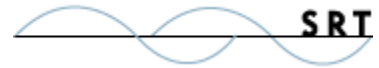




WebDrive

Host Key Authentication Quick Start Guide



Welcome to WebDrive®

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 instruction contain options that do not pertain to using Host Key Authentication with WebDrive. If you need additional information regarding these steps, please see the [WebDrive User's Guide](#). For the purpose of this Host Key Authentication quick start guide, we will guide you through these options without configuring additional settings.

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

- Make sure all Windows Service Packs and Updates have been installed.
- No other TCP/IP stacks are currently supported.
- 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.
- To uninstall WebDrive, you must also be logged in with the user account that has administrative rights. Next, from the Control Panel, select Add or Remove Programs and then select WebDrive or select the uninstall icon in the WebDrive program folder.

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

Anti-virus Compatibility

- **ZoneAlarm®**: To use Zone Alarm make sure you have the Internet security level set to medium to allow access to the remote server. You might also need to disable the "block local servers" option in the security section.
 - **F-Secure® Anti-Virus**: You may experience hanging problems when using F-Secure Anti-Virus under Windows NT/2000/XP/2003. We recommend that you disable F-Secure before use.
 - **KasperSky® Anti-Virus**: You may experience problems under Windows NT/2000/XP/2003 while using KasperSky Anti-Virus software. Please disable the anti-virus software before use.
 - **InoculateIT/E-Trust® Anti-Virus**: You may experience sluggish performance when real-time file system protection is enabled. As a work around, you can configure the anti-virus software to not scan files that are in the WebDrive cache directory (normally **c:\program files\WebDrive\cache**). You can also configure the anti-virus software to scan for executable files only.
- ➔ If you are using an anti-virus software package that is not listed above and you are having problems, try disabling the real-time protection feature of that product or configure it to not scan network drives or drives that you are using. You may also want to exclude the cache directory from the files that should be scanned. Norton Anti-virus software is recommended.

Troubleshooting

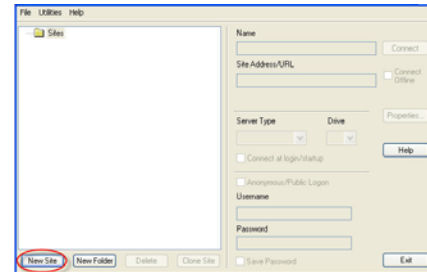
When attempting to connect to an FTP server, keep in mind the following requirements:

- Windows operating system.
- The Microsoft TCP/IP Network Client must be installed. This can be setup from the Network control panel applet. Other TCP/IP clients can be used if they conform to the Microsoft TCP/IP TDI Standard.
- An active connection with the Internet must be established. For dial up networking users, this just means that you need to be connected to your ISP.

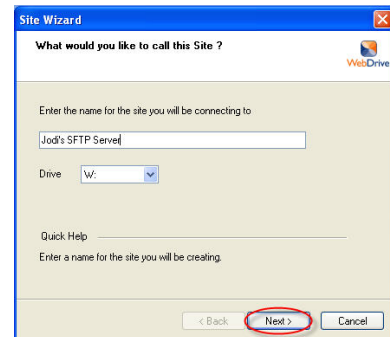
The following instructions will help you to set up WebDrive for use with Host Key Authentication. If you need additional assistance the [WebDrive User's Guide](#) is available on line. Also, a listing of Frequently Asked Questions (FAQ) is available at our [Knowledgebase Support Center](#).

Using Host Key Authentication with WebDrive

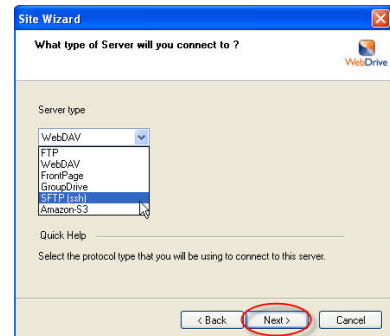
1. Click **New Site**. The WebDrive *Site Wizard* will launch.



