



CornerstoneMFT

Cornerstone MFT
SFTP/Host Key Authentication Quick Start Guide

January 2010

Notices

Thank you for purchasing Cornerstone MFT®.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement, OEM, or reseller agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of South River Technologies, Inc.

South River Technologies, Titan FTP Server, Cornerstone MFT, WebDrive, DMZedge, and GroupDrive are registered trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP and Windows Vista are registered trademarks of Microsoft Corporation, Inc. The names of other actual companies and products mentioned herein may be the trademarks of their respective owners. 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.

South River Technologies, Inc.
2635 Riva Road
Suite 100
Annapolis, Maryland 21401
USA
Telephone: 410-266-0667
Fax: 410-266-1191
www.southrivertech.com

Please Note:

The following instructions will help you to set up Cornerstone MFT using Secure File Transfer Protocol (SFTP) and to use Host Key Authentication. Some screens in this instruction contain options that do not pertain to Host Key Management and SFTP server configuration. If you need additional information regarding these steps, please see the [Cornerstone MFT User Guide](#). For the purpose of this SFTP Quick Start guide, we will guide you through these options without configuring additional settings. A listing of Frequently Asked Questions (FAQ) is also available at our [Knowledgebase Support Center](#).

Client Host Key Pairs

The client host key pair will be created by **each individual client**. They will then need to export their Public Host Key in SSH2 or OpenSSH format and send that .pub file to the Cornerstone Administrator so that it can be imported into the Cornerstone Host Key Database. See the [appendix](#) for more information.

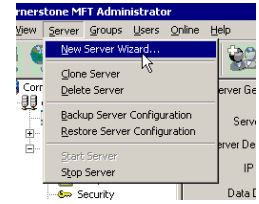
Host Key Best Practices

Each entity in a secure SFTP environment, both the client and the server, should generate its own host key pair. This host key pair will have a public key and a corresponding private key. Never share or send your private key to anyone as this will compromise the integrity of your host key pair. It is always a good practice to password protect your private key as well, and Cornerstone MFT requires this.

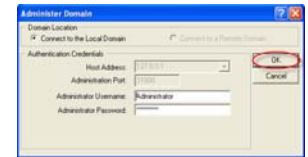
While it is possible to use the Host Key Management features in Cornerstone MFT to create user host key pairs and then export them for use by your clients, it is highly discouraged because it is difficult to ensure the integrity of the user's private host key during the physical transfer of the host key file from the server computer to the client computer. If it is impossible to have the clients create the own host keys, it is recommended that the transfer of the host key pair from the server computer to the client computer be performed over a secure medium. Export the keys to an encrypted USB drive, or encrypt the files onto a DVD/CDROM and manually hand deliver them to the client. However, never email the host key files to the user. Email is natively insecure and there is no way to ensure the integrity of the files during electronic transfer.

Configuring the Cornerstone Server

1. Run the *Cornerstone Administration utility* and start the **New Server Wizard**.



2. When the *Administer Domain* window appears, select the radio button to connect to the Local Domain*. Choose the Host Address by using the drop-down arrow. Type the **Administration Port**, **Administrator Username**, and **Administrator Password** and click **OK**.

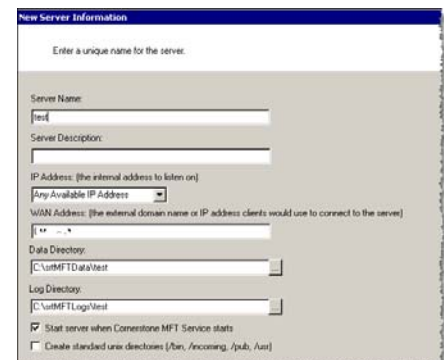


*NOTE: The ODBC based user authentication requires configuration of an ODBC data source for the PC on which Cornerstone MFT is physically installed so this process must be performed through a Local Domain connection. Configuring ODBC based user authentication through a Remote Domain session is not supported.

3. Select the Server Type and click **Next**.

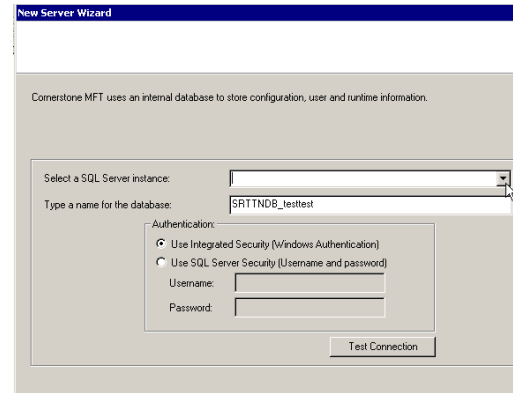


4. Type a unique **Server Name**. Click the drop-down arrow to choose your **IP Address**. (*Any available IP address* indicates that the server will listen on all IP addresses that are configured on the PC along with the local IP address of 127.0.0.0, also known as *localhost*.) Type the **WAN address**. You do not need to type "**http**", for example, "**myserver.com**". Select the check box to start this server when Cornerstone MFT starts. When you are finished, click **Next**.*

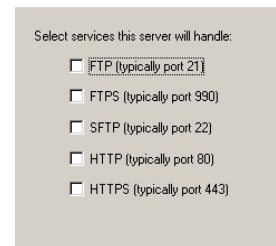


*If you need to create standard UNIX directories you can find additional information in the [Cornerstone MFT User's Guide](#).

