2019

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.

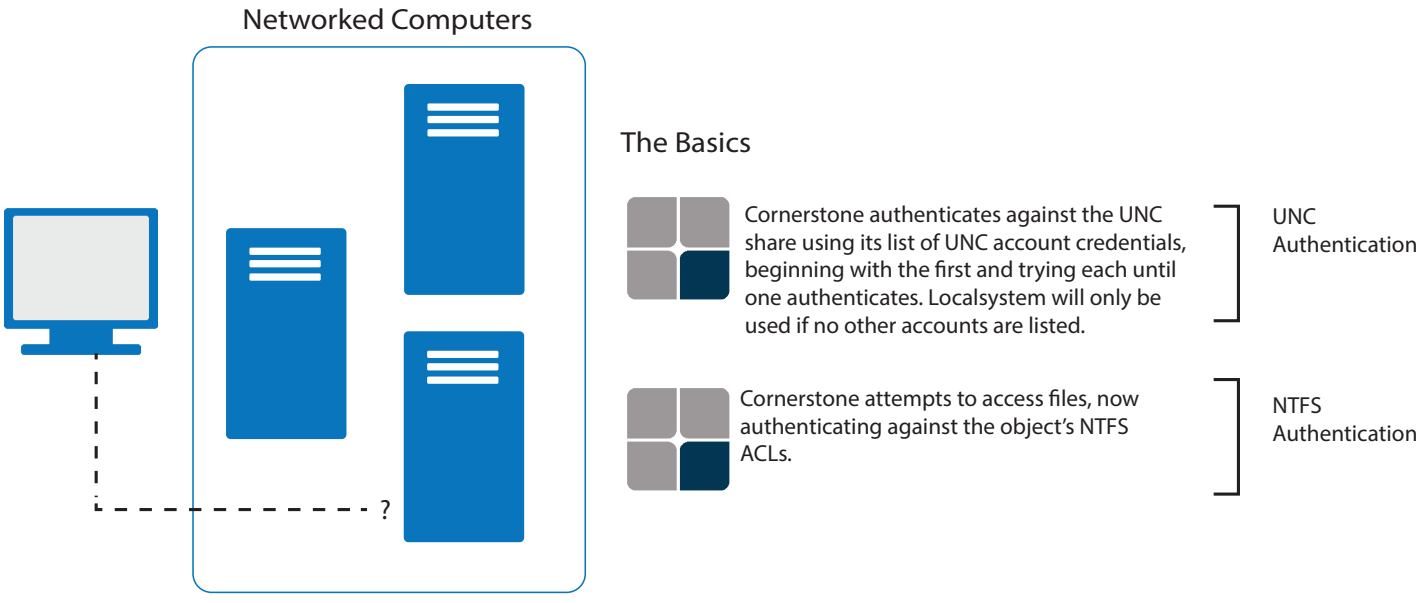
Universal/Uniform Naming Convention (UNC)

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

Cornerstone MFT supports this capability in order to share information in a scalable environment. By assigning addresses any machine in the network can recognize, one or more servers can run in parallel and access the same back-end data storage to service any 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. This is a separate permissions set than the New Technology File System (NTFS) Access Control Lists (ACLs). The Cornerstone Service usually runs under a Localsystem account in Windows. By default, this account does not have rights to access a UNC resource located on a remote server.



How It Works

When Cornerstone needs to access any file or folder on the network, it will preface the operation with a call to an internal function named UNC_Authenticate() and will send the fully qualified path and filename of the resource as it is known locally in the system.

For instance, if a Virtual Folder named 'Some-Directory' for UserA has been set up in \\Server\Share\Some\Directory\, when UserA attempts to access that folder, the server will call UNC_Authenticate("\\Server\Share\Some\Directory") first to see if the user has any access at all to that folder.

UNC_Authenticate will do the following:

1. Check to see if the supplied path is a UNC. If it is not a UNC, it simply returns Success to allow the server to continue.
2. Check to see if there are any UNC Accounts set up in Cornerstone to be used for authentication **against the share**. This is critical to note: UNC Accounts are used only to authenticate against the share; they are NOT used for accessing the endpoint file or folder. More about this in the next section on NTFS permissions.
    a. If there are no UNC Accounts set up, Success is returned to the caller and the server continues processing.
3. If one or more UNC Accounts are set up:
    a. Cornerstone extracts the share name for the path '\\Server\Share\'
    b. Check the 'In memory' list to see if we already have a success authentication from a previous call. The In memory list, or cache, keeps track of UNC shares that have been authenticated and the date/time of the authentication.
        i. Yes? Great, Cornerstone has previously authenticated. Check the timestamp; if it's been more than an hour, re-authenticate.
            1. Less than 1 hour? Return SUCCESS. Cornerstone will use the cached information.
            2. More than an hour? Flush the information from cache and proceed to re-authenticate using the next steps.
    c. Enumerate through the list of UNC Accounts entered into Cornerstone, in order, and:
        i. Make a call to WNetAddConnection2('\\Server\Share\',UncUsername, UncPassword,0). This Windows function call checks to see if the specified UNC Account username & password has access to the requested UNC. This function could return:

