



CornerstoneMFT

Configuring Cornerstone MFT with a Router/Firewall
Quick Start Guide

Notices

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, WebDrive, Titan FTP Server, Cornerstone MFT, and GroupDrive are registered trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP and Windows Vista are registered 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 your Cornerstone Server with a router/firewall. Some screens in this instruction contain options that do not pertain to configuring your Cornerstone Server with a router/firewall. If you need additional information regarding these steps, please see the [Cornerstone User's Guide](#). 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](#). For the purpose of this router/firewall Quick Start guide, we will guide you through these options without configuring additional settings.

Configuring Cornerstone for use with a Router/Firewall—Overview

Most corporate and home networks today rely on a router and/or firewall to protect the internal computers or LAN (Local Area Network) from unauthorized access by outside users. The firewall is designed to block inbound TCP/IP access on any ports that are not designated as *open*.

Opening a port means that TCP/IP traffic is permitted to travel inbound or outbound through the router. A port that is not open blocks traffic from travelling through that port.

Firewalls provide a high level of security by preventing most inbound traffic (but allowing most outbound traffic); and they will prevent any server that is installed on your internal LAN from being accessed by computers located on the Internet.

When installing a server on the internal LAN, additional steps are necessary so that users can gain proper access to the server without creating risk to other computers on the internal LAN. This is done by using *port forwarding* on the firewall to direct the TCP/IP traffic to the proper computer. Port forwarding is a feature that is used by most router/firewalls. When you are using port forwarding, data arriving on a specific port is *redirected* to the same port on a different computer.

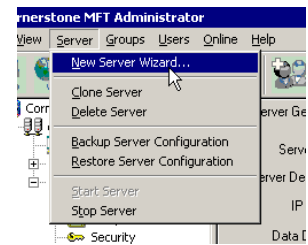
Configuring your Router/Firewall

1. Install Cornerstone on the internal LAN based computer. Configure the PC so that it has a *Static IP address*. This will be necessary because the firewall will be forwarding traffic to the Cornerstone server based on IP address. If the Cornerstone Server's IP address is DHCP (Dynamic Host Configuration Protocol) based, the firewall could forward the data to the wrong computer.
2. Once you have the Cornerstone Server installed, draw a diagram similar to our example and label the external public IP address of the firewall, the internal IP address of the router, and the internal LAN IP address of the Cornerstone server.
3. Have the Network/LAN Administrator reconfigure the firewall so that all server traffic is forwarded over to the Cornerstone Server. Ports 21 and 20 should be forwarded to the server because these are the default *control* and *data connection* ports for the server. (For FTPS use ports 21 and 990.) You will also want to have a *range of ports* opened and forwarded to the server. These are referred to as the *passive (PASV) port range*. These ports will be used for data connections¹ necessary for transferring data and directory listing to the client. For this example we will use ports 10000-10500. Note that this is just an example; you can use any port range that is available on your network. We recommend using a small range that will still provide for enough ports to cover the needed number of simultaneous file transfers from clients. Do not use a single port as this may cause data transfer failures for clients; 10 to 50 ports are recommended.

¹ FTP uses a main control connection for basic commands and then uses a separate data connection when the server needs to transfer/receive a file, or when it needs to send a directory listing to the client. Data connections need a *dedicated port* separate from the main control connection.

Configuring Cornerstone MFT using a Router/Firewall

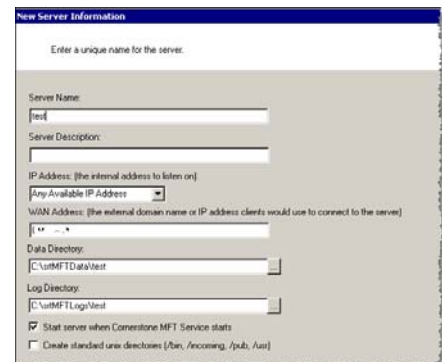
1. Run the **Cornerstone Administration utility** and start the **New Server Wizard**. When the Administer Domain window appears, Type the **Administrator Username** and **Administrator Password** and click **OK**.



