2017

Cornerstone MFT Server and SSH Host Key Authentication

A guide for configuring and maintaining SSH Host Key Authentication for SFTP connections in Cornerstone MFT Server.

QuickStart Guide

Host Key Authentication with SFTP

Cornerstone MFT Server can use Secure File Transfer Protocol (SFTP), a Host Key Authentication method which adds Secure Shell (SSH) protection to your data transfers.

Most encryption methods for information transfer involve Public Key Infrastructure (PKI), which is the use of a key pair made up of a public and private key to encrypt data. The public key can be disseminated by the key pair owner, and any recipient can use it to encrypt data. That data can then only be decrypted by the matching private key the owner keeps secret.

Both the client and server using SFTP should generate a separate host key pair and exchange public keys. Both parties can then send encrypted data that can only be decrypted by the intended recipient.

The client host key pair should be exported and sent to the Cornerstone Administrator in .pub format. Cornerstone will import it into the Host Key Database.

Note that **Cornerstone can only read OpenSSH** format keys. See the **Appendix** for more information.

Host Key Best Practices

While it is possible to use the Host Key Management features in Cornerstone MFT to create user host key pairs for your clients, it is highly discouraged. It's difficult to ensure the integrity of the transfer from the server computer to the client computer.

If it is impossible to have clients create their own host keys, ensure your transfer is secure. Export the keys to an encrypted USB drive, or encrypt the files onto a DVD/CDROM and physically hand deliver them to the client. Never email the host key files to the user. Email is natively insecure; there is no way to ensure the integrity of the files during electronic transfer.

Never share or send your private key to anyone; this will compromise the integrity of your host key pair. It's good practice to password protect your private key as well, and Cornerstone MFT requires this.

Creating the SFTP Server

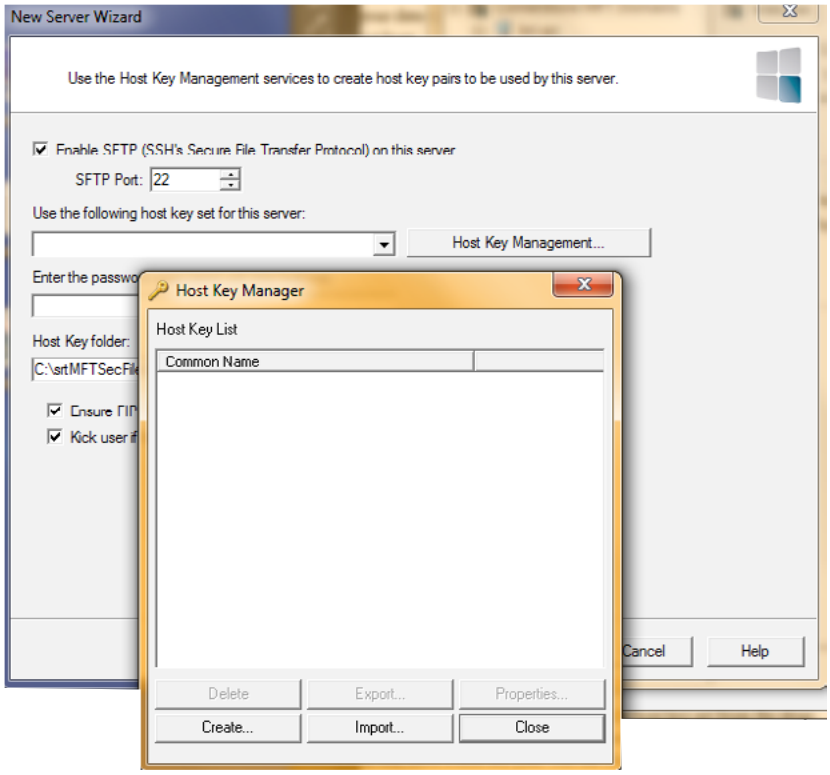
Begin by launching your Cornerstone administrator and creating a new server. Follow the prompts in the New Server Wizard until the step where you choose which services this server will support:

1. If your sole purpose for this server is to make SFTP transactions, select only the **SFTP (typically port 22)** service from the list. This guide only covers the instructions pertaining to SFTP.
2. Check the **Enable SFTP (SSH's Secure File Transfer Protocol) on this server** box and choose the port number using the up/down arrows. Choose the host key set from the dropdown menu. If this is a new server installation, most likely there will be no host keys defined. To use SFTP services, you will need a host key pair. Use the Host Key Management utility to either create a new

host key or import an existing host key pair from an external file. Once you have created a host key pair, select it from the list and type the password associated with the host key. Click the "…" button to browse to the Host Key folder.

