2017

Cornerstone MFT Server UNC Path Based Data Storage Guidelines

Instructions for configuring Cornerstone MFT to use UNC based storage locations on a SAN or network.

QuickStart Guide

Using UNC Paths for Data Storage & Scalability

The following instructions will help you set up Cornerstone MFT using Universal/Uniform Naming Convention (UNC) paths for data storage and scalability.

Universal/Uniform Naming Convention (UNC)

Cornerstone MFT supports a powerful feature that allows you to store and access data on any server in your network using a public UNC (Universal/Uniform Naming Convention). The UNC is a pathway name that refers to a resource—this could be a file or folder or even a printer, any asset that can be used by a network—by specifying the **computer name**, **share name**, and optional **subdirectory** where the resource is stored. This path is a fixed point the server can locate in order to access data.

Cornerstone MFT supports this capability in order to share information in a scalable environment. By assigning addresses all machines in the network can recognize, one or more servers can run in parallel and 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 must configure the primary server to use UNC to access all data files instead of a local drive or a mapped network drive letter.

A UNC requires altered permissions in order to allow Cornerstone access to the UNC data. The Cornerstone Service usually runs under a Local System account in Windows. By default, this account does not have rights to access a UNC resource located on a remote server.

To utilize the powerful function of UNC-based resources with Cornerstone:

1. **Create a Special User Account for Cornerstone on Your Active Directory Server**
2. **Use Sharing Properties to Create a UNC**
3. **Update the Access Control Lists on the UNC to allow Cornerstone Access**

1. Create a Special User Account for Cornerstone on Your Active Directory Server

For Cornerstone to access the UNC with full permissions, SRT recommends creating a special Windows User Account for the Cornerstone Service and adding it to the Access Control List (ACL) for both the share and the underlying New Technology File System (NTFS).

The special Windows User Account you create will require rights not usually available to other user accounts. The Cornerstone Service will also need to be modified to use this new Windows user account.

Follow these steps to create the account and connect it to Cornerstone:

1. From a computer on the Active Directory (AD) network, 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: The Access Control List (ACL) for the Share is different than the ACL for the underlying folder on the NTFS drive. Be sure that the ACL for the folder matches the one for the share.

2. Make Cornerstoneuser a member of the Domain Admins and Domain Users groups by opening the Local Security Policy applet on the AD and, under Security Settings > Local Policies > User Rights Assignment, grant Cornerstoneuser the right to **Access Computer From The Network** and **Act As Part Of Operating System**.

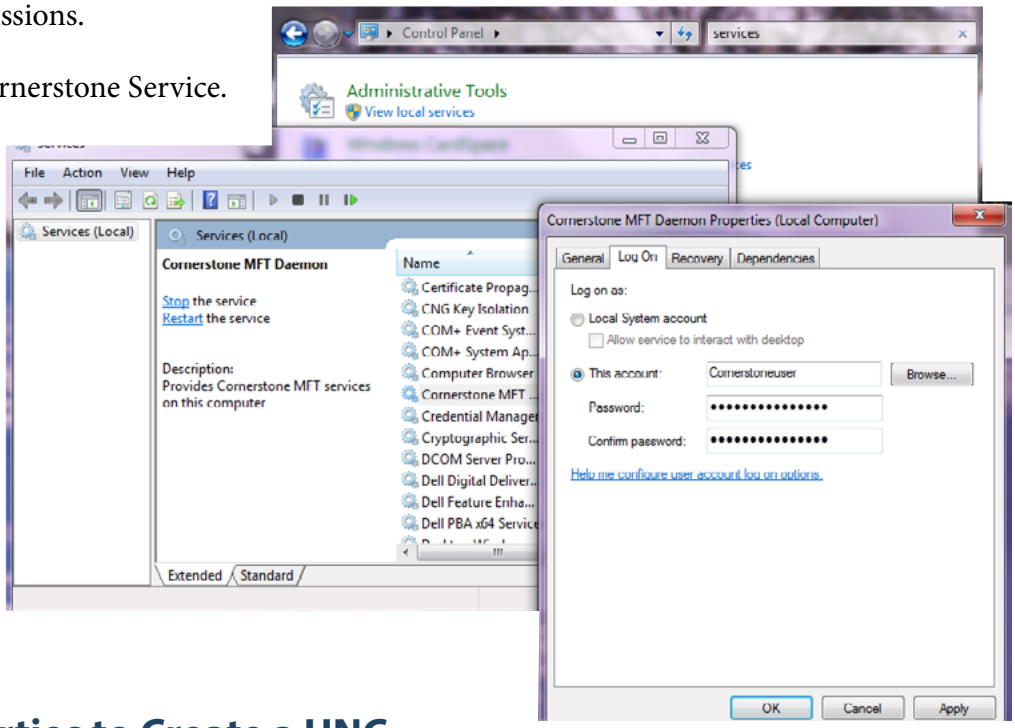
3. Install Cornerstone MFT Server on the target computer, which may or may not be the AD but must be a member of the domain.

