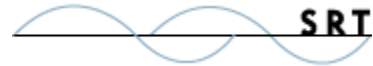




WebDrive

User's Guide
Version 9



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

Table of Contents

Notices-----	ii
Table of Contents -----	iii
Getting Started-----	5
System Requirements	5
Application Compatibility Issues	6
Installation Notes	7
Software Activation	7
Troubleshooting.....	12
Tips on FTP	14
Reporting Problems.....	14
FIPS Compliance.....	15
Navigation Overview	16
Exploring the Tray Icon	17
WebDrive® Monitor	18
Working with the Site Manager-----	19
Setting up the Site Manager	19
Simplified Site Manager	22
Site Wizard	24
Site Properties Dialogs-----	25
Site General Dialog Tab	25
Site Connection Dialog Tab.....	25
Site HTTP Settings Dialog Tab.....	26
Site FTP Settings Dialog Tab.....	28
Site DAV Dialog Tab.....	29
Site Certificate Dialog Tab.....	29
Site SSL Encryption Dialog Tab	30
Site File Settings Dialog Tab	30
Site File Substitution Dialog Tab.....	34
Site File Permissions Dialog Tab	34
Site Auto ASCII Transfer Dialog Tab	35
Site Hidden Directories Dialog Tab.....	35
Site Cache Settings Dialog Tab	35
Site Advanced Dialog Tab	36
Site SFTP Settings Dialog Tab.....	36
Site SFTP Host Key Settings Dialog Tab.....	37
Site FTP Settings Dialog Tab.....	37
Site FTP Encryption Dialog Tab	39
Exploring the File Menu -----	40
Export Settings to Registry File	41
Import Settings from a Registry File	42
Program Settings-----	43
Program General Settings	43
Program Cache Settings	45
Program Cache Options	45
Program Proxy-FTP Settings	47
Program Proxy-HTTP Settings.....	48
Program Logging Settings	50
Program Popup Window Errors Settings	51
Program Backup Files Settings.....	51
Program Certificate Management	52

Program Host Key Management	52
Advanced Topics -----	54
Amazon S3	54
Caching Options	61
Automating Connections/Disconnections	64
Command Line Parameters	64
Scripting or Batch Files	65
Registry Settings	66
UNC - Universal Naming Convention	68
Setup Options	69
Using WebDrive® from an NT Service.....	71
Shell Extensions	73
File Transfer Manager.....	75

Getting Started

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.**

Application Compatibility Issues

This section describes compatibility issues with the following applications:

- **ZoneAlarm®:** To use ZoneAlarm, 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 only scan for executable files.


 A small icon of two orange flags on a silver pole, used to denote a warning or important note.	<p>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. For anti-virus software, we recommend using Norton Anti-virus.</p>
--	---

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.

	<ul style="list-style-type: none">• 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.
--	---

Software Activation

To activate WebDrive and convert it from a trial version to a full version, enter your registration code on the **Activation** dialog. To access the **Activation** dialog, on the WebDrive **Help** menu, expand **License** and click **Registration & License Information**. After you enter a valid registration code, WebDrive will contact our licensing server to validate your license. After your license has been validated, WebDrive will no longer contact the activation server when you connect. To move WebDrive to another computer, uninstall WebDrive to deactivate the license.

Questions or Comments? Please visit our online support area at www.southrivertech.com/support/

Terminology

Amazon S3[®] – Amazon Simple Storage Service (Amazon S3). An Internet storage server.

ASCII - Acronym for the *American Standard Code for Information Interchange*. Pronounced ask-ee, ASCII is a code for representing English characters as numbers. Each letter is assigned a number from 0 to 127. Most computers use ASCII codes to represent text, which makes it possible to transfer data from one computer to another.

Binary - A numeral system that represents numeric values using two symbols only; also known as the base-2 numbering system. Computers are based on the binary numbering system, which consists of just two unique digits, 0 and 1.

Cache - A temporary storage area where frequently accessed data can be stored for rapid access. The most recently accessed data from the disk (as well as adjacent sectors) is stored in a memory buffer. When a program needs to access data from the disk, it first checks the disk cache to see if the data is there. Disk caching can dramatically improve the performance of applications, because accessing a byte of data in RAM can be thousands of times faster than accessing a byte on a hard disk.

CGI - *Common Gateway Interface*, a specification for transferring information between a World Wide Web server and a CGI program. A CGI program is any program designed to accept and return data that conforms to the CGI specification.

CHMOD - A UNIX command that means *change mode* and changes the access permissions for files or directories in order to read, write, or execute files.

CWD - An FTP command that means *Current Working Directory*.

DOS - Acronym for *Disk Operating System*. The term DOS can refer to any operating system, but it is most often used as an abridgment for MS-DOS (Microsoft Disk Operating System). Originally developed by Microsoft for IBM, MS-DOS was the standard operating system for IBM-compatible personal computers.

FTP - Abbreviation for *File Transfer Protocol*, the protocol used on the Internet for exchanging files. FTP uses the Internet's TCP/IP protocol suite to enable data transfer. FTP is most commonly used to download a file from a server using the Internet or to upload a file to a server (for example, uploading a Web page file to a server). The FTP file transfer is not random access (for example, *seeks* are not allowed in the file). This is why the entire file is downloaded into the cache when you open it. Most companies use FTP to enable their customers to download software updates or patches. Most access to FTP servers is done by way of an anonymous logon. This type of logon usually allows the user to have read-only access to the FTP server. Some companies also allow users to upload files to the FTP server into specific directories.

Firewall - A technology that inspects network traffic and permits or denies access based on a set of rules. It prevents unauthorized access to or from private networks. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks that are connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria

FrontPage® - Refers to servers that run the Microsoft FrontPage Server Extensions.

GroupDrive® - Refers to the WebDAV server with custom extensions developed by South River Technologies. [GroupDrive® Collaboration Server](#) is a multi-threaded, dynamic WebDAV Server for the Windows operating system.

HTTP - Abbreviation for *Hypertext Transfer Protocol*, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

ISP - Abbreviation for *Internet Service Provider*, a company that provides access to the Internet.

LAN - Acronym for *Local Area Network*, a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.

PASV - An FTP command indicating *passive mode* that is a more secure mode in FTP where the client initiates the data connection. Some FTP clients and servers do not support PASV transfers.

PERL - *Practical Extraction and Report Language* (Perl) is a programming language especially designed for processing text.

Proxy Server - A server that acts as a gateway between a client and another server (the "real" server). A proxy server sits between a client application, such as a Web browser, and forwards requests to another server. A proxy server intercepts all requests to the "real" server to see if the requests should be permitted. If the request is permitted, the proxy server will forward the request.

Root Directory - The top directory in a file system. The root directory is provided by the operating system.

S/Key - Refers to a one-time password system. Each password used in the system is usable for one authentication only and cannot be reused.

