2018

Using SSL Public Key Security with Cornerstone MFT Server

Instructions for configuring and maintaining Public Key Certificate based security in conjunction with FTP, HTTP, and WebDAV services on Cornerstone MFT Server.

QuickStart Guide

SSL Public Key Authentication in Cornerstone

Public key security, more formally known as asymmetric cryptography, involves the use of a key pair to encrypt data. Unlike symmetric cryptography, which uses only one key to both encrypt and decrypt, asymmetric cryptography involves two keys that perform opposite functions but make up one process. The public key encrypts the data, which can then only be decrypted by the matching, secret private key. The private key cannot be divined with the public key, so a user can safely disseminate the public key to users, who can then send coded data only the key pair owner can decode.

Cornerstone uses public key security through Secure Sockets Layer (SSL), which is incorporated into several file transfer protocols, including FTPS, HTTPS, and WebDAVS. SSL offers a higher level of security by optionally accepting connections with only authorized certificates.

Configuring the Cornerstone Administrator

To configure your Cornerstone server to utilize public key authentication, start by running your Cornerstone MFT Server administrator. Launch the New Server Wizard and follow the steps.

1. Select the file transfer protocols this server will handle. Enable FTP access if you are using FTPS with explicit SSL (also known as AUTH SSL). If you will only be using Implicit SSL, you may disable FTP. Enable HTTPS for secure web browser access, including secure WebDAV access. Click Next.

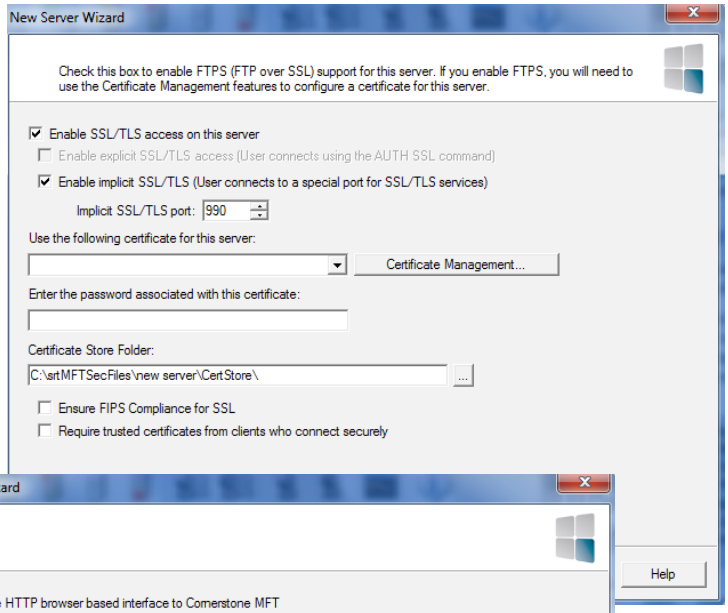
Explicit SSL – When using Explicit SSL, Cornerstone MFT will allow SSL connections on the standard FTP port. This port will be used for both FTP connections and FTPS connections. In order to enter into a secure SSL session, the FTP client will need to issue either the AUTH SSL or AUTH TLS command prior to establishing the secure connection. You must enable **Require all FTP connections from the clients to be secure** if you are using explicit SSL and do not wish to allow unsecured access to your server. Explicit SSL is the preferred standard, but either method is secure. Explicit SSL is the recommended method for HIPAA compliance because implicit SSL is not formally adopted in an RFC.

Implicit SSL – When using implicit SSL, Cornerstone MFT 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.

2. Depending on the options selected in step 1, you will be taken to an FTPS and/or HTTPS configuration page. To enable SSL/TLS access on this server, select the appropriate check box:

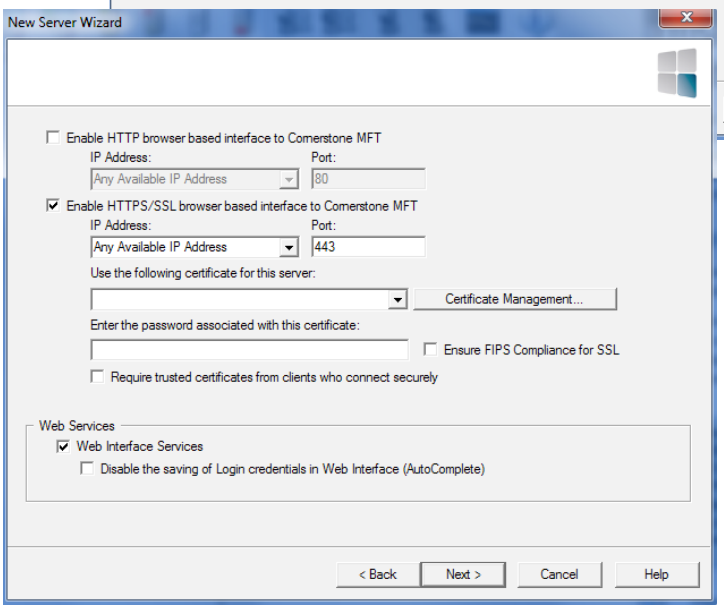
a. **Enable SSL/TLS access on this server**, after which you can also Enable Explicit SSL/TLS and/or Enable Implicit SSL/TLS

b. **Enable HTTPS/SSL browser based interface to Cornerstone MFT** -



3. Select a certificate using the dropdown menu, click Certificate Management to launch the Certificate Wizard to create a certificate for this server, or use the "…" button to browse to your Certificate Store Folder.

4. When you are finished configuring certificate options, click Next.



Once the server is created, it will start and appear in the main Cornerstone MFT Administrator window with a green icon to indicate that the server is running. You may now add users to the system.

If you would like to review the server's settings, select Security from the left-hand tree view and select the FTPS/SSL tab under the server settings. Once you have configured your settings, click Apply. Click Yes to restart the server and apply the new settings.

We recommend selecting **Protocol Version TLS v.1.0** (SSL v3.1), which has enhanced security compared to SSL v3.0, and **Encrypt Data Channel**, which will force encryption unless the client explicitly turns it off.

The **Enable CCC** feature allows plaintext communication to occur, so this feature should be disabled in cases where encryption is preferred.

If you enable **Require Trusted Certificates**, please be aware that this feature requires all FTPS clients to provide a trusted certificate to connect. This is the most secure method of connecting, but, as it requires trusted keys to be distributed to each user offline, it may not be practical.

For additional information on the configuration steps not included in this QuickStart, consult the online Cornerstone Cornerstone MFT User Guide at **http://webdrive.com/product-support/cornerstone-mft/** or the Knowledge Base at **http://srthelpdesk.com/**.

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