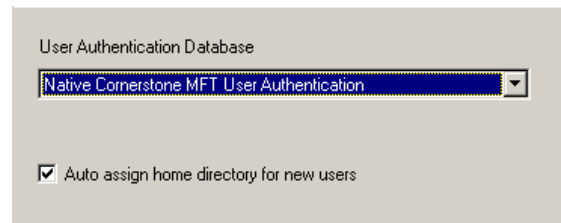
5. Cornerstone uses an internal database to store configuration, user, and runtime information. Use the drop-down arrow to select a SQL Server instance. Type a name for this database. Select **Windows Authentication** or **SQL Server Security**, and then click **Test Connection**. Once you connect successfully, click **Next**.



6. Select the **Services** that this server will handle.

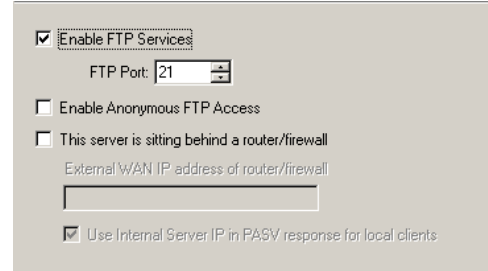


7. Select your *User Authentication Database* using the drop-down arrow. After you have configured your User Authentication Database, click **Next**.*



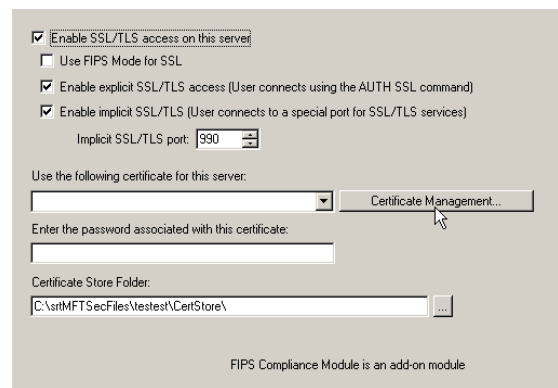
*Once you select a User Authentication Database in Cornerstone, you cannot change to a different method once the server wizard has completed. If you need more information about configuring user authentication, please see the [Cornerstone MFT User's Guide](#) or the [SRT User Authentication Quick Start Guide](#) for your specific user authentication database.

8. If you wish to enable FTP Services select the *Enable FTP Services* check box. Select the *FTP Port* number by using the up/down arrows. To enable anonymous FTP access, select the check box. If your server is sitting behind a router/firewall select this check box and type the external WAN address of the router/firewall. You do not need to type “**http**”, for example, **mywanaddress.com**. When you are finished with *FTP Services* options* click **Next**.



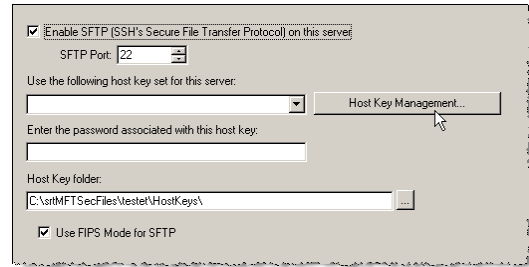
*For more detailed information pertaining to these configuration options see the [Cornerstone MFT User’s Guide](#).

9. To enable SSL/TLS access on this server, select this check box* and choose the appropriate sub-options for which FTPS access methods will be allowed. Click the drop-down arrow to choose the certificate. Click **Certificate Management** to configure a certificate for this server. Enter the password associated with the certificate. Use the “...” button to browse to the *Certificate Store Folder*. When you are finished configuring SSL/FTPS Security Settings, click **Next**.



*If your sole purpose for this server is SFTP, we recommend that you *do not* select this check box.

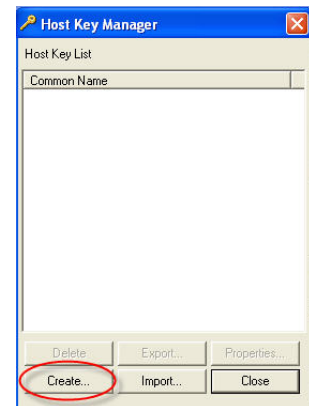
10. To enable **SFTP** (SSH's Secure File Transfer Protocol) on this server select this check box and choose the port number using the up/down arrows. Choose the *host key set* by using the drop-down arrow. If this is a new server installation, most likely there will be no host keys defined. To use **SFTP services**, you will need a host key pair that will be used by the Cornerstone MFT. Use the Host Key



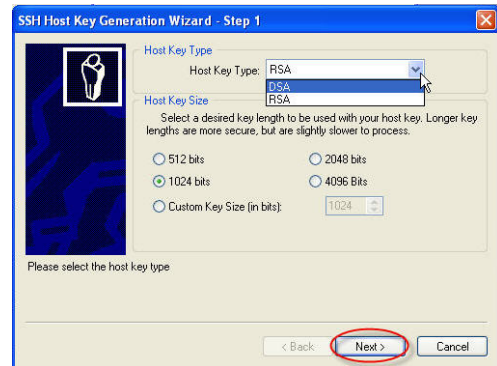
Management utility to either create a new host key pair to be used by the Cornerstone MFT or to import an existing host key pair from an external file set. Once you have created a host key pair, select it from the list and then type the password associated with the host key. Click the "... " button to browse to the *Host Key folder*.

