



TitanFTP

S E R V E R

Windows NT SAM User Authentication Quick Start Guide

February 2010

Notices

Copyright 2010 South River Technologies, Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement, OEM, or reseller agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of South River Technologies, Inc.

South River Technologies[®], GroupDrive Collaboration Server[®], Cornerstone MFT[™], Titan FTP Server[®], DMZedge Server[™], and WebDrive[®] are trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP, and Windows Vista are trademarks of Microsoft Corporation, Inc. The names of other actual companies and products mentioned herein may be the trademarks of their respective owners. Any information in this document about compatible products or services should not be construed in any way to suggest SRT endorsement of that product or service.

South River Technologies, Inc.
2635 Riva Road
Suite 100
Annapolis, Maryland 21401
USA
Telephone: 410-266-0667
Fax: 410-266-1191
www.southernrivertech.com

Please Note: The following instructions will help you to set up Titan FTP Server for user authentication with Microsoft Windows NT Security Accounts Manager (SAM). For the purpose of this quick start guide, we will guide you through these options without configuring additional settings. If you need additional assistance, the [Titan FTP User Guide](#) is available on line. A *Frequently Asked Questions* (FAQ) is available at our [Knowledgebase Support Center](#) and a complete listing of our help documentation is available on our [Web site](#).

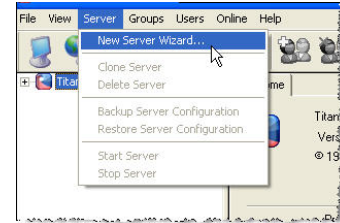
Creating a special NT User Account

If you would like to use Windows NT SAM (Security Accounts Manager) for user authentication with Titan FTP Server, a special NT User Account must be created. The special NT User Account will be used by the Titan Service when it needs to authenticate FTP clients when they connect to the system (it will **not** be used by the FTP clients to connect to the server). This special NT User Account will be given certain rights not usually available to other NT User accounts. The Titan Service will also need to be modified to use this new NT User account that will be created. Please see [Appendix A](#) for instructions on how to create a special NT User Account for use with Titan FTP Server.

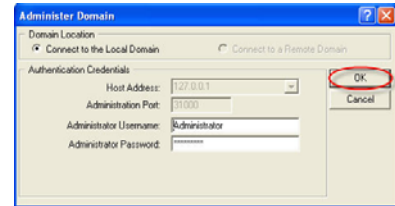
Please Note: Some screens in this instruction contain options that do not pertain to Windows NT SAM Authentication. If you need additional information regarding these steps, please see the [Titan FTP User Guide](#). For the purpose of this Windows NT SAM User Authentication quick start guide, we will guide you through these options without configuring additional settings.

Configuring NT SAM User Authentication

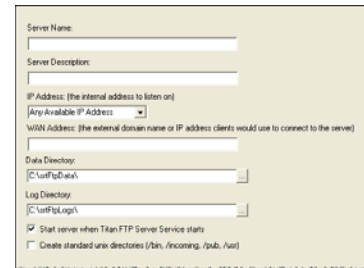
1. Run the *Titan Administration utility* and start the **New Server Wizard**.



2. When the *Administer Domain* window appears, select the radio button to connect to the Local Domain. Choose the Host Address by using the drop-down arrow. Type the **Administration Port**, **Administrator Username**, and **Administrator Password** and click **OK**.



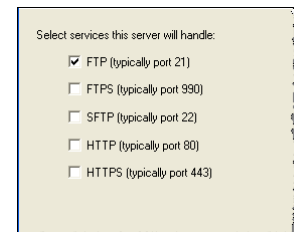
3. Type a unique **Server Name**. Click the drop-down arrow to choose your IP Address. (*Any Available IP Address* indicates that 127.0.0.1 is localhost.) Type the **WAN** address, for example, **myserver.com**. Click the *Data Directory "..."* button to browse to the Data Directory. Click the *Log Directory "..."* button to browse to the Log Directory. Select the check box to start this server when Titan FTP Server starts. When you are finished, click **Next**.*



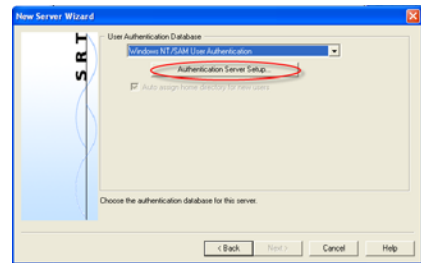
*If you need to create standard UNIX directories you can find additional information in the [Titan FTP Server User's Guide](#).

