



WebDrive

**Configuring WebDrive for use with
Windows SharePoint Services WSS 3.0
Quick Start Guide**

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, Sharepoint, 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.southernrivertech.com

Please Note: The following instructions will help you to set up WebDrive[®] for use with SharePoint[®] Services. Some screens in this instruction contain options that do not pertain to configuring WebDrive for use with SharePoint Server. If you need additional information regarding these steps, please see the [WebDrive User's Guide](#). For the purpose of this quick start guide, we will guide you through these options without configuring additional settings.

Table of Contents

Notices	ii
Table of Contents	3
System Requirements	4
Installation Notes	5
WebDAV, IIS, and SharePoint Overview	6
Configuring SharePoint Services WSS 3.0	7
Configuring WebDrive	8
Appendix A: WebDrive Certificate Manager	13
Appendix B—Trusted Certificate Authorities	18

System Requirements

Operating System	Windows XP® (32-bit & 64-bit) Windows Server 2003® (32-bit & 64-bit) Windows Vista® (32-bit & 64-bit) Windows Server 2008® (32-bit & 64-bit) Windows 7® (32-bit & 64-bit)
Processor	Pentium® Class or better Minimum 32MB system memory
Disk Space	Minimum 40MB free disk space for product and caching space
Internet Connection	Direct Internet connection or modem with a minimum baud rate of 28.8 (56K is recommended)
Network Components	Microsoft® 32-bit TCP/IP networking component

**Make sure all Windows Service Packs and Updates have been installed.
No other TCP/IP stacks are currently supported.**

Installation Notes

To install WebDrive, you must be logged on with the user account that has administrative rights. If you are using Vista, you must run the install with elevated privileges; right-click on the setup program and select **Run as Administrator**. Once installed, you can use WebDrive from any user account.

For 64-bit Windows support you will need to install the Native 64-bit version of WebDrive which you can download here

<http://www.webdrive.com/products/webdrive/index.html>

To uninstall WebDrive, you must also be logged in with the user account that has administrative rights. From the **Control Panel**, select **Add or Remove Programs** and then select **WebDrive**, or select the **uninstall** icon in the WebDrive program folder.

**Make sure all Windows service packs and updates have been installed.
No other TCP/IP stacks are currently supported.**

**DO NOT LOSE YOUR REGISTRATION INFORMATION. You will need the
Product Registration Code each time you install the registered version
of WebDrive.**

WebDAV, IIS, and SharePoint Overview

Many people are under the misconception that SharePoint uses the WebDAV functionality provided by IIS. Actually, SharePoint provides its own WebDAV implementation using the Stsfilt.dll ISAPI filter that is installed with both Windows SharePoint Services and SharePoint Portal Server. Enabling or disabling the WebDAV extension in IIS 6.0 has no effect on SharePoint functionality. Installing WebDAV 7.5 in IIS 7.0 (even if it is disabled) breaks SharePoint's built in WebDAV. Consequently, the first step in configuring WebDAV access for Sharepoint running with IIS 7 is to **uninstall WebDAV 7.5** in ADD/REMOVE PROGRAMS.

Configuring SharePoint Services WSS 3.0

Installing Windows SharePoint Services—WSS 3.0

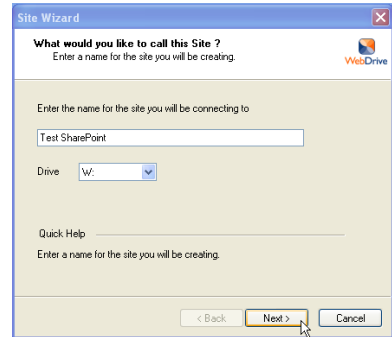
After you have installed Windows SharePoint Services 3.0, you may need to perform administrative tasks to complete your deployment. See the Windows SharePoint Services quick start guide for more information: <http://technet.microsoft.com/en-us/library/cc288608.aspx>

NOTE: WebDAV capability is built into SharePoint Services WSS 3.0. If you have previously installed IIS WebDAV, you must UNINSTALL WebDAV 7.5 to use the WebDAV that is included in SharePoint Services WSS 3.0. If you need more information about configuring SharePoint Services, please see your SharePoint Server Administrator.

