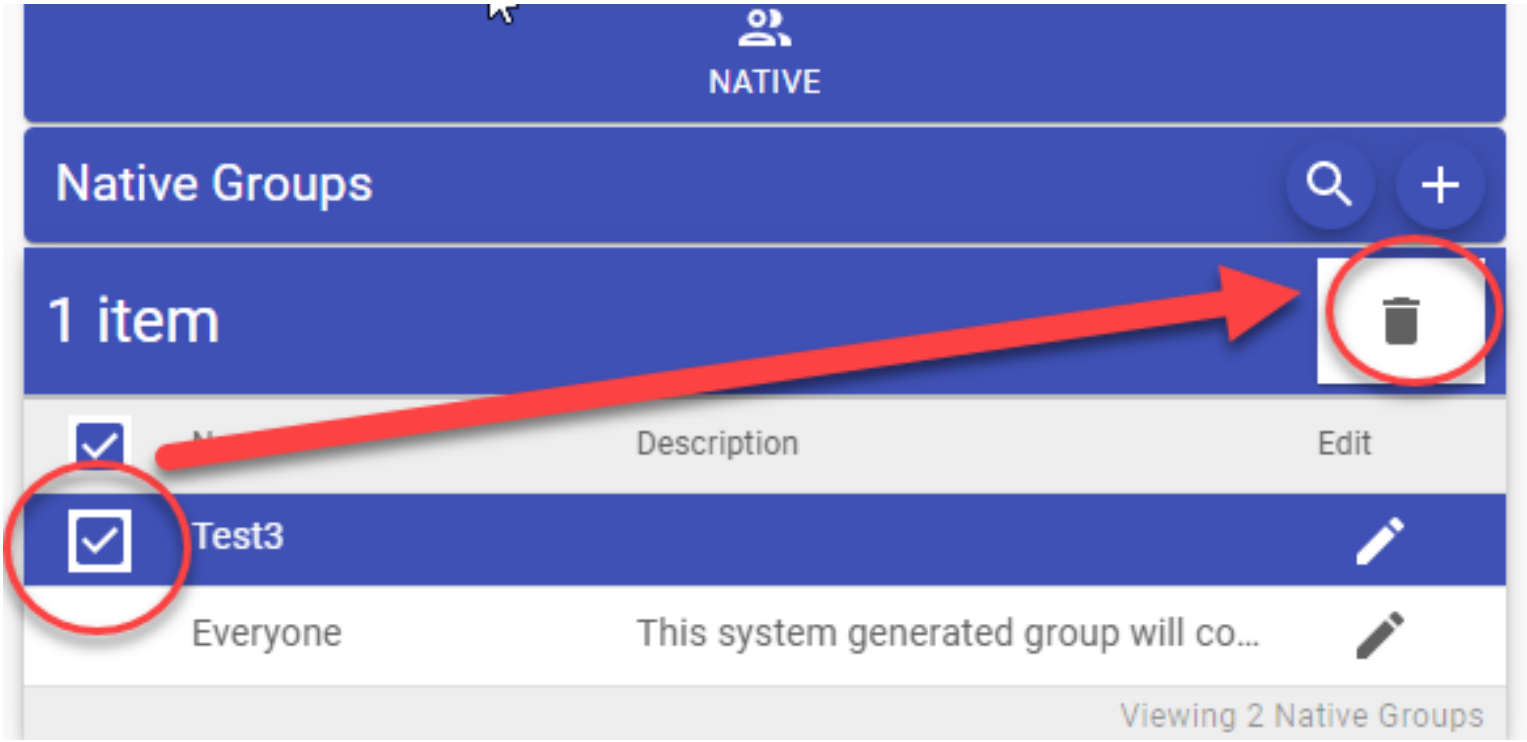
To delete a group, navigate to the Group on your left navigation. The Group screen displays. You can delete a Group in two ways.