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

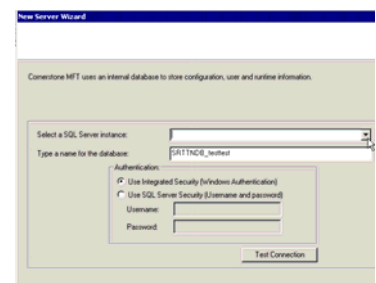


3. Type a unique **Server Name**. Click the drop-down arrow to choose your **IP Address**. (**Any available IP address** indicates that the server will listen on all IP addresses that are configured on the PC along with the local IP address of **127.0.0.0**, also known as localhost.) Type the **WAN address**. 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**.*

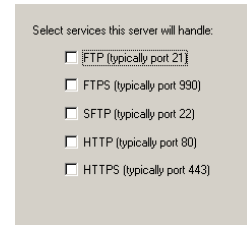


*If you need to create standard UNIX directories you can find additional information in the [Cornerstone MFT User's Guide](#).

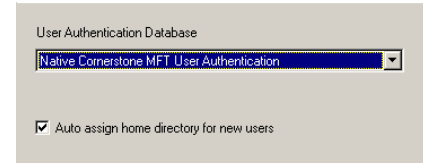
4. Cornerstone uses an internal database to store configuration, user, and runtime information. Use the drop-down arrow to select a SQL Server instance. Type a **name** for this database. Select **Windows Authentication** or **SQL Server Security**, and then click **Test Connection**. Once you connect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



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

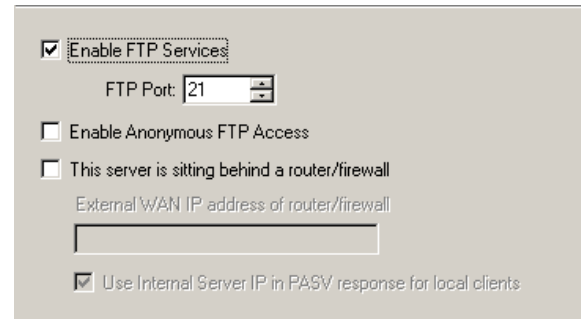


6. Select your **User Authentication Database** using the drop-down arrow. After you have configured your User Authentication Database, click **Next**.*



*Once you select a User Authentication Database in Cornerstone, you cannot change to a different method after the server wizard has completed. If you need more information about configuring user authentication, please see the [Cornerstone MFT User's Guide](#) or the [Cornerstone User Authentication Quick Start Guide](#) for your specific user authentication database.

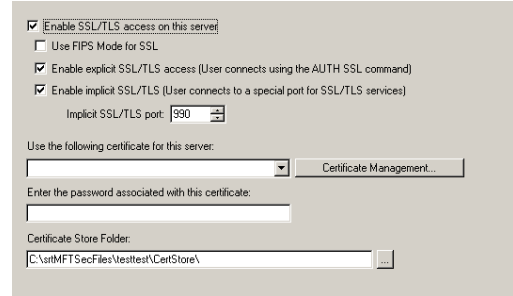
7. If you wish to enable FTP Services,* select the **Enable FTP Services** check box. Select the **FTP Port number** by using the up/down arrows. To **enable anonymous FTP access**, select the check box. Select **This server is sitting behind a router/firewall** and type the **External WAN IP address** of router/firewall. Click **Next**.



*The FTP protocol (RFC-959) establishes default ports to be used for FTP traffic. Port 21 is the default port that should be used for the primary control connection, and port 20 is sometimes used for the default data connection. If you install a Cornerstone Server on your internal LAN and have the requirement that users must be able to access the server from the Internet, your router must be configured so that ports 21 and 20 are open. (For FTPS, ports 21 and 990 must be open.) The router must also be configured to provide *port forwarding* of traffic through the firewall to the computer being used as the FTP Server.

You must enable FTP access if you are using FTPS with explicit SSL (also known as AUTH SSL). For more detailed information pertaining to these configuration options see the [Cornerstone MFT User's Guide](#).