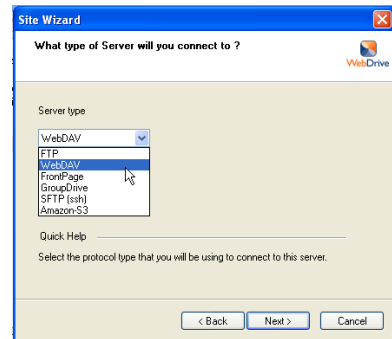
For information about configuring WebDAV without using SharePoint Services, see <http://learn.iis.net/page.aspx/350/installing-and-configuring-webdav-on-iis-70/>

Configuring WebDrive

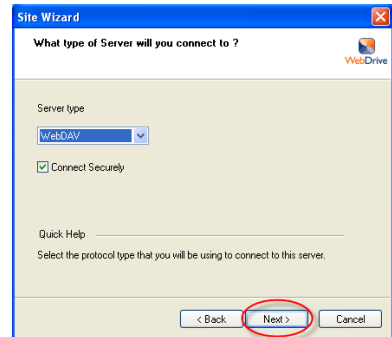
1. Launch the WebDrive Site Manager and click **New Site**. Type the **name of the site** that you will be connecting to. Use the drop-down arrow to select an **available Drive letter**. Click **Next**.



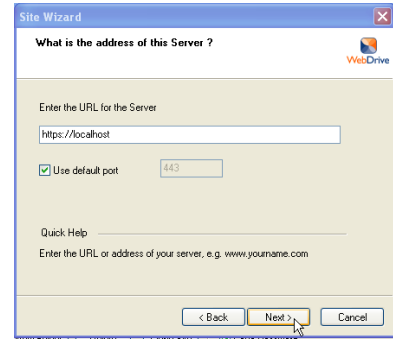
2. Use the drop-down arrow to select **WebDAV** as the Server type.



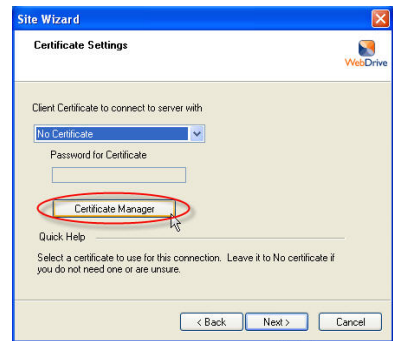
3. If you enabled HTTP^S, select the **Connect Securely** check box. Click **Next**.



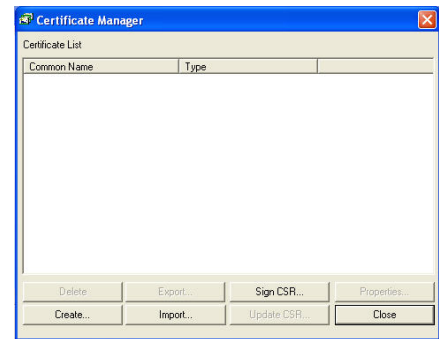
4. Type the **URL** for the Server. Your SharePoint Administrator will provide this information. You must type a fully qualified path. For example: **http://servername/site**. The default port for secure connections is 443. If you would like to change this port, clear the check box and type in the port number.



5. If you are using SSL certificates, use the drop-down arrow to select your certificate or click **Certificate Manager** to manage your certificates. If you are not using SSL certificates, click **Next**.

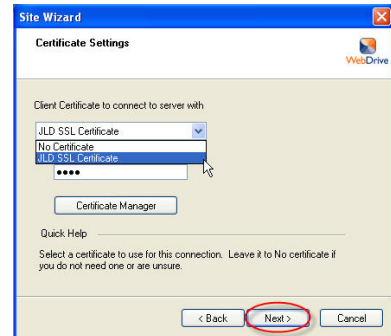


6. Configuring Certificates—WebDrive's *Certificate Manager* provides several options. You can choose to [Create a new certificate](#). You can [Import your certificate](#) and private key. If you select [Sign CSR](#) the *Certificate Signing Wizard* will launch. Once you have certificates stored in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



See the [Appendix A](#) for instructions regarding the options available in the Certificate Manager.

