



GroupDrive

**GroupDrive Collaboration Server
SSL & Public Key Certificate-based Authentication
Quick Start Guide**

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

Please Note: Some screens in this quick start guide contain options that do not pertain to SSL or public key certificate-based authentication. If you need additional information regarding these steps, please see the [GroupDrive Administrator User's Guide](#). For the purpose of this SSL/public key certificate-based authentication quick start guide, we will guide you through these options without configuring additional settings.

Public Key Authentication—Best Practices

Each entity in a secure environment, both the client and the server, should generate its own key pair. This 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 key pair. It is always a good practice to password protect your private key, and GroupDrive requires this.

Each GroupDrive client's public certificate must be provided to the GroupDrive server administrator to be installed on the GroupDrive Server. While it is possible to use the *Certificate Management* features in GroupDrive to export your private key, it is highly discouraged unless it is for backup purposes because it is difficult to ensure the integrity of the private key during the physical transfer of the key file. If it is necessary to export the private key, it is recommended that the transfer be performed over a secure medium. Export the keys to an encrypted USB drive, or encrypt the files onto a DVD/CDROM. However, never e-mail the private key. E-mail is natively insecure and there is no way to ensure the integrity of the files during electronic transfer.

Configuring the Server

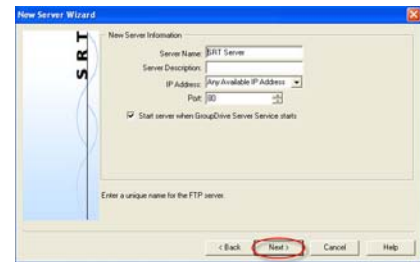
1. Run the GroupDrive *Administration Utility* and select **New Server Wizard**. The *New Server Wizard* will launch.



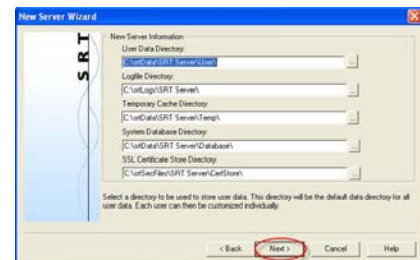
2. Select the Server Type (clustered or non-clustered).



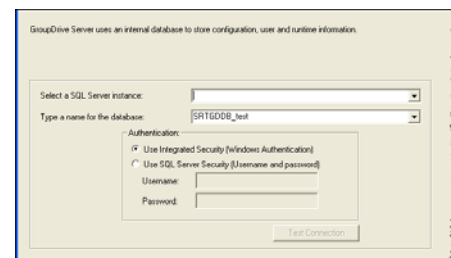
3. Type a unique **Server Name**. Type a **Server Description** (optional). Click the drop-down arrow to select your **IP Address**. (*Any available IP address* indicates that the server will listen on all IP addresses that are configured on the PC, along with the local IP address of 127.0.0.0, also known as *localhost*.) Select the **Port number** by using the up/down arrows. Click **Next**.



4. Select a **directory** to be used to store user data. This directory will be the default directory for all user data. Each user can then be customized individually. Use the browse "..." buttons change the default location of your User Data Directory, Logfile Directory, Temporary Cache Directory, System Database Directory, and SSL Certificate Store Directory. Click **Next**.

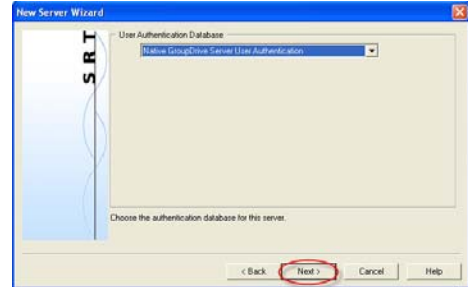


5. GroupDrive uses an internal database to store configuration, user and runtime information. Use the drop-down arrow to select the **SQL Server instance**. Type the name of the **SQL database**. Select your **authentication method**. Click **Test Connection** to test the database connection to the GroupDrive server.