*Port 22 is reserved for SSH (Secure Shell)/SFTP and is the default/recommended port.

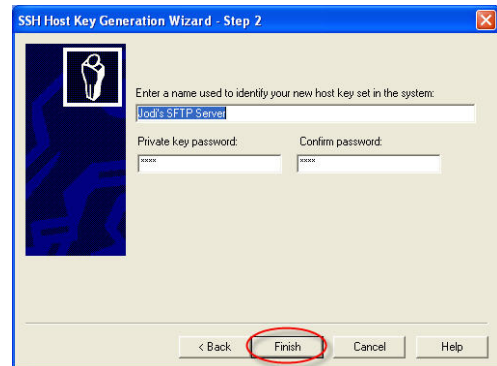
11. Click **Create** to create a Host Key pair for this server. (Or click **Import** to import a Host Key pair.)



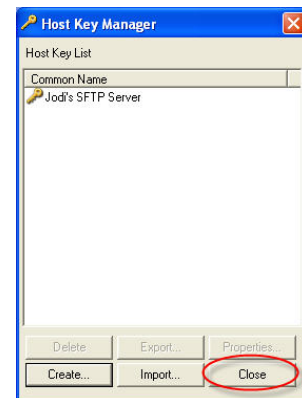
12. Choose your Host Key Type using the drop-down arrow. Note that DSA host keys must be 1024 bits in length. RSA keys do not have this restriction and can range from 512 bits in length to 4096 bits in length. Longer key lengths provide better security, but result in slower performance. Shorter keys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



13. Type a name to identify your new **host key set** in the system. Avoid using characters that any system treats as special characters. Create a **Private Key password**. Your password must be at least four characters with no spaces and is case sensitive. After you confirm your password, click **Finish**.

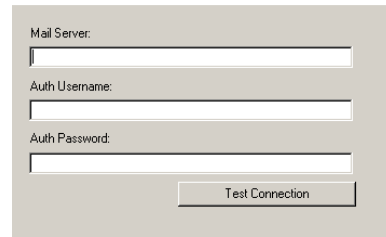


14. Click **Close** to return to the Cornerstone MFT New Server Wizard.



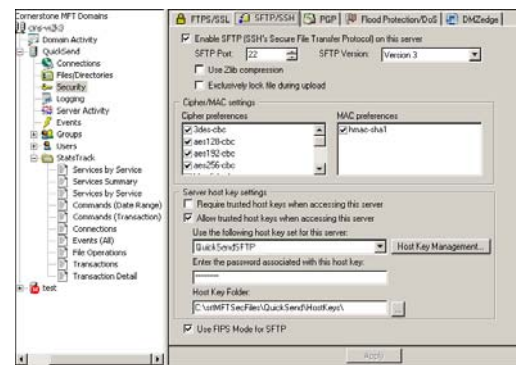
15. You are now returned to the *New Server Wizard*. Select your newly created *host key set* from the drop down list, enter the password for the host key pair, and click **Next**.

16. Type the URL or IP address of the SMTP mail server that will be used to send email notifications to users. You may test the connection by clicking **Test Connection**. (For more detailed information pertaining to these configuration options see the [Cornerstone MFT User's Guide](#).) When you are finished, click **Next** and then click **Finish** to create the server.



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

18. At this point, your SFTP Server is configured and will be running. 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. In the tree pane, select *Security*, and then in the tab pane, select the *SFTP/SSH* tab.

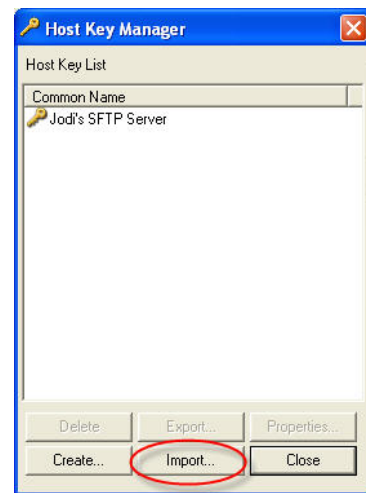


- If you wish to have Cornerstone MFT support Password Authentication only, then **deselect both** the *Require Trusted Host Keys* and *Allow Trusted Host Keys* options.
- If you wish to support both Password Authentication and Public Key Authentication (meaning that client can use either Password OR Public Key Authentication), then **select** the *Allow Trusted Host Keys...* option and **deselect** the *Require Trusted Host Keys...* option.
- If you want your SFTP Server to ONLY support Public Key Authentication, then **select** the *Require Trusted Host Keys...* option.* The *Allow Trusted Host Keys...* option will now be ignored. Note that if you enable the *Require Trusted Host Keys...* option, each user account MUST have a public host key attached to their user account.