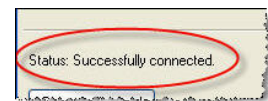
- After you have configured your certificate from the appendix and closed the *Certificate Manager*, you are returned to *Certificate settings*. Select your **certificate** using the drop-down arrow and enter your **password**. Click **Next** when you are finished.



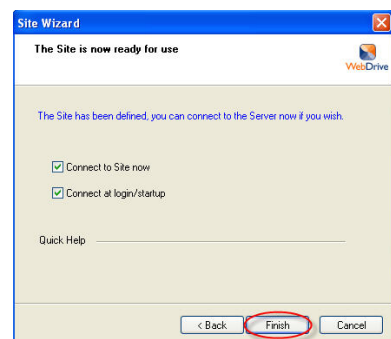
- Type the **Username** and **password** to access the SharePoint server. **Note:** Do not click **Test Connection**; we have not finished configuring your settings.



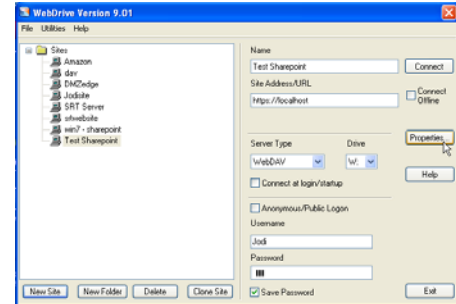
- If you can successfully connect to the server you will see *Status: Successfully Connected*. If you do not successfully connect you will receive an error message explaining why you cannot connect. Click **Close**.



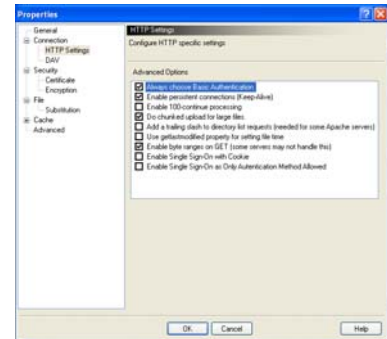
- Select **Connect to Site now** if you would like to connect to the site now. If you would like to **Connect at login/startup**, you may select this check box. Click **Finish**.



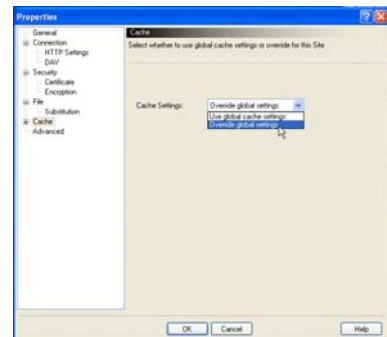
11. Now that you have finished your initial configuration using the *Site Wizard*, there are a few additional settings that you must configure using the *Site Manager*. In the *Site Manager*, be sure that you have your **SharePoint site** selected, and then click **Properties**.



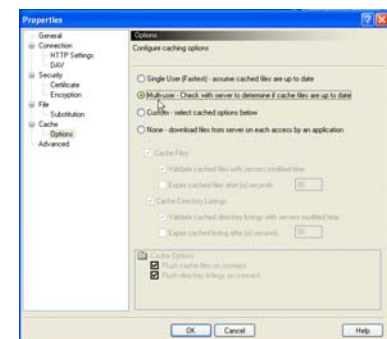
12. Click **HTTP Settings** and select **Always choose Basic Authentication**.



13. Click **Cache** and use the drop-down arrow to select **Override global settings**.

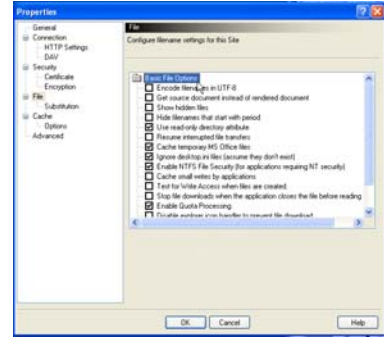


14. Click **+** to expand **Cache**, and then click **Options**. Select **Multi-user-Check with server to determine if cache files are up to date**.