4. Open the Services Control Panel Applet and scroll down to the Cornerstone Service. Right-click on the Cornerstone Service and select Properties.

5. Modify the Log on As: section to allow the Cornerstone Service to log on using the Cornerstoneuser/Cornerstonepass account that was created. When Cornerstone accesses data on the UNC share, it will be running under this account and have all of its permissions.

6. Stop and Restart the Cornerstone Service.

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. You must also add ACE in the Access Control List for the Share so that the special Windows user account can access the data on the UNC share.



2. Use Sharing Properties to Create a UNC

Before you continue to set up Cornerstone, a UNC must be configured for Cornerstone MFT to access.

To accomplish this:

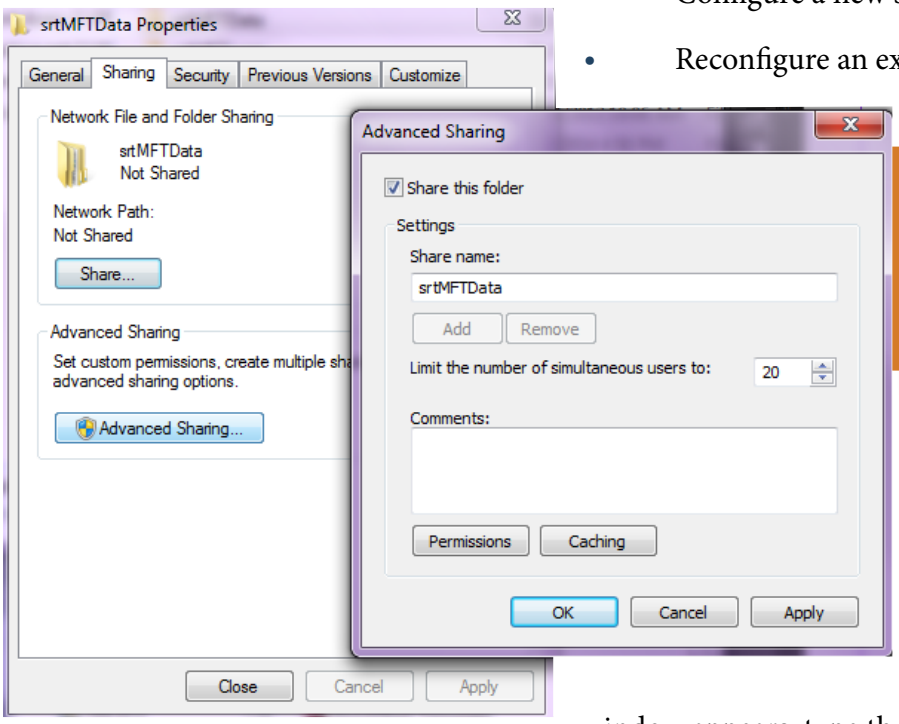
1. Run Windows Explorer and locate the directory where data will be stored. For our example, all data is stored under C:\SRTDATA\. Right-click on the folder and select properties from the menu. Select the Sharing tab. This will display the UNC Sharing dialog for the selected folder.

2. Select the **Advanced Sharing...** button. Select the **Share This Folder** radio button and add the AD account you created in the first step. Once you have properly set the permissions for the NTFS folder and share, click OK.

Update the Access Control Lists

Once you have configured the UNC for access by the Cornerstone server, instruct a Cornerstone server to look to the UNC instead of the local drive for user data in one of two ways:

- Configure a new server
- Reconfigure an existing server



NOTE: Incorrect permissions will prevent the Cornerstone server from being able to access UNC data.

Configuring 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 Password and click OK.

   - When creating the primary/first server of the cluster, select **This Server Will be the Primary Server in a Clustered Environment** and click Next.

   - Once the primary Cornerstone server has been configured to use UNC-based directories, you can install Cornerstone on additional nodes. 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**.

3. Type a unique server name, click the dropdown arrow to choose your IP Address, and type the

WAN address; you do not need to type "http" (ie, mywanaddress.com).