SFTP - Refers to an SSH (Secure Shell) based encryption protocol that is more efficient and secure than FTP.

SSH - Abbreviation for Secure Shell. A protocol that allows data to be exchanged over secure channels. Encryption ensures confidentiality and integrity of the data being exchanged.

SSL - Abbreviation for Secure Sockets Layer, a secure protocol developed by Netscape for transmitting private documents over the Internet. SSL works by using a private key to encrypt data that is transferred over the SSL connection.

Select - Refers to an instruction given in the help system, meaning to click with your mouse on a specific icon or file.

TCP/IP - Abbreviation for *Transmission Control Protocol/Internet Protocol*, the suite of communication protocols used to connect hosts on the Internet. TCP/IP combines several protocols; the two main protocols are TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.

TLS - Abbreviation for *Transport Layer Security*, a protocol that ensures privacy between communicating applications and users on the Internet. TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to SSL.

UNC - Abbreviation for *Universal Naming Convention*. Universal Naming Convention is a file name format used to specify the location of network resources or files on a network share.

UNIX - A multi-user, multitasking operating system. UNIX was one of the first operating systems to be written in C, a high-level programming language.

URL - Abbreviation for *Uniform Resource Locator*, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP (Internet Protocol) address or the domain name where the resource is located.

VMS - Abbreviation for *Virtual Memory System*, a multi-user, multitasking, virtual memory operating system that runs on VAX and Alpha computers.

VPN - Abbreviation for *Virtual Private Network*, a network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

WebDAV - Refers to the *Web-Based Distributed Authoring and Versioning Protocol*. An extension to the HTTP protocol that many servers now support on the Internet.

Troubleshooting

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

- The Microsoft [TCP/IP](#) Network Client must be installed. This can be set up from the Network control panel applet. Other TCP/IP clients can be used if they conform to the Microsoft TCP/IP TDI (Transport Driver Interface) Standard.
- An active connection with the Internet must be established. (For dial-up networking users this means that you need to be connected to your [ISP](#).)

Common problems and how to resolve them:

- **Why can't I see new files that are created by other users?**
Try flushing the cache from the tray icon. To see updates from other users you can select the Multi-user cache mode or set directory listings to expire after a specified amount of time.
- **Why can't I create files using Microsoft Word?**
Your FTP server may not support filenames that have the tilde (~) character. You can configure WebDrive to remove/replace this character when interacting with your FTP server. See the site properties File Names tab.
- **Why can't I create a directory using the Windows Explorer?**
Your FTP server may not support spaces in file names. You can configure WebDrive to remove/replace this character when interacting with your FTP server. To configure this option, launch the WebDrive Site Manager and click Properties. Expand the General menu tree and click Substitution.
- **Why can't I connect to an FTP server?**
Check your username and password; they are case sensitive. Check if your Internet connection is still alive. Check the URL to make sure it is entered correctly.
- **Why am I getting the Drive is in use error message?**
When this error is displayed, it means that the drive that you are attempting to connect to is already in use as a network drive. You need to select a drive that is not currently in use. To see what drives are available, open Windows Explorer and look in the left-hand pane for drives that are currently in use.

- **Why am I getting the Unable to map network drive X to server error message?**
This error message is displayed when a mount (install) for the selected drive fails. This normally happens when you have a lastdrive=g statement in your config.sys file. Remove this entry from your config.sys file and restart your system.

- **Why is the directory listing empty for the FTP site?**
Try flushing the directory cache. WebDrive might not understand the directory listing format of the FTP server or it can't Auto Detect the listing type. Try changing the server type from Auto Detect to the actual type. Currently UNIX, NT/DOS, VMS, Macintosh, AS/400, and Novell servers are supported. Try enabling Passive Mode (PASV). If you have a problem with a particular FTP server, please send the URL to us so we can add support for it.

- **Why can't I copy a file from the FTP drive?**
Check the Drive Monitor log window for FTP status responses. It may report access denied or some other FTP error.

- **Why can't I find a file on the server that should be there?**
Flush your directory cache. This can be done from WebDrive or the Monitor application.

- **Why doesn't the Rename function work?**
Your FTP server probably does not support this command.

Visit our Knowledge Base at www.southrivertech.com for more solutions to common problems.

Tips on FTP

Limitations/Precautions:

- **Back up files on your FTP server** - FTP is not always a 100% reliable method of transferring files, especially when dial-up or Internet connections are involved. You should always have a backup of the files that reside on your FTP server.
- **No Locking mechanism** - FTP does not provide a mechanism for locking files. For example, when one user opens a file for download, another user could open the same file for upload and corruption could occur. If you require a locking mechanism for files, [WebDAV](#) and [GroupDrive®](#) provide this option.

Reporting Problems

To report a problem, visit the WebDrive® support site at www.southernrivertech.com/support/. Please furnish our Support Engineers with the following information:

1. The Windows platform that you are running.
2. The WebDrive version that you are using.
3. The URL of the server that you were using when the problem occurred.
4. A detailed description of the problem. Include the file name and complete sub-directory name if applicable.
5. Attach a copy of the Log file to your e-mail.

FIPS Compliance

FIPS—SFTP

The Federal Information Processing Standards (FIPS) Publication Series of the National Institutes of Standards and Technology (NIST) certifies hardware and software modules to determine levels of conformance for security and encryption.

Publication 140-2 discusses the Security Levels for Cryptographic Modules and outlines the set of requirements that cryptographic software must meet to be in compliance and applicable for U.S. Government use.

WebDrive Version 9 and later is fully compliant with FIPS-140-2 when running in Secure File Transfer Mode. This mode, using the SFTP protocol, and running over an SSH v2.0 encrypted tunnel, meets or exceeds the current FIPS-140-2 standards.

In WebDrive, FIPS-140-2 mode is the default when using SFTP, and for security reasons, cannot be disabled. When WebDrive initializes, FIPS-140-2 compliance tests are run and information is written to the logfile (and displayed in the WebDrive Administration Console).

If any of the FIPS-140-2 level tests fails to pass, FIPS-140-2 mode will be disabled and the SFTP services for WebDrive will not start.

When running in FIPS compliant mode, only FIPS approved algorithms will be available in WebDrive. These are:

FIPS-approved Algorithms:

- Skipjack (Cert. #17)
- Triple-DES (Cert. #512)
- AES (Cert. #499)
- SHS (Cert. #569)
- DSA (Cert. #206)
- RSA (Cert. #216)
- ECDSA (Cert. #49)
- HMAC (Cert. #253)
- RNG (Cert. #279)
- Triple-DES MAC (Cert #512 vendor affirmed)
- Diffie-Hellman (key agreement)

WebDrive's SFTP technology is based on the Crypto++™ Cryptographic Library by Wei Dai, which is certified FIPS-140-2 compliant with certificate #819.

The certificate can be viewed on the NIST website:

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt819.pdf>

FIPS—SSL

WebDrive uses the FIPS compliant Microsoft SSL engine.

