



CornerstoneMFT

Using Group Level Virtual Folders 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.southernrivertech.com

Please Note: The following instructions will help you to configure Group Level Virtual Folders in Cornerstone MFT. Some screens in this quick start guide may contain options that do not pertain to Group Level Virtual Folders. If you need additional information regarding these steps, please see the [Cornerstone MFT Administrator User's Guide](#). For the purpose of this quick start guide, we will guide you through these options without configuring additional settings. A list of Frequently Asked Questions (FAQ) is available at our [Knowledgebase Support Center](#), and a complete listing of SRT Quick Start guides is also available online.

Group Level Virtual Folders—Overview

Virtual Folders are folders that can be mapped into a server's data directory and are used to link or map *external* folders into a user's directory space. In a Virtual Folder it appears as if the data resides within folder structure; however, the data is actually stored somewhere else. If you are a Windows user, you can think of a *Virtual Folder* as a Windows Shortcut. The link appears in one location and the data lives in another location. For UNIX users, *Virtual Folders* are very similar to Symbolic Links.

Group Level Virtual Folders allow data to be shared with all users of a given group. In a *Group Level Virtual Folder*, all users can share the same data and have Directory Access Rights to that data. Virtual Folders can be added at the Server, Group, or User level. Virtual Folders added at the Group level can be made accessible to all users in the group, depending on the Directory Access Permissions that are set for that group. Virtual Folders added at the User Level are limited to that specific user. When you add a Virtual Folder to a Cornerstone MFT configuration, the default Directory Access Permissions will be set to *Read Only*. *Read Only* permissions means that users are allowed to browse the folder, and download information, but cannot modify the contents or upload files. You can modify the standard Directory Access Permissions after the Virtual Folder has been added to the configuration.

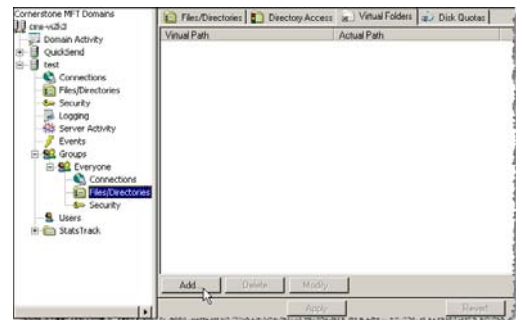
One of the benefits of Virtual Folders is that you can access network shares from the Cornerstone MFT through the use of Virtual Folders. Cornerstone MFT supports the ability to add a UNC (Universal Naming Convention) path into the name space. For example, if you have a share on your network called `\\MyServer\My Music\` you can use Virtual Folder support to map that into your Server Data Directory as `/pub/My Music/` or `/usr/joe/My Music/`

If you attempt to create a Virtual Folder for a mapped network drive, Cornerstone MFT will replace the drive mapping with the actual UNC name. This is because the Cornerstone Service does not have access to mapped drives, only to UNC shares. Cornerstone MFT runs as an *Windows Service*, which, by default, does not have access to shared network resources because shared network resources are based on the authorized Windows User. If you are mapping a UNC share, you must make sure that the account under which the Cornerstone Service is running has access to the UNC. Otherwise, you will need to enter the appropriate username and password under the UNC Accounts tab.

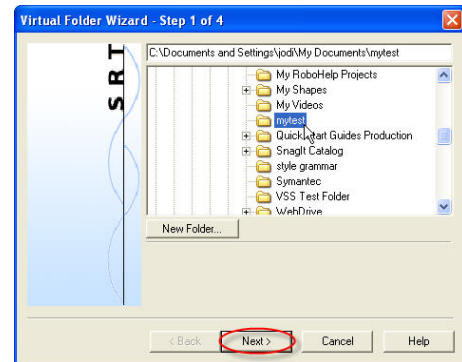
See [Appendix A](#) for more information about UNC configuration and how to create a special Windows User account for Cornerstone MFT.

Configuring the Virtual Folder

1. Run the *Cornerstone MFT Administrator*. On the *Cornerstone MFT Domains* menu tree, select the **Group** that will access the Virtual Folder, and then select **Files/Directories**. Select the **Virtual Folders** tab and then click **Add**.



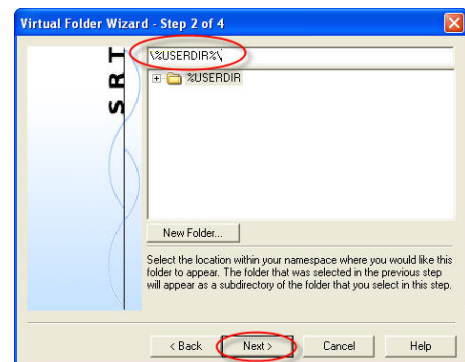
2. To select the *fully qualified path* that will be mapped to the namespace for this group, browse to the actual/real **physical folder**. You may select a folder on your *local* computer, or you may choose a network folder that has been *previously shared*.* Click **Next**.



