



**TitanFTP**  
S E R V E R

**FTP/S & Public Key Certificate-based Authentication  
Quick Start Guide**

**February 2010**

## Notices

Copyright 2010 South River Technologies, Inc. All rights reserved.

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.

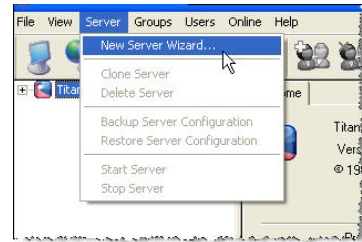
South River Technologies®, GroupDrive Collaboration Server®, Cornerstone MFT™, Titan FTP Server®, DMZedge Server™, and WebDrive® are trademarks of South River Technologies, Inc. in the U.S. and other countries. Microsoft, Windows, Windows NT, Windows XP, and Windows Vista are trademarks of Microsoft 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.  
127 Lubrano Drive, Suite 202  
Annapolis, Maryland 21401  
USA  
Telephone: 410-266-0667  
Fax: 410-266-1191  
[www.southrivertech.com](http://www.southrivertech.com)

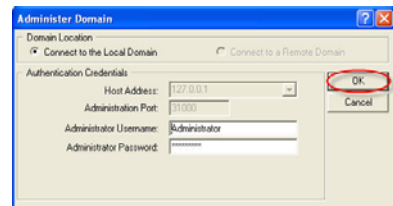
**Please Note:** The following instructions will help you to set up Titan FTP Server using FTPS (FTPS/SSL) and public key certificate-based authentication. Some screens in this instruction contain options that do not pertain to FTPS or public key certificate-based authentication. If you need additional information regarding these steps, please see the [Titan FTP User Guide](#). A Frequently Asked Questions (FAQ) is available at our [Knowledgebase Support Center](#) and a complete listing of our help documentation is available on our [Web site](#). For the purpose of this FTPS/public key certificate-based authentication Quick Start guide we will guide you through these options without configuring additional settings.

## Configuring FTPS & Public Key Certificate-based Authentication

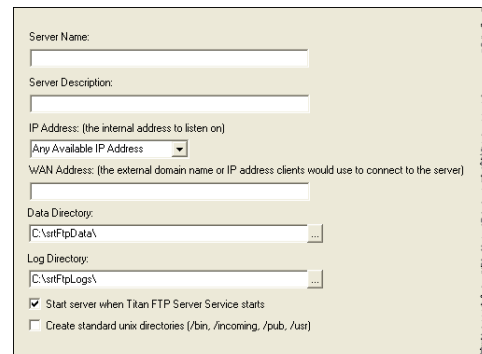
1. Run the *Titan FTP Server Administrator* and click **New Server Wizard**.



2. When the *Administer Domain* window appears, Type the Administrator Username and Administrator Password and click **OK**.



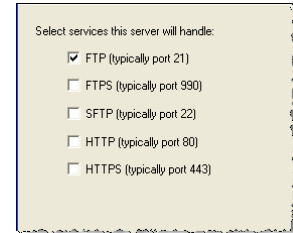
3. Type a unique **server name**. Click the drop-down arrow to choose your **IP Address**. (Any available IP address indicates that the server will listen on all IP addresses that are configured on the PC along with the local IP address of 127.0.0.0, also known as localhost.) Type the WAN address, for example, **myserver.com**. Click the **Data Directory "..."** browse button to browse to the Data Directory. Click the **Log Directory "..."** button to browse to the Log Directory. Select the check box if you would like to start this server when Titan FTP Server starts. When you are finished, click **Next**.\*



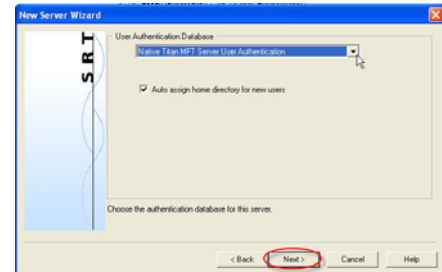
\*If you need to create standard UNIX directories, you can find additional information in the [Titan FTP Server User's Guide](#).