Navigation Overview

After installing the software, you will notice a **tray icon** located in your Windows taskbar tray area.

Starting WebDrive using the tray icon is optional. You can disable the tray icon using the tray menu or the [application window](#). To display the tray menu, right-click on the tray icon and the menu will appear.

To launch the application window, you can either double-click the WebDrive icon located in the program folder created by the installation program, or you can right-click on the tray icon and select **Open WebDrive**. Most of the functionality of the application window is also provided on the tray icon.

The installation program may create several predefined sites. To connect to one of these predefined sites, select the **site** and click the **Connect** button. To create a new site, click the **New Site** button.

Once you have successfully connected to the server and a drive has been mapped, an Explorer window will be launched to explore the newly mapped drive. (This is the default setting. To change this setting, launch the *WebDrive Site Manager* and select **File>Program Settings**. On the *Program Settings* menu tree, select **General Settings**.)

Once you are connected to the server, you can navigate the site with Explorer or a DOS command prompt. Copy files with the DOS copy command, or cut and paste with Explorer. You can use Explorer to disconnect from the server (right-click on the **drive** icon and select **Disconnect**), or you can use the Monitor dialog to disconnect (right-click on the WebDrive **tray** icon, click **Show Monitor** and then click the **Disconnect** button.)

Since a connection can be interrupted in the middle of a file transfer, you should always keep a backup copy of files that are transferred or modified on your server. You can use the **Backup Files** setting to backup files if the upload fails. This feature puts files into the Backup directory when an upload fails. This will prevent you from losing your changes to a file if a connection is dropped. To access the **Backup Files** feature, click **File>Program Settings>Backup Files**.

Exploring the Tray Icon

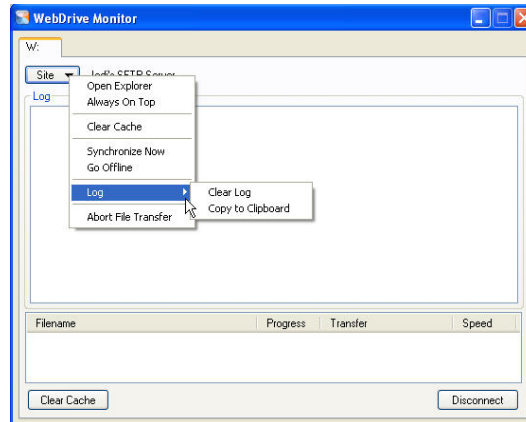
To view the options available in the WebDrive **tray icon**, right-click the **tray icon** in the Windows taskbar. The following options are provided to give you quick and easy access to selected tasks:

- **Open WebDrive** - Opens the WebDrive Program.
- **Program Settings** - Displays the Program Setting dialogs.
- **Connect To >** - Displays a Popup menu of FTP sites that have the **Add to Tray/Connect Menu** feature enabled.
- **Show Monitor** - Displays the WebDrive Monitor.
- **Run at Startup** - Selecting this option enables the tray icon to **Run at Startup**.
- **Help Topics** - Launches WebDrive Help files.
- **About WebDrive** - Provides you with the Program Version Number, Registration Code, License Type, Product Registration Date, Upgrade Status, and Registration Status.

WebDrive® Monitor

To display the **WebDrive Monitor**, right-click the **WebDrive tray icon** found in the Windows taskbar. Select **Show Monitor**.

Use the **Site** drop-down menu to display WebDrive Monitor options.



WebDrive Monitor .jpg

- **Open Explorer:** Launches Explorer.
- **Always On Top:** Keeps this window always on the top of your screen so that it is always visible.
- **Clear Cache:** Select **Clear Cache** to immediately clear the cache. You can also use the *Clear Cache* button.
- **Synchronize Now:** Performs immediate synchronization to the server.
- **Go Offline/Online:** Work offline or online.
- **Log>**

Clear Log: Click this button to clear the log list box.

Copy to Clipboard: The Clipboard feature copies the contents of the Monitor dialog box to the Windows clipboard. You can then paste the contents into an e-mail or Notepad.

➡ *This is useful for sending information to technical support.*

- **Abort File Transfer:** Click this button to immediately abort a file transfer.
- **Disconnect:** Click the **Disconnect** button to end your connection with the currently displayed network drive.

Working with the Site Manager

Setting up the Site Manager

WebDrive's *Site Manager* is used to add or edit site information, change program settings, and configure WebDrive. Sample sites may appear on the *Site Manager* after installation. You can edit or delete these sample sites. The main *Site Manager* window is shown below. You also have an option to use a [Simplified Site Manager](#) interface. The *Simplified Site Manager* interface can be enabled from the **Program Settings/General Settings** dialog.

Mapping your Drive to a Server

1. Click the **New Site** button.
2. Follow the prompts in the **Site Wizard** to create a new site.
3. Click the **Connect** button.

Name: The name of this Site. You can also rename a site by using this edit box.

Site Address/URL: The URL to connect to.

For **Amazon S3**[®] users there are two options: The first option is to use the URL **http://s3.amazonaws.com**, which should show all buckets that you have access to in the root folder; then you can navigate to the buckets and treat them as folders. The second option is to **root your drive in a bucket** by using the following syntax **http://s3.amazonaws.com/mybucket** where **mybucket** is the name of the bucket you wish to use. For European buckets, use the syntax:
http://<euro-bucket-name>.s3.amazonaws.com.

Server Type: Select the type of server you are connecting to from the drop down menu. Your choices are:

- [FTP](#)
- [WebDAV](#)
- [SFTP](#)
- [GroupDrive](#)[®]
- [FrontPage](#)[®]
- [Amazon-S3](#)[®]

Drive: Select the drive letter to map to the server.

Connect at login/startup: Enable this option if you want the drive to be automatically connected to the server when you logon to your computer.

Anonymous/Public Logon: Allows anonymous or public logon.

Username & Password: The username/password for the site. For Windows servers that support Windows Authentication you can leave the username/password box empty to log on using the default NT credentials of the currently logged on NT user. For **Amazon-S3**[®] servers, type your **Amazon Access Key** in the username box and type your **Secret Key** in the password box.

Connect: Connect and map a drive to the selected server.

Connect Offline: Map a drive in offline mode; no connection to the server is established. Files marked **available for offline access** will be available to you. You will also be able to create new files and folders. You can synchronize your changes the next time you connect to the server. To delete a file permanently you must be online to delete it.

Properties: Displays the **Site Properties** dialog.

Help: Launches WebDrive Help.

New Site: Launches the WebDrive *Site Wizard*.

New Folder: This button creates a new folder in the site list, and allows you to group and organize multiple sites into a folder.

Delete: This button deletes the selected site from the site list.

Clone Site: This button creates a duplicate/clone of the currently selected site and allows you to rename it.