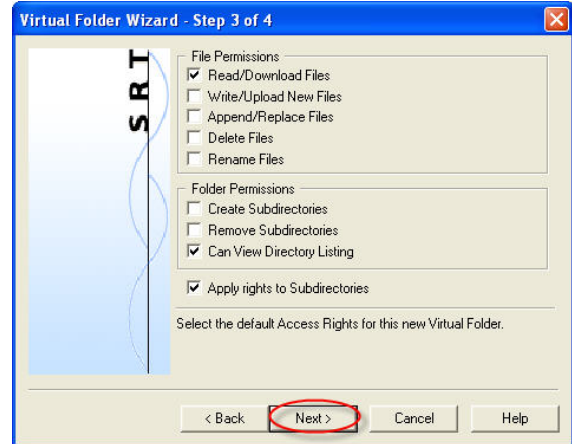
*If you are mapping a UNC share, make sure that the account under which the Cornerstone MFT Service is running has access to the UNC. See [Appendix A](#) for more information about mapping UNC shares.

3. Select the **location within your namespace** where you would like this folder to appear. The folder that you selected in the previous step will appear as a subdirectory of the folder that you select in this step. To ensure that the *Virtual Folder* will appear as a subfolder under the user's home directory, type **\%USERDIR%**

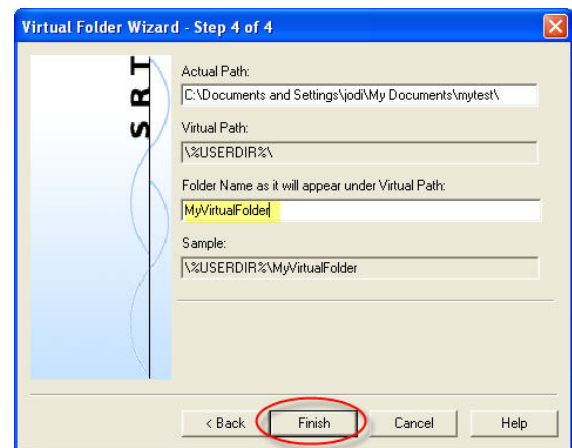
Click **Next**.



- Select the **default Access Rights** for this new Virtual Folder using the check boxes. Click **Next**.

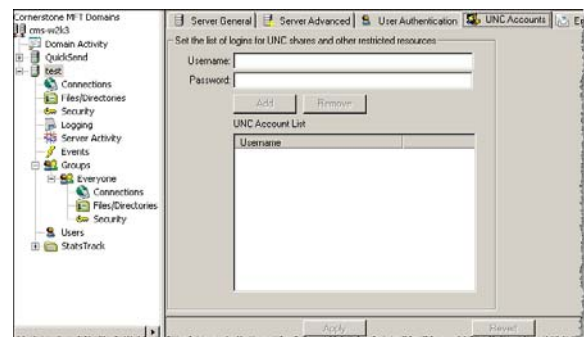


- The Actual Path of the folder is displayed and the Virtual Path is displayed. You can change the **Folder Name as it will appear under the Virtual Path**, or you can leave the default name (which is the same as the *Actual Path* name). In our example, the name of the *actual* folder is *mytest*. We typed in *MyVirtualFolder* so that in the *Virtual Folder* path the folder *mytest* will appear as the Folder Name *MyVirtualFolder*. Click **Finish** to generate the Virtual Folder mapping.



- The *Virtual Path* and the *Actual Path* are now displayed in the *Virtual Folders* tab. Click **Apply**.

- Select the [UNC Accounts tab](#). To select the *UNC Accounts* tab, in the tree pane, click the **Server**, and then, in the tab pane, click the **UNC Accounts** tab. Type the **Username** and **Password** and then Click **Add**. When you are finished adding users, click **Apply**.*

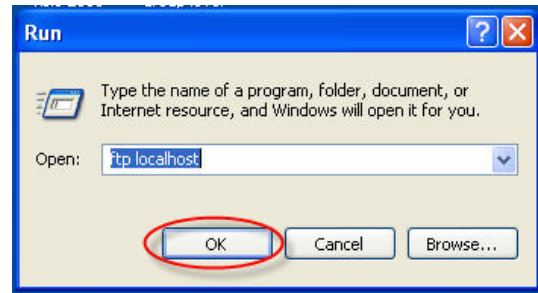


*If you are mapping a *UNC Share*, make sure that the account under which the Cornerstone MFT Service is running has access to the UNC share. Otherwise, you will need to enter the appropriate username and password into the *UNC Accounts* tab. See the [appendix](#) for more information.