4. Select the **Services** this server will handle. Click **Next**.

Note: You must enable FTP access if you plan on using FTP/S with explicit SSL (Auth SSL).

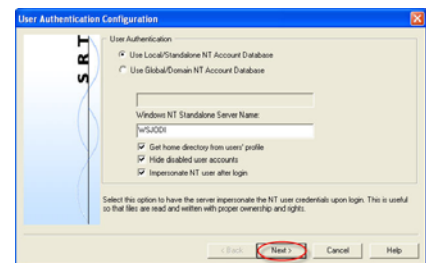


5. Select **Windows NT/SAM User Authentication** and then click the **Authentication Server Setup** button. This will launch the *Windows NT/SAM User Authentication sub-wizard*.

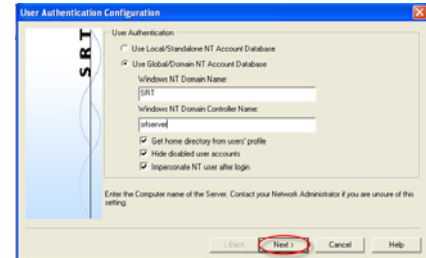


6. Choose *Use Local/Standalone NT Account Database* or *Use Global/Domain NT Account Database*. Configuration options will vary depending on which option you choose.

If you select **Use Local/Standalone NT Account Database**, the *Standalone Server Name* will be pre-populated with the name of the local computer. Select additional options using the check boxes. We recommend that you select all three additional options.



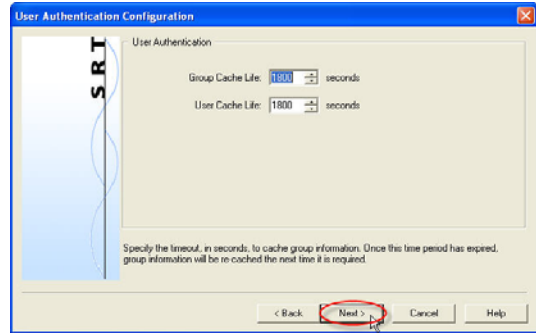
If you select **Use Global/Domain NT Account Database**,* Type the *Windows NT Domain Name* and the *Windows NT Domain Controller Name*. Select additional options using the check boxes. We recommend that you select all three additional options.



When you are finished, click **Next**.

*A special NT User Account must be created to use NT SAM User Authentication with Titan FTP Server. See [Appendix A](#) for instruction on how to create this special NT User Account.

7. Set the *Group Cache Life** using the up/down arrows. Click **Next**.



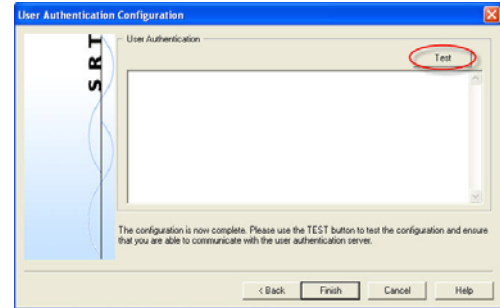
* Titan FTP Server will cache user and group information to increase performance and decrease the load on your back-end authentication server. The number of seconds that Titan caches this information is controlled by the *User Cache Life* and *Group Cache Life* values. The *Group Cache Life* value is used by Titan to determine how long to wait before refreshing the group information and also the list of members of that group. Once the cache life has expired, Titan will flag the cached group information as “stale” and the next time Titan needs that group information it will reload the group properties (and the list of members of the group) from the remote database. This means that if you modify the membership of the group by adding new users, or deleting users from the group, those changes will not appear in Titan until the *Group Cache Life* value has expired and Titan can reload that information. Therefore, if you have a dynamic system where the users/groups change frequently, set the *Group Cache Life* value to a short value, such as 300 seconds (five minutes).