NOTE: *This is useful when you have a site configured with custom settings that you want to duplicate for another site.*

Save Password: Stores the password internally so that it is automatically entered for you each time

Exit: Closes the **Site Manager** dialog.

Simplified Site Manager

WebDrive's *Simplified Site Manager* is used to add or edit site information, change program settings, and configure WebDrive. Sample sites may appear on the Site Manager after installation. You can edit or delete these sample sites. The Simplified Site Manager window is shown below. You can switch between the simplified and standard site manager interface from the **Program Settings/General Settings** dialog. You can access **Program Settings/General Settings** by right-clicking the WebDrive **tray icon**.

Mapping your drive to a server:

1. Click the **New Site** button.
2. Follow the prompts in the **Site Wizard** to create a new Site.
3. Click the **Connect** button.

Site: This drop-down menu can be used to add a new site, edit an existing site, or remove a site.

Connect: Connect and map a drive to the selected server.

Connect Offline: Map a drive in offline mode; no connection to the server is established. Files marked **available for offline access** will be available to you. You will also be able to create new files and folders. You can synchronize your changes the next time you connect to the server. To delete a file permanently you must be online to delete it.

Properties: Displays the **Site Properties** dialog.

Site Address/URL: The URL to connect to. For **Amazon S3**[®] users there are two options: The first option is to use the URL **http://s3.amazonaws.com** that should show all buckets you have access to in the root folder; you can then navigate to the buckets and treat them as folders. The second option is to **root your drive in a bucket** by using the following syntax: **http://s3.amazonaws.com/mybucket** where **mybucket** is the name of the bucket you wish to use. For European buckets, use the syntax:
`http://<euro-bucket-name>.s3.amazonaws.com.`

Restore drive at login: Restores the connection when you log on to your computer.

Drive: Select the drive letter to map to the server.

Secure connection: Connect securely to the server using [SSL](#).

Username & Password: The username/password for the site. For Windows servers that support Windows Authentication you can leave the username/password box empty to log on using the default NT credentials of the currently logged on NT user. For **Amazon-S3**[®] servers, type your **Amazon Access Key** in the username box and type your **Secret Key** in the password box.

Save username/password: Stores the username and password internally so that it is automatically entered for you each time

Exit: Closes the Site Manager dialog.

Site Wizard

The *Site Wizard* allows you to create a new site. You will be prompted by the Site Wizard to enter site-specific information such as URL, server type, and the user credentials required to access the server. To access the Site Wizard, click the **Site** drop-down arrow and select **New**.

The *Site Wizard* options will change depending on the configuration options that you choose. If you would like to connect securely, be sure the **Connect Securely** check box is selected on the Site wizard server address page. For more information about connecting securely, see the [WebDrive Public Key Authentication or Host Key Authentication Quick Start Guide](#).

Site Properties Dialogs

Site General Dialog Tab

You can use the **Site General** dialog Tab to configure general settings for a site. To access **Site General** dialog tab, launch the WebDrive **Site Manager** and then click **Properties**. On the **Properties** menu tree, click **General**.

Open Explorer in the following folder: Opens Explorer in the specified folder on the remote site.

Make drive read-only: Select this check box to mark all files on the site as read-only so that you cannot accidentally make changes to the files.

Synchronize Offline files at Connect time: Select this check box to synchronize all files marked as **Offline** with the server when you connect. To delete a file permanently you must be online to delete it.

Synchronize Offline files at Disconnect time: Select this check box to synchronize all files marked as **Offline** with the server when you disconnect. To delete a file permanently you must be online to delete it.

Site Connection Dialog Tab

To access the **Site Connection** dialog tab, launch the WebDrive **Site Manager**, and click **Properties**. On the **Properties** menu tree, click **Connection** to configure connection settings.

Bypass proxy server for this Site: Select this check box if you have a proxy server configured but you do not need to go through the proxy server for this specific site. Normally used for internal LAN connections.

Command timeout: Specify the number of seconds to wait for the server to respond to a command before timing out.

Connection Port: Specify the port to connect to the server on. You can use the value of "0" (zero) to have WebDrive select the default port for the protocol in use.

Failed transfer retry count: Specify the number of times to retry a failed upload/download request.

Active Connection Limit: Select the maximum number of simultaneous connections that WebDrive will use to connect to the server. Initially WebDrive will only establish a single connection to the server; however, if one connection is busy transferring a file, WebDrive will attempt to establish another connection if another file transfer or directory listing transfer is required. Use this setting to limit the number of connections WebDrive will attempt to use.

Active Upload Limit: Select the maximum number of simultaneous uploads that WebDrive will use. Generally, you would want to set this to a lower limit than the Active Connection Limit so that other operations can also occur when uploading multiple files.

Site HTTP Settings Dialog Tab

Use the **Site HTTP Settings** dialog tab to configure HTTP settings. To access the **Site HTTP Settings** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, expand **Connection** and click **HTTP**.

Always choose Basic Authentication: When enabled, WebDrive will use **Basic Authentication** when the server supports multiple types of authentication. Normally when the server supports multiple authentication types such as Digest or NTLM (NT LAN Manager), WebDrive will choose the most secure authentication method supported by the server. Basic Authentication is faster but less secure.

Enable persistent connections: Enables **HTTP keep-alive**; this is highly recommended because it increases performance significantly.

Enable 100-continue processing: When enabled, this interim response is used to inform the client that the initial part of the request has been received and has not yet been rejected by the server. The client should continue by sending the remainder of the request or, if the request has already been completed, ignore this response. Some servers do not support 100-continue processing.

Do chunked upload for large files: Enables large files/ WRITE packets to be broken into parts or chunks during upload to the server.

Add a trailing slash to directory list requests (needed for some Apache servers): When enabled, this option automatically adds a trailing slash "/" to directory list requests. When you access a directory without a trailing slash "/" Apache needs to send what is called a redirect to the client to tell it to add the trailing slash. Without this trailing slash, relative URLs would not work properly in some Apache servers.

Use a getlastmodified property for setting file time: When enabled, WebDrive will attempt a **PROPPATCH** on the **getlastmodified** Property to set a **files modified** time so that it will match the local time of a file, needed for file synchronization. Few **DAV** servers support this, if the server returns an error WebDrive will simply ignore it and continue.

Enable byte ranges on GET (some servers may not handle this): Use this feature to enable WebDrive to download only portions of a file, which may be useful when using applications that allow you to, for example, only extract an icon from a large executable file or when streaming an audio file.

Enable Single Sign On with Cookie: Enables Siteminder™ cookie-based single sign-on authentication. The user will authenticate to the server using a browser and a cookie is generated. WebDrive will search the Internet Explorer browser cookie cache for the specific URL that is being connected to and if a cookie is found, it will then pass this along to the server for HTTP connections. WebDrive will use this cookie for authentication instead of using the username/password in the WebDrive Site Manager.