*During server configuration we recommend that you deselect this option until you successfully connect to the server. Once you can successfully connect, return to the SFTP/SSH tab and select this option. Click **Apply** to apply the configuration options.

19. Click **Yes** to restart the server.
20. 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 is supplied by the client. They will need to send you their public host key in SSH2 (or OpenSSH) format so that 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**.

21. Click **Import** to import the client's public host key into the Cornerstone MFT's host key database.



22. Navigate to the client's *public key filename* and click **Import**. * Note that the client host key pair will be created by each individual client. They will then need to export their Public Host Key in SSH2 or OpenSSH format and send that .pub file to the Cornerstone Administrator so that it can be imported into the Cornerstone Host Key Database.



*If you receive the following error when you are trying to import OpenSSH host key pairs into the Cornerstone server : "Unable to import host key due to invalid format or bad password. Make sure the SSH key is OpenSSH format (Error 1610)", see the [appendix](#) for more information.

23. 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.

24. To associate a host key with a User's account, 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**.

25. 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 and type: **psftp** and then press the enter key.

Type either:

open localhost

-OR-

the IP Address that you specified in step 4.

If you specified a port number in [Step 8](#) you must add the port number.

For example, type: open localhost 21

↓ ↓ ↓
(open computer port#)

This will begin an SFTP session with the local Cornerstone MFT that you created.

When prompted, enter the user name.

When prompted, enter the user's password.

You are now logged on to the Cornerstone MFT.

Type **quit** to exit DOS and return to Windows.

Appendix: Creating Client Host Key Pairs

If you are using WebDrive, see the [WebDrive Host Key Authentication quick start guide](#).

Server Error 1610 & Generating Usable Keys

Some SFTP clients may generate host keys that cannot be used by Cornerstone. If you receive the following error when you are trying to import OpenSSH host key pairs into Cornerstone:

"Unable to import host key due to invalid format or bad password. Make sure the SSH key is OpenSSH format (Error 1610)",

we have included some options to work around this issue.

- If you have created Open SSH KEYGEN pairs using Linux/Unix, you can choose [Option #1](#) or [Option #2](#) to convert your previously created key.
- If you have created key pairs using CoreFTP, Filezilla, or other FTP clients that do not specifically create OPENSSH compatible key pairs, you can [create and convert key sets in Puttygen](#) using the instructions included in this appendix.
- If you are using [SecureFX](#), we have included instructions for creating keys that can be used with Cornerstone.

Option #1, Performed on the client:

1. Download Puttygen, available for download at <http://www.putty.nl/download.html>
2. Run Puttygen. Select **Conversions>Import Key**.
3. Select the **Private Key** and click **Open**.
4. Type the password for the Public Key and click **Save Public Key**.
5. 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 a OpenSSH key pair with the ssh-keygen command, you can use the following command to create a usable public key:

```
ssh-keygen -e -f >
```

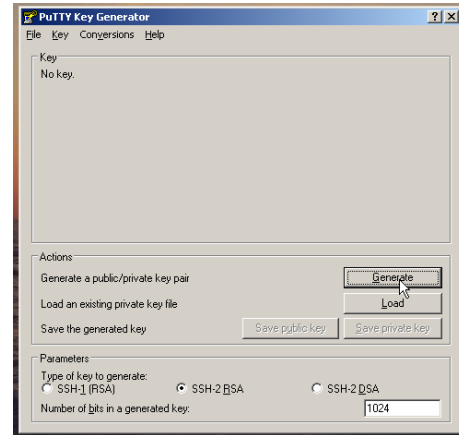
for example:

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

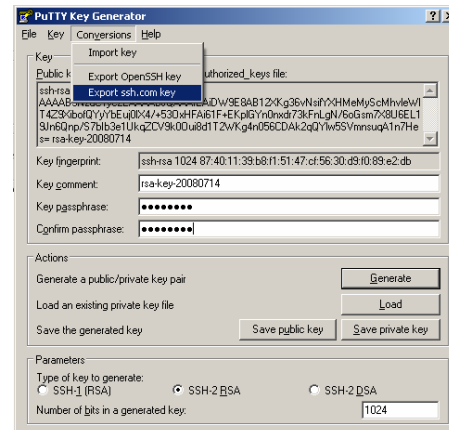
This command will read the private key and generate a public key that can be used by the Cornerstone server.