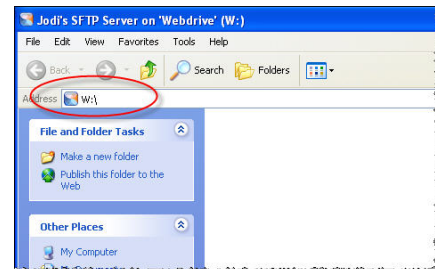
15. Click **File** and under **Basic File Options**, select :


- **Cache temporary MS Office files,**
- **Ignore destop.ini files (assume they don't exist),**
- **Disable explorer icon handler to prevent file download,**
- and **Enable Directory change notification.**

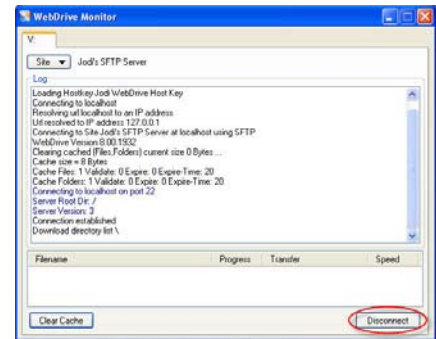


Click **OK** when you are finished. Your WebDrive site is now ready for use with SharePoint Services (WSS 3.0).

WebDrive displays your server connection as a mapped drive letter.

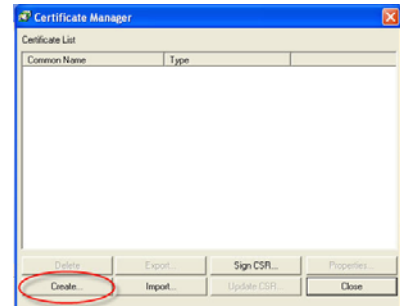


Double-click the WebDrive tray icon  to view the WebDrive Monitor or to disconnect from the server.

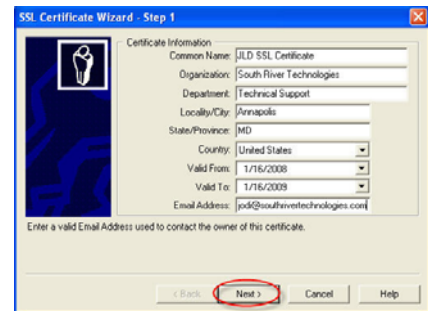


Appendix A: WebDrive Certificate Manager

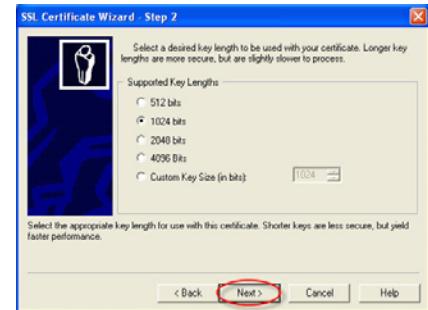
1. Click **Create** to create a certificate. This will launch the *SSL Certificate Wizard*.



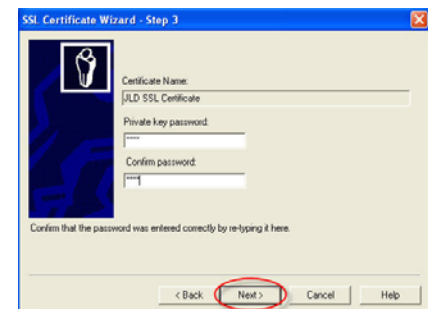
2. Type your **Certificate Information**. You must supply your information for each field. Use the drop-down arrows to select the **Country** and **Valid From** and **Valid To** dates. Enter the valid **Email address** that will be used to contact the owner of the this certificate. Click **Next**.



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. There are three options available for generating your certificate:

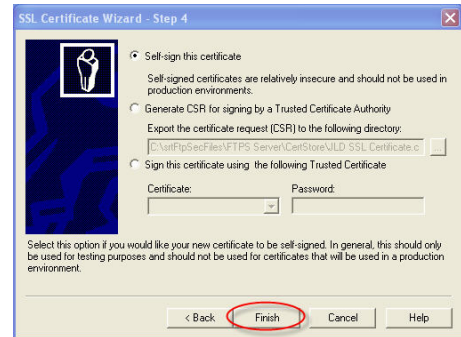
•Self-sign this certificate—Select this option if you would like your new certificate to be self-signed. Self-signed certificates are relatively insecure. In general, this option should only be used for testing purposes and should not be used for certificates that will be used in a production environment.

