

CornerstoneMFT

Windows Active Directory (AD) User Authentication Quick Start Guide

January 2010

Notices

© Copyright South River Technologies, 1996-2010. 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.

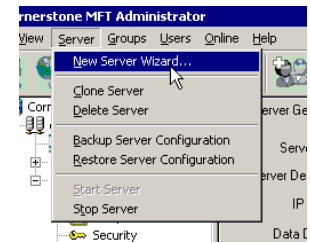
South River Technologies[®], GroupDrive Collaboration Server[®], Cornerstone MFT[™], Titan FTP Server[®], DMZedge Server[™], and WebDrive[®] are trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP, and Windows Vista are trademarks of 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.southrivertech.com

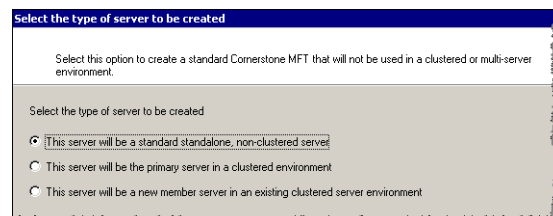
Please Note: The following instructions will help you to set up Cornerstone MFT for user authentication with Microsoft Windows Active Directory (AD). Some screens in this instruction contain options that do not pertain to Windows Active Directory Authentication. If you need additional information regarding these steps, please see the [Cornerstone MFT User Guide](#). For the purpose of this Windows Active Directory User Authentication Quick Start guide, we will guide you through these options without configuring additional settings. A listing of Frequently Asked Questions (FAQ) is also available at our [Knowledgebase Support Center](#)

Configuring the Cornerstone Administrator

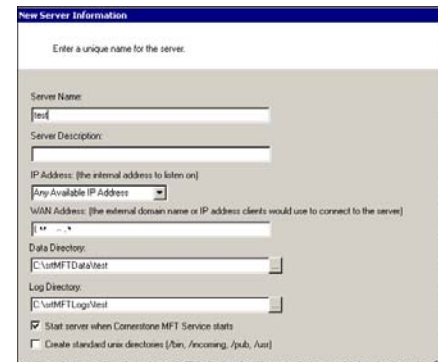
1. Run the Cornerstone Administration utility and start the New Server Wizard. When the *Administer Domain* window appears, Type the **Administrator Username** and **Administrator Password** and click **OK**.



2. Select the *Server Type* and click **Next**.

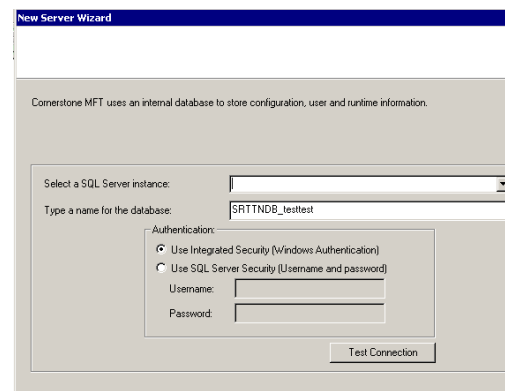


3. Type a unique **Server Name**. Click the drop-down arrow to choose your **IP Address**. (*Any available IP address* indicates that the server will listen on all IP addresses that are configured on the PC along with the local IP address of 127.0.0.0, also known as *localhost*.) Type the **WAN address**. You do not need to type "**http**", for example, "**myserver.com**". Select the check box to start this server when Cornerstone MFT starts. When you are finished, click **Next**.*

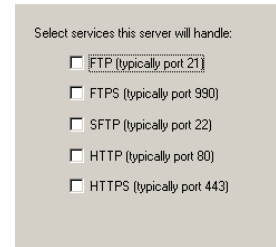


*If you need to create standard UNIX directories you can find additional information in the [Cornerstone MFT User's Guide](#).

