



CornerstoneMFT

Using UNC Paths for Data Storage & Scalability Quick Start Guide

Notices

Thank you for purchasing Cornerstone MFT®.

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, Titan FTP Server, Cornerstone MFT, WebDrive, DMZedge, 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 Cornerstone MFT using UNC (Universal Naming Convention/Uniform Naming Convention) paths for data storage and scalability. Some screens in this instruction contain options that do not pertain to using UNC (Universal Naming Convention/Uniform Naming Convention) paths for data storage and scalability. If you need additional information regarding these steps, please see the [Cornerstone MFT User Guide](#). For the purpose of this 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](#)

Using UNC Paths for Data Storage & Scalability—Overview

Cornerstone MFT supports a powerful feature that allows for the storage and access of data that is physically stored on any server in your network. Remote data is accessed by a public UNC (Universal/Uniform Naming Convention) that specifies the computer name, share name, and optional subdirectory where the data is stored. For example: a computer named **QALAB1**, has a shared folder called **SrtData**, and a subdirectory named **Cluster Test**. The UNC that references this location is:

\\QALAB1\SrtData\Cluster Test

The main benefit to using UNC paths to refer to data storage locations is scalability. Cornerstone MFT supports the ability to be deployed in a scalable environment, meaning that one or more servers can run in parallel and can access the same back end data storage to service the same front end clients.

If you intend to scale Cornerstone MFT to multiple boxes, you need to configure the primary server so that all data files are accessed by UNC share rather than a local drive or a mapped network drive letter.

For illustration purposes, let's assume that you will have multiple Cornerstone servers in your multi server cluster. QALAB1 is the primary/first Server that will be installed; QALAB3 will be backup server that will be added at a later date. In a multi-server environment, there are two scenarios, but both require the same configuration.

Scenario 1—User data will be stored on a local fixed disk; on the QALAB1 primary server box. Both QALAB1 and QALAB3 Servers will need access to the same data.

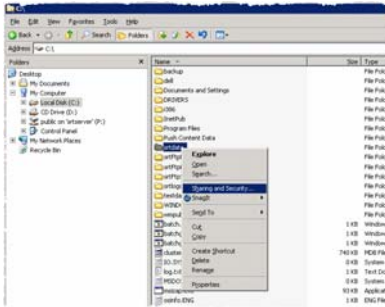
Scenario 2—User data will be stored on a remote/third box on the network; a box that is neither QALAB1 nor QALAB3. For example, Network Attached Storage (NAS1).

For either scenario, the configuration setup is basically the same.

Configuring the UNC

The UNC must be configured so that it can be accessed by the Cornerstone server. This requires a UNC “share” and NTFS (NT File System) permissions adjustments to the folder where the data is stored.

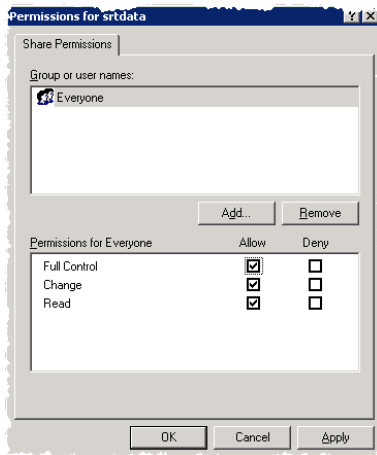
1. Run *Windows Explorer* and locate the directory where data will be stored. For our example, all data is stored under C:\SRTDATA\. Right-click on the folder and select **Sharing and Security** from the pop-up menu. This will display the *UNC Sharing dialog* for the selected folder.



2. Select the **Sharing** tab and then select the **Share This Folder** radio button. When you are finished, click **Permissions**.



- Update the *Permissions* on the share so that the Cornerstone servers will be able to access data on the share.* Once you have properly set the permissions for the NTFS folder and share, click **OK**.