a. Click Create to create a Host Key pair for this server. (Or click Import to import a Host Key pair.)

b. Choose your Host Key Type using the dropdown arrow. Note that DSA host keys must be 1024 bits in length. RSA keys do not have this restriction and can range from 512 to 4096 bits. Longer key lengths provide better security but result in slower performance. Shorter keys run faster but are less secure. Key lengths of 1024 bits or larger are recommended for secure environments. Click Next.



c. Type a name to identify your new host key set in the system. Avoid using special characters. Create a private key password. Your password is case sensitive and must be at least four characters with no spaces. After you confirm your password, click Finish.

d. Click Close to return to the Cornerstone MFT New Server Wizard.

3. Select your newly created host key set from the dropdown list, enter the password for the host key pair, and click Next.

Once the server is created, the server starts and appears in the main Cornerstone MFT Administrator window. A green-lit icon appears to indicate that the server is running. You may now add users to the system.

Configure Your SFTP Server

The default SFTP settings allow for standard password authentication when accessing the SFTP server. For most situations, this is sufficient. However, if you plan to use Host Key Authentication for clients accessing your SFTP Server, you will need to make some additional modifications to the standard SFTP configuration.

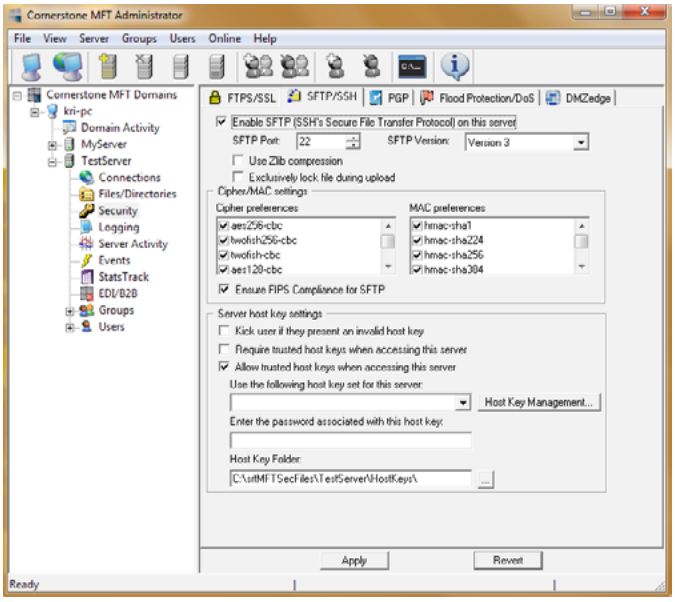
From the Cornerstone administrator, expand your new server and select Security. In the tab pane, select the

SFTP/SSH tab.

- If you wish to have Cornerstone MFT support Password Authentication only, deselect both the **Require Trusted Host Keys when accessing this server** and **Allow Trusted Host Keys when accessing this server** options.
- If you wish to support both Password Authentication and Public Key Authentication (meaning that client can use either Password OR Public Key Authentication), then select the **Allow trusted host keys when accessing this server** option and deselect the **Require trusted host keys when accessing this server** option.
- If you want your SFTP server to ONLY support Public Key Authentication, select the **Require Trusted Host Keys when accessing this server** option.

During server configuration we recommend deselecting this option until you successfully connect to the server. Once you can successfully connect, return to the SFTP/SSH tab and select this option. Apply the configuration options and restart your server.

Assigning and Importing Host Keys



If you have selected Allow Host Keys or Require Host Keys, then you will need to assign a public host key to each user. This public host key will be supplied by the client. They will need to send you their public host key in SSH2 or OpenSSH format so you can import it into the server and associate it with their Cornerstone MFT User account.

To allow public key log on for a user, expand Users and select the user's name. Select the SFTP/SSH tab and click Host Key Management.