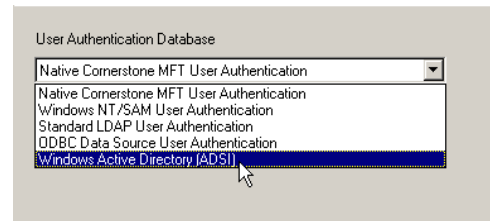
4. Cornerstone uses an internal database to store configuration, user, and runtime information. Use the drop-down arrow to select a SQL Server instance. Type a name for this database. Select **Windows Authentication** or **SQL Server Security**, and then click **Test Connection**. Once you connect successfully, click **Next**.



5. Select the **Services** that this server will handle.

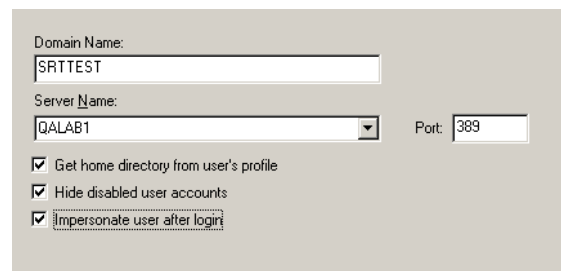


6. Select **Windows Active Directory User Authentication** and then click the **Authentication Server Setup** button. This will launch the *Windows Active Directory User Authentication sub-wizard*.*

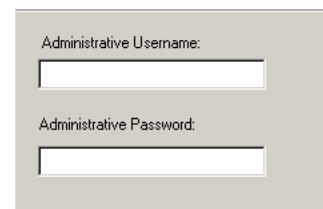


*Once you select a User Authentication Database in Cornerstone, you cannot change to a different method once the server wizard has completed.

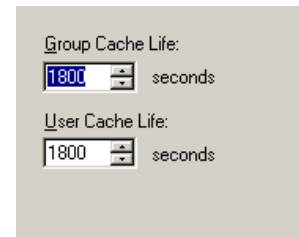
7. Type your **Windows AD Domain Name**, for example, **“mydomain.com”**. Use the drop-down arrow to choose your **AD Server Name**. Type your **port number** (the default port is 389). Select additional options using the check boxes. We recommend that you select all three additional options. When you are finished, click **Next**.



8. Type the **Administrative Username** and **password**. The Domain Administrator must have full administrative access to the AD server. For most AD servers, you will want to use the Domain Administrator account. The format for the username must be: **<username>@<domainname>**



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



Group Cache Life:
1800 seconds

User Cache Life:
1800 seconds

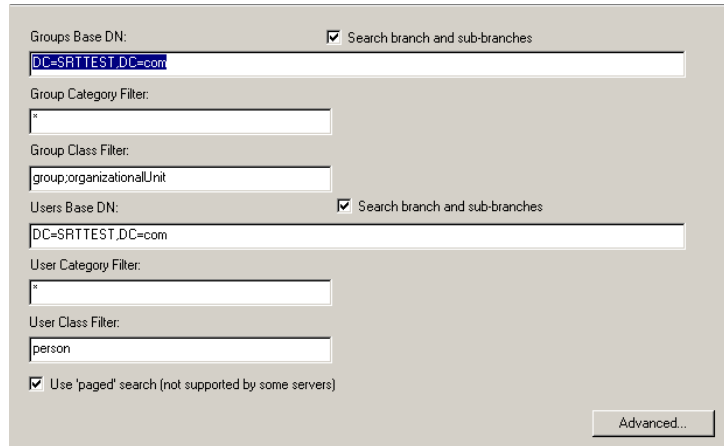
*Cornerstone MFT will cache user and group information to increase performance and decrease the load on your back-end authentication server. The number of seconds that Cornerstone caches this information is controlled by the *User Cache Life* and *Group Cache Life* values. The *Group Cache Life* value is used by Cornerstone MFT 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, Cornerstone will flag the cached group information as “stale” and the next time Cornerstone 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 Cornerstone until the *Group Cache Life* value has expired and Cornerstone 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 (5 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 Cornerstone until the *User Cache Life* value has expired on that user account. The exception to the rule is the user's password. Cornerstone MFT never caches user passwords so any changes to the user's password in the Active Directory 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 Cornerstone 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.

