2018

Certificate Management

This guide focuses on using the Cornerstone Certificate Managament Wizard to create, import, or sign certificates.

QuickStart Guide

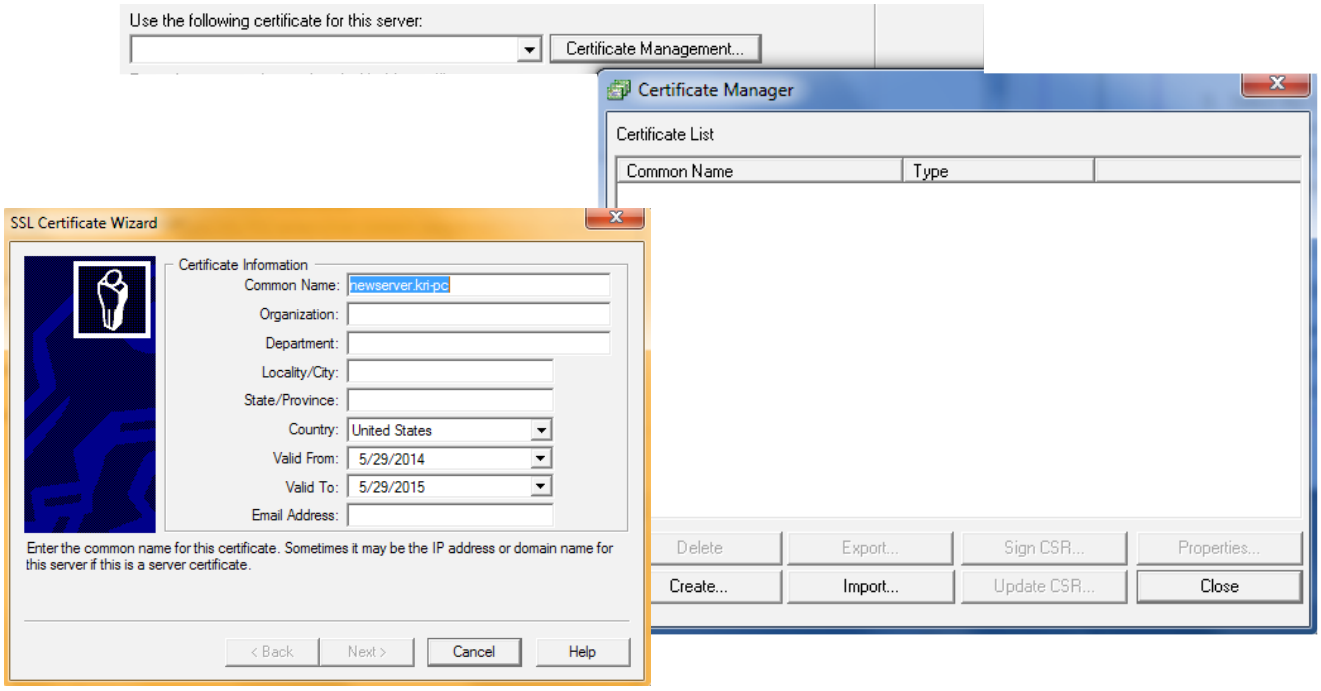
Cornerstone MFT Server Certificate Manager

Certificates provide an essential layer of security to file transfers by verifying the origin of the transfer. An electronic document can be signed with a certificate, bound to the sender's public key, which creates a unique signature that can only be decoded by the matching private key.

Cornerstone MFT's Certificate Manager allows you to create new certificates, import previously-made certificates and private keys, and sign your own certificates. Once you have certificates stored in Cornerstone, you can also use the Certificate Manager to Delete, Export, Update, or view the Properties of your certificates.