4. Select the **Services** this server will handle.

**Note:** You must enable FTP access if you plan on using FTP/S with explicit SSL (Auth SSL).

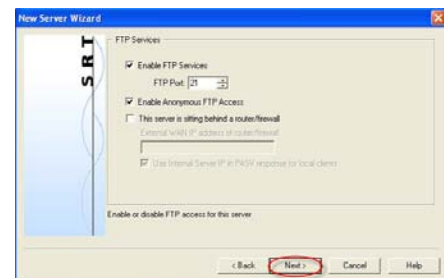


5. Select your **User Authentication Database** using the drop-down arrow. After you have configured your User Authentication Database, click **Next**.\*



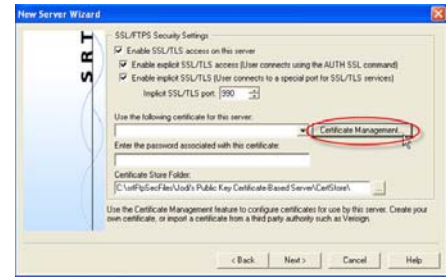
\*Once you select a User Authentication Database in Titan, you cannot change to a different method after the server wizard has completed. If you need more information about configuring user authentication, please see the [Titan FTP Server User's Guide](#) or the [SRT User Authentication Quick Start Guide](#)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

6. 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 IP address** of router/firewall. Click **Next**.



\*You must enable FTP access if you are using FTPS with explicit SSL (also known as AUTH SSL). For more detailed information pertaining to these configuration options see the [Titan FTP Server User's Guide](#).

- To enable SSL/TLS access on this server, select the **Enable SSL/TLS access on this server** check box and then select either **Enable explicit SSL/TLS** or **Enable implicit SSL/TLS**.\* Use the drop-down arrow to select a certificate, or click **Certificate Management** to launch the *Certificate Wizard* to configure a certificate for this server, or use the "..." browse button to browse to your *Certificate Store Folder*.

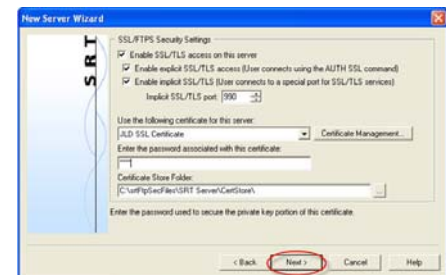


See [Appendix A](#) for the options available to you when you select **Certificate Management**.

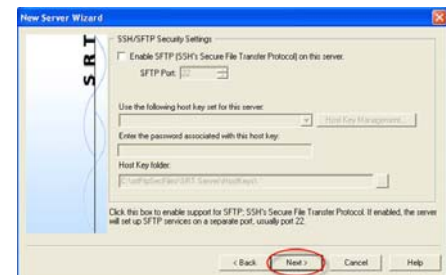
**\*Explicit SSL**—When using Explicit SSL, Titan FTP will allow SSL connections on the standard FTP port that was specified in [Step 6](#). This port will be used for both FTP connections and FTP/S connections. In order to enter into a secure SSL session, the FTP client will need to issue either the AUTH SSL or AUTH TLS command prior to establishing the secure connection.

**\*Implicit SSL**—When using implicit SSL, Titan FTP 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. Change your port number by using the up/down arrows.

- Click **Next**.



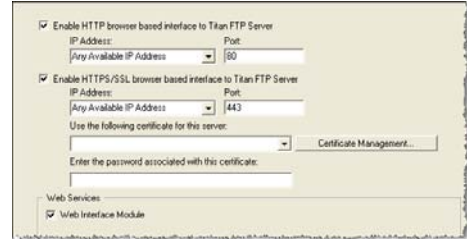
- If you would like to use *SSH/SFTP security settings* along with *FTPS*, enable SFTP using the check box.\* Click **Next**.



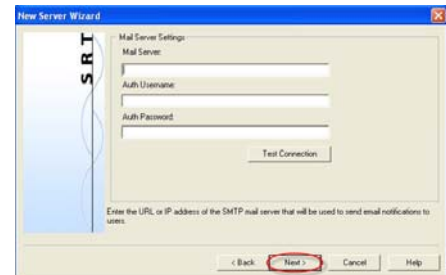
\* For more information see the [Titan FTP SFTP & Host Key Authentication Quick Start Guide](#).