* Incorrect permissions will prevent the Cornerstone server from being able to access the data. Typically the Cornerstone Service runs under the context of a special built-in Windows system account, such as *Local System* or *Local Service*. These built-in accounts do not have proper NTFS rights to access files stored on remote UNC's. There are two options, you can either grant *full NTFS rights* to all users, which will allow Cornerstone MFT to gain access to the UNC, **or** you can *create a special Windows user Account* for the Cornerstone Service and then add that special Windows user Account to the ACL list for both the share and the underlying NTFS file system. (NOTE: the ACL (Access Control List) for the *Share* is different than the ACL for the underlying folder on the NTFS drive). After you create a special Windows user account for the Cornerstone server, you must give that Windows user account an *Access Control Entry (ACE)* for the underlying folder **and** an *ACE in the Access Control List (ACL)* for the Share so that the special Windows user account can access the data on the UNC share.

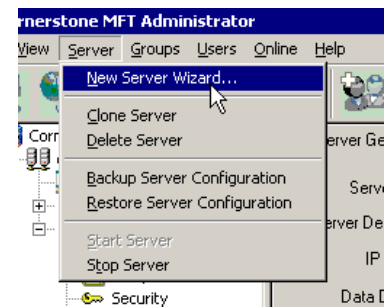
See the [Appendix](#) for more information on how to create a special Windows user Account. If you would like information about how to configure Cornerstone MFT for use with Windows NT/SAM user authentication, see the [Cornerstone MFT Windows NT/SAM User Authentication Quick Start Guide](#).

Updating the User Directory

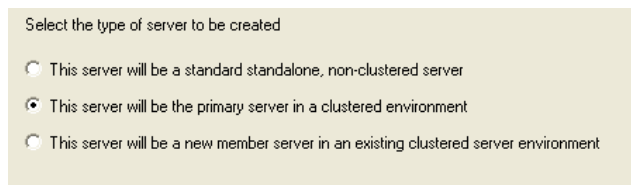
Once you have configured the UNC for access by the Cornerstone server, you can run the Cornerstone Administration program and launch the [New Server Wizard](#) to configure your server or you can [reconfigure an existing server](#) to use the UNC instead of the local drive. If you would like more information about configuring Cornerstone servers in your multi-cluster server environment, please see the [Cornerstone MFT Clustering Wizard Quick Start Guide](#).

If you are configuring your Cornerstone using the *New Server Wizard*:

1. Run the *Cornerstone Administrator* and click **New Server Wizard**.

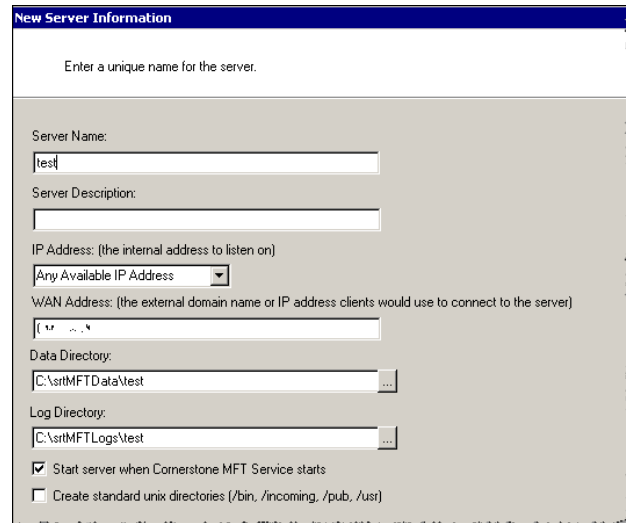


2. When the *Administer Domain* window appears, Type the Administrator Username and Administrator Password and click **OK**.
3. When creating the primary/first server of the cluster, select **This server will be the primary server in a clustered environment*** and click **Next**.