Generating Key(s) using Putty Keygen

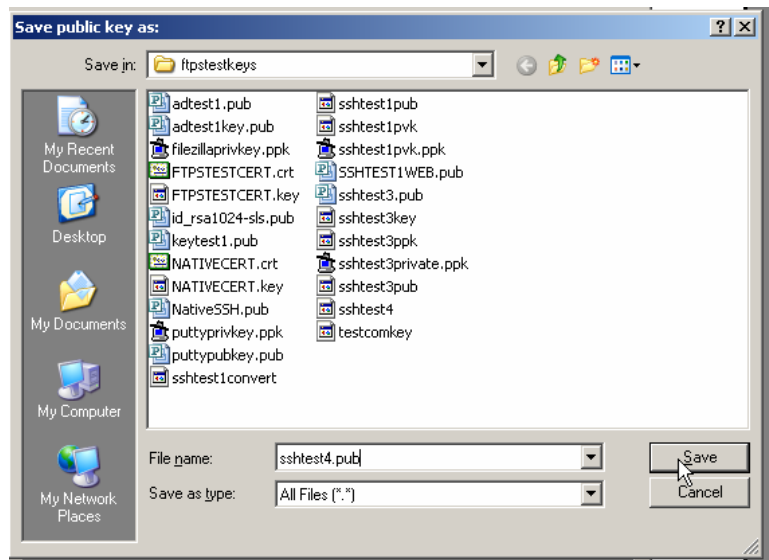
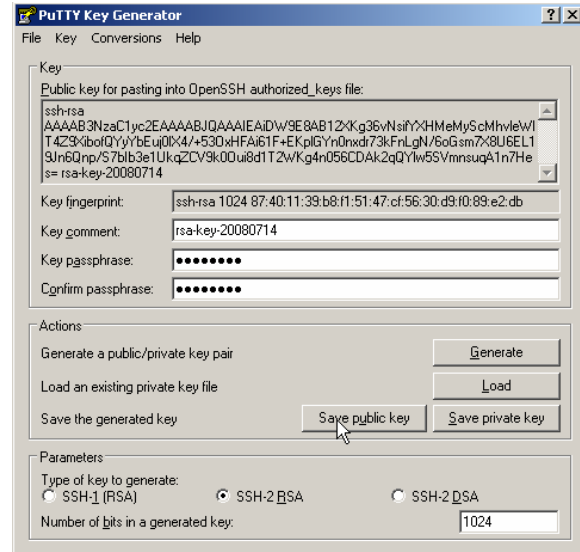
1. Download Puttygen, available for download at <http://www.putty.nl/download.html>
Click **Generate**.



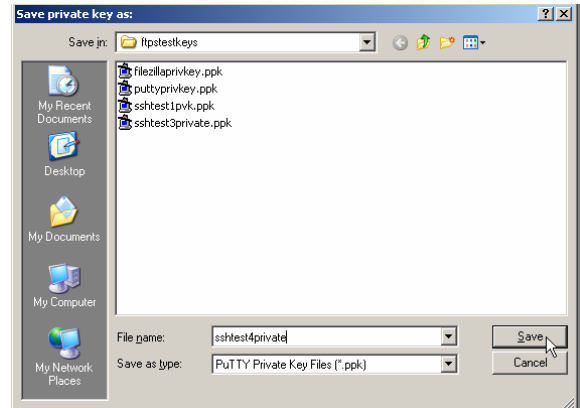
2. Type in the password for the key and change the **Conversion option** to **Export ssh.com key**.



3. Click **Save public key**. **Note:** You must add the *.pub extension to the filename.



- Export the **private key** from puttykeygen. (Note that you do not have to change file extensions on this file.)



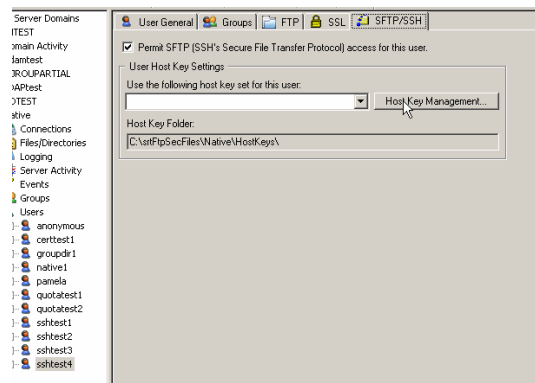
- You should now have 2 key files:

Name	Size	Type	Date Modified
sshtest4private.ppk	1 KB	PuTTY Private Key File	7/14/2008 11:33 AM
sshtest4.pub	1 KB	Microsoft Office Pu...	7/14/2008 11:29 AM

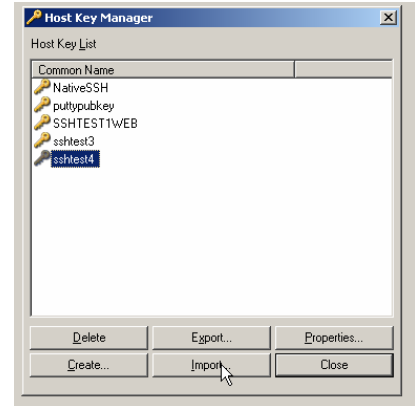
Importing the New Public Key into Cornerstone

You must import the public key into Cornerstone and replace the existing putty key.