10. Type your **Groups Base DN**, **Group Category Filter**, **Group Class Filter**, **Users Base DN**, **User Category Filter** and **User Class Filter**. * To Use *paged search*, be sure that the check box is checked. Click the **Advanced**** button for additional configuration options. When you are finished, click **Next**.



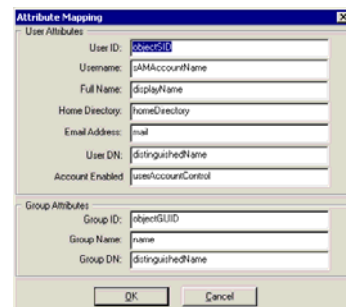
*Cornerstone MFT needs to be configured with the proper search strings in order to locate user and group information in the Active Directory. For most AD installations, the default values can be used and will return the proper user and group information from your AD. However, there are some instances where these values may need to be enhanced to allow Cornerstone MFT to find the user information in the AD.

Group/User Base DN—These values specify the LDAP search string(s) necessary to search the various trees/paths in the AD. By default, Cornerstone MFT will search under the **Users** and **BuiltIn** paths of your AD. Since these paths are sub-paths under the Domain that you specified in step 6, the full Distinguished Name (DN) for the search path needs to include the parent domain. To search the **USERS** path, the DN needs to be “**CN=Users, DC=SRT**”. If the domain name that you specified was “**XYZ.COM**”, then the DN would be “**CN=Users,DC=XYZ,DC=COM**”. Since Cornerstone MFT will search multiple paths, each path is separated with a **semicolon**. So the complete entry to search both **Users** and **BuiltIn** is “**CN=Users,DC=SRT;CN=BuiltIn,DC=SRT**”.

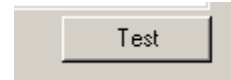
Group/User Category—These values are used to filter out certain categories of users and groups. In general you will want to include all users and groups, so this value should remain as an **asterisk**.

Group/User Class Filter—These values are used to filter out certain classes of users and groups. Multiple classes should be separated by **semicolons**.

** If you wish to configure Advanced User and Group Attributes, type your information and then click **OK**. You will then click **Next** to test your settings.

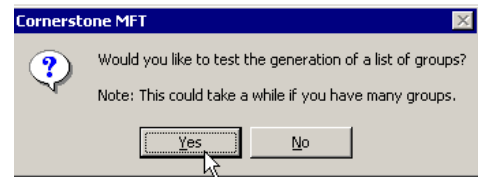


- Click **Test*** to test the configuration and ensure that you are able to communicate with the user authentication server.

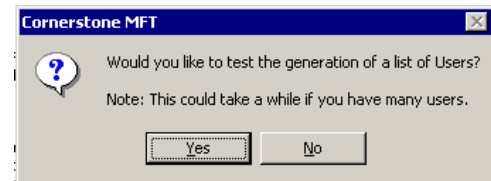


*If this process fails, the most common reason is that either the AD Domain Name is not specified correctly, or the AD Server Name is not accessible. Click the Back button to return to previous pages and adjust the values. If Cornerstone MFT can successfully communicate with the AD Authentication database the message that displays is *Success*. Click **OK**. (If an error is displayed, Cornerstone was not able to connect to the server.)

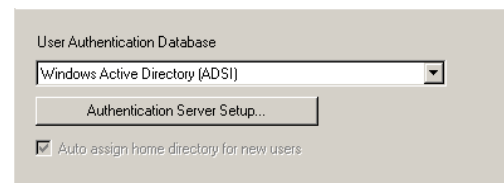
- After Cornerstone MFT successfully connects to the database, Cornerstone will attempt to generate a list of groups. Click **Yes** to test the generation of a list of groups.



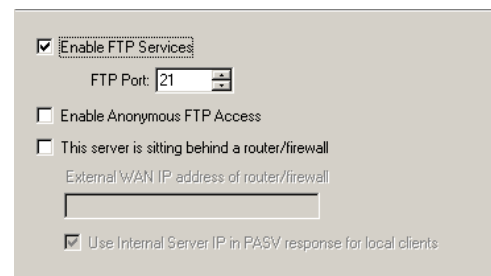
- Click **Yes** to test the generation of a list of Users, and then click **Finish**.