1. You can delete a Group using the Edit Group & Assigned Users option:
    a. Click on the **pencil** icon next to the group that you want to edit.
    b. Click **Edit Group & Assigned Users**. The Enter Group Information window displays.
    c. Click on the **Delete** button at the bottom-left corner of the window.
    d. Click **Confirm Delete**.


Enter Native Group Information
Enter Group Information
1 of 2
Group Name *
test
Group Description
Home Directory *
No home directory
DELETE
NEXT


Enter Native Group Information
CANCEL
CONFIRM DELETE

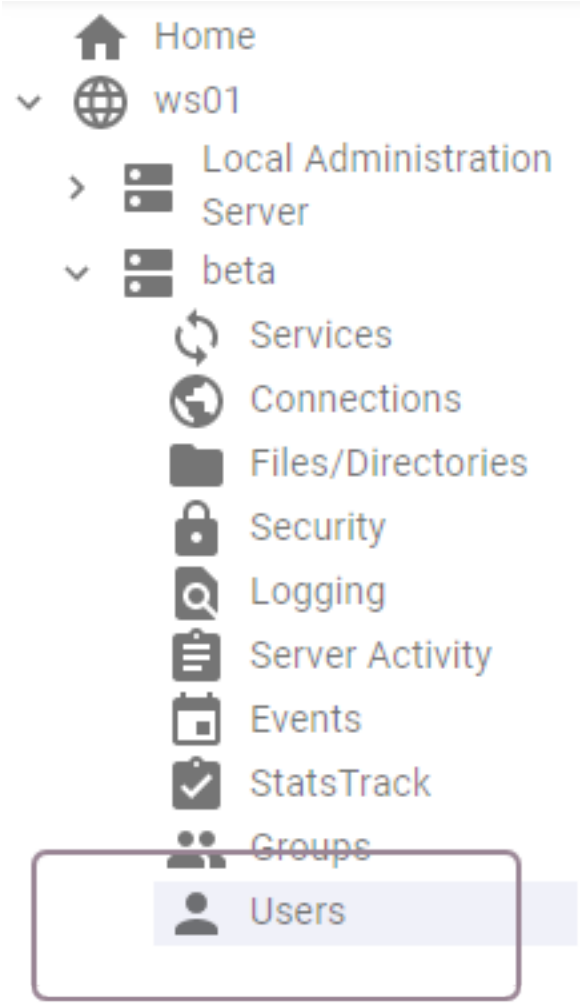
2. You can also delete a Group using the Main Group page.
    a. Navigate to **Groups** > **Native Groups**.
    b. Select the **check box** next to the group you want to delete.
    c. Click on the **trash bin** icon located on the top-right corner of the screen.



Users

Administrators can use the Users node to create new users or import them from an AD or LDAP source. Administrators can also use Users to specify authentication types (password, host key authentication, or both), connection limits, and access rights for all or select user accounts.

By default, settings in this section are inherited from the Group level, which inherits its settings from the Server level. However, an administrator can override settings at the User level.