- To enable SSL/TLS access on this server, select the **Enable SSL/TLS access on this server** check box and then select either **Enable explicit SSL/TLS** or **Enable implicit SSL/TLS**. * Use the drop-down arrow to select a certificate, or click **Certificate Management** to launch the *Certificate Wizard* to configure a certificate for this server, or use the "..."
Management to launch the *Certificate Wizard* to configure a certificate for this server, or use the "..."
 browse button to browse to your *Certificate Store Folder*.



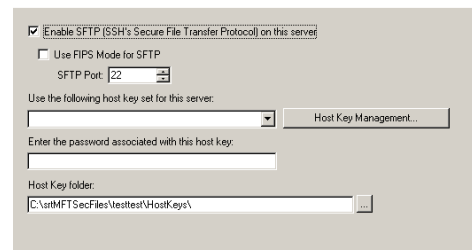
***Explicit SSL**—When using Explicit SSL, Cornerstone will allow SSL connections on the standard FTP port that was specified in [Step 6](#). This port will be used for both FTP connections and FTP/S connections. In order to enter into a secure SSL session, the FTP client will need to issue either the *AUTH SSL* or *AUTH TLS* command prior to establishing the secure connection.

***Implicit SSL**—When using implicit SSL, Cornerstone will listen on a specific port that will only be used for SSL connections. By default this is port 990; however, any port may be used. Change your port number by using the up/down arrows.

If you would like more information about certificate management, see the [Cornerstone MFT FTPS Public Key Certificate-based Authentication Quick Start Guide](#).

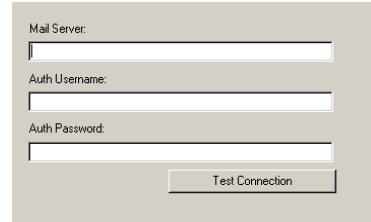
- After you are done configuring SSL/FTPS Security Settings, click **Next**.

- If you would like to use *SSH/SFTP security settings* along with FTPS, enable **SFTP** using the check box. * Click **Next**.



* For more information see the [Cornerstone SFTP & Host Key Authentication Quick Start Guide](#).

11. 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**, and then click **Finish** to create the server.



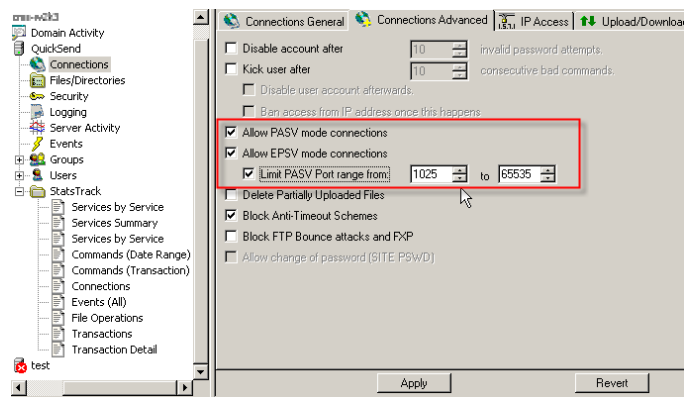
Mail Server:

 Auth Username:

 Auth Password:

12. Once the server is created, the server starts and appears in the main *Cornerstone Administrator* window. A green icon appears to indicate that the server is running. You may now add users to the system.

13. At this point, your server is configured and will be running. Select the server in the *Server Domain* menu. Then select the *Connections Advanced* tab. Enable **Allow PASV mode connections**. Enable **Limit PASV Port range** from and using the up/down arrows, **set the range** to the same range as the **firewall**. Once you have configured your settings, click **Apply**.



14. Click **Yes** to restart the server.

Testing Your Server

If you would like to test your server, you may download [WebDrive](#), our secure FTP client, or use the following instructions to test your server using a command prompt.