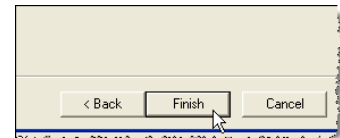
NOTE: SRT supports GroupDrive configurations using SQL Server 2005 or later or SQL Server 2005 Express or later, test or production environment. No other databases are supported.

6. Select your User Authentication Database using the drop-down arrow. For our example, we will use **Native GroupDrive Server User Authentication**.* Click **Next**.

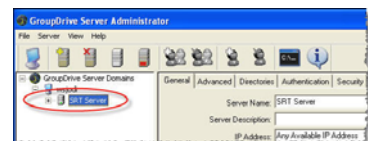


*Once you select a *User Authentication Database* option in GroupDrive, you cannot change to a different method after the server wizard has completed. Use the drop-down arrow to select a different type of User Authentication. If you need more information about configuring user authentication, please see the [GroupDrive Administrator User's Guide](#) or the [SRT User Authentication Quick Start Guide](#) for your specific user authentication database.

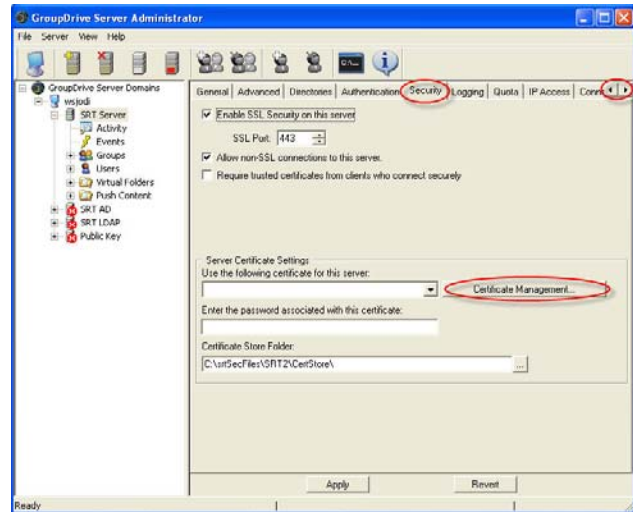
7. The wizard will walk you through the steps for configuring your **SMTP Mail Server** and **User Account for Web-Based Server Administration**. Click **Finish** to create the server.



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

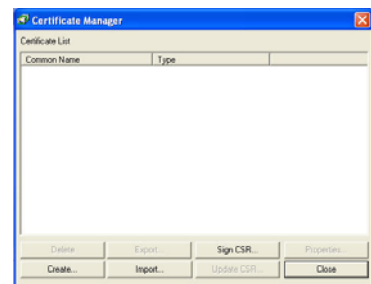


9. At this point, your Server is configured and will be running. Use the right/left arrows until you can select the **HTTPS/SSL** tab under the *server* settings. The HTTPS/SSL tab is used to configure **SSL** and **Server Certificate** settings for the server. To enable SSL on this server, select the **Enable SSL Security on this server** check box and select the **port number** using the up/down arrows (default port 443). If you would like to **Allow non-SSL connections** to this server, select the check box. If you enable **Require Trusted Certificates**, please be aware that this feature requires that all clients who connect securely 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. Click **Certificate Management** to manage certificates for this server.



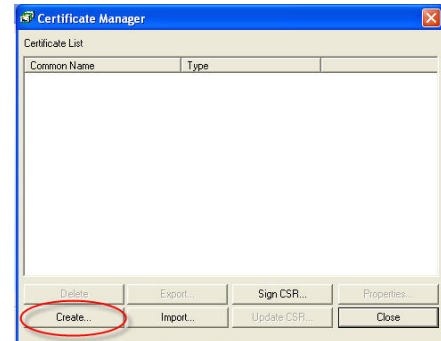
*If you enable **Require trusted certificates from clients who connect securely**, you must install the GroupDrive Client Certificate on the GroupDrive server and configure each user to the appropriate certificate. See [Appendix A](#) for additional information about requiring trusted certificates and adding users to GroupDrive Collaboration Server.