4. Click the Data Directory "…" browse button to browse to the UNC.

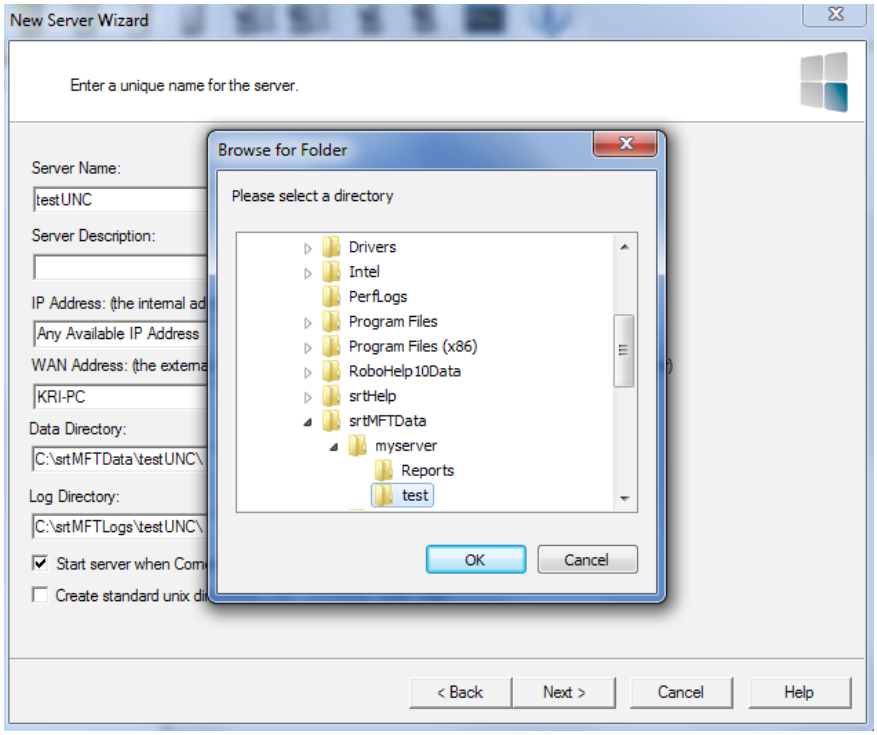
    a. The Browse for Folder dialog box will appear. Browse the Network Places and find the machine name, share name, and folder where the Cornerstone User Data will be stored. Click OK. You will be returned to the New Server Wizard to continue configuring your server.

5. Continue in the New Server Wizard to complete the new server's configuration. Once created, the server will start and appear in the main Cornerstone Administrator window. A green-lit icon will appear to indicate that the server is running.

If you would like to test your server, connect with a secure FTP client such as WebDrive.

Reconfiguring an existing server:

If you already have a server you would like to link to a UNC, follow these steps:



1. Launch the Cornerstone Administrator. In the tree view, select your server. On the Server General tab, beside Data Directory, use the "…" 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. When you change your User Data Directory, Cornerstone will internally update all Shares, Links, and ACLs to the new location. Click OK.

4. Click Yes to restart the server so these changes will take effect immediately.

If you would like to test your server, connect with a secure FTP client such as WebDrive.

System Requirements

Supported Operating Systems

- Windows Server 2012, all editions, 32-bit and 64-bit
- Windows Server 2008-R2, all editions, 32-bit and 64-bit
- Windows Server 2008, all editions, 32-bit and 64-bit

Minimum Hardware Requirements

- 2 GHz Pentium® class processor
- 4GB of RAM is required; 8GB of RAM is recommended
- Minimum 100MB of free disk space for the application
- Minimum SVGA (800x600) resolution display is required to run the Administration console program.

Minimum Software Requirements

- Microsoft .NET Framework v4.0 is required
- Microsoft SQL Server 2005 or later is required
- Microsoft SQL Server Management Studio Express is recommended

Limitations

- Cornerstone MFT server is a multi-threaded, dynamic server solution for the Microsoft Windows operating system. While designed to handle an unlimited number of user connections and servers, like all software, Cornerstone is limited by the resources of the computer; most notably, those limitations imposed by the Windows Sockets (WINSOCK) Library.

About South River Technologies

South River Technologies (SRT) is an innovator in secure file management software. SRT software allows users to securely access, manage, and collaborate on files over the Internet, streamlining business processes to improve productivity. SRT's products enhance customers' existing applications by instantly enabling secure access and collaboration within those applications. More than 90,000 customers in 140 countries use 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. South River Technologies, Cornerstone MFT, Titan FTP Server, WebDrive, and DMZedge Server are registered trademarks of South River Technologies, Inc. in the U.S. and other countries. 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.

Contact Information

South River Technologies, Inc.
1910 Towne Centre Blvd
Suite 250
Annapolis, Maryland 21401
USA

Toll Free: 1-866-861-9483
Main: 443-603-0290
Fax: 410-266-1191
Corporate Web site: www.southrivertech.com
Online Support: www.srthelpdesk.com