            1. SUCCESS – the UNC username and password are valid credentials for accessing the '\\Server\Share'.

2. ACCESS DENIED – the UNC username and password are invalid credentials for accessing the '\\Server\Share'.

3. CONFLICTING CREDENTIALS – another username and password has already been successfully presented to the OS for accessing '\\Server\Share\'.

ii. In the case of (1) or (3), the server has been successfully authenticated against the UNC. At this point, Cornerstone makes a record of the UNC '\\Server\Share' along with the date/time of when the authentication successfully happened. Cornerstone stores this in memory for later use and returns SUCCESS to the caller.

iii. If Cornerstone receives ACCESS DENIED, it returns to enumerate through the next UNC account in the list until one works or all options in the list are exhausted.

That's all UNC_Authenticate/UNC Accounts does. It is used to get the Cornerstone server in the 'front door' when accessing data that lives on a UNC share. Once the user gets past the UNC share gatekeeper, Generic NTFS permissions and ACLs kick in just as if you were trying to access a file on C:\Some\Directory\.

NTFS Permissions

When Cornerstone needs to access a file such as C:\some\directory\somefile.ext, Windows will engage NTFS file permissions to check access to see if the current Windows user who is trying to access the file has proper NTFS file permissions. When someone logs into the Windows Desktop using their username and password, they get a process token which identifies them in Windows. When the user runs Explorer and tries to open a file, Windows uses the same process token against the NTFS ACL to see if the Windows User associated with the process token has proper access rights to the underlying file. If the user does not have rights, an Access Denied (error 5) is returned.

When the Cornerstone server runs, it also needs to log into Windows with a username and password. By default, all Windows Services such as Cornerstone will run under the context of a special account called LocalSystem. The service starts, 'logs in' as LocalSystem, and then acquires the process token for LocalSystem.

When Cornerstone needs to access a file on behalf of the FTP client user, the Windows OS will need to check the NTFS file permissions. It takes Cornerstone's process token for LocalSystem and checks to see if LocalSystem has NTFS permission to access the file.

Normally, the LocalSystem account has NTFS permission for all files located on the local hard drive (C:\). However, LocalSystem normally has NO rights to access files stored on a UNC, as those files are foreign.

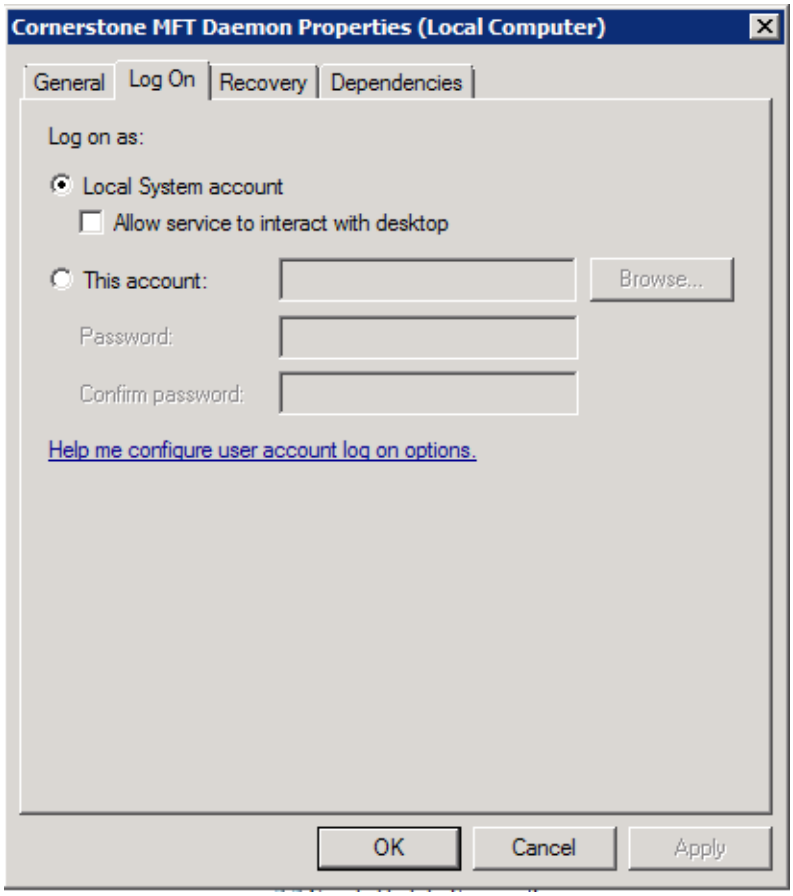
This is an important concept to grasp. While a UNC Account will allow Cornerstone to gain access to resources stored on a UNC Share, it's the process token of the Cornerstone server combined with the login credentials on the Cornerstone's home system which is ultimately responsible for granting or denying access.