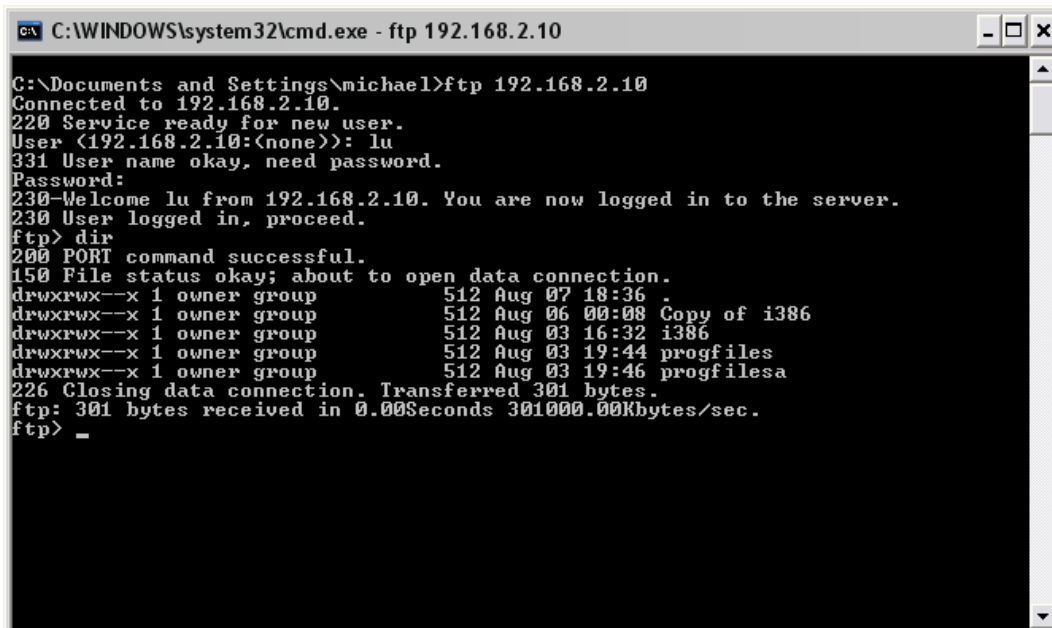
Test your Server Using a Command Prompt

1. On the Cornerstone PC, open a command prompt (CMD.EXE) and use the command line FTP utility to connect to the Cornerstone server.

Type: **ftp <ip-address of server>**

2. You will see a welcome message from the Cornerstone server.
3. Log on to the Cornerstone server using a user account or using *anonymous* if anonymous access is enabled.
4. Once you have logged on, issue the DIR command to see if a directory listing can be created. This should succeed. By default, the Windows FTP client will run in Active/Port mode so you should see a directory listing of files if any exist.