Creating Users

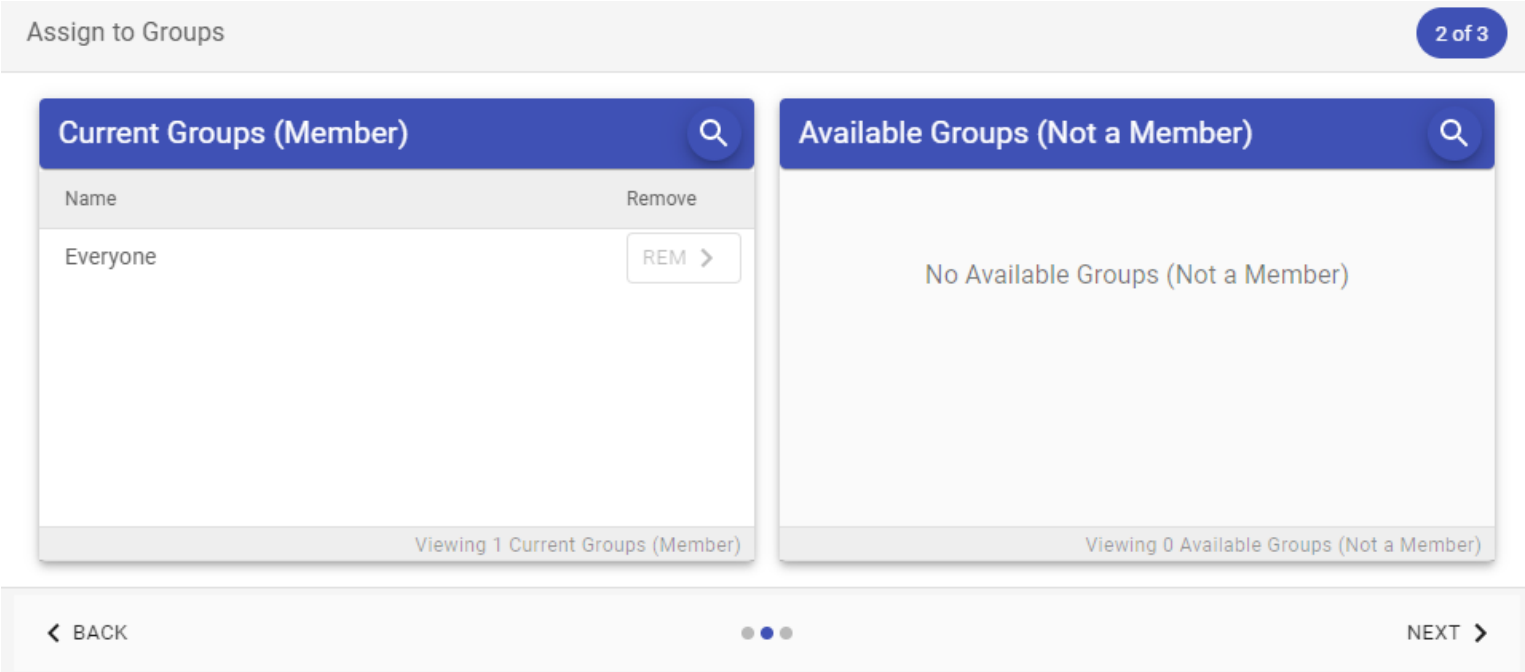
To create a user:

1. Select the **plus** icon at the top of the Native Users page. The Enter User Information screen appears.
2. Fill in the following fields for the User Information Screen and click **Next**:
    a. **User 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.
    b. **User Name:** A unique name used to log into the Titan server.
    c. **Password:** Specify the password.
    d. **Confirm Password:** Retype/confirm the password.
    e. **Email Address:** The email address of the user.
    f. **Mobile Number:** The mobile phone number of the user.
    g. **Preferred Notification Method(s):** The notification method the user would prefer. The options are by **Email** or **SMS**. Please keep in mind that Titan FTP Server will need the user's email address and/or mobile number in order for notifications to be sent to the user.
    h. **Additional User Roles:**
        A. **Server Admin:** Provides users with access to Server-level settings (Services, Connections, Files/Directories, Security, etc.) through the WebUI. This role will be limited to Server-level settings and will not have access to Group or User-level settings.
        B. **Group Admin:** Provides users with access to Group-level settings (adding, importing, deleting Groups, modifying Group Services, Connections, File/Directories, Security, etc.) through the WebUI. This role will be limited to Group-level settings and will not have access to Server or User-level settings.

C. **User Admin:** Provides users with access to User-level settings (create/delete users, change/reset passwords, and modify user access) through the WebUI. This role will be limited to User-level settings and will not have access to Server or Group-level settings.

i. **User Description:** A descriptor of the user name to help easily identify its purpose.