So if Cornerstone is running under the context of LocalSystem, and UNC Accounts only grant access to the

share, not the foreign file the UNC share, how can Cornerstone access the file?

There are two methods to achieve this:

1. Create an NT Domain Account which has NTFS permission to access the file/ folder located on the UNC share, then update the Cornerstone service to use this Domain Account instead of LocalSystem.
2. In Cornerstone, use Windows NT/SAM or ADSI Authentication instead of Native Authentication, and make sure to enable 'NT Impersonation'. This is the method SRT recommends.
    a. NT Impersonation allows the remote client to log into Cornerstone, which then impersonates that user when accessing files. In other words, Cornerstone takes the users' process token and assumes their identity, tricking the Windows OS into thinking that the other user is accessing the files. Once authenticated against the NTFS ACL, Cornerstone reverts back to its own process token until the next file request comes in.



Setting It Up

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**

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 ACL for both the share and the underlying 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.

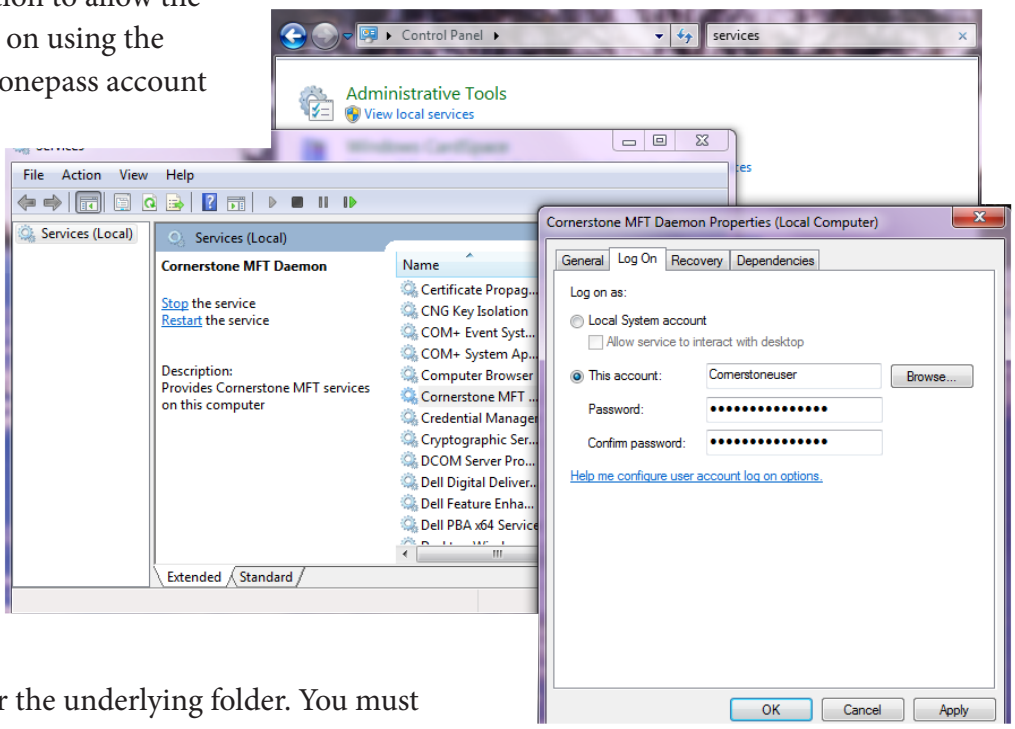
2. Make Cornerstoneuser a member of the Domain Admins and Domain Users groups by opening the Local Security Policy applet on the AD and, under Security Settings > Local Policies > User Rights Assignment, grant Cornerstoneuser the right to **Access Computer From The Network** and **Act As Part Of Operating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

3. Install Cornerstone MFT Server on the target computer. This may or may not be the AD, but it 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.