The same applies to the *User Cache Life* setting. If you make a change to a user account in the back-end authentication server, these changes will not appear in Titan until the *User Cache Life* value has expired on that user account. The exception to the rule is the user’s password. Titan never caches user passwords so any changes to the user’s password in the NT SAM user database will take effect immediately.

Warning: Avoid setting the Cache Life values too small. If you set the values too small, the performance could degrade because Titan will be spending too much time flushing and reloading the user/group information from the authentication server.

If you add and delete users frequently, change the Group Cache to 300 seconds.

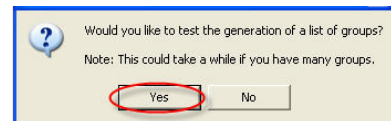
- Click **Test** to test the configuration and ensure that you are able to communicate with the user authentication server.



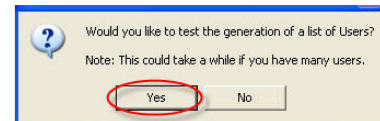
- If Titan FTP Server can successfully communicate with the NT SAM Authentication database the message that displays is *Success*. Click **OK**. (If an error is displayed, Titan was not able to connect to the server.)



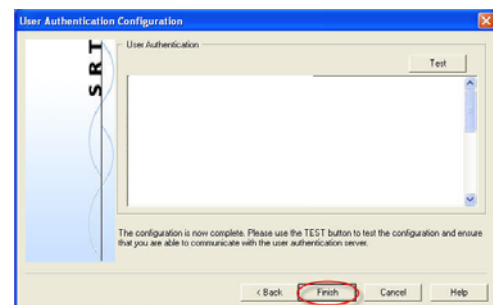
- After Titan FTP successfully connects to the database, Titan will attempt to generate a list of groups. Click **Yes** to test the generation of a list of groups.



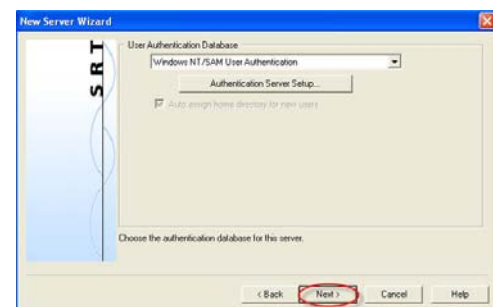
- Click **Yes** to test the generation of a list of Users.



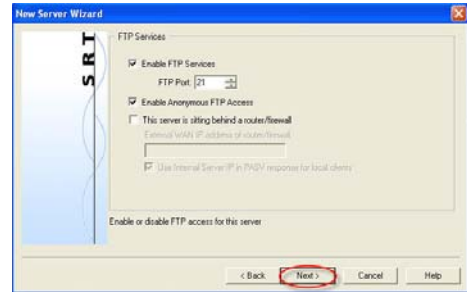
- Click **Finish**.



- You are now returned to the *Titan FTP New Server Wizard*. Click **Next**.

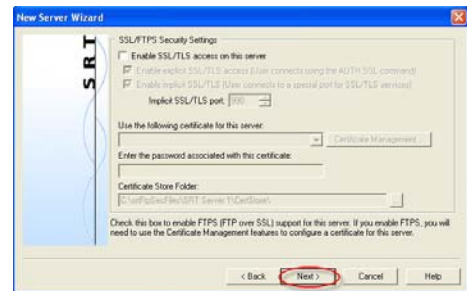


14. If you wish to enable FTP Services select the *Enable FTP Services* check box. Select the *FTP Port* number by using the up/down arrows. To enable anonymous FTP access, select the check box. If your server is sitting behind a router/firewall select this check box. When you are finished with *FTP Services* options* click **Next**.



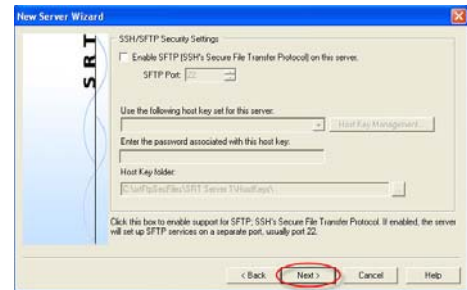
*For more detailed information pertaining to these configuration options see the [Titan FTP Server User's Guide](#).