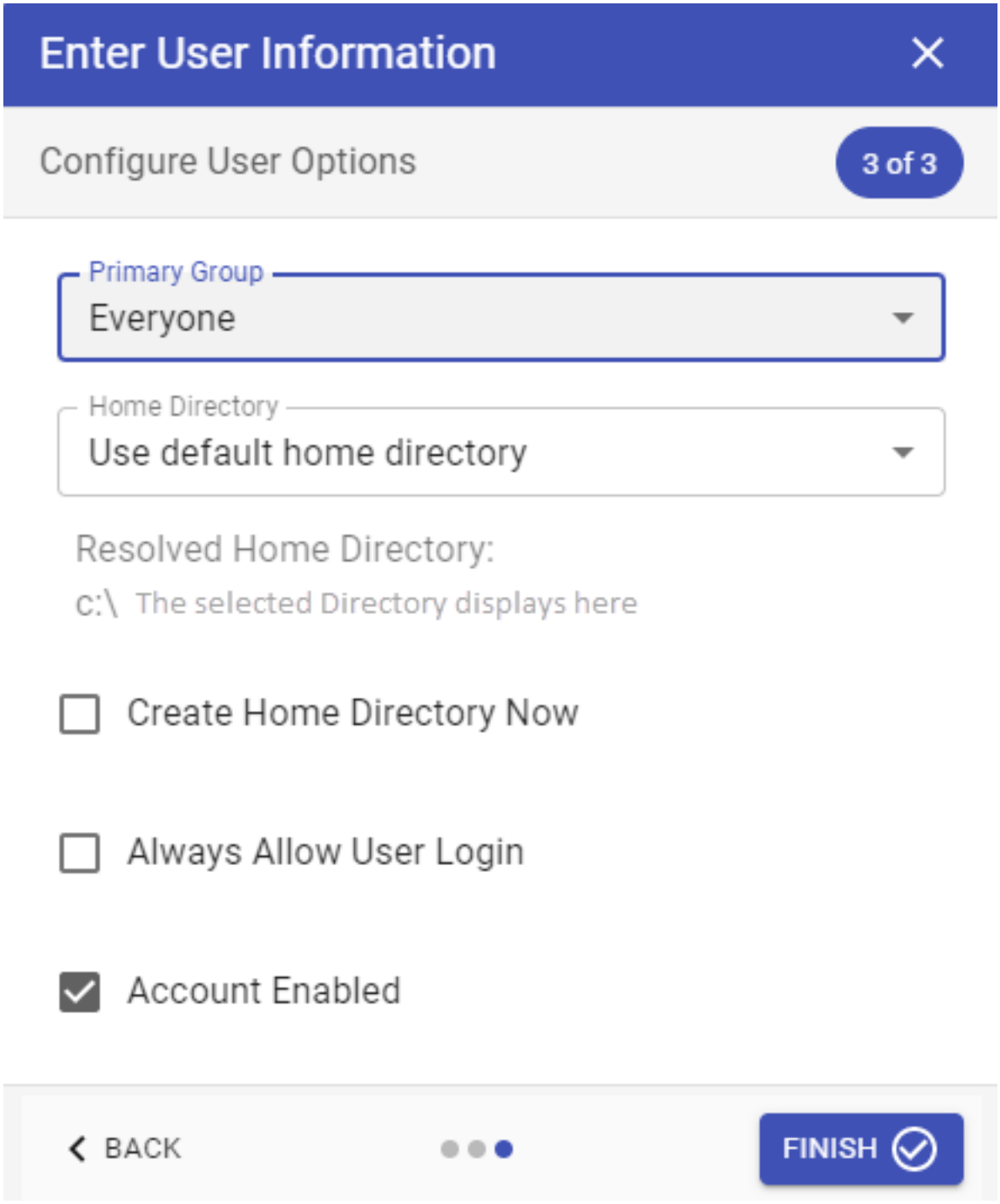
3. The Assign to Groups screen appears and lists the groups this user is a part of. To add groups, select a **group** in the Available Groups (Not a member) list and use the **arrows** to shunt the group back and forth until the member is a part of the appropriate groups. Click **Next** when you have completed your changes.



Note: The Current Groups window displays groups that the user is currently assigned to. You can click the **Remove** button to remove the user from a group. By default, all users are added to the Everyone group, and users cannot be removed from it.

The Available Groups window displays groups available to assign.

4. The Configure User Options screen appears. Fill in the following fields for the User Information Screen:
    a. **Primary Group:** The main group for a user account if multiple groups are assigned to the user.
    b. **Home Directory:** The directory that will display automatically to the user.
        A. **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.
        B. **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.
        C. **Use custom 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).
    c. **Create Home Directory Now:** 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.
    d. **Always Allow User Login:** 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).
    e. **Account Enabled:** The user account is enabled by default, but the administrator can choose to create it in a disabled state.



5. Click the **Finish** button. The Success confirmation displays at the bottom of your screen.

Editing User Properties

To edit a Group, do the following:

2. Click on the **pencil** icon next to the User that you want to edit. The Enter User Information screen displays. You can update the following on this screen:

   For **Edit User & Assigned Groups:**

   - **User 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.
   - **User Name**: A unique name used to log into the Titan MFT server.
   - **Email Address**: The email address of the user.
   - **Mobile Number**: The mobile phone number of the user.
   - **Preferred Notification Method(s)**: The notification method the user would prefer. The options are by **Email** or **SMS**. Please keep in mind that Titan FTP Server will need the user's email address and/or mobile number in order for notifications to be sent to the user.
   - **Additional User Roles**:
     - **Server Admin**: Provides users with access to Server-level settings (Services, Connections, Files/Directories, Security, etc.) through the WebUI. This role will be limited to Server-level settings and will not have access to Group or User-level settings.
     - **Group Admin**: Provides users with access to Group-level settings (Adding, importing, deleting Groups, modifying Group Services, Connections, File/Directories, Security, etc.) through the WebUI. This role will be limited to Group-level settings and will not have access to Server or User-level settings.

    - **User Admin**: Provides users with access to User-level settings (create/delete users, change/reset passwords, and modify user access) through the WebUI. This role will be limited to User-level settings and will not have access to Server or Group-level settings.
- **User Description**: A descriptor of the user name to help easily identify its purpose.

3. The Assign to Groups screen displays. Update the groups this user is a part of. To add groups, select a **group** in the Available Groups (Not a member) list and use the **arrows** to shunt the group back and forth until the member is a part of the appropriate groups. Click **Next** when you have completed your changes.
4. The Configure User Options screen appears. Fill in the following fields for the User Information Screen:
    - **Primary Group**: The main group for a user account if multiple groups are assigned to the user.
    - **Home Directory**: The directory that will display automatically to the user.
        - **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 for inheritance to work.
        - **Use custom 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 Home Directory Now**: 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.
    - **Always Allow User Login**: 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).

- **Account Enabled**: The user account is enabled by default, but the administrator can choose to create it in a disabled state.

For **User Services**:

- These *Server access (FTP/S, SFTP, & HTTP/S)* values within the User Services are inherited (see Inheritance table below) from the Services setting set at the Group level. These settings can be overridden to restrict control and/or access to the user. For more information on these settings, please see "File Transfer Protocol (FTP) Configuration" on page 73.

For **User Connections**:

- These *General & Advanced Connection* values within the User Connections are inherited (see Inheritance table below) from the Connections setting set at the Group level. These settings can be overridden to enforce or ease end user connections for the user. For more information on these settings, please see "Connection Settings" on page 88.

For **User Files & Directories**:

- These *Files & Directories* values within the User Files & Directories are inherited (see Inheritance table below) from the Files & Directories setting set at the Group level. These settings can be overridden to add additional directories, virtual folders, file restrictions, or quotas for the user. For more information on these settings, please see "Files and Directories" on page 92.

For **User Security**:

- These *Security* values within the User Security are inherited (see Inheritance table below) from the Security settings set at the Grouplevel. These settings can be overridden to fine tune the IP Access and PGP setting for the user. For more information on these settings, please see "Security" on page 103.

Inheritance Value	Meaning
	Setting is inherited from Parent

Inheritance Value	Meaning
	Setting overridden from Parent
	Setting is disabled

- **Set User Password**: This option allows an administrator to reset a user's password. Please keep in mind that no email will be sent out to the end user unless the administrator created such an Event.
- **Send Password Reset Email**: This option allows an administrator to send an email with a password reset link for the user to reset the password to their account. Titan FTP Server will automatically populate the email address in the email address field if the user account has an email address associated with the account. If not, it will need to be entered manually.

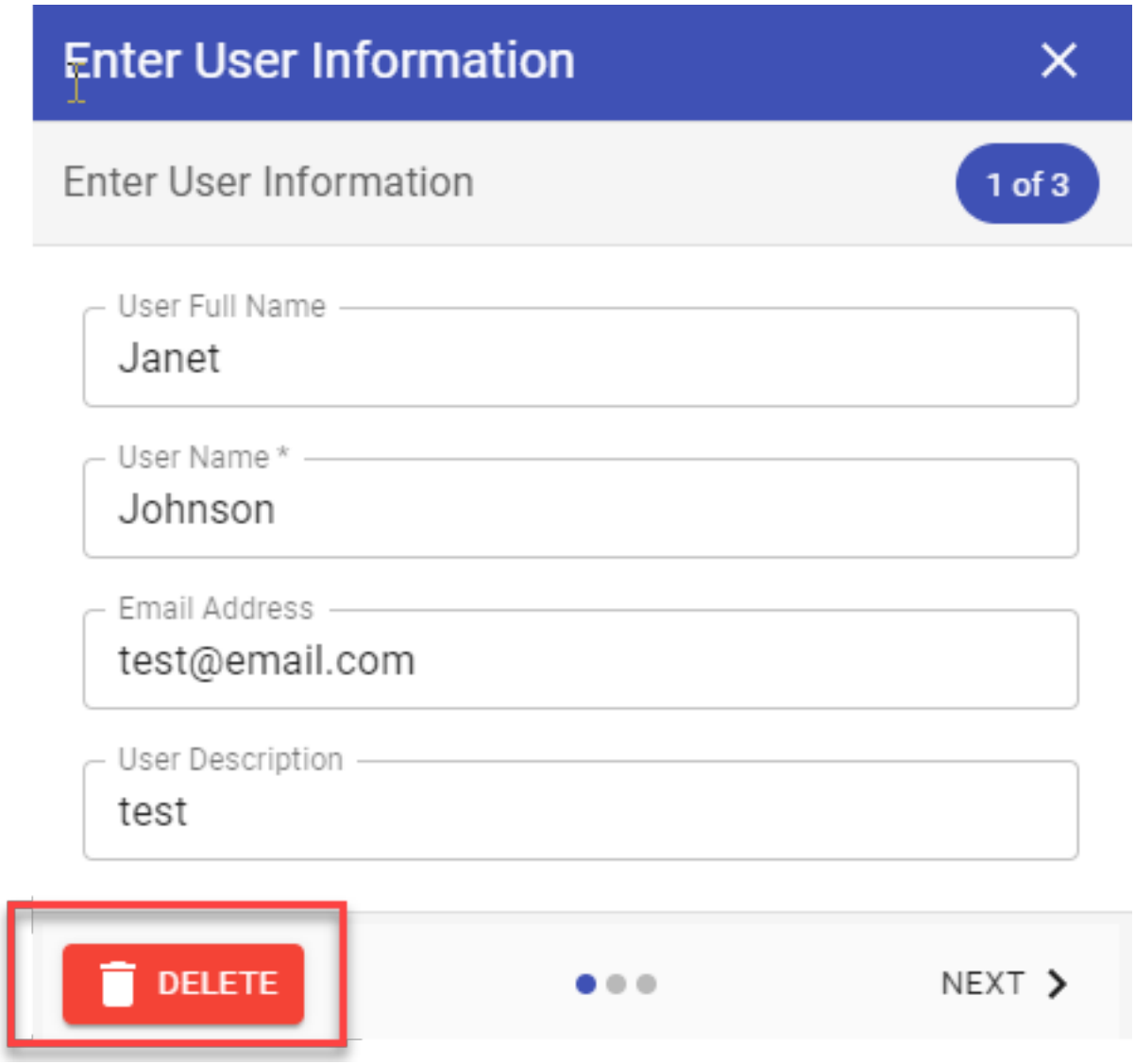
Deleting Users

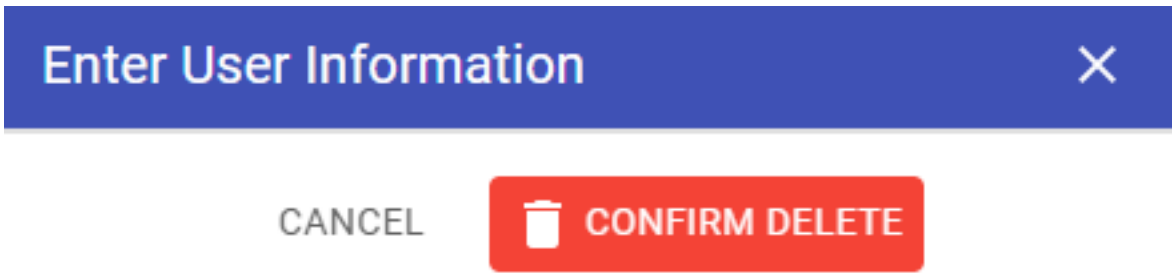
Deleting a user is *permanent*. If you are unsure about deleting a user account from the system, you may want to *Disable* the account. When you delete a user account, Titan FTP Server also removes the user from all groups.

To delete a user, click **Users** on the left navigation pane. The Native Users screen displays.

You can delete a user by using either of the following methods:

- Select the **check box** next to the user's name, and select the **trash bin** icon, or
- Select the **pencil** icon next to the user's name. The Enter User Information window displays. Then, click the **Delete** button at the bottom of the window and **Confirm Delete**:




Enter User Information
CANCEL
CONFIRM DELETE

Uninstall Cornerstone

To uninstall or remove Titan FTP Server from your system, do the following:

1. From the Windows Start menu, click **Control Panel**.
2. Click **Uninstall a Program** and locate Titan FTP Server on the list.
3. Click **Uninstall**. The Uninstall Successfully completed window displays:
4. Restart Windows to complete the process to uninstall Titan FTP Server.

How to Contact Support

For assistance, contact South River Technologies Support via phone or the portal, using the contact information below.

Contact Support through the Support Portal

Assistance through the support portal is available for all Levels of Support (Base, Business Standard, and Business Premium). Sign up is required to submit tickets for troubleshooting assistance. Access the portal at this link: https://helpdesk.southrivertech.com.

Contact Support by Phone

Assistance by phone is available for business standard and business premium members from 8:30am – 5:30pm EST by calling 443-603-0290 or by requesting callback in a support ticket, including dates and time of availability.

Appendix A: FTP Commands

Command	Purpose
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.

Command	Purpose
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 RNTO.
RNTO	Renames a file/folder. Used in conjunction with RNFR.
SITE	Special command used to issue site-specific instructions to Cornerstone MFT 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.

Command	Purpose
USER	Sends the username to the server.