10. GroupDrive'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 GroupDrive Collaboration Server, you can also use the *Certificate Manager* to Delete, Export* or Update your CSR, or to look at the Properties of your CSR. *Certificate Manager* options are described next. Choose the option that best suits your needs and then continue to [step 12](#) of this quick start guide.

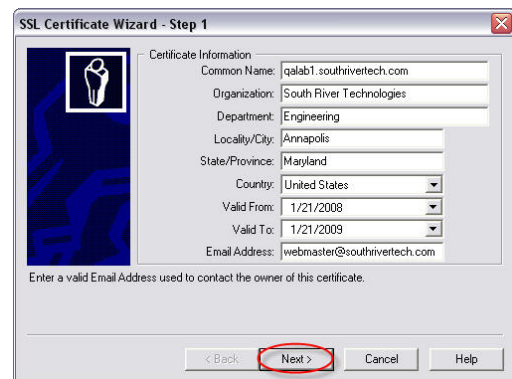


To Create a New Certificate

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**.

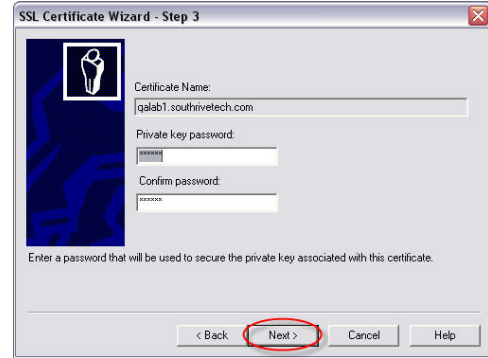


*The Common Name (CN), also known as the URL (Uniform Resource Locator), is the fully qualified domain name used for DNS lookups of your server. Avoid using characters that any system treats as special characters. Please note that some Certificate Authorities do not allow you to abbreviate the State/Province 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**.

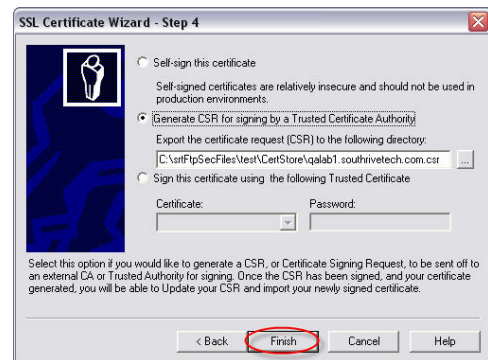


- Your *Certificate Name* will populate automatically. Create a **Private Key password**. Your password must be at least four characters with no spaces and is case sensitive. After you confirm your password, click **Next**.



- 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.



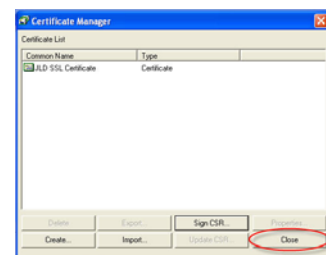
•Generate CSR for signing by a Trusted Certificate Authority

—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.

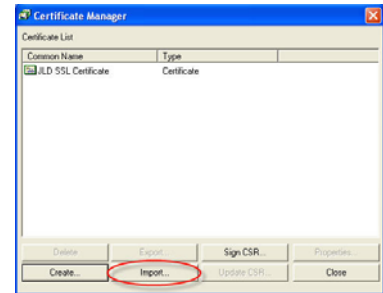
Click **Finish** when you are done configuring these options.

- Click **Close** to exit the *Certificate Manager* and then continue to [step 12](#) of the main body of this Quick Start Guide.