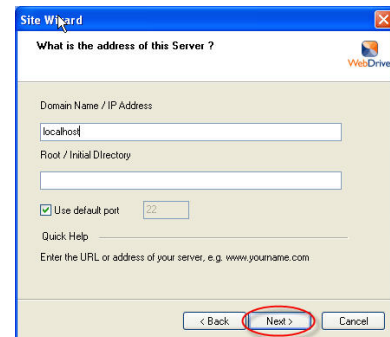
2. Type the **name of the site** that you will be connecting to. Choose an available **Drive letter** using the drop-down arrow. Click **Next**.



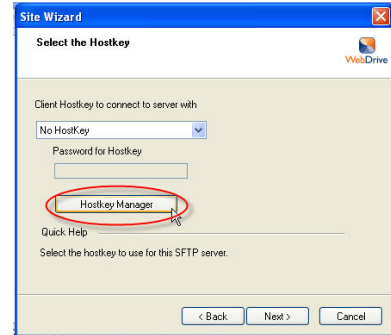
3. Choose the **Server type** by using the Drop-down arrow. To use Host Key Authentication, choose **SFTP (ssh)**. Click **Next**.



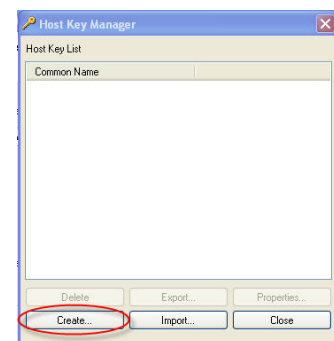
4. Type the **Domain Name or IP Address of the Server**. Type the **Root or Initial Directory**. The default port is port 22. To change the port number, clear the check box and type your port number. Click **Next**.



- From the drop-down list, select the **Host Key** to be used for authentication with the remote SFTP server. If your host key is not listed, you can use the *Host Key Manager* to generate a host key pair to be used with your SFTP server. To generate a host key pair, click **Hostkey Manager**. The *Host Key Manager* will launch.



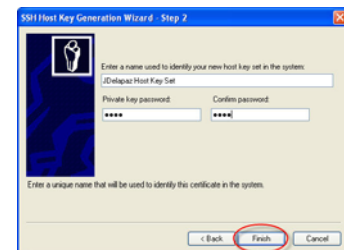
- Click **Create** to create your host key pair.



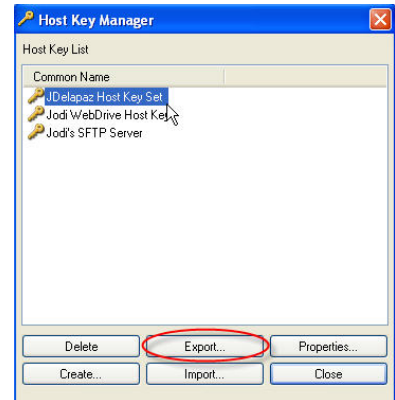
- Choose your **Host Key Type** using the drop-down arrow. Note that DSA host keys **must** be 1024 bits in length. RSA keys do not have this restriction and can range from 512 bits in length to 4096 bits in length. Longer key lengths provide better security, but result in slower performance. Shorter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



- Type a **name** that will be used 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**. Passwords must be at least four characters with no spaces and are case sensitive. **Confirm your password** and then click **Finish**.



- Once the host key pair has been created, you will need to **export the public key** (*not the private key*) and send it to your SFTP Server Administrator so they can load your **public key** into the server host key database. Select the **Host Key Set** that you wish to export and click **Export**.

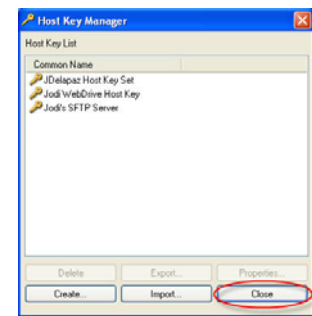


- You may change the location of your **Public key filename** by using the "..." browse button. If you would like to *export private key information* you may select the check box and use the "..." button to browse to a location. You must type your **Private key password** and confirm your password to export your Private Key.* Click **Export**.