Enable Single Sign Only Authentication Method allowed: When enabled along with **Enable Single Sign On with Cookie**, WebDrive will **only** allow cookie-based authentication. If no cookie is found or if the cookie is invalid or expired, then no other authentication methods will be attempted. When enabled and WebDrive cannot authenticate using the cookie, then it will simply fail to connect and display the error to the user. If this feature is not enabled and WebDrive cannot find the cookie or it is expired, then WebDrive will prompt for username/password.

Preserve S3 ACLs on overwrites and renames: (Amazon S3 only) When enabled, WebDrive will preserve a file's Access Control List (ACL) when a user overwrites or renames a file.

Site FTP Settings Dialog Tab

Use the **Site FTP Settings** dialog tab to configure FTP settings. To access the **Site FTP Settings** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, expand **Connection** and click **FTP**.

Host Type: Default: **Automatic Detect** or use the drop-down arrow to select the host type:

- Unix (Standard)
- Microsoft NT & 95
- VMS/VAX/Multinet
- Novell
- Macintosh
- AS/400
- IBM MVS
- OS/2 Warp
- OS/2 Hethman Brothers
- AIX
- AS/400 IFS
- VSE
- Novell Plexus
- Tandem
- Alpha Micro

Server Time Zone: Default: **Don't adjust file times** or use the drop-down arrow to select the server time zone.

Password Encode: Default: None or use the drop-down arrow to select the password encode scheme. Select from:

- S/KEY MD4
- S/KEY MD5
- ROT13 (Ceyoniq)

List Options: Use the text box to define list options.

Root Directory: Displays the root directory.

Initial Command(s): Use the text box to define initial commands. You must use a semi-colon (;) between commands.

Account(ACCT): Use the text box to define the **ACCT**.

Passive Mode (PASV): Select the check box to enable **PASV** mode.

Keep Connection Alive: When enabled, this option automatically keep the connection alive for the interval that you define in minutes.

Limit Local Port Range: When enabled, this option will limit the port range according the to minimum and maximum range that you define.

Site DAV Dialog Tab

Use the **Site DAV** dialog tab to configure WebDav specific settings for the site. To access the **Site DAV** dialog tab, launch the WebDrive **Site Manager** and select **Properties**. On the **Properties** Menu tree, expand **Connection** and then click **DAV**.

Lock Owner property: Leave this box empty to let WebDrive choose a default value for the **WebDAV lock owner** property when a DAV lock is taken on a file.

Enable Auto DAV Locking: Select this check box to enable **auto DAV locking**. WebDrive will establish DAV Locks on files that are opened by applications that use the *win32 share flags*. This works well for Microsoft Office applications and other applications that adhere to proper sharing semantics.

Only lock files with the following extensions: It is often useful to have WebDrive take out DAV Locks on certain file types only, for example, .doc, .xls.

Use DAV lock to check if user has Write access to file: If the file being opened is one of the files in the Auto DAV extension list and the user is requesting *write* access to it, then enabling this option will alert WebDrive to attempt to take out a DAV lock on the file. If the DAV lock fails, WebDrive will return an access denied error message to signify that the user only has read access to a file. This is mainly intended to be used for Microsoft Office files such as Word and Excel.

Get filename from "displayname" DAV property: When you enable this feature, WebDrive will use the **displayname** property instead of the **href** in the **PROPFIND** response for a directory listing.

Site Certificate Dialog Tab

The **Site Certificate** dialog tab allows you to configure a certificate to use when connecting to the server. To access the **Site Certificate** dialog tab, launch the WebDrive **Site Manager** and then click **Properties**. On the **Properties** menu tree, expand **Security** and select **Certificate**. Select the **Certificate** from the drop down list and type the **password** for the certificate. To use this feature, the certificate must have previously been imported by WebDrive.

If you would like more information about configuring and managing SSL Certificates, please see the [WebDrive Public Key Certificate-based Authentication Quick Start Guide](#).

Site SSL Encryption Dialog Tab

Use the **Site SSL Encryption** dialog tab to configure the SSL encryption algorithm to use when connecting securely to the server. To access the **Site SSL Encryption** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** Menu tree, expand **Security** and click **Encryption**. Select your Encryption Method using the drop-down arrow. To encrypt your **data channel**, select the **Secure Data Channel (Prot P)** check box.

Site File Settings Dialog Tab

Use the **Site File Settings** dialog tab to configure various options for filenames for this server. Some options are specific to server type and will only be displayed in the list when editing properties for a site with that specific server type. To access the **Site File Settings** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, select **File**.

Basic File Options

Encode filenames in UTF-8: Encode filenames before sending them to the server in UTF-8.

Get source document instead of rendered document: Enable this option to get the source document for dynamic content files like ASP or PHP files.

Show hidden files: When enabled, the hidden directory attribute is ignored.

Hide filenames that start with period: When enabled, files that begin with a period are not listed.

Use read-only directory attribute: Marks files as read-only when specified in the directory listing.

Resume interrupted file transfers: This option restarts broken file transfers at the point of interruption if the server supports this feature.

Cache temporary MS Office files: Microsoft Word and Excel use temporary files when editing .doc or .xls files. Enable this option to have these temporary files cached instead of being uploaded to the server. This will save time when you edit these types of files; when you save the document it will only be uploaded to the server when the temporary file is renamed into the original .doc or .xls file.

Ignore Desktop.ini files: Always return **file not found** when Explorer tries to open desktop.ini files. Explorer attempts to open desktop.ini files when browsing folders and this overhead can slow down operations.

Enable NTFS File Security: Returns fake NTFS permission information for applications that require it, for example, WordPerfect.

Cache small writes by applications: When enabled, WebDrive will cache small writes by applications to increase performance.

Test for Write Access when files are created: If you enable this option, when a file is created WebDrive will upload a zero length file to the server to test for *write* access. This allows you to catch **access denied** error messages before the application writes the file and WebDrive uploads the file in the background. By then it is too late to send an error message to the server that the upload has failed because the user does not have write access to the specified file. **Note:** not all servers allow zero byte files.

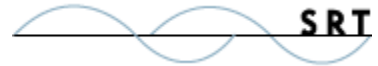
Stop file downloads when application closes the file before reading all data: When enabled, this option stops file downloads that are in progress when the application that opened and read from the file has stopped reading data. This is useful for preventing download of very large files when the application only reads the first few bytes of the file. For example, Explorer often does this when browsing folders.

Enable Quota Processing: Enables *Quota Processing* for servers that support quotas so that file writes will fail if the quota is exceeded.

Disable Explorer icon handler to prevent file download: Prevents files from being downloaded so that icons cannot be extracted (for example, .html, .zip).

Perform Cache File Read Ahead: Enable this option to perform read ahead operations on files for better performance. **NOTE:** This is only available for servers that support block I/O, for example, SFTP and GroupDrive.