- You are now returned to the *Cornerstone MFT New Server Wizard*. Click **Next**.

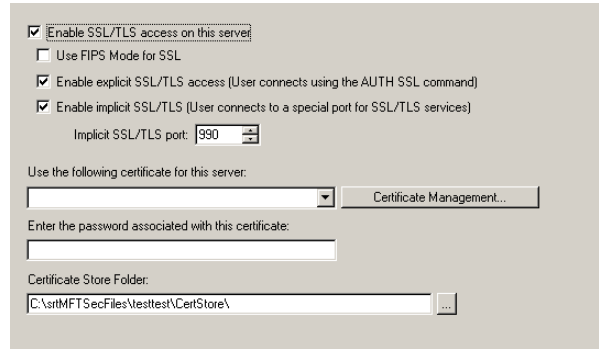


- If you wish to enable FTP Services select the *Enable FTP Services* check box. Select the *FTP Port* number by using the up/down arrows. To enable anonymous FTP access, select the check box. If your server is sitting behind a router/firewall select this check box and type the external WAN address of the router/firewall. You do not need to type "**http**", for example, **mywanaddress.com**. When you are finished with *FTP Services* options* click **Next**.



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

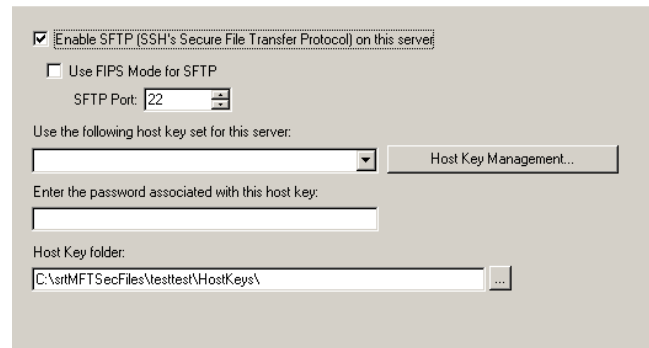
16. To enable SSL/TLS access on this server select this check box and choose the appropriate sub-option. Click the drop-down arrow to choose the certificate. Click **Certificate Management** to configure a certificate for this server. Enter the password associated with the certificate. Use the "..."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



Enable SSL/TLS access on this server
 Use FIPS Mode for SSL
 Enable explicit SSL/TLS access (User connects using the AUTH SSL command)
 Enable implicit SSL/TLS (User connects to a special port for SSL/TLS services)
 Implicit SSL/TLS port: 990
 Use the following certificate for this server:
 [Certificate Management...]
 Enter the password associated with this certificate:
 [_____
 Certificate Store Folder:
 C:\sr\MFTSecFiles\Mestest\CertStore\

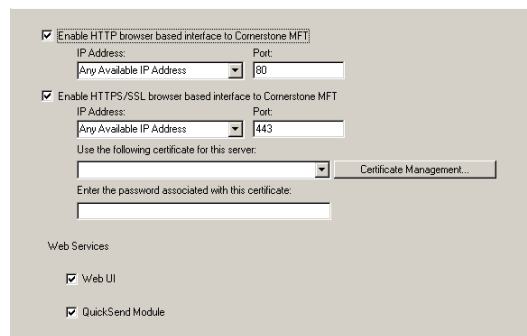
*For more detailed information pertaining to these configuration options see the [Cornerstone MFT User's Guide](#).

17. 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 browse "..." button to browse to the *Host Key folder*. For more detailed information pertaining to these configuration options, see the [Cornerstone MFT User's Guide](#). Click **Next** when you are finished configuring SSH/SFTP Security Settings.