15. To enable SSL/TLS access on this server select this check box and choose the appropriate sub-option. Click the drop-down arrow to choose the certificate. Click **Certificate Management** to configure a certificate for this server. Enter the password associated with the certificate. Use the "..." button to browse to the *Certificate Store Folder*. When you are finished configuring SSL/FTPS Security Settings,* click **Next**.



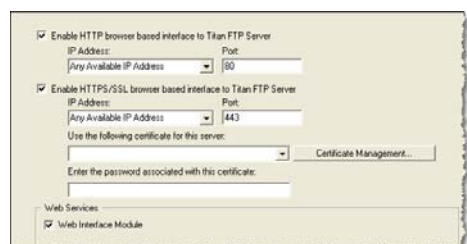
*For more detailed information pertaining to these configuration options see the [Titan FTP Server User's Guide](#).

16. To enable SFTP (SSH's Secure File Transfer Protocol) on this server select the check box and choose the SFTP port (default port 22) using the up/down arrows. Choose the *host key set* by using the drop-down arrow. Click **Host Key Management** for host key configuration options. Type the password associated with the host key. Click the "..." button to browse to the *Host Key folder*. For more detailed information pertaining to these configuration options, see the [Titan FTP Server User's Guide](#). Click **Next** when you are finished configuring SSH/SFTP Security Settings.

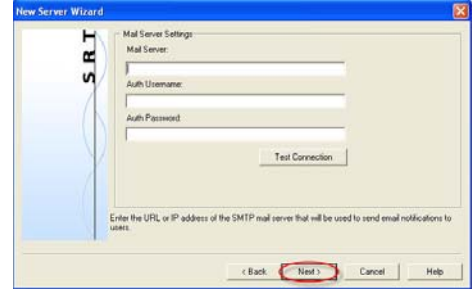


17. If you would like to enable **HTTP/HTTPS** access on this server, select the check boxes. To configure a certificate, click **Certificate Management**.

Note: The Titan Web Interface is an optional module. Contact sales@southrivertech.com for more information.

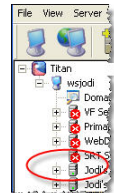


18. Type the URL or IP address of the SMTP mail server that will be used to send email notifications to users. You may test the connection by clicking **Test Connection**. (For more detailed information pertaining to these configuration options see the [Titan FTP Server User's Guide](#).) When you are finished click **Next**.



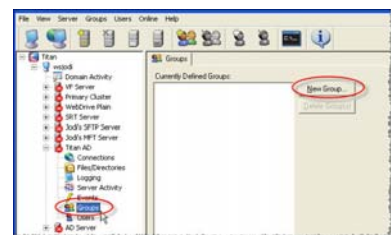
19. Click **Finish** to create the server.

20. Once the server is created, the server starts and appears in the main Titan FTP Administrator window. A green icon appears to indicate that the server is running. At this point, there are no external groups or users mapped to Titan FTP Server.*

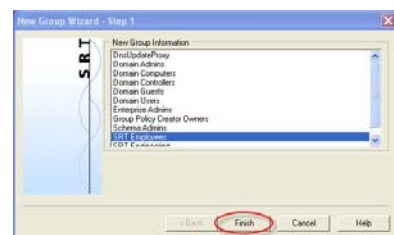


***PLEASE NOTE:** All Titan FTP Server users must belong to a group. Before any users can access the system, you must add one or more groups to the server. Because Titan FTP Server uses the NT SAM user database, groups that will participate in the Titan FTP Server must be selected/mapped into Titan FTP Server from the NT SAM database. To do this, you must run the *New Group Wizard* to add a new group to the Titan FTP Server.

21. Expand the server menu and click **Groups**. Click **New Group** to launch the *New Group Wizard*.



22. Select one or more NT Groups to be granted access to this server. Click **Finish**.



23. It is now time to test the server.*

Open a command prompt and type:

ftp and then press the Enter key.

Type either:

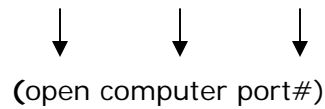
open localhost

-OR-

the IP Address that you specified in [step 4](#).

If you specified a port number in [Step 16](#) you must add the port number.