Enable Directory change notification: When enabled, WebDrive will check the folders modified time and update the directory listing whenever it detects a change in the folders modified time. For example, if Explorer has a folder open then WebDrive will periodically check with the server to see if the folder contents have changed on the server and if they have changed, cause Explorer to refresh its display. This way, if "User A" has Explorer open on a folder called "photos" and then "User B" writes a new file to the "photos" folder, then "User A" will see this new file in his open Explorer window. This option works well for servers/protocols that support providing WebDrive with the folder's modified time. SFTP and WebDAV servers generally support this option efficiently. On the other hand, FTP servers generally do not support this option very well because many FTP servers do not support reporting a *directories modified* file time. **NOTE:** This feature uses the current cache settings to determine if a file is out of date. You should only enable this feature for **multi-user** or **custom** cache mode. This feature will not work for Single-User cache mode because the folder will never be considered out of date.



Set files modified time after upload to preserve date/time: When enabled, WebDrive will set the files modified time on the server to match the original file date/time, instead of using the upload time (for servers that support this feature).

FTP Specific Options

VMS strip extension ';: When enabled, this option removes the VMS (Virtual Memory System) extension from filenames.

VMS get most recent version: Enable this option to always get the most recent version when downloading a file and add ";0" to the filename.

VMS delete all versions: When deleting a file specify all versions ";*".

Use [.dirname] syntax on CWD for VMS logicals: When enabled allows you to use the .dirname syntax on the current working directory for VMS (Virtual Memory System) logicals.

Delete files before PUT: When enabled, the file on the server is deleted before uploading.

Maintain existing directory attributes: during upload, existing files retain the previous UNIX permissions for the file.

Resolve UNIX symbolic links: Determine whether a symbolic link refers to a file or folder.

Use MLSD to list full date/time: Use the MLSD command to return machine readable directory listings; not all FTP servers support this command.

Use MLST to get file information: Use the MLST command to return machine readable file information; not all FTP servers support this command.

Server supports FEAT command: Enables the FEAT (Get the feature list implemented by the server) command.

Site File Substitution Dialog Tab

To access the **Site File Substitution** dialog tab, launch the WebDrive **Site Manager** and select **Properties**. On the **Properties** menu tree, expand **File** and click **Substitution**. Use the **Site File Substitution** dialog tab to enable filename character substitution for servers that do not support specific characters in filenames, for example, \$ or ~. Select the **Enable character substitution in remote filename** check box. In the **List the characters to be replaced/substituted** box, type the characters that are not supported. These characters will be substituted using ASCII code in a string that is formatted as follows: **wdx>NNwdx** where **NN** is the ASCII code for the character being substituted. This option allows WebDrive to automatically undo the character substitution when downloading a file that has been character substituted.

Site File Permissions Dialog Tab

Use the **Site File Permissions** dialog tab to configure UNIX file permissions for new files or directories. To access the **Site File Permissions** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, expand **File** and then click **File Permissions**.

Set attributes on new or modified files by extension: When enabled, WebDrive will set permissions on files that are uploaded to the server. Permissions are set based on file extension. To add a new extension, select the **Set attributes on new or modified files by extension** check box and then select the **desired permissions** to use for the **file type**. Click **Add** to add it to the list.

Site Auto ASCII Transfer Dialog Tab

To access the **Site Auto ASCII Transfer** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, expand **File** and click **Auto ASCII Transfer**. Use the **Site Auto ASCII Transfer** dialog tab to configure which mode, ASCII or BINARY, file types are transferred to the server in.

Transfer Mode: Select the mode to use, ASCII, BINARY or Auto ASCII and then click **Add**.

- **ASCII** - Transfer all files in ASCII mode.
- **BINARY** - Transfer all files in BINARY mode.
- **Auto ASCII** - Transfer files in the list in ASCII mode, all others are transferred in BINARY.
- **Auto BINARY** - Transfer files in the list in BINARY mode, all others are transferred in ASCII.

NOTE: The **Site Auto ASCII Transfer** feature is available for FTP protocol only.

Site Hidden Directories Dialog Tab

To access the **Site Hidden Directories** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, expand **File** and click **Hidden Directories**. Some FTP servers will not list hidden directories but will allow you to see the contents if you specify the directory name ahead of time. Select **Enable Hidden Directories** and add hidden directory names to the list by typing a full file specification to the hidden subdirectory. For example, to add a hidden folder under the folder named **subdir** add it as **/subdir/myhiddendir**.

Site Cache Settings Dialog Tab

To access the **Site Cache Settings** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On **Properties** menu tree, select **Cache**. Use the drop-down list to configure whether or not this site uses the global cache settings for all sites. You can override the global cache settings with custom cache settings that will only apply to this site. This can be used for sites that require specific caching options that may not necessarily apply to most of your sites.

Site Advanced Dialog Tab

Use the **Site Advanced** dialog tab to configure advanced site settings. To access the **Site Advanced** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, click **Advanced**.

Enable Custom UNC name for this Site: Allows you to define a custom [UNC](#) (Universal Naming Convention) name for the site. By default, the UNC server name is **WebDrive** and the sharename is the **site name**.

Allow NT Services to access mapped drive: Allows you to map the drive under the NT **LocalSystem** context, which allows services like IIS to access the mapped drive letter.

Warning: When you enable this setting the site can no longer be used interactively; you may or may not even see the drive mapped in Explorer when you are logged in. Also, you will not be able to disconnect the drive. The drive will only be available to NT services. Do not enable this option unless you are experienced with NT services and NT user context issues. See the section on [Using WebDrive from a Service](#) for more details.

Map drive at system startup: Maps the drive at system start, not user logon. This may be useful when NT services needs access to the drive. If you enable this option, you should not configure the drive to connect at login/startup on the main **Site Manager** dialog.

For more information about using WebDrive with an NT service, please see the [Using WebDrive from a Service](#) topic.

Site SFTP Settings Dialog Tab

Use the **Site SFTP Settings** dialog tab to configure SFTP specific settings. To access the **Site SFTP Settings** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, expand **Connection** and click **SFTP Settings**.

Root Directory: Allows you to override the default login directory for your server.

SFTP Version: Select which version of the SFTP protocol to use. Version 4 of the SFTP protocol uses UTF-8 encoding for filenames, which is useful for international filenames. If the server does not support version 4, WebDrive will use version 3.

Cipher & MAC preferences: Select the desired encryption ciphers.

Use Zlib compression: Enable Zlib compression.

Enable file block I/O (random access): This feature enables random access/byte range transfer support for SFTP (stream download).

Site SFTP Host Key Settings Dialog Tab

To access the **Site SFTP Host Key Settings** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **General** menu, expand **Security** and click **SFTP Host Key**. Using the drop-down menu, select the **Client SSH Host Key** to use to connect to the SFTP server. You must first import the Host Key into the Host Key Store.

If you would like more information about Host Key Authentication, please see the [WebDrive Host Key Authentication Quick Start Guide](#).