•Generate CSR for signing by a Trusted Certificate Authority

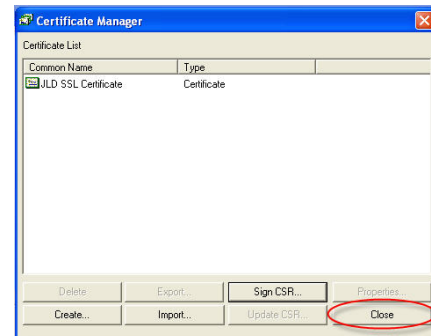
—Select this option if you would like to generate a CSR (Certificate Signing Request) to be sent to an external CA (Certificate Authority) or Trusted Authority for signing. Once the CSR has been signed, and your certificate generated, you will be able to update your CSR and import your newly signed certificate. 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.



6. Click **Close**. You will be returned to the *WebDrive Site Wizard, step 7* of the main body of this quick start guide.



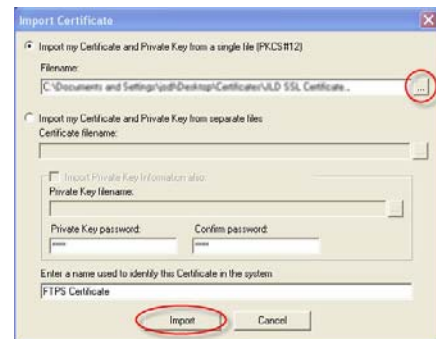
Importing a Certificate

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



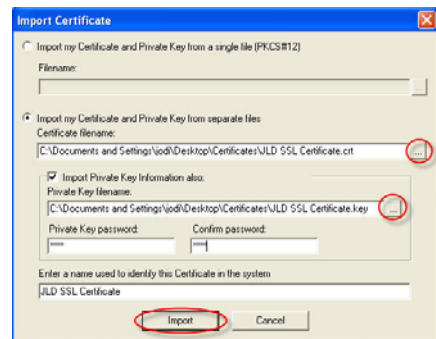
2. *Import Certificate* provides two options for importing your certificate:

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**.

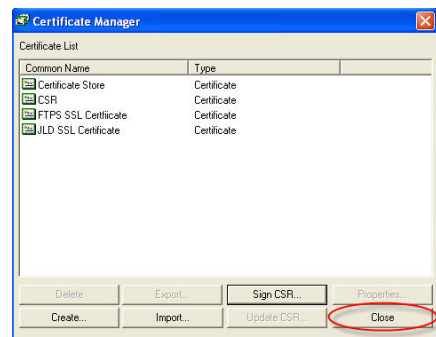


-OR-

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

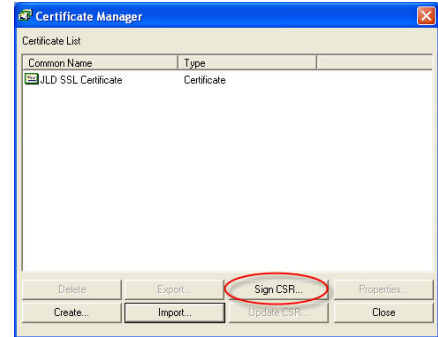


3. Your certificate has now been imported and you can see it listed in the *Certificate list*. Click **Close**. You will be returned to the WebDrive *Site Wizard*, [Step 7](#) of the main body of this Quick Start Guide.



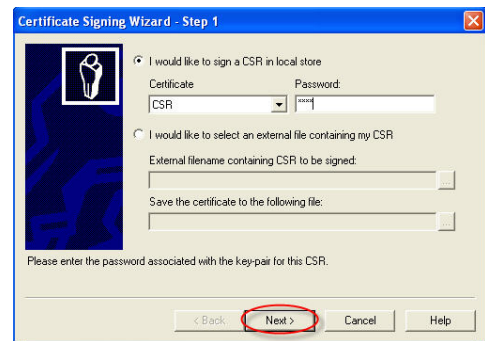
Signing the CSR

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



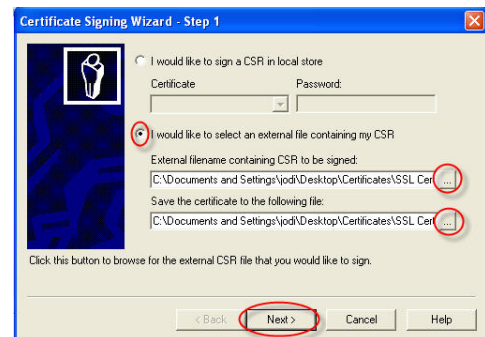
2. The *Certificate Signing Wizard* provides two options for signing your certificate:

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.