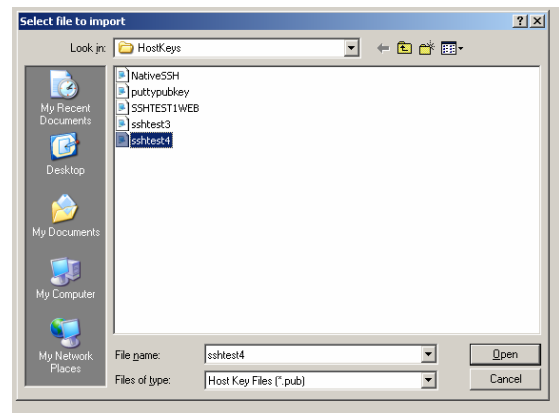
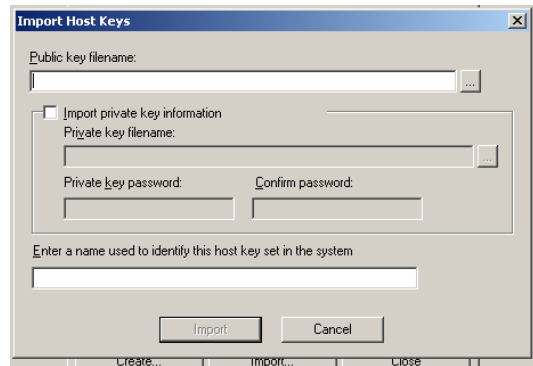
- Launch the Cornerstone Server Administrator. In the tree pane, select the **user**, in the tab pane select the **SFTP/SSH** tab, and then click **Host Key Management**. The Host Key Manager will launch.



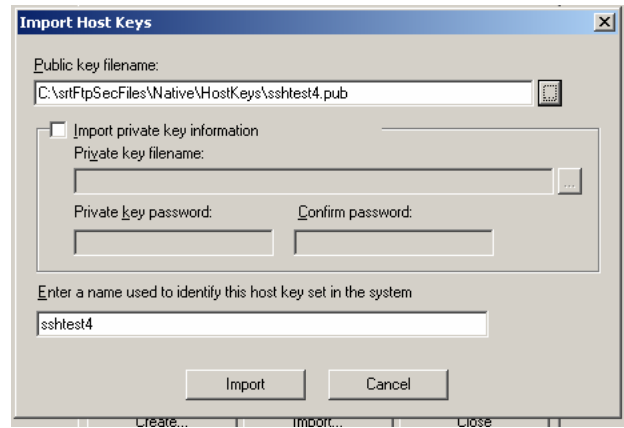
2. Click **Import**.



3. Use the Browse “...” button to browse to your **Public key** filename.



4. Click Import.

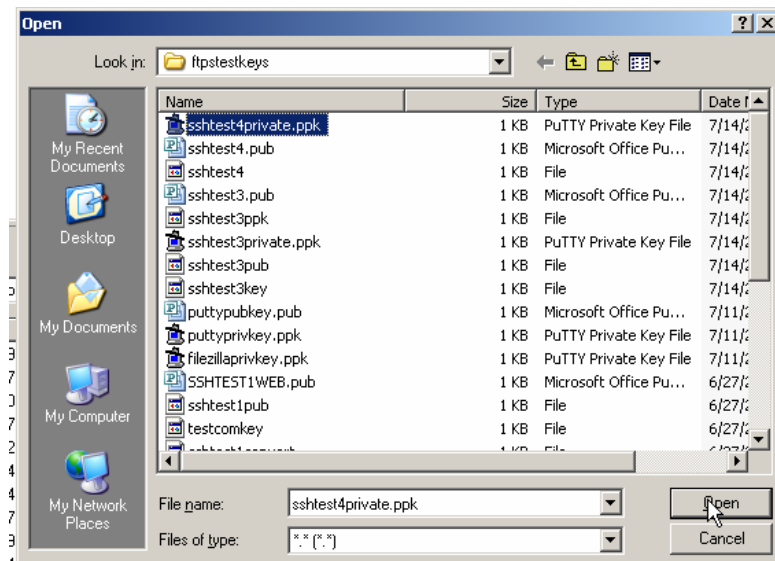
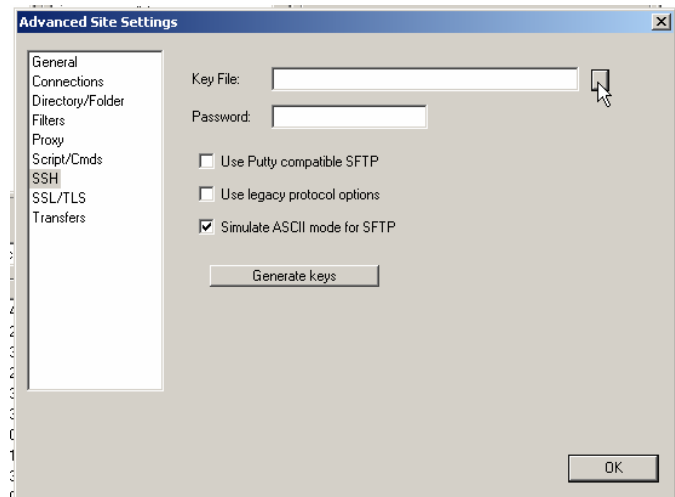


You must **replace the older putty generated public key** with the one you are importing into Cornerstone, so when you are asked if you would like to overwrite the existing certificate, click **Yes**.