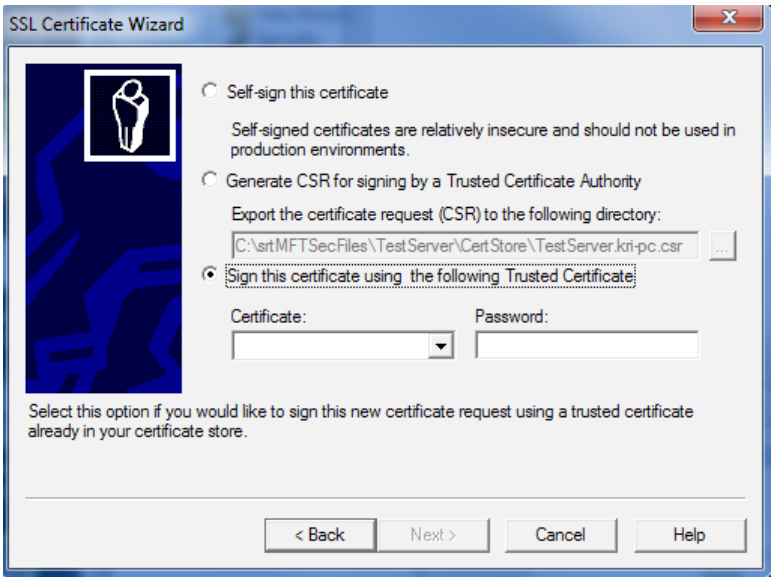
To find the Certificate Manager, launch the Cornerstone Administrator, expand your Server, and select Security. Under the FTPS/SSL tab, enable SSL/TLS and click the **Certificate Management...** button.

The Certificate Manager is accessible from other locations in Cornerstone; it will appear on any screen that deals with SSL, including during the Server Creation Wizard.



Create a New Certificate

1. Click Create to create a certificate. This will launch the SSL Certificate Wizard.
2. You must supply valid information for each field for the certificate to validate. The Common Name (CN) is the name of the server. Avoid using special characters (though the asterisk (*) symbol is valid when used as a wildcard to cover many different domains). Please note that some Certificate Authorities do not allow you to abbreviate the State/Province name. Click Next.
3. Select a desired key length for your certificate. Longer key lengths provide better security but result in slower performance. Shorter keys run faster but are less secure. Key lengths of 2048 bits or larger are recommended for secure environments. Click Next.



4. Your certificate name will populate automatically. Create a Private Key password. Your password is case sensative and must be at least four characters with no spaces. After you confirm your password, click Next.
5. There are three options available for generating your certificate:

   - **Self-sign this certificate**—Self-signed certificates are relatively insecure. In general, this option should only be used for testing purposes and should not be used in a production environment.
   - **Generate CSR for signing by a Trusted Certificate Authority**—Select this option if you would like to generate a Certificate Signing Request (CSR) to send to an external Certificate Authority (CA) or Trusted Authority for signing. Once the CSR has been signed and your certificate generated, you will be able to update your CSR and use your newly signed certificate. Export the certificate request to a directory by using the "…" browse button. For more information about generating a CSR for signing by a Trusted Certificate Authority, see the section on Generating & Updating a CSR.
   - **Sign this certificate using the following Trusted Certificate**—Select this option if you would like to sign this new certificate using a trusted certificate already

in your certificate store.

6. Click Finish when you are done configuring these options and Close the window.

To configure Cornerstone to start using the certificate, select Security in the tree pane and select the FTPS/SSL tab. Select your new certificate and and enter the corresponding password.

Import a Certificate

1. Click Import to import an already-existing certificate and private key.
2. Import Certificate provides two options for importing your certificate, which depend on whether your certificate is stored in one file or two:
   a. **Import my Certificate and Private Key from a single file (PKCS#12)**—Use the "…" browse button to browse to your .p12 file. Type your Private Key password, confirm your password, and type a name used to identify this certficate in the system. When you are finished, click Import.
   b. **Import my Certificate and Private Key from separate files**—Use the "…" button to browse to your .crt file. If you would also like to Import your Private Key Information, select this check box and browse to your .key file. You must then type your Private Key password and confirm your password. Type a name used to identify this certificate in this system. When you are finished, click Import.