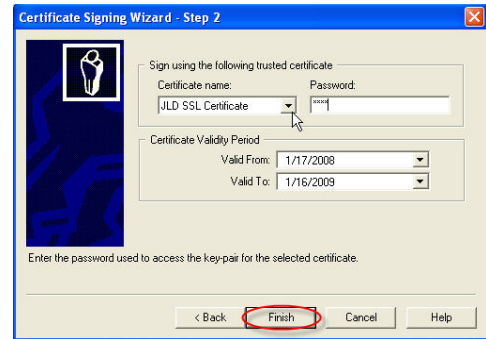


OR

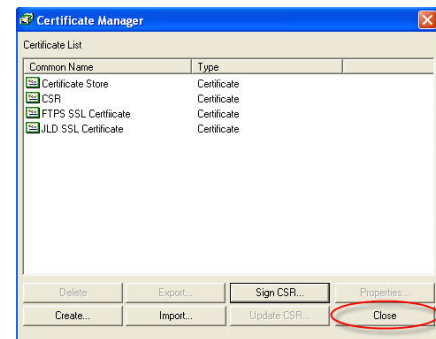
You can select an external file that contains your CSR and use the browse "..." buttons to browse to the certificate and to save the certificate. Click **Next** when you are finished.



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**.



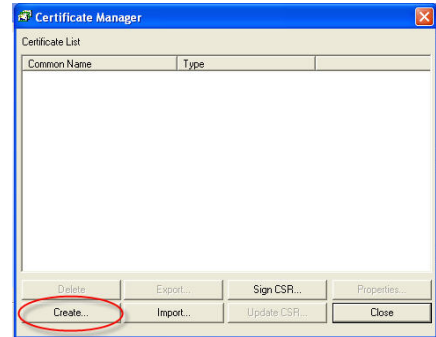
4. Your certificate is now ready for use and appears in the *Certificate List*. Click **Close**. You will be returned to the *WebDrive Site Wizard*, [Step 7](#) of the main body of this quick start guide.



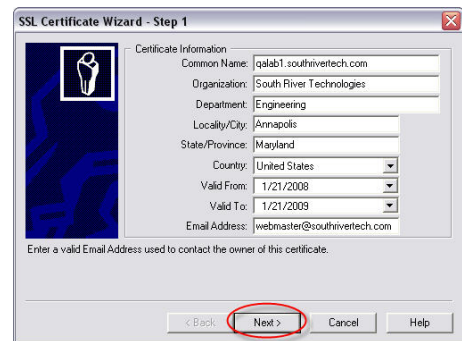
Appendix B—Trusted Certificate Authorities

Generating the CSR for Signing

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

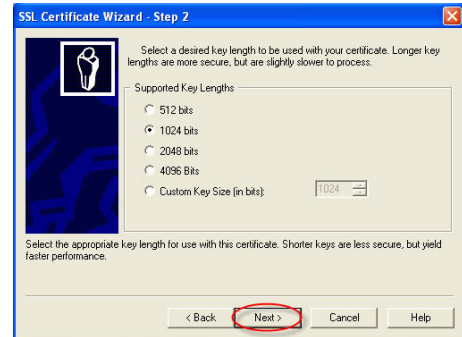


2. Type your **Certificate Information**. You must supply your information for each field.* Use the drop-down arrows to choose the **Country** and **Valid From** and **Valid To** dates. Enter the valid **Email Address** that will be used to contact the owner of the this certificate. Click **Next**.



*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.