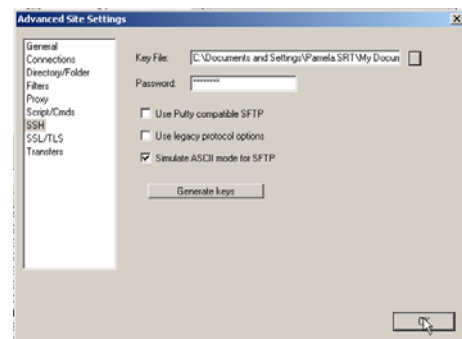
5. After you have imported the public key and closed the Certificate Manager, you must **attach the public key to the user** via the **SFTP/SSH** tab on the user's configuration.

Importing the New Public Key into the Client

1. Open CoreFTP (or other SFTP client software). Under the Advanced Site Settings, use the Browse “...” button to import the private key into user’s configuration.

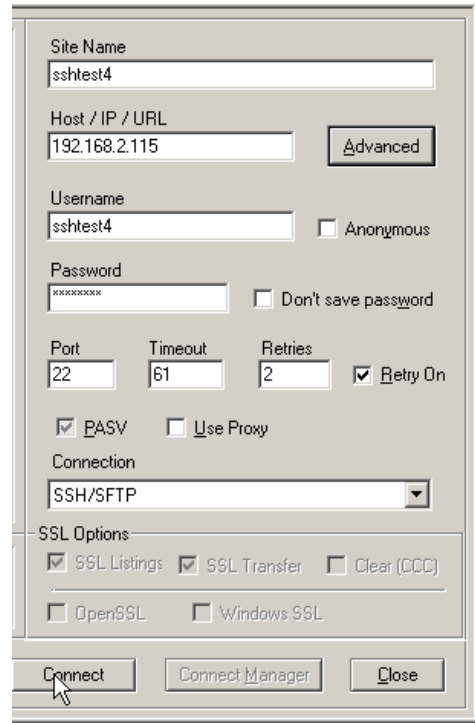


2. Type the **Key File Password** and click **OK**.



Testing the Configuration

1. To test, make sure that the Cornerstone server is configured to **Require trusted host keys when accessing this server** at the **server level>security>SFTP/SSH** tab.
2. Have your test user try to connect using SFTP.

A screenshot of a software dialog box for configuring an SFTP/SSH connection. The dialog has a light gray background and a standard Windows-style border. It contains several input fields and checkboxes. At the bottom, there are three buttons: 'Connect', 'Connect Manager', and 'Close'. A mouse cursor is pointing at the 'Connect' button.

Site Name
sshtest4

Host / IP / URL
192.168.2.115

Username
sshtest4 Anonymous

Password
***** Don't save password

Port
22

Timeout
61

Retries
2 Retry On

PASV Use Proxy

Connection
SSH/SFTP

SSL Options
 SSL Listings SSL Transfer Clear (CCC)
 OpenSSL Windows SSL

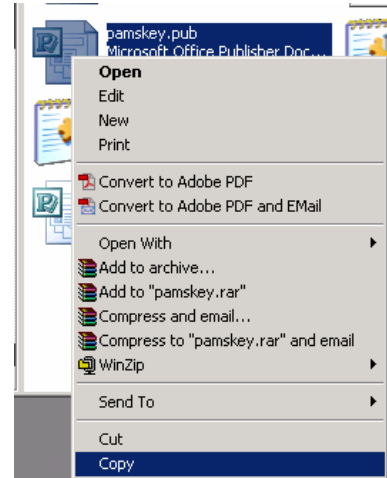
SecureFX Instructions

Create your public key using the tools menu within SecureFX. Once the key has been created in the Secure FX Key Generation Wizard, you will be prompted to select a key format. Select **Standard Public Key and VanDyke Private Key format**. You will be prompted to name your key. Name your key something that you can remember easily. When you are asked if you would like to use this key as your global public key, select **Yes**.

Importing the SecureFX key into Cornerstone Server

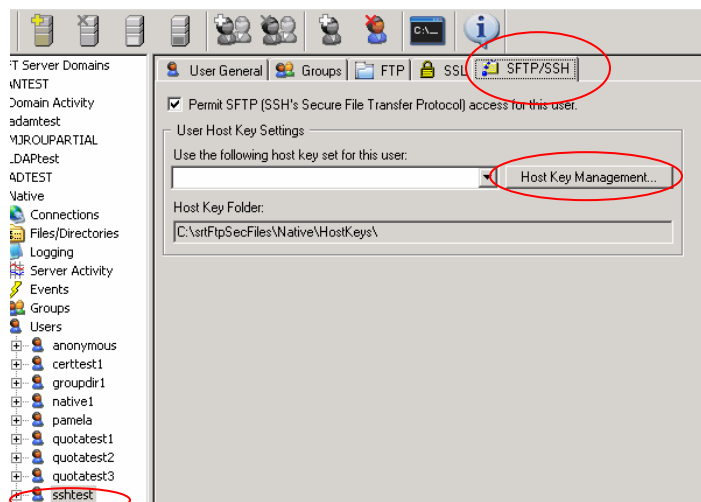
1. Find the public key you created in SecureFX and make a copy of it.