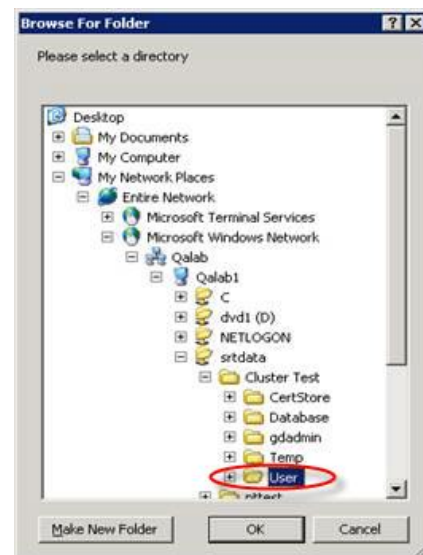
*To create or connect to an existing clustered Cornerstone server select **This server will be a new member server in an existing clustered server environment**. For more information about configuring Cornerstone servers in your multi-cluster server environment, please see the [Cornerstone MFT Clustering Wizard Quick Start Guide](#).

4. 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, "**mywanaddress.com**". Click the **Data Directory** "... " browse button to browse to the **UNC**.



5. The *Browse For Folder* dialog box will appear. Browse the **Network Places** and find the **machine name, share name, and folder** where the Cornerstone User Data will be stored. Click **OK**. You will be returned to the New Server Wizard to continue configuring your server.* Once the primary Cornerstone server has been configured to use UNC based directories, you can install Cornerstone on additional nodes.

*For more information about configuring Cornerstone servers in your multi-cluster server environment, please see the [Cornerstone MFT Clustering Wizard Quick Start Guide](#).



6. Continue configuring your options in the New Server Wizard. 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.
7. In the tree pane, select the **server**, and then select the **UNC Accounts** tab using the right/left arrows. The UNC Accounts tab is used to define a list of domain user names and passwords that will be used for authentication when Cornerstone needs to access a remote UNC share. * Type a **Username**. The Username can be simply a user name or <username@domain> or <domain/username>. Type a **Password**. The password will be used for authentication against the remote UNC share. Click **Add** to add the new Username/Password to the UNC Account List. Click **Apply**.

*Since Cornerstone Service usually runs under the context of a *Local System Windows User Account* which is defined for the local PC, it does not normally have rights to access a UNC resource that is located on a remote server. When Cornerstone attempts to access a file/folder stored on a UNC share, it will attempt to connect/authenticate itself against the remote UNC by sending over a UNC user name and password along with the UNC.

How Cornerstone uses the UNC Accounts List

Cornerstone will check the users in the list one at a time until it authenticates against the UNC share. This list is not intended to be a list of your MFT users. You will likely only need to add one username to the UNC Accounts tab. The UNC account should have all of the permissions any of your users will need on the UNC share.

The permissions of the UNC user can be further restricted by Cornerstone, but Cornerstone cannot elevate the permissions of the UNC user. For example, a user may have write access in Cornerstone but if the UNC user does not have write access, the user will not be able to write to files.

NOTE: If you are using Window NT Impersonation, the UNC Accounts tab will be disabled. UNC accounts are not used in conjunction with Windows Impersonation. When you use Windows Impersonation, the access rights of individual users will be used to authenticate against UNC shares.

Username - Type a domain username that will be used for authentication against the remote UNC share. The username can be simply a **user name**, or **username@domain** or **domain\username**.

Password - Type the corresponding password that will be used for authentication against the remote UNC share.

Add/Remove - Use these buttons to add a new Username/Password to the UNC Accounts list, or to remove the currently selected UNC Account from the list.

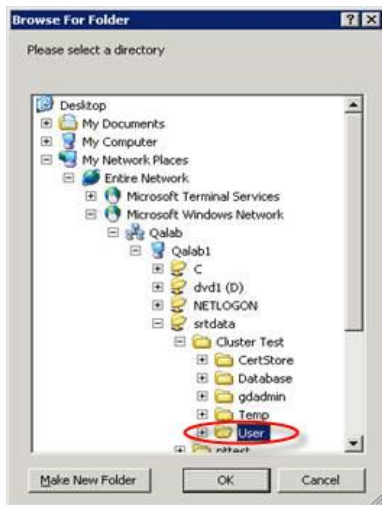
UNC Account List - Contains the list of domain accounts that will be used for authentication against the remote UNC share. Cornerstone will present each username/password to the UNC server until it receives a successful authorization.

Cornerstone MFT is now configured using UNC paths for Data Storage and Scalability.