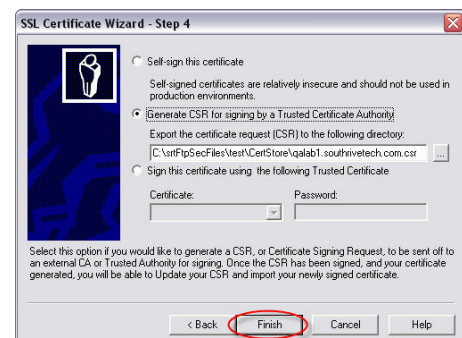
3. Select a desired **key length** to be used with your certificate. Longer key lengths provide better security, but result in slower performance. Shorter keys run faster but are less secure. Key lengths of 1024 bits or larger are recommended for secure environments. Click **Next**.



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**.



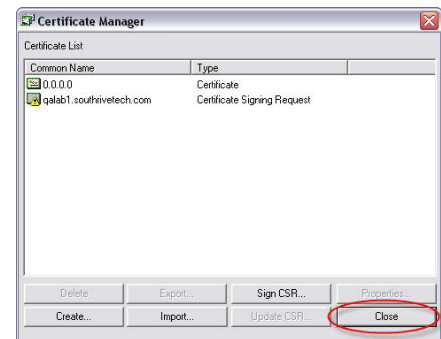
5. Select **Generate CSR for signing by a Trusted Certificate Authority**. Export the certificate request to a directory by using the "... " browse button. *Be sure to take note of where you save the .csr file because you will need to access it again to send it to the Certificate Authority.* Click **Finish**.



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.

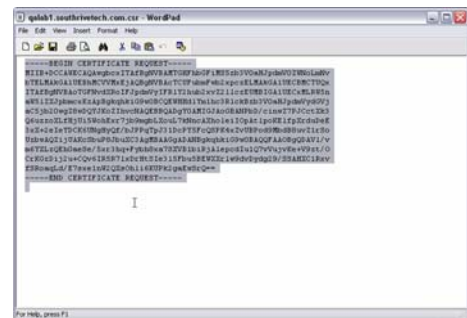
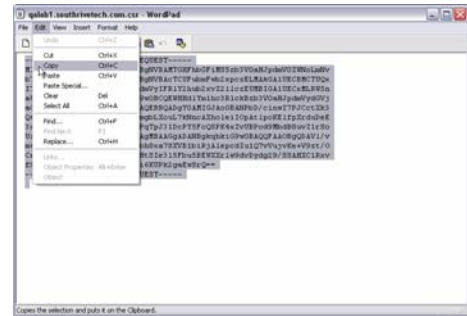


7. Click **Close** to close the Certificate Manager.



Sending 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.



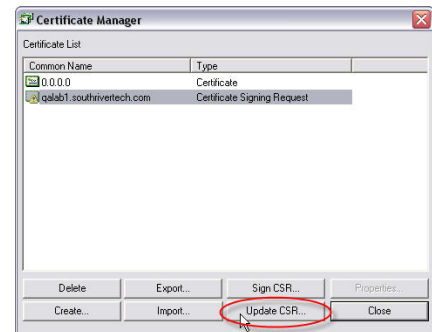
After you submit your Certificate Signing Request, the Certificate Authority will verify the certificate request information and create a certificate for you. The time necessary to create a certificate varies from authority to authority, so check with the specific certificate authority for turn-around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

Updating CSR in WebDrive

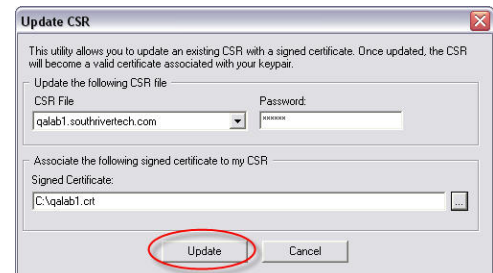
1. After the Certificate Authority approves your CSR, they will email you a secure link to access your certificate. Copy your certificate to WordPad and save in **.crt** format. When you name your .crt file, do not use extra periods or characters that any system treats as special characters. *Be sure 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 WebDrive *Certificate Manager*. Select **Update CSR.*** (***DO NOT CHOOSE Import.** If you choose *Import* it will **invalidate** your CSR. To properly configure this certificate to WebDrive 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**.