Note: Secure FX defaults its keys to:
C:\Documents and Settings\%username%\Application Data\VanDyke\Config



2. Place the copy of the public key under the Cornerstone server default directory for host keys: **C:\srtFtpSecFiles\%servername%\HostKeys**

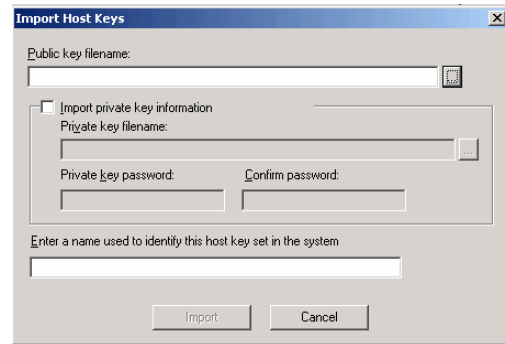
3. Launch the Cornerstone Administrator. Expand the **Server**, expand **Users**, and click the **User**. Click the **SFTP/SSH** tab for this user and then click **Host Key Management**.



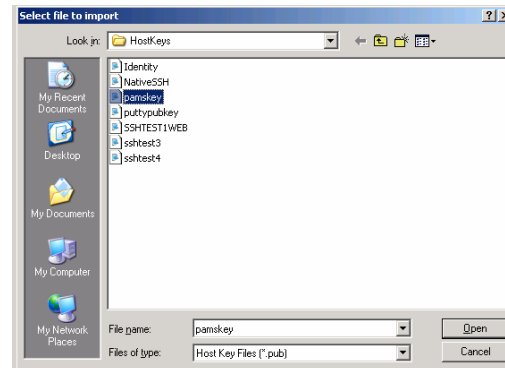
- Highlight the **public key** you created in Secure FX and click **Import**.



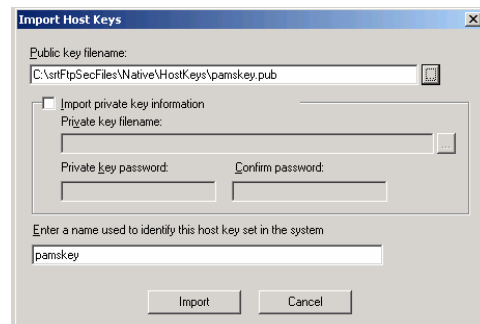
- Browse to the directory that holds the **public key**.



- Highlight your **public key** and click **Open**.

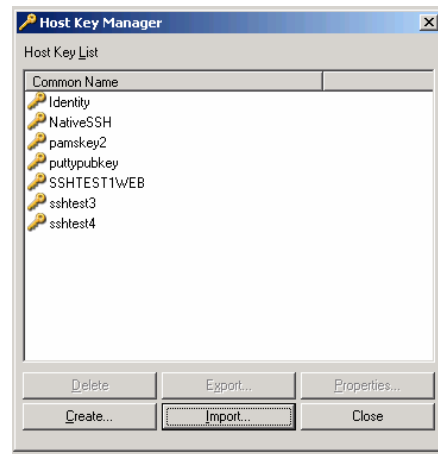


- Click **Import**.

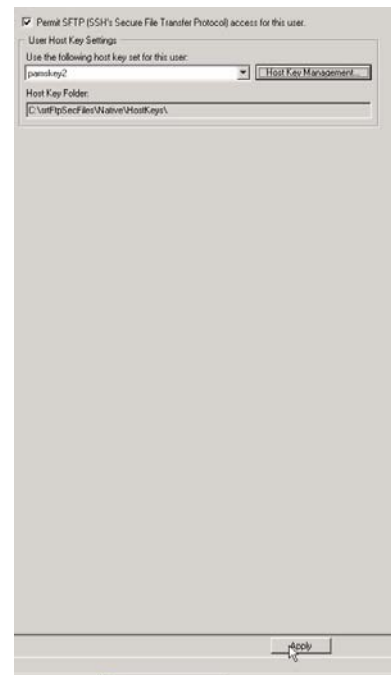


8. When you are asked if you want to replace the key, click **Yes**.

9. Click **Close** to close the Host Key Manager.



10. Make sure the appropriate key shows up under the **Use the following host key set for this user** dialog box and then click **Apply**.



About South River Technologies

South River Technologies (SRT) is an innovator in managed file transfer and basic content services software. SRT's software seamlessly integrates access to remote files into the desktop applications that users rely on, creating an instantly familiar interface for collaborating, sharing, and accessing files. SRT's enterprise class server products are built using industry standard encryption, highly granular security configuration controls, and technologies to reduce the risk of network intrusions. Over 60,000 customers, including more than 70 colleges and universities, government agencies such as NASA and FAA, and other blue chip companies in more than 110 countries rely on 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.

Cornerstone MFT® is a registered trademark of South River Technologies, Inc.

© Copyright South River Technologies, 1996-2010. All rights reserved.