To Import a Certificate

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



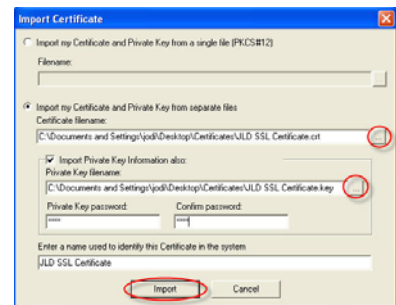
2. *Import Certificate* provides two options for importing your certificate:

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**.

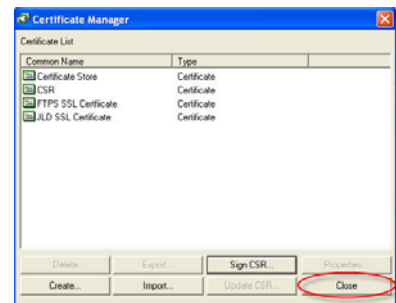


OR

You can select **Import my Certificate and Private Key from separate files**. Use the "... " button to browse to your .cert 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**.

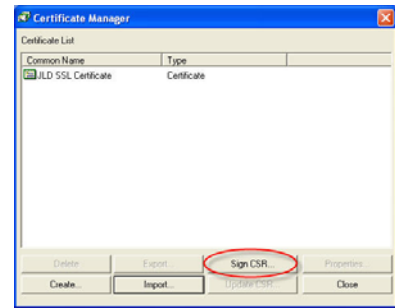


3. Your certificate has now been imported and you can see it listed in the *Certificate list*. Click **Close** to exit the *Certificate Manager*. Continue to [step 12](#) of the main body of this Quick Start Guide.



To Sign the CSR

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

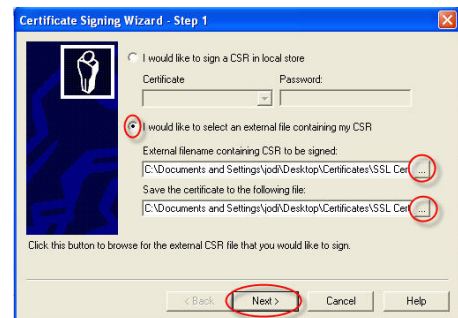


2. The *Certificate Signing Wizard* provides two options for signing your certificate:

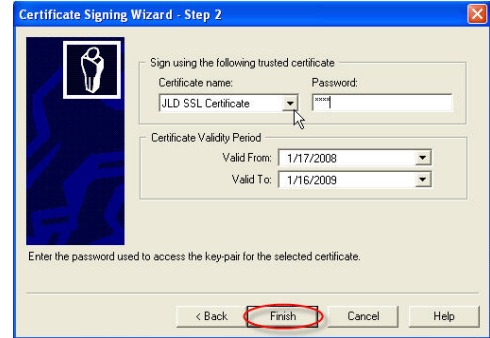
You can choose to **sign a CSR in local store**. Use the drop-down arrow to **select your certificate** and then type your **password**. Click **Next** when you are finished.

OR

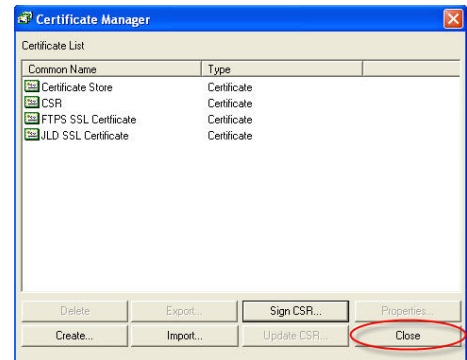
You can select an **external file that contains your CSR** and use the browse “...” buttons to browse to the certificate and to save the certificate. Click **Next** when you are finished.



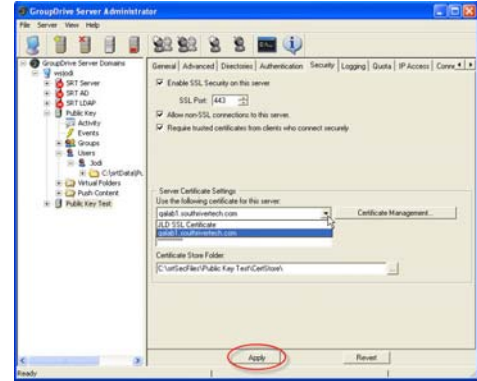
3. Select the **Certificate name** using the drop-down arrow. Type the **password** used to access the key-pair for the selected certificate. You can change the **Valid From** and **Valid To** dates by using the drop-down arrow. Click **Finish**.