- If you would like to enable **HTTP/HTTPS** access on this server, select the check boxes. To configure a certificate, click **Certificate Management**.

**Note:** The Titan Web Interface is an optional module. Contact [sales@southernrivertech.com](mailto:sales@southernrivertech.com) for more information.



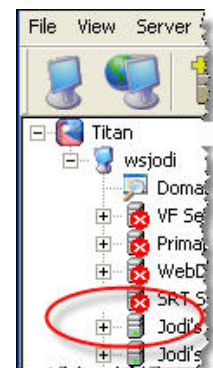
- Type the **URL** or **IP address** of the SMTP mail server that will be used to send email notifications to users. You may test the connection by clicking **Test Connection**. (For more detailed information pertaining to these configuration options, see the [Titan FTP Server User's Guide](#).) When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



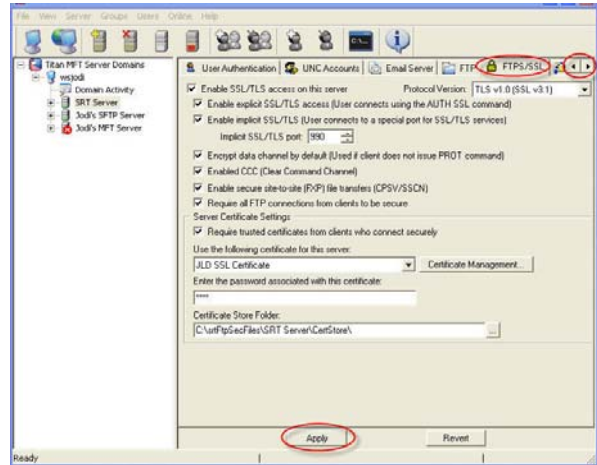
- Click **Finish** to create the server.



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

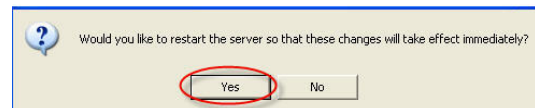


14. At this point, your FTPS Server is configured and will be running. If you would like to review the settings for the FTPS server, in the tab pane, select **Security**, and then select the **FTPS/SSL** tab. The FTPS/SSL tab is used to configure FTPS/SSL settings for the server. Once you have configured your settings, click **Apply**.\*



\*We recommend that you select Protocol Version *TLS v. 1.0 (SSL v3.1)* because it has security enhancements that are not found in SSL v3.0. We also recommend that you enable *Encrypt data channel by default* to 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 always wanted. As a reminder, 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.) If you enable *Require Trusted Certificates*, please be aware that this feature requires that all FTPS clients provide a trusted certificate to connect. This is the most secure method of connecting but it requires that trusted keys be distributed to each user offline, so it may not be practical.

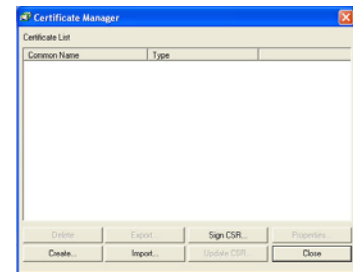
15. Click **Yes** to restart the server.



If you would like to test your server, you may [download WebDrive](#), our secure FTP client.

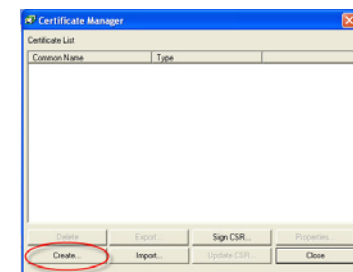
## Appendix A—Titan FTP Certificate Manager

Titan's *Certificate Manager* provides several options. You can choose to [Create a new certificate](#). You can [Import your certificate and private key](#). If you select [Sign CSR](#) the *Certificate Signing Wizard* will launch. Once you have certificates stored in Titan, you can also use the *Certificate Manager* to *Delete*, *Export* or *Update* your CSR, or to look at the *Properties* of your CSR.