Enable SFTP (SSH's Secure File Transfer Protocol) on this server
 Use FIPS Mode for SFTP
 SFTP Port: 22
 Use the following host key set for this server:
 [Host Key Management...]
 Enter the password associated with this host key:
 [_____
 Host Key folder:
 C:\sr\MFTSecFiles\Mestest\HostKeys\

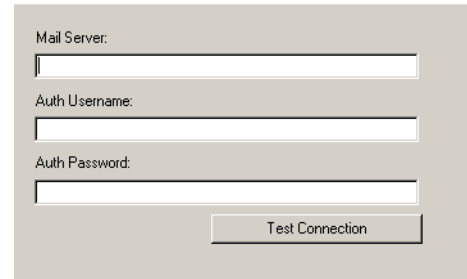
18. To enable **HTTP browser based interface** to this server, select the check box. To enable **HTTPS browser based interface** to this server, select the check box and use the drop-down arrow to select a certificate or click **Certificate Management** to manage certificates. Select the **Web UI** check box if you would like to enable the Cornerstone Web User Interface on this server. Select **QuickSend Module** if you would like to enable ad-hoc transfer.



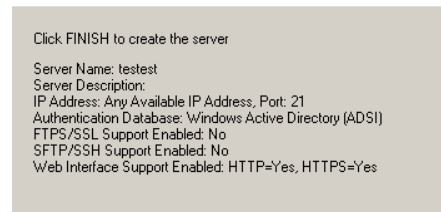
Enable HTTP browser based interface to Cornerstone MFT
 IP Address: [Any Available IP Address] Port: 80
 Enable HTTPS/SSL browser based interface to Cornerstone MFT
 IP Address: [Any Available IP Address] Port: 443
 Use the following certificate for this server:
 [Certificate Management...]
 Enter the password associated with this certificate:
 [_____
 Web Services
 Web UI
 QuickSend Module

NOTE: QuickSend and the Cornerstone Web UI are optional modules. For more information, contact sales@southernrivertech.com.

19. 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 [Cornerstone MFT User's Guide](#).) When you are finished click **Next**.



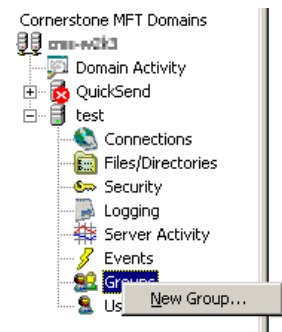
20. Click **Finish** to create the server.



21. Once the server is created, the server starts and appears in the main *Cornerstone MFT 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 Cornerstone MFT.*

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

22. Expand the server menu and click **Groups**. Click **New Group** to launch the *New Group Wizard*. Select one or more AD 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:

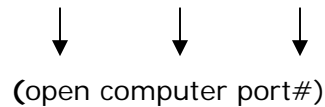
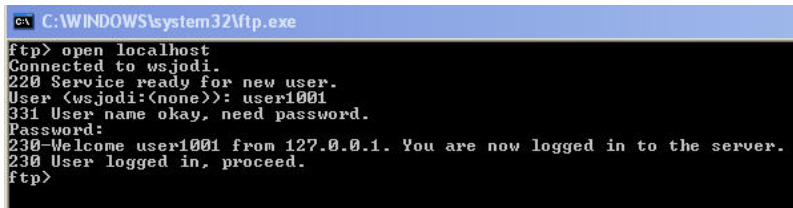
open localhost

-OR-

the IP Address that you specified in step 3.

If you specified a port number in Step 15 you must add the port number.

For example, type: `open localhost 21`



This will begin an FTP session with the local Cornerstone MFT 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 Cornerstone MFT.

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

If you enabled SFTP, please see step 26 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:

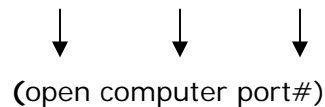
open localhost

-OR-

the IP Address that you specified in step 4.

If you specified a port number in Step 14 you must add the port number.

For example, type: `open localhost 21`



This will begin an SFTP session with the local Cornerstone MFT 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 Cornerstone MFT.

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

About South River Technologies

South River Technologies (SRT) is an innovator in managed file transfer and 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.