Site FTP Settings Dialog Tab

Use the **Site FTP Settings** dialog tab to configure FTP specific settings. To access the **Site FTP Settings** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, expand **Connection** and click **FTP Settings**.

Host type: Allows you to select the FTP host operating system type. This is used for parsing directory listings. **Automatic Detect** works in most situations. If your directory listing appears empty, then select the server type manually for the particular site and reconnect. FTP servers return file listing information in different formats largely because different FTP servers support different information. When WebDrive retrieves file listing information from any given FTP server, it needs to dissect the information and extract only that information that is relevant to WebDrive. For **VMS Servers**, and other **non UNIX FTP Servers**, you should **explicitly select** the server type instead of using Automatic Detect. If you are using **Amazon S3[®]**: Amazon S3 does not have a concept of folders, but WebDrive uses the **S3** prefix/delimiter option to make it appear as folders with '/' as the delimiter. This allows you to create folders with WebDrive and put files into them. If your particular FTP server type is not listed, please send us an e-mail message so we can add support for it.

Server Time Zone: Select the time zone where the FTP server is located.

Password Encode: Configure how passwords are encoded.

List Options: Enter custom options for the **LIST** command sent to the server for listing directory contents.

Root Directory: Allows you to enter a directory that exists on the remote FTP site and treat that directory as the root directory for the mapped drive. After logging on, a **CWD** is performed to this directory.

NOTE: *The directory is case sensitive for FTP.*

Initial command: Allows you to enter custom FTP commands to perform after logon. You can separate multiple commands with a comma.

Account: If your FTP server requires an account, type your account information here.

Passive Mode (PASV): Transfers data in FTP passive (PASV) mode.

Keep Connection Alive: Attempt to keep connection to server alive by sending **NOOP**'s to the server. Not all protocols support this option. Generally you do not need to enable this option. If the remote server *times out* the connection and closes it due to inactivity, WebDrive will automatically reconnect to the server when it needs to communicate with the server.

Limit Local Port Range: To limit the Local Port Range, select the check box and type the minimum and maximum port numbers.

Site FTP Encryption Dialog Tab

Use the **Site FTP Encryption** dialog tab to configure FTP encryption settings. To access the **Site FTP Encryption** dialog tab, launch the WebDrive **Site Manager** and click **Properties**. On the **Properties** menu tree, expand **Security** and click **Encryption**.

Encryption Method: Select the SSL encryption method from the drop down list.

Secure data channel (PROT P): When enabled, this option secures the data connection with SSL in addition to the control connection.

Exploring the File Menu

The application's **File** menu has several options that can be used to configure WebDrive.

Program Settings: Displays the **Program Settings** dialog.

Export settings to registry file: Exports the settings used by WebDrive to a registry file so that they can be imported to another machine.

Import settings from a registry file:

Imports the settings from a registry file that was exported using the option above.

Create Desktop Shortcut: This option creates a shortcut on the desktop for the currently selected item. You can then double-click on the shortcut to connect to the site.

Exit Application: Exits the application.

Export Settings to Registry File

The **Export Settings** dialog can be used to save your application and site information to a registry file. This registry file can be imported on another machine. The registry settings file can also be imported by the setup application. This provides system administrators with a way to pre-configure the software when it is installed on each computer at the company.

To access **Export Settings**:

1. Select **File > Export settings to registry file**.
2. Select the check box to select **Export Site Database** to export the site/connection listings.
3. Select the check box to select **Export User Settings** to export the program settings
4. Type the **Filename to export to**, or click the **Browse** button to browse to the file.
5. Click **OK**.

Import Settings from a Registry File

The **Import Settings** dialog can be used to import a registry file that contains application and site settings information.

This feature is useful for transferring settings from one computer to another.

Importing settings from a registry file:

1. Select **File > Import settings from a registry file**.
2. Type the **Filename to import**, or click the **browse** button to browse the displayed files and then double-click to select the desired file.
3. Click **OK**.

Program Settings

Program General Settings

The **Program General Settings** dialog allows you to customize various program options. To access this tab, select **File > Program Settings**. From the **Program Settings** menu tree, select **General Settings**.

Basic Settings

Open Explorer after connecting: When selected, an Explorer window is opened when a drive is mapped to a site.

Open Explorer in folder view: Controls how the Explorer window is opened after a connection is established. If **folder view** is enabled, then the Explorer window will contain only one pane with the folder of files.

Run in taskbar tray at startup: Automatically starts the program after logging in and displays a tray icon.

Display [Drive Monitor](#) after connecting: When selected, the **Drive Monitor** dialog will be displayed after connecting to the server.

Use simplified Site Manager Dialog: Displays the **simplified Site Manager** dialog.

Prompt for password on failed logins: If the user's logon fails, the user will be prompted to type a password.

Display errors in popup dialog: When selected, a pop-up window will appear to provide error message information.

Always open Site Manager dialog on tray icon double click: When selected, this option will allow you to launch WebDrive's Site Manager by double-clicking the WebDrive tray icon.

Advanced Settings

Display custom drive icon in Explorer: Displays a custom drive icon in Explorer for connected drives. Turn this setting off to use the standard drive icon.

Automatically select drive to use: Automatically select the next available drive when connecting to server.

Set persistent drives to disconnected state at startup: Allows you to define persistent connections, but when the system starts these predefined persistent drives will not automatically connect. The persistent connections will show up in the Explorer window as disconnected drives. To connect to the remote server, double-click on the drive.

Disable shell column handlers: Windows 2000 and later editions of Windows have a feature called **Column Handlers**. The Column Handlers feature allows Explorer to add extra columns of information in addition to the file name. For example, this could include information such as the file author and other information about the file. This extra information is displayed when you click on a file in Explorer.

Disable DFS: Disables **distributed file system support** to increase performance of Microsoft Office applications.

Warning: Disabling DFS will prevent inbound Remote Desktop connections. A client attempting to connect to this system will get the error "the remote computer has ended the connection". You can enable DFS again to allow inbound **Remote Desktop** connections; however, you will have to reboot for the setting to take effect.

Enable delayed close for open files: This is a performance enhancement that keeps files open for a short time after the application closes it, in case the file is reopened. For example, files are often repeatedly opened and closed when data is being read from them.

Program Cache Settings

The **Cache Settings** dialog allows you to configure the amount of disk space to use, to select the cache folder where all cache files will be stored, and to clear the cache. The **bytes in use** is also displayed. To access this tab, select **File > Program Settings**. On the **Program Settings** menu, click **Cache Settings**.

Amount of disk space to use: Specifies the size of the **cache** in megabytes. Use the slider to select a percentage of the drive size or type a value in the edit box.

Cache folder: The folder where you will store cache files and directory listings.

Select folder: Click this button to browse to a folder

Clear Cache: Click this button to clear the cache.