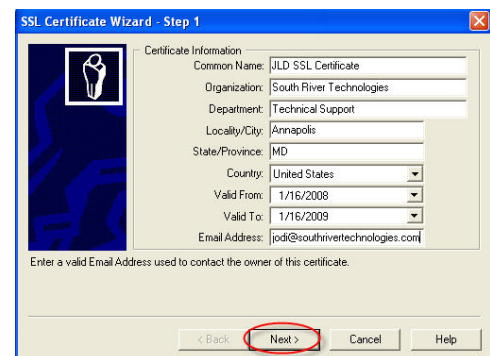


### To Create a New Certificate

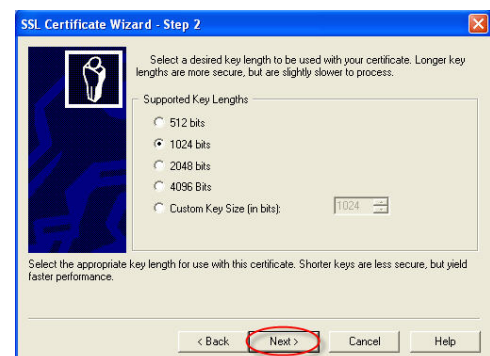
1. Click **Create** to create a certificate. This will launch the *SSL Certificate Wizard*.



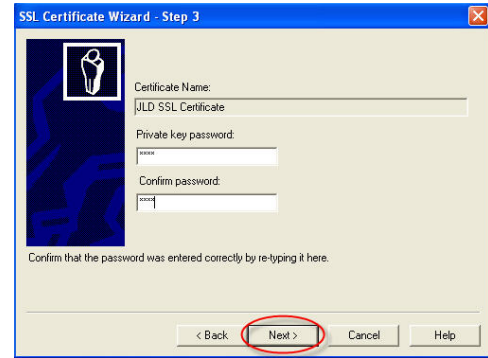
2. Type your **Certificate Information**. You must supply your information for each field. Use the drop-down arrows to choose the **Country** and **Valid From** and **Valid To** dates. Enter the valid **Email Address** that will be used to contact the owner of this certificate. Click **Next**.



3. Select a desired **key length** to be used with your certificate. 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**.

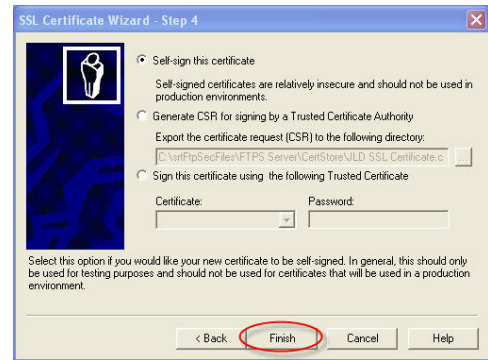


Your certificate name will populate automatically. Create a **Private Key password**. Your password must be at least four characters with no spaces and is case sensitive. After you confirm your password, click **Next**.



4. There are three options available for generating your certificate:

**•Self-sign this certificate**—Select this option if you would like your new certificate to be self-signed. Self-signed certificates are relatively insecure. In general, this option should only be used for testing purposes and should not be used for certificates that will 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 CSR (Certificate Signing Request) to be sent to an external CA (Certificate Authority) 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 [Appendix B](#).

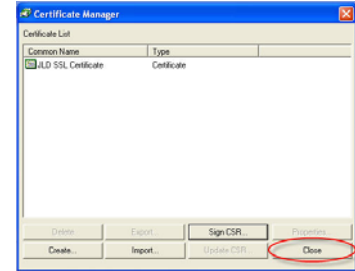
**•Sign this certificate using the following Trusted Certificate**—Select this option if you would like to sign this new certificate using a trusted certificate already in your certificate store.

Click **Finish** when you are done configuring these options.

- Click **Close**. You will be returned to the Titan FTP New Server Wizard, [step 8](#) of the main body of this quick start guide.

## To Import a Certificate

- Click **Import** to import your certificate and private key.