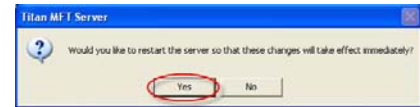
4. Your certificate is now ready for use and appears in the *Certificate List*. Click **Close** to close the *Certificate Manager*. Continue to [step 12](#) of the main body of this Quick Start Guide.



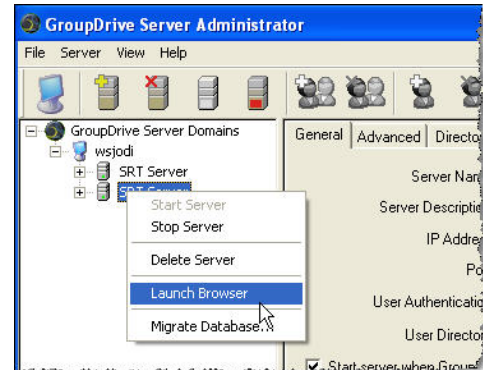
- When you have finished managing your certificates, select your certificate using the drop-down arrow. Use the browse “...” button if you would like to change the default location of your *Certificate Store Folder*. Click **Apply** to apply your settings.



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

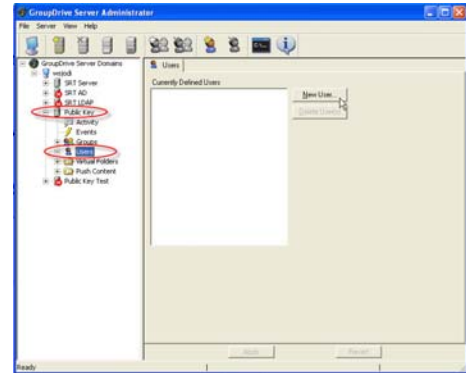


- It is now time to test the server. To test the server, right-click on the **Server** in the *GroupDrive Administrator* and select **Launch Browser**. By default, the browser will launch in *NON SSL* mode, so when the browser launches, your URL will appear as: < HTTP://yourURL/>. To test the SSL access, **Change the URL** to: < HTTPS://yourURL/>. If you changed the port number from default port 443 in [step 8](#), you will also need to add the port number using this format: < HTTPS://yourURL:PORTNUMBER/>. Then logon using your credentials.



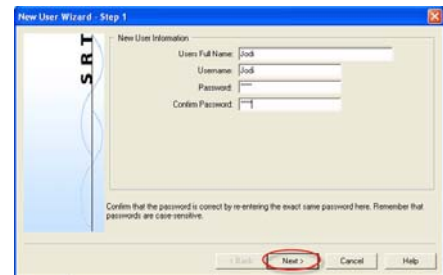
Appendix A: Requiring Certificates/Adding Users

1. To add users to the system, select **users** from the *GroupDrive Server Domain* tree and click **New User**.*

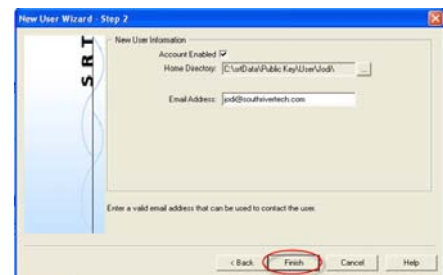


* In GroupDrive Collaboration Server, users are *Group-based*. By default each user is a member of the *Everyone Group*. If you need more information about *User Authentication* databases, see the [GroupDrive Administrator User's Guide](#) or the [SRT GroupDrive User Authentication Quick Start Guide](#) for your specific User Authentication database.