If you would like to test your server, you may [download WebDrive](#), our secure FTP client.

If you are reconfiguring an existing server:

1. Launch the *Cornerstone Administrator*. In the tree, under **Domains**, select your **server**. On the **Server General** tab, use the browse “...” button to browse to the UNC.
2. The *Browse For Folder* dialog box will appear. Browse the **Network Places** and find the **machine name**, **share name**, and **folder** where the Cornerstone User Data will be stored. Click **OK** to accept the new directory and return to the *Server General* tab.



3. Click **Apply** to save the new directory settings.
4. When you change your User Data Directory, Cornerstone will internally update all Shares, Links and ACLs that referenced the old location to reference the new location. Click **OK**.
5. Click **Yes** to restart the server so that these changes will take effect immediately.

6. In the tree pane, select the **server**, and then select the **UNC Accounts** tab using the right/left arrows. The UNC Accounts tab is used to define a list of domain user names and passwords that will be used for authentication when Cornerstone needs to access a remote UNC share. * Type a **Username**. The Username can be simply a user name or <username@domain> or <domain/username>. Type a **Password**. The password will be used for authentication against the remote UNC share. Click **Add** to add the new Username/Password to the UNC Account List. Click **Apply** to apply the settings.

*Since Cornerstone Service usually runs under the context of a *Local System Windows User Account* which is defined for the local PC, it does not normally have rights to access a UNC resource that is located on a remote server. When Cornerstone attempts to access a file/folder stored on a UNC share, it will attempt to connect/authenticate itself against the remote UNC by sending over a UNC user name and password along with the UNC.

How Cornerstone uses the UNC Accounts List

Cornerstone will check the users in the list one at a time until it authenticates against the UNC share. This list is not intended to be a list of your MFT users. You will likely only need to add one username to the UNC Accounts tab. The UNC account should have all of the permissions any of your users will need on the UNC share.

The permissions of the UNC user can be further restricted by Cornerstone, but Cornerstone cannot elevate the permissions of the UNC user. For example, a user may have write access in Cornerstone but if the UNC user does not have write access, the user will not be able to write to files.

NOTE: If you are using Window NT Impersonation, the UNC Accounts tab will be disabled. UNC accounts are not used in conjunction with Windows Impersonation. When you use Windows Impersonation, the access rights of individual users will be used to authenticate against UNC shares.

Username - Type a domain username that will be used for authentication against the remote UNC share. The username can be simply a **user name**, or **username@domain** or **domain\username**.

Password - Type the corresponding password that will be used for authentication against the remote UNC share.

Add/Remove - Use these buttons to add a new Username/Password to the UNC Accounts list, or to remove the currently selected UNC Account from the list.

UNC Account List - Contains the list of domain accounts that will be used for authentication against the remote UNC share. Cornerstone will present each username/password to the UNC server until it receives a successful authorization.

Cornerstone MFT is now reconfigured using UNC paths for Data Storage and Scalability.

Appendix—Creating a Special Windows User Account

If you would like to configure Cornerstone MFT for using UNC paths for data storage and scalability, a special Windows user Account must be created. This special Windows user Account will be given certain rights not usually available to other Windows user accounts. The Cornerstone Service will also need to be modified to use this new Windows 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 *Cornerstoneuser* as the username and *Cornerstonepass* 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 *Cornerstoneuser* 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 *Cornerstoneuser* is granted the right to **Access Computer From The Network** and **Act As Part Of Operating System**.
4. Install Cornerstone MFT on the PDC and restart the PDC.
5. Open the **Services** Control Panel Applet and scroll down to the **Cornerstone Service**. Right-click on the **Cornerstone Service** and select **Properties**.
6. Modify the **Log on As:** section so that the Cornerstone Service will log on using the *Cornerstoneuser/Cornerstonepass* account that was created.
7. **Stop** then **Restart** the Cornerstone Service.

If you would like more information about configuring Cornerstone MFT using Windows NT/SAM user authentication, see the [Cornerstone MFT Windows NT/SAM User Authentication Quick Start Guide](#).

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.