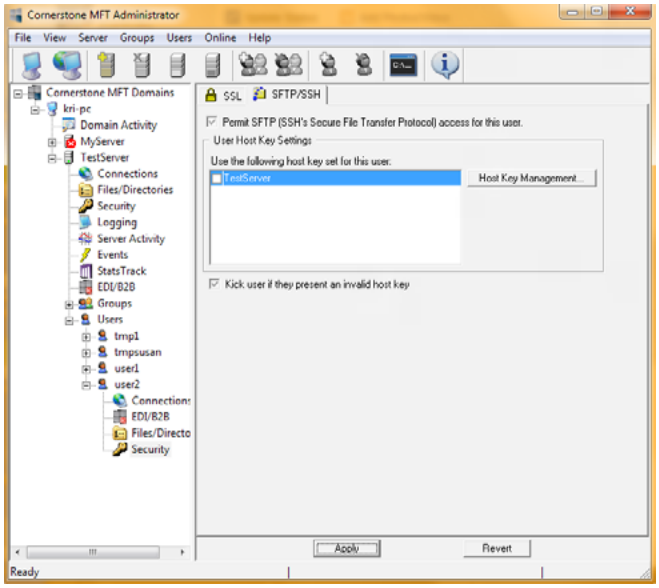
1. Import the client's public host key into the Cornerstone MFT's host key database.
2. Navigate to the client's public key filename and click Import. If you receive the "Unable to import host key due to invalid format or bad password. Make sure the SSH key is OpenSSH format (Error 1610)" error, see the **Appendix** for more information.
3. Once the client's public host key has been successfully imported into the Cornerstone MFT Host Key Database, it will appear in the list with the other host keys. Click Close to return to the user's SFTP settings where you can associate this new key with the user's account.
4. Select the user and choose the SFTP/SSH tab. Select Permit SFTP (SSH's Secure File Transfer Protocol) access for this user. Use the drop-down arrow to select a host key set. Click Apply.

5. You can download an SFTP client, such as psftp.exe, to test your server. After you have downloaded your SFTP client:

Open a command prompt, type "psftp," and press the enter key. Type either "open localhost" or the IP Address of the server. If you specified a port number, add it here. For example, "open localhost 21" (open computer port#).

This will begin an SFTP session. When prompted, enter the username and user's password. You should now be logged onto the Cornerstone MFT. Type quit to exit DOS and return to Windows.

Appendix: Creating Client Host Key Pairs



Generating Keys Using PuTTYgen

There are many easy and free ways to create host key pairs. We recommend PuTTYgen, but feel free to look for other options.

1. Download PuTTYgen from http://www.putty.nl/download.html.
2. Click Generate and move your mouse around on the screen while the key is formed to add human-variable randomness.
3. Type a password for the key and change the Conversion option to **Export ssh.com key**.
4. Click Save public key. You must add the .pub extension to the filename.
5. Export the private key from PuTTY keygen. Note that you do not have to change file extensions on this file.

You should now have 2 key files.

Importing the New Public Key into Cornerstone

You must import the public key into Cornerstone to replace the existing PuTTY key.

1. Launch the Cornerstone Server Administrator. In the tree pane, select the user, and in the tab pane select the SFTP/SSH tab. Click Host Key Management. The Host Key Manager will launch.
2. Click Import and use the "…" button to browse to your public key filename.
3. Click Import.

You must replace the older PuTTY-generated public key with the one you are importing into Cornerstone,

so when you are asked if you would like to overwrite the existing key, click Yes.

After you have imported the public key and closed the Certificate Manager, you must attach the public key to the user via the SFTP/SSH tab on the user's configuration.

Troubleshooting

Keys can be saved in two formats: OpenSSh and SSH2. Cornerstone can only read OpenSSH files. Some SFTP clients may generate host keys that cannot be used by Cornerstone.

Server Error 1610 & Generating Usable Keys

If, while trying to import OpenSSH host key pairs into Cornerstone, you receive the "Unable to import host key due to invalid format or bad password. Make sure the SSH key is OpenSSH format (Error 1610)" error, these workarounds might help.

Option #1, Performed on the client:

1. Download PuTTYgen: http://www.putty.nl/download.html
2. Run PuTTY and select Conversions > Import Key.
3. Select and open the Private Key. Type the password for the Public Key and click Save Public Key.
4. Send the public key file to the Server Administrator to import into the Cornerstone server.

Option #2, Performed on the client:

If you have created an OpenSSH key pair with the ssh-keygen command, you can use the "ssh-keygen -e -f" command to create a usable public key. For example:

```
ssh-keygen -e -f $HOME/.ssh/id_dsa > $HOME/.ssh/SSH_dsa.pub
```

This command will read the private key and generate a public key that can be used by the Cornerstone server.

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