For example, type: open localhost 21



```
C:\WINDOWS\system32\ftp.exe
ftp> open localhost
Connected to wsjodi.
220 Service ready for new user.
User (wsjodi:(none)): user1001
331 User name okay, need password.
Password:
230 Welcome user1001 from 127.0.0.1. You are now logged in to the server.
ftp>
```

This will begin an FTP session with the local Titan FTP Server that you created.

When prompted, enter the user name: **user1001**

When prompted, enter the user's password: **password**

You are now logged on to the Titan FTP Server.

Type **quit** to exit DOS and return to Windows.

*If you [enabled SFTP](#), please see **step 24** for an alternate method to test the server.*

24. If you enabled SFTP you can download an SFTP client, such as **psftp.exe**, to test your server. After you have downloaded your SFTP client:

Open a command prompt and type: **psftp** and then press the enter key.

Type either:

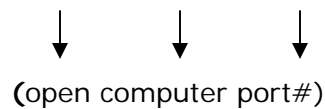
open localhost

-OR-

the IP Address that you specified in [step 3](#).

If you specified a port number in [Step 16](#) you must add the port number.

For example, type: open localhost 21



This will begin an SFTP session with the local Titan FTP Server that you created.

When prompted, enter the user name: **user1001**

When prompted, enter the user's password: **password**

You are now logged on to the Titan FTP Server.

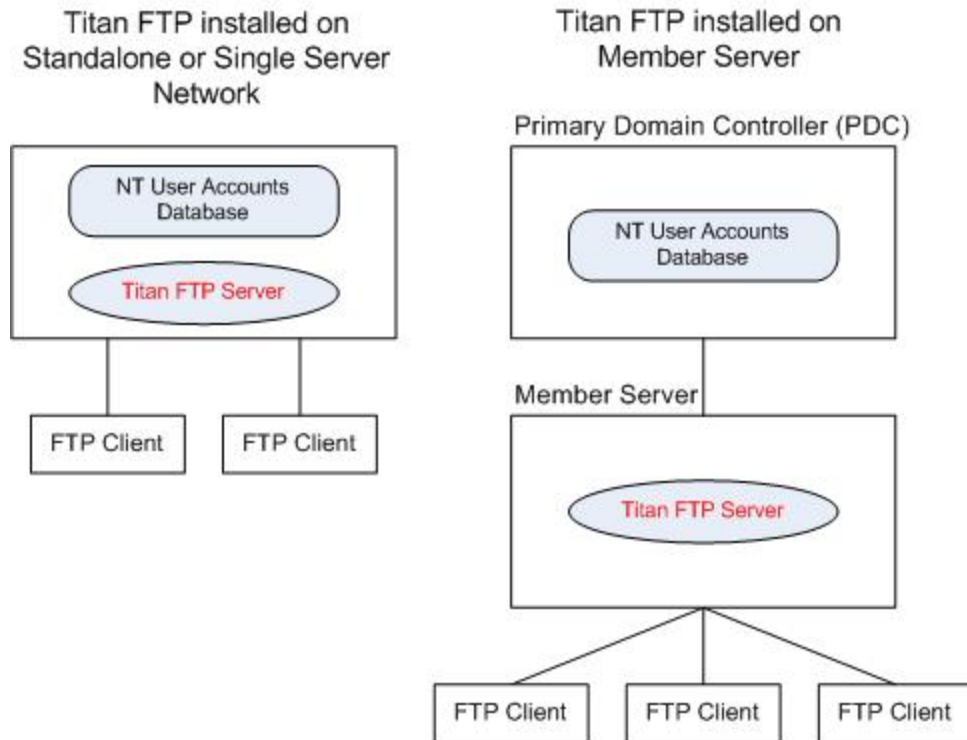
Type **quit** to exit DOS and return to Windows.

Appendix A: Creating a special NT User Account

If you would like to use Windows NT SAM (Security Accounts Manager) for user authentication with Titan FTP Server, a special NT User Account must be created. The special NT User Account will be used by the Titan Service when it needs to authenticate FTP clients when they connect to the system (it will **not** be used by the FTP clients to connect to the server). This special NT User Account will be given certain rights not usually available to other NT User accounts. The Titan Service will also need to be modified to use this new NT User account that will be created.