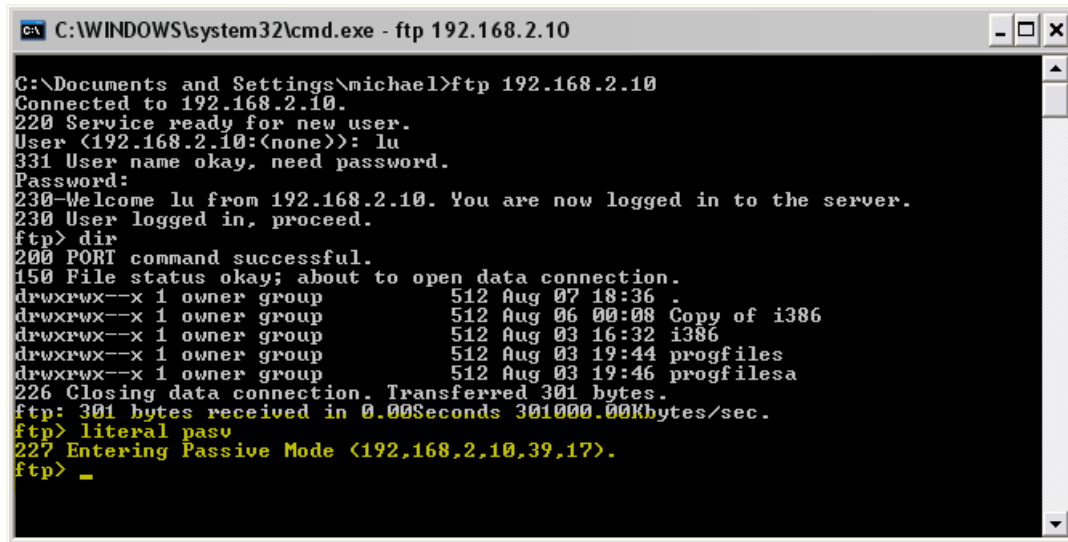
Type: **dir**



```
C:\WINDOWS\system32\cmd.exe - ftp 192.168.2.10
C:\Documents and Settings\michael>ftp 192.168.2.10
Connected to 192.168.2.10.
220 Service ready for new user.
User (192.168.2.10:(none)): lu
331 User name okay, need password.
Password:
230 Welcome lu from 192.168.2.10. You are now logged in to the server.
230 User logged in, proceed.
ftp> dir
200 PORT command successful.
150 File status okay; about to open data connection.
drwxrwx--x 1 owner group          512 Aug 07 18:36 .
drwxrwx--x 1 owner group          512 Aug 06 00:08 Copy of i386
drwxrwx--x 1 owner group          512 Aug 03 16:32 i386
drwxrwx--x 1 owner group          512 Aug 03 19:44 progfiles
drwxrwx--x 1 owner group          512 Aug 03 19:46 progfilesa
226 Closing data connection. Transferred 301 bytes.
ftp: 301 bytes received in 0.00Seconds 301000.00Kbytes/sec.
ftp> _
```

5. While still in the FTP session, test to see if the Cornerstone Server will return the proper passive address & port for internal LAN clients.

Type: **literal pasv**



```

C:\WINDOWS\system32\cmd.exe - ftp 192.168.2.10
C:\Documents and Settings\michael>ftp 192.168.2.10
Connected to 192.168.2.10.
220 Service ready for new user.
User (192.168.2.10:(none)): lu
331 User name okay, need password.
Password:
230 Welcome lu from 192.168.2.10. You are now logged in to the server.
230 User logged in, proceed.
ftp> dir
200 PORT command successful.
150 File status okay; about to open data connection.
drwxrwx--x 1 owner group      512 Aug 07 18:36 .
drwxrwx--x 1 owner group      512 Aug 06 00:08 Copy of i386
drwxrwx--x 1 owner group      512 Aug 03 16:32 i386
drwxrwx--x 1 owner group      512 Aug 03 19:44 progfiles
drwxrwx--x 1 owner group      512 Aug 03 19:46 progfilesa
226 Closing data connection. Transferred 301 bytes.
ftp: 301 bytes received in 0.00Seconds 301000.00Kbytes/sec.
ftp> literal pasv
227 Entering Passive Mode (192,168,2,10,39,17).
ftp> _

```

6. The Cornerstone server will respond with something that resembles (192,168,2,10,234,99) which is the *IP address* and *Port* that Cornerstone is listening on for a data connection from the client. The first four numbers should match the same IP address that the Cornerstone Server is listening on (in our case, 192.168.2.10). The last two numbers will be the port that Cornerstone is listening on, mathematically broken down. Since our port range is 10000-10500, the port will fall into this range, beginning at the low end and incrementing sequentially until it reaches the top port, then it will return to the beginning port in the range. For our example, Cornerstone decided to use port 10000 which is written to the client as **39 * 256 + 17** .
7. Once these tests are successful, connect to the server from the Internet using Passive mode and Cornerstone should return information. If you receive an error such as *unable to open data connection*, or *timeout waiting for data connection*, then the firewall is not routing the passive ports correctly to the Cornerstone server, or the Cornerstone server is not returning the public/external IP address of the firewall as part of the response to the Passive (PASV) command.

About South River Technologies

South River Technologies (SRT) is an innovator in managed file transfer and basic content services 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.southrivertech.com.

Cornerstone MFT® is a registered trademark of South River Technologies, Inc.

© Copyright South River Technologies, 1996-2010. All rights reserved.