Your certificate will be imported and added to the Certificate list.

Sign a CSR

1. Select Sign CSR. The Certificate Signing Wizard will launch.
2. The Certificate Signing Wizard provides two options for signing your certificate:
   a. **Sign a CSR in local store**—Use the dropdown arrow to select your certficate and type your password. Click Next when you are finished.
   b. **Select an external CSR**—Use the "…" button to browse to and save the certificate. Click Next when you are finished.
3. Select the certificate name using the dropdown arrow. Type the password used to access the keypair for the selected certificate. You can change the Valid From and Valid To dates by using the dropdown arrow. Click Finish.

Your certificate should appear in the Certificate List.

Generating & Updating a CSR

Having a certificate signed by a Certificate Authority (CA) adds a robust layer of authenticity and security to your certificate. If you opted to create a certificate and have it signed by a Certificate Authority, follow these steps:

1. After selecting **Generate CSR for signing by a Trusted Certificate Authority**, export the certificate request to a directory by using the "…" browse button. Be sure to take note of where you save the .csr file; you will need to access it again to send it to the Certificate Authority. Click Finish.
2. You will see a message indicating that your CSR has been successfully exported to the directory you specified. Click Close to close the Certificate Manager.

Sending the CSR to the Certificate Authority

1. Open your .csr file in a WordPad or other text editor. Copy the text of the entire file, including the words "Begin Certificate Request" and "End Certificate Request".
2. You must choose a Certificate Authority. There are many to choose from, such as:
   - https://www.thawte.com
   - http://www.verisign.com
   - http://www.digicert.com

The CA's website should include a place for you to paste your CSR and provide any additional information required by the Certificate Authority.

After you submit your Certificate Signing Request, the CA will verify the information and create a certificate for you. The time necessary to create a certificate varies from authority to authority, so check with the specific CA for turn-around times.

To Update CSR in Cornerstone MFT

There are two common methods of updating your certificate. The easier method is to renew your current certificate and then copy the new private key information into the old file, which doesn't require a new CSR. If you require a new CSR, you'll need to replace the file and take the server offline briefly.

Steps for renewing a certificate:

1. Go through the normal process for renewing your existing certificate and download the new SSL certificate .zip in from the manager. Make sure to select

Other server type, which determines the format of the certificate.

2. Unzip the folder, which should contain two files: one is common name certificate, while the other will likely be special to your certificate host (for instance, GoDaddy certificate files begin with gd in the filename).
3. Since the running server is using the old certificate, you can't change that file. Go to the old cert store folder and make a copy of the old .pem file. There is a public and private section of the file.
4. Open new certificate, select all, and copy. Paste this over the existing private key information in the new .pem file.
5. Rename the old file to something new (for example, cornerstone.com_OLD), and change the copied filename to the old filename, so Cornerstone will draw from the correct certificate information.
6. To cement the new information, open the Cornerstone administrator to the Services > FTPS/SSL tab and select the correct file again under "Use the following certificate for this server" and enter the password (which should be same as before).

To test this, pull up a web browser and go to your server login page and click the HTTPS link in the URL to check the certificate; it should show the Valid From and To as the updated dates.

After the Certficate Authority approves your CSR, it will email you a secure link to access your certificate. Copy your certificate to WordPad and save in .crt format. When you name your .crt file, do not use extra periods or special characters. Be sure to take note of where you save the .crt file; you will need to access it again to update the certificate stored in the server.

1. Launch the Cornerstone MFT Certificate Manager. Select Update CSR. **Do not choose Import**—this will invalidate your CSR.
2. The Update CSR Utility will launch. Use the dropdown arrow to select the CSR File you would like to update with a signed certificate. Once updated, the CSR will become a valid certificate associated with your key pair. Type your password. Use the "…" button to browse to the location of your certificate file. When you are finished, click Update. Click OK.

Your CSR is now upgraded to a verified certificate file. You may now use the certificate.

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