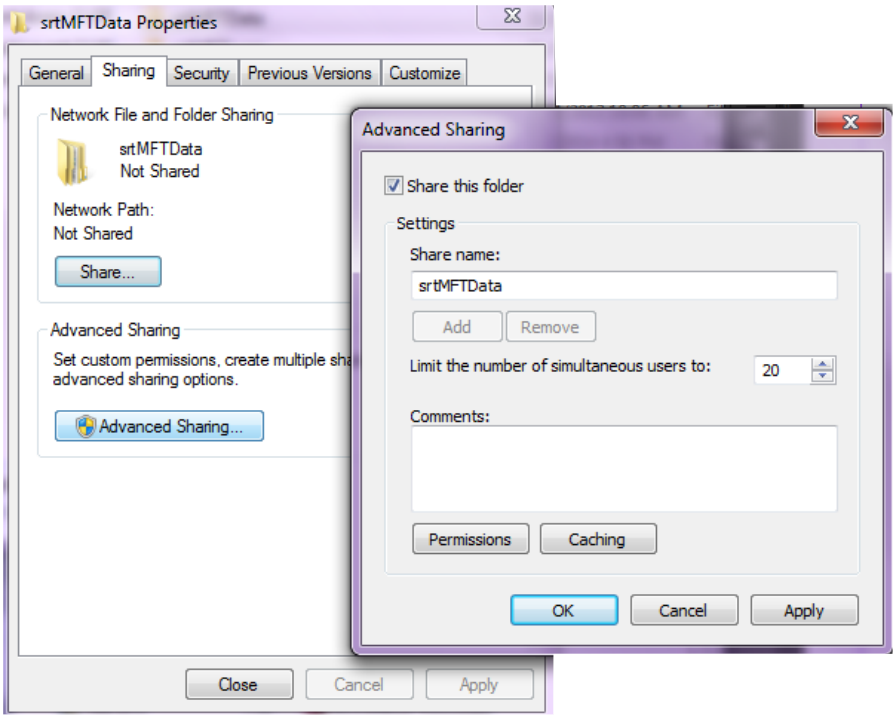
Use Sharing Properties to Create a UNC

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

To set up a UNC Share in Cornerstone:

1. Run Windows Explorer on the computer where the appropriate directory is stored locally. Don't perform this action remotely. 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** or **Reconfigure an existing server**.

Configuring Cornerstone using the New Server Wizard:

1. Run the Cornerstone Administrator and click New Server Wizard.
2. When creating the primary/first server of the cluster, select whether this will be the primary node of a clustered environment. If it will be clustered, this should be your primary server.
    - 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:

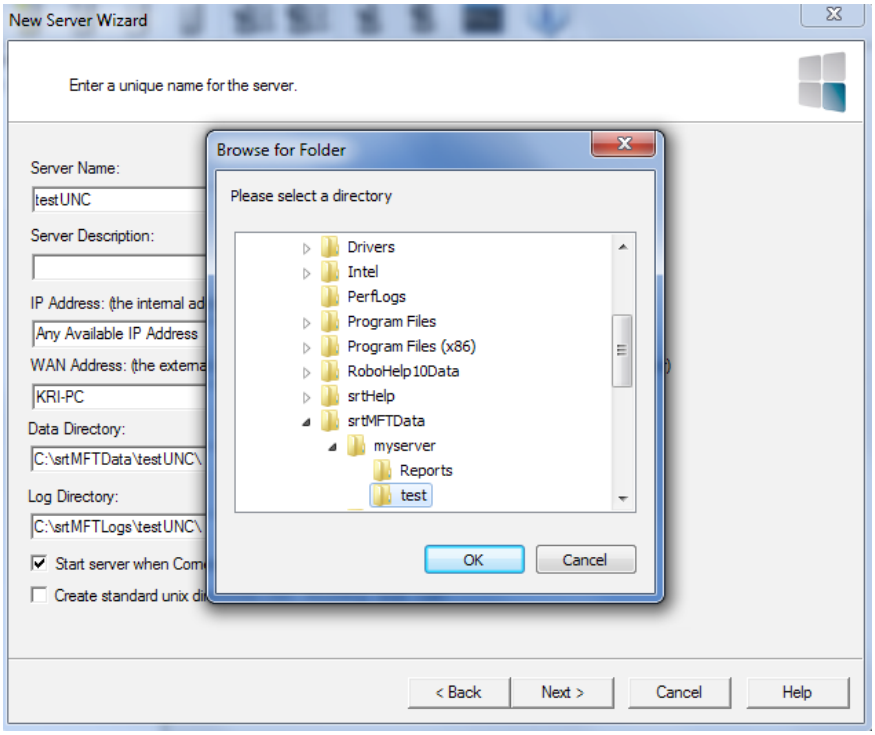
If you already have a server you would like to link to a UNC, follow these steps:

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
- Windows Server 2016, 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