- To test the Virtual Folder, open a *Command Prompt* window by selecting **Start** and then **Run**

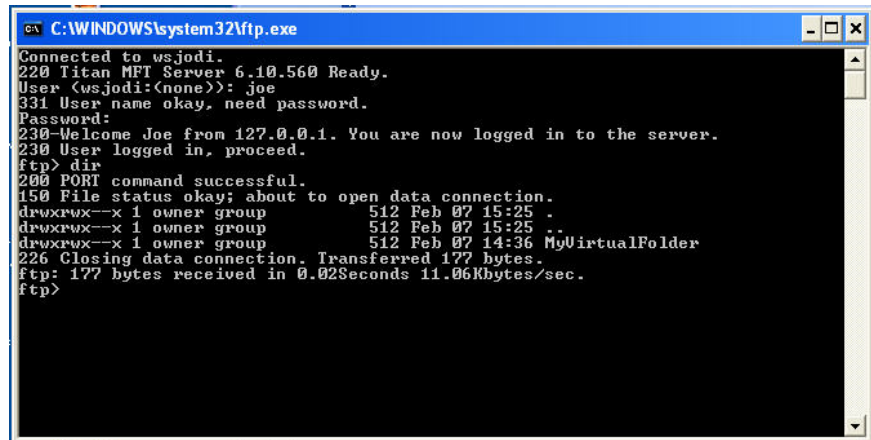


- Type **ftp localhost**. Click **OK**.



- Type the **Username** and **Password**. At the next *ftp prompt* type **dir**

The VirtualFolder that you just created is now displayed as a subdirectory under the user's home directory.

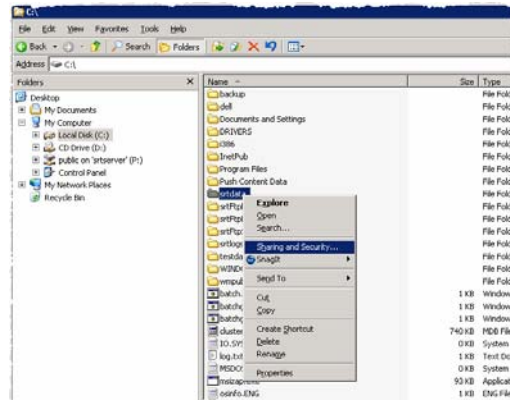


Note: Virtual Folder updates are not real-time. If a user is currently connected to the server, and you make changes to the Virtual Folder list, users will need to log out and then log back into the system to see the Virtual Folder changes.

Setting up a UNC Share

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

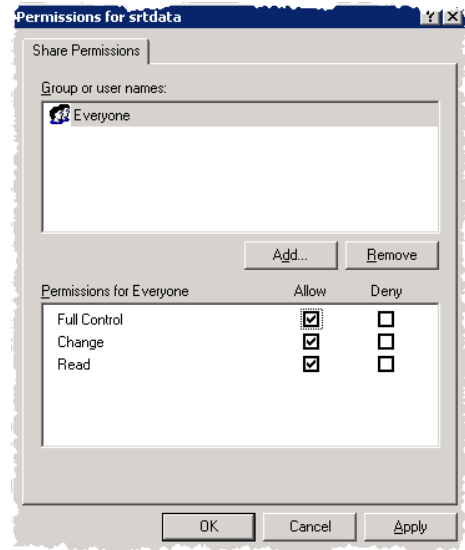
1. Run *Windows Explorer* and locate the directory where data will be stored. For our example, all data is stored under C:\SRTDATA\. Right-click on the folder and select **Sharing and Security** from the pop-up menu. This will display the *UNC Sharing dialog* for the selected folder.



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 MFTs 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 Cornerstone MFT from being able to access the data. Typically the Cornerstone MFT 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 MFT 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 MFT, 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.

Creating a Special Windows User Account

You can configure Cornerstone MFT for mapping to a UNC Share in *Group Level Virtual Folders* using a special Windows User Account. This special Windows User Account will be given certain rights not usually available to other Windows User accounts. The Cornerstone MFT 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 MFT** service. Right-click on the **Cornerstone MFT** service and select **Properties**.
6. Modify the **Log on As:** section so that the Cornerstone MFT Service will log on using the *Cornerstoneuser/Cornerstonepass* account that was created.
7. **Stop** then **Restart** the Cornerstone MFT Service.

Cornerstone MFT UNC Accounts Tab

The UNC Accounts tab is used to define a list of domain usernames and passwords that will be used for authentication when Cornerstone MFT needs to access a remote UNC share. If you have mapped a UNC Share, make sure that the account under which the Cornerstone Service is running has access to the UNC share. Otherwise, you will need to enter the appropriate username and password into the UNC Accounts tab.

Since the Cornerstone Service usually runs under the context of the *Local/System* Windows User 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 username 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.

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.