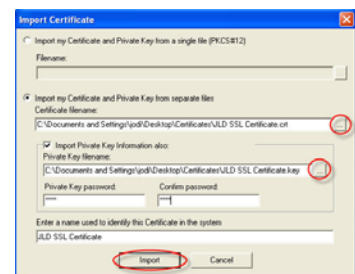
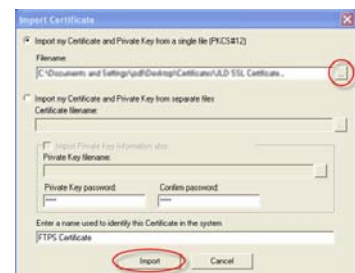
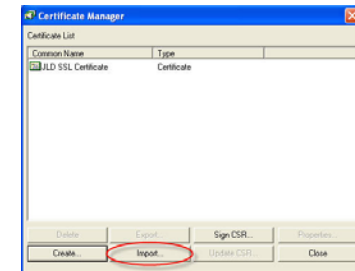


- Import Certificate* provides two options for importing your certificate:

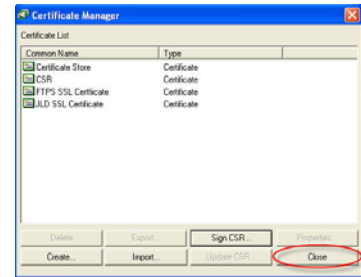
You can select **Import my Certificate and Private Key from a single file** in PKCS#12 format. Use the "..." browse button to browse to your .p12 file. Type your **Private Key password** and Confirm your password. Type a **name used to identify this certificate in the system**. When you are finished, click **Import**.

OR

You can select **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**.

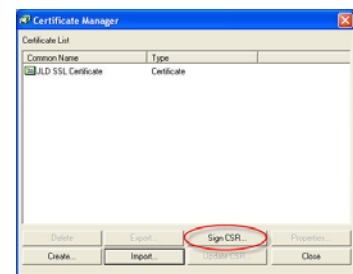


3. Your certificate has now been imported and you can see it listed in the *Certificate list*. Click **Close**. You will be returned to the *Titan FTP New Server Wizard*, [step 8](#) of the main body of this Quick Start Guide.



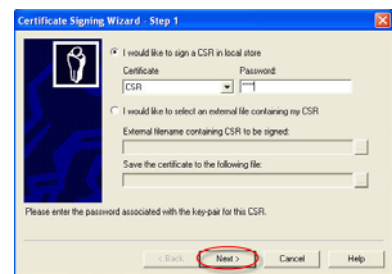
## To Sign the CSR

1. Select **Sign CSR**. The *Certificate Signing Wizard* will launch.



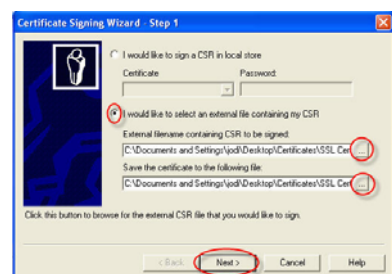
2. The *Certificate Signing Wizard* provides two options for signing your certificate:

You can choose to **sign a CSR in local store**. Use the drop-down arrow to select your certificate and then type your password. Click **Next** when you are finished.

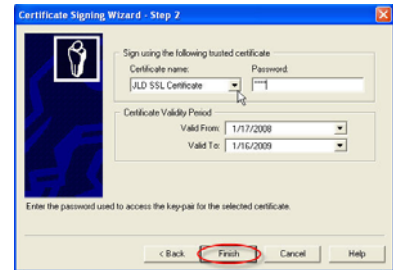


OR

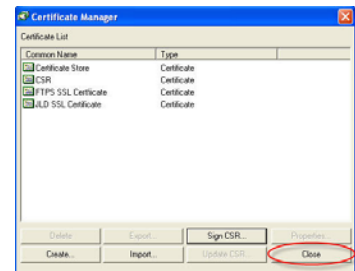
You can select an **external file that contains your CSR** and use the browse "..." buttons to browse to the certificate and to save the certificate. Click **Next** when you are finished.



3. Select the **Certificate name** using the drop-down arrow. Type the **password** used to access the key-pair for the selected certificate. You can change the **Valid From** and **Valid To** dates by using the drop-down arrow. Click **Finish**.



4. Your certificate is now ready for use and appears in the *Certificate List*. Click **Close**. You will be returned to the *Titan FTP New Server Wizard*, [step 8](#) of the main body of this Quick Start Guide.