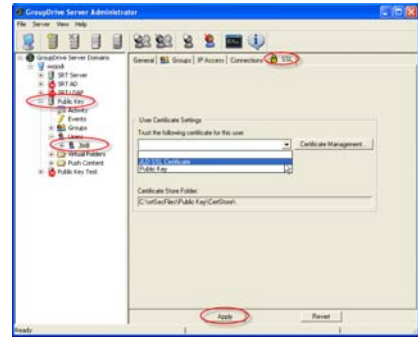
2. Type the **User's Full Name**, the **Username** and **Password**. After you **confirm the Password**, click **Next**.



3. By default, the user's account is enabled. If you would like to disable the user's account, deselect the check box. Use the browse "..." button to change the location of the user's Home Directory. Type the user's **Email Address**. Click **Finish**. The user is now added to the server.



4. If you enabled **Require Trusted Certificates from Clients who Connect Securely** in [step 8](#) you must configure a certificate for each user in GroupDrive Server. After you have added the user to the server, select the *SSL* tab.* To configure **User Certificate Settings/Trust the following certificate for this user**, use the drop-down arrow to select the appropriate certificate. Click **Apply**.

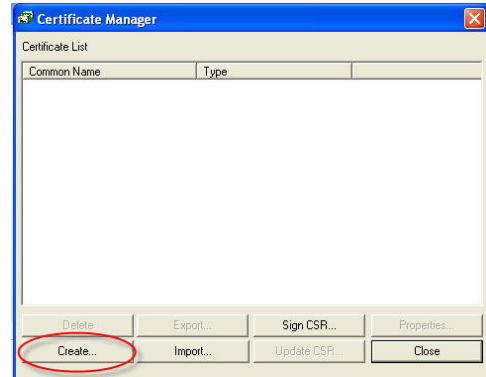


* The GroupDrive client public certificate must be provided to the GroupDrive Server administrator to be installed on the GroupDrive server.

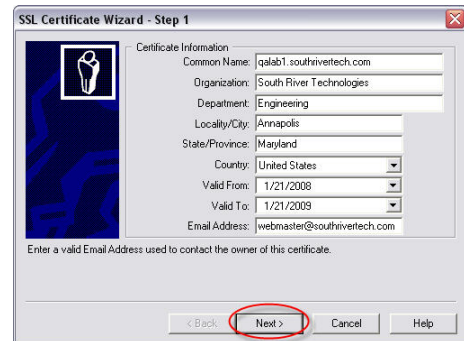
Appendix B: Certificate Authorities

To Generate the CSR for Signing

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

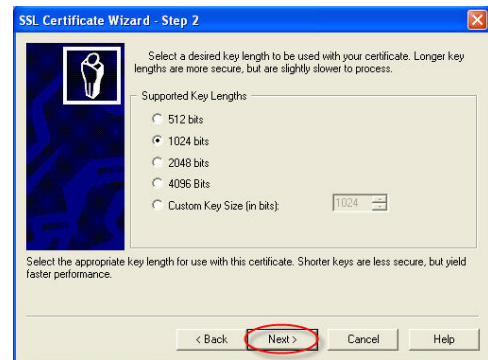


2. Type your **Certificate Information**. You must supply your information for each field.* Use the drop-down arrows to choose the **Country** and **Valid From** and **Valid To** dates. Enter the valid **Email Address** that will be used to contact the owner of the this certificate. Click **Next**.

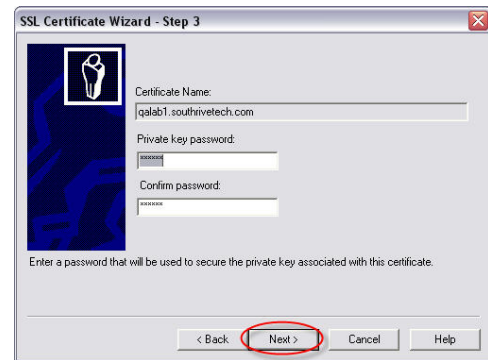


*The Common Name (CN), also known as the URL (Uniform Resource Locator), is the fully qualified domain name used for DNS lookups of your server. Avoid using characters that any system treats as special characters. Please note that some Certificate Authorities do not allow you to abbreviate the State/Province name, so it is best to spell out the State or Province name.