Program Cache Options

To access this dialog tab, select **File > Program Settings**. On the **Program Settings** menu tree, expand **Cache Settings** and click **Options**. WebDrive has many caching options to improve performance. The various caching options can be configured from this dialog. **Single User Mode** is the default and provides the best performance. Once a file or directory listing is cached, it will not be removed from the cache until you connect again or flush the cache manually from the WebDrive tray icon or the Explorer right-click context menu. If you need to see new files that are created on the server, you can select **Custom mode** and configure the directory listings to expire, for example, every ten seconds.

Cache Mode: Select the cache mode.

- **Single User Mode** - This mode uses cache settings that will provide the best performance. It assumes that files and directory listings that are cached will not be modified by another user and will not validate the cached files with the server using the *files modified* time.

- **Multi-user mode** - This mode will validate cached files with the server to verify if they are up to date. This way, if a cached file has been modified by another user it will be detected and purged from the cache so that you will receive the latest copy of the file. DAV & SFTP servers allow WebDrive to easily get the modified time for a file or directory listing; however, most FTP servers do not support this. If your server does not support the MLST command, you may want to use the *Custom* cache mode and configure files to expire after a specified amount of time.
- **Custom** - This mode allows you to choose custom cache options.
- **None** - This mode disables file and directory listing caching. Files will still be temporarily cached so that applications that perform random access to the file data will work. But the next time the application opens the file, it will download a fresh copy from the server.

Cache Files: Save files in the cache folder for quicker access.

Validate Cache Files: Validates that a cached file is up to date by checking the modified time of the cache file with the modified time on the server. This works well for SFTP and WebDAV servers; however, not all FTP servers have the ability to determine the file date/time of a specific file. While this ensures that a file or listing is up to date, it does affect performance.

Expire cached files after (X) Seconds: Causes a file that has been cached longer than (X) seconds to be considered expired so that it will be removed from the cache when accessed and a new file will be downloaded from the server. Normally it is not necessary to enable this feature because WebDrive will automatically check to see if cache files are up to date before using them.

Cache directory listings: Store directory listings in the cache folder for quicker directory and file access.

Validate Cached Directory Listings: Validates that a cached directory listing is up to date by checking the modified time of the cache file with the modified time on the server.

Expire cached listings after (X) Seconds: Causes a directory listing that has been cached longer than (X) seconds to be considered expired so that it will be removed from the cache when accessed and a new directory listing will be downloaded from the server. Enable this setting if you want to see changes from other users without having to manually flush the cache.

Flush cache files on connect: When enabled, this feature will delete files in the cache at connect time. Normally it is not necessary to enable this option because WebDrive will automatically check to see if cache files are up to date before using them.

Flush directory listings on connect: When enabled, this feature will delete files in the cache at connect time. Normally it is not necessary to enable this option because WebDrive will automatically check to see if cache files are up to date before using them.

Program Proxy-FTP Settings

The **Program Proxy-FTP Settings** dialog is used to define the type of firewall/proxy server logon that is required for FTP sites. Some companies set up firewalls to prevent unauthorized access to local area networks that are connected to the Internet. To access this tab, select **File > Program Settings**. On the **Program Settings** menu tree, click **Proxy FTP**.

Proxy Type: Select the type of logon required for your firewall using the drop-down arrow. For all logon types except **USER no logon** (no logon to the firewall), the Firewall User ID is sent followed by the Firewall Password. If these entries are left blank, the Firewall User ID and the Firewall Password are not sent.

- **No Proxy Server:** Do not use a FTP proxy server.
- **SITE <site name>:** After logon to firewall, connect using **SITE <remote site name>**.
- **OPEN <site name>:** After logon to firewall, connect using **OPEN <remote site name>**.
- **USER after logon:** After logon to firewall, connect using **<site user name>@<remote site name>**.
- **USER no logon:** After connecting to firewall, connect to remote site using **<site user name>@<remote site name>**.
- **MS Proxy 2.0 (SOCKS v4.3a):** Use SOCKS protocol version 4.3. This is used by Microsoft Proxy Server 2.0, as well as the Internet RideWay Proxy Server. When the remote server is specified in domain name format, for example, **ftp.microsoft.com**, then the 4a extension to SOCKS will be used for the connect request.
- **SOCKS v5.0:** Connect to Socks Server using version 5 of the protocol. Currently the only supported authentication methods are username/password and no authentication. Many SOCKS Proxy Servers require you to use passive (PASV) mode when using SOCKS.
- **Raptor (Gwpasswd):** Used for Gwpasswd logon on a Raptor Proxy Server. The logon sequence is as follows: **USER remote_id@remote_host firewall_username, PASS remote_password, ACCT firewall_passwd**.

- **WinProxy 'SITE user@host':** Used by WinProxy Server when in gateway mode. This behaves the same as the server type **USER after logon**.
- **UserID=UserID@Site:** Used by Check Point and other firewalls. The format sent to the proxy server would be as follows, **USER FtpSiteUsername@ProxyUsername@FtpSiteURL**, then **PASS FtpSitePassword@ProxyPassword**, if no proxy username password is entered, it will not be sent.

Proxy server address: Enter the URL or IP address of your proxy server.

Port: Enter the port number for your firewall. The default port is 21. For SOCKS Servers, use port 1080.

Proxy server username: Some proxy servers require a user name. Leave empty if your proxy server does not require a user name.

Proxy server password: Enter the password for your proxy server, if required.

Program Proxy-HTTP Settings

The **Program Proxy-HTTP Settings** dialog is used to define the type of proxy server logon that is required for HTTP sites. To access this tab, select **File > Program Settings**. On the **Program Settings** menu tree, click **Proxy HTTP**.

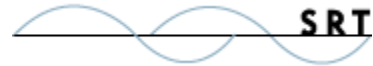
Proxy Type: Select the type of proxy server that you have using the drop-down arrow.

- **No Proxy Server:** Do not use a HTTP proxy server.
- **HTTP Standard (CERN):** This is the most common type of proxy server.
- **HTTP Tunnel:** This uses the HTTP tunneling protocol to establish a connection to the remote site.

***NOTE:** This is generally used for SSL proxies; however, you may find this option useful if the program does not work with the proxy server type set to CERN.*

- **HTTP Port Forwarding (SSH):** This method can be used for SSH port forwarding. It will connect to the specified address and expect the server to be listening on this port and to forward the connection to the desired remote server. F-Secure SSH client can be used under Windows to SSH encrypt communications.

***NOTE:** This can be useful if your server does not support SSL.*



Proxy server address: Enter the URL or IP address of your proxy server.

Port: Enter the port number for your proxy server. The default is 8080. Other common port numbers for HTTP proxies are 8888 and 8000.

Proxy server username: Some proxy servers require a user name. Leave this text box empty if your proxy server does not require it.

Proxy server password: Enter the password for your proxy server if required.

Program Logging Settings

The **Program Logging Settings** dialog allows you to log server command/responses to a file and to configure logging options. To access this tab, select **File > Program Settings**. On the **Program Settings** menu tree, click **Logging**.

- **