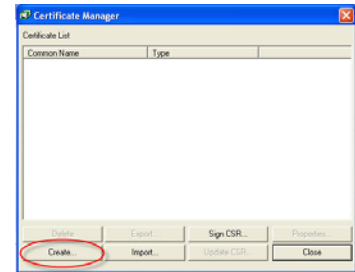


## Appendix B—Certificate Signing Requests

Generate A CSR (Certificate Signing Request) for Signing by a Trusted Certificate Authority, Send the CSR to Certificate Authority for Approval, and Update the Certificate after it is Approved

### To Generate the CSR for Signing

1. Launch the *Titan FTP Certificate Manager*. Click **Create** to create a certificate. This will launch the *SSL Certificate Wizard*.

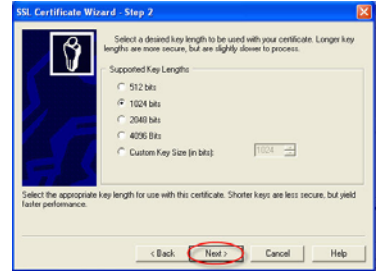


2. Type your **Certificate Information**. You must supply your information for each field.\* Use the drop-down arrows to choose the **country** and **Valid From** and **Valid To** dates. Enter the valid **Email Address** that will be used to contact the owner of the this certificate. Click **Next**.



\*The **Common Name** (CN) is the name of the server. Avoid using characters that any system treats as special characters. Please note that some Certificate Authorities do not allow you to abbreviate the State/Province name, so it is best to spell out the State or Province name.

3. Select a desired **key length** to be used with your certificate. 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**.



4. Your certificate name will populate automatically. 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 **Next**.



5. Select **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 because you will need to access it again to send it to the Certificate Authority.* **Click Finish.**



6. You will see a message that indicates that your CSR has been successfully exported to the directory that you chose to in Step 5.

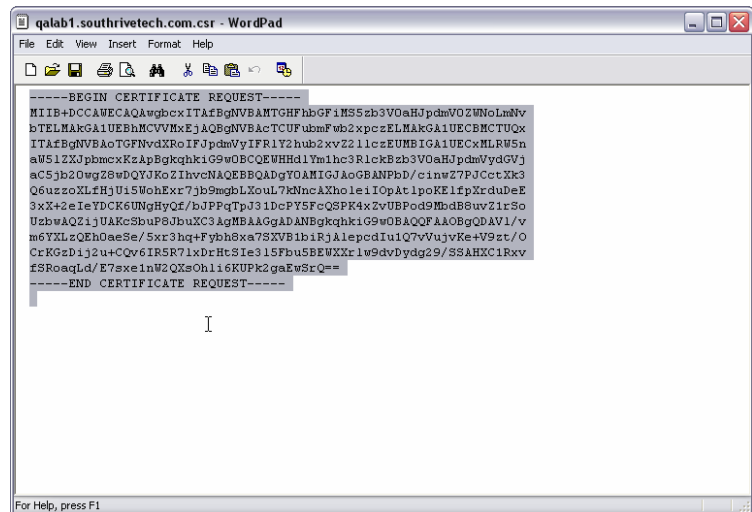
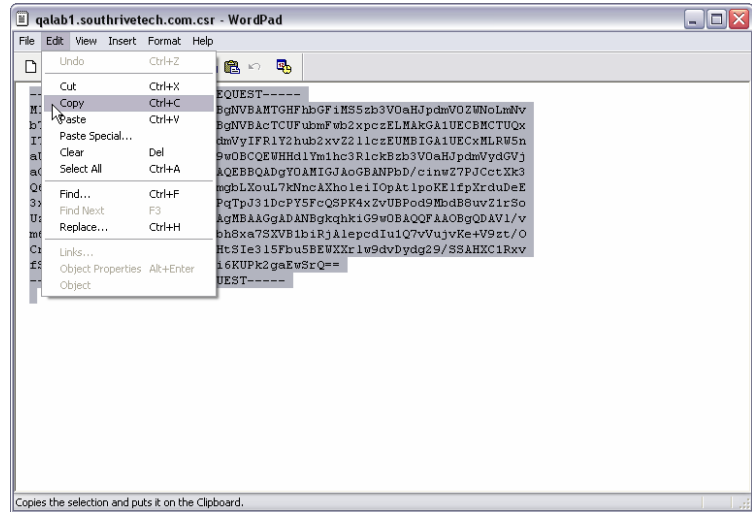


7. Click **Close** to close the *Certificate Manager*.



## To Send the CSR to the Certificate Authority/Certification Authority

1. Open *WordPad* and browse to the location of your .csr file. Copy the text of the entire file, including the words "Begin Certificate Request" and "End Certificate Request".