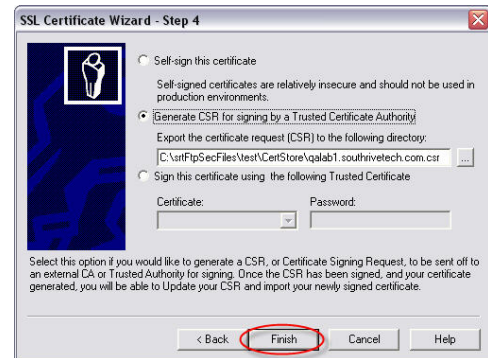
3. Select a desired **key length** to be used with your certificate. Longer key lengths provide better security, but result in slower performance. Shorter keys run faster but are less secure. Key lengths of 1024 bits or larger are recommended for secure environments. Click **Next**.



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**.



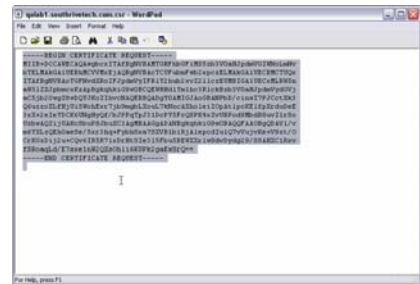
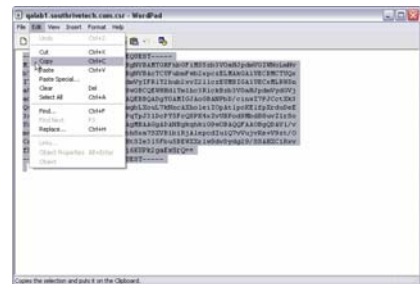
6. You will see a message that indicates that your CSR has been successfully exported to the directory that you chose to in Step 5.



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".

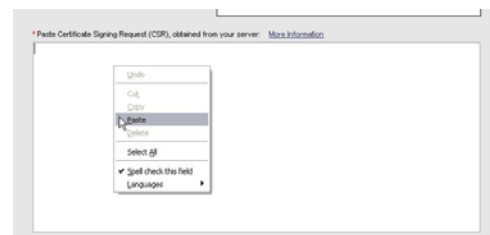


2. You must choose a Certificate Authority/Certification Authority. There are many Certificate Authorities/Certification Authorities to choose from, such as:

<https://www.thawte.com>

<http://www.verisign.com>

<http://www.digicert.com>



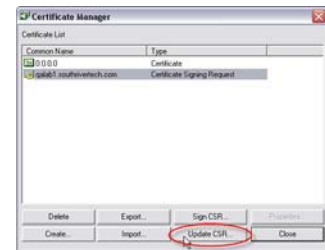
Once you have chosen your Certificate Authority, navigate to the area on the CA's web site where they have provided a place for you to paste your CSR. Paste your CSR, and provide any additional information that is required by the Certificate Authority.

After you submit your Certificate Signing Request, the Certificate Authority will do a background check to verify and authenticate the Certificate Signing Request. The average wait time for approval is approximately one week.

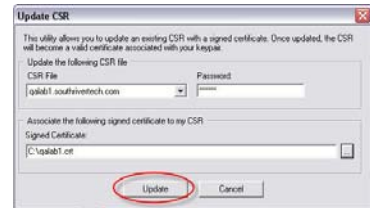
- After the Certificate Authority approves your CSR, they will email you a secure link to access your certificate. Copy your certificate to WordPad and save in .crt format. When you name your .crt file, do not use extra periods or characters that any system treats as special characters. Be sure to take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



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



- 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**.



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

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.