*We recommend that you **do not** share or export your private key information unless it is for backup purposes.

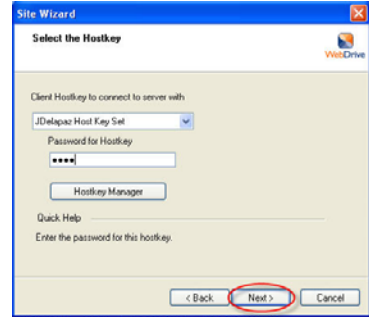
- Click **Close** to exit the *Host Key Manager*.



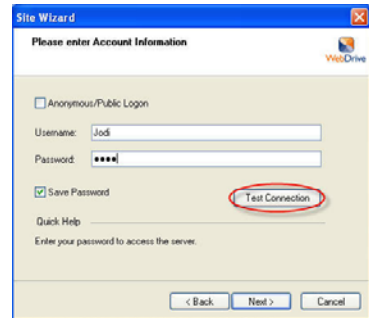
- Select your **Host Key Set** by using the drop-down arrow.



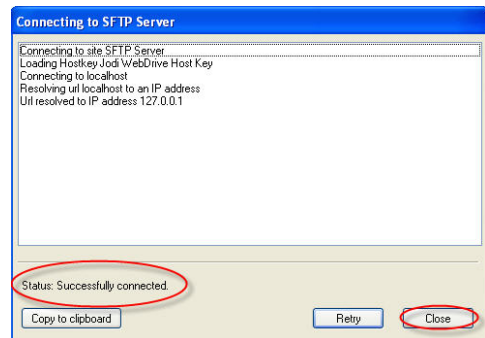
13. Type your host key set **Password** and then click **Next**.



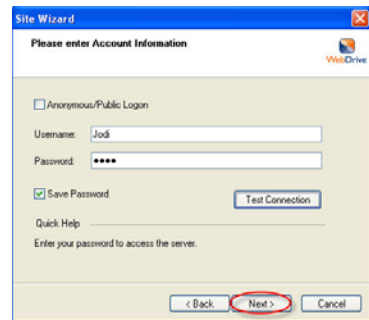
14. Type your **Username**, necessary to access the remote SFTP server. If you will be using Host Key Authentication with the remote SFTP server, you do not need to specify a password. If you are using Password Authentication with the remote SFTP server, type your **Password**. Click **Test Connection**.



15. 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**.



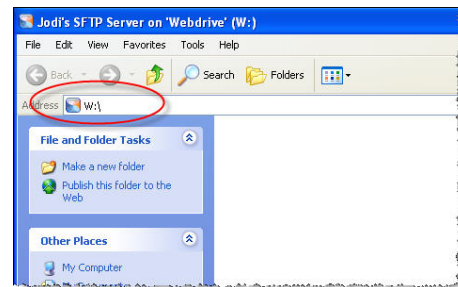
16. Click **Next**.




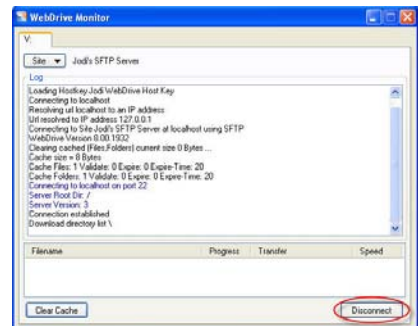
17. Select **Connect to Site now** if you would like to connect to the site now. If you would like to **Connect at login/startup**, you may select this check box. Click **Finish**. Your Site is now ready for use.



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.



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 a good practice to also password protect your private key, and WebDrive requires this.

While it is possible to use the Host Key Management features in WebDrive to export your private, it is highly discouraged unless it is for backup purposes because it is difficult to ensure the integrity of the private host key during the physical transfer of the host 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.

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.