2. You must choose a Certificate Authority/Certification Authority. There are many Certificate Authorities/Certification Authorities to choose from, such as:

- <https://www.thawte.com>
- <http://www.verisign.com>
- <http://www.digicert.com>



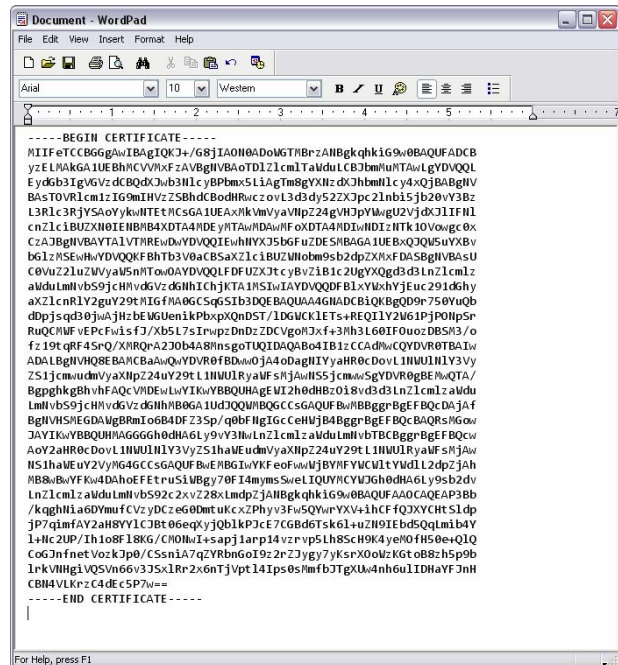
Once you have chosen your Certificate Authority, navigate to the area on the CA's web site where they have provided a place for you to paste your CSR. Paste your CSR, and provide any additional information that is required by the Certificate Authority.



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

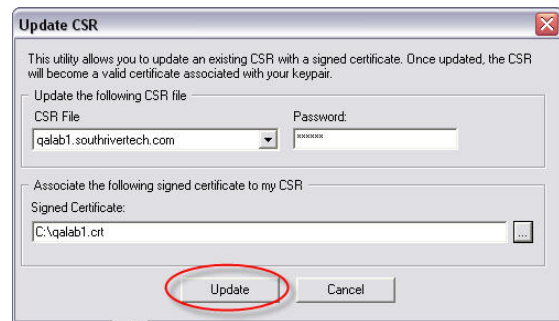
### To Update CSR in Titan FTP

1. After the Certificate Authority approves your CSR, they 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 characters that any system treats as special characters. *Be sure to take note of where you save the .crt file because you will need to access it again to update the certificate stored in the server.*

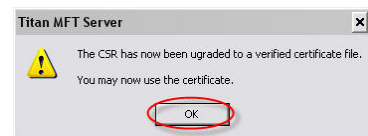


2. Launch the Titan FTP Certificate Manager. Select **Update CSR.\*** (**\*DO NOT CHOOSE Import.** If you choose *Import* it will **invalidate** your CSR. To properly configure this certificate to Titan FTP Server **you must choose Update CSR.**)

3. The *Update CSR Utility* will launch. Use the drop-down arrow to select the CSR File that you would like to update with a signed certificate. Once updated, the CSR will become a valid certificate associated with your KeyPair. Type your password. Use the browse "..." button to browse to the location of your certificate (.crt) file. When you are finished, click **Update**.



4. Your CSR is now upgraded to a verified certificate file. You may now use the certificate. Click **OK**.



If you would like to test your server, you may [download WebDrive](#), our secure FTP client.

## About South River Technologies

South River Technologies (SRT) is an innovator in managed file transfer and document collaboration 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](http://www.southrivertech.com).