Titan FTP must be able to access the Windows NT SAM User Accounts Database whether Titan FTP is installed on a standalone or single server network, or on a multi-server network. There can be other servers on the network, but Titan will only interact with the server that stores the Windows NT SAM User Accounts database.

Using Titan FTP with Windows NT SAM Authentication



If Titan FTP Server is installed on the PDC, use the following steps to create the new NT User account:

1. On the PDC, create a new domain user account and make note of the username and password. For our example, we will use *titanuser* as the username and *titanpass* as the password. **NOTE: DO NOT USE THESE NAMES IN YOUR CONFIGURATION; USE SOMETHING VERY DIFFERENT TO PREVENT SOMEONE FROM POSSIBLY HACKING IN TO YOUR SYSTEM!**
2. Make *titanuser* a member of the *Domain Admins* and *Domain Users* groups.
3. Open the **Local Security Policy** applet on the **PDC** and under **Security Settings - > Local Policies -> User Rights Assignments** make sure that *titanuser* is granted the right to **Access Computer From The Network** and **Act As Part Of Operating System**.
4. Install Titan FTP Server on the PDC and restart the PDC.
5. Open the **Services** Control Panel Applet and scroll down to the **Titan FTP Server** service. Right-click on the **Titan FTP Server** service and select **Properties**.
6. Modify the **Log on As:** section so that the Titan FTP Service will log on using the *titanuser/titanpass* account that was created.
7. **Stop** then **Restart** the Titan FTP Service.

If Titan FTP Server is not being installed on the PDC, then the PC on which Titan is installed must be a Member Server of the domain:

1. On the **PDC**, create a new **Domain User Account** and make note of the username and password. For our example, we will use *titanuser* as the username and *titanpass* as the password. **NOTE: DO NOT USE THESE NAMES IN YOUR CONFIGURATION; USE SOMETHING VERY DIFFERENT TO PREVENT SOMEONE FROM POSSIBLY HACKING IN TO YOUR SYSTEM!**
2. Make *titanuser* a member of the *Domain Admins* and *Domain Users* groups.
3. Open the **Local Security Policy** applet on the **PDC** and under **Security Settings - > Local Policies -> User Rights Assignments** make sure that *titanuser* is granted the right to **Access Computer From The Network** and **Act As Part Of Operating System**.
4. On the **Member Server**, create a new **Local User Account** using the same username and password as the user in step 1. Make this user a member of the **Power Users** group.
5. Open the **Local Security Policy** applet on the **Member Server** and under the **Security Settings -> Local Policies -> User Rights Assignments** make sure that *titanuser* is granted the right to **Log on as a Service**.
6. Install Titan FTP Server on the **Member Server** and restart the **Member Server**.
7. Open the **Services** Control Panel Applet on the **Member Server** and scroll down to the **Titan FTP Server** service. Right-click on the **Titan FTP Server** service and select **Properties**.
8. Modify the **Log on As:** section so that the Titan FTP Service will log on using the *titanuser/titanpass* account that was created.
9. **Stop** then **Restart** the Titan FTP Service.

Titan FTP is now configured properly. The Titan FTP Service is now using a special NT User Account that has the proper rights necessary to query the PDC User Accounts Database during the authentication of an FTP client session. When a FTP client attempts to connect to a Titan FTP Server that has been set up to use NT Authentication, Titan FTP sends the FTP client's username and password over to the PDC User Accounts Manager asking if the FTP client username/password are valid. If they are, then Titan FTP will allow the FTP client to connect.

About South River Technologies

South River Technologies (SRT) is an innovator in managed file transfer and document collaboration software. SRT's software seamlessly integrates access to remote files into the desktop applications that users rely on, creating an instantly familiar interface for collaborating, sharing, and accessing files. SRT's enterprise class server products are built using industry standard encryption, highly granular security configuration controls, and technologies to reduce the risk of network intrusions. Over 60,000 customers, including more than 70 colleges and universities, government agencies such as NASA and FAA, and other blue chip companies in more than 110 countries rely on SRT's software to make remote file access and collaboration more efficient for their customers, partners, and distributed workforce. For more information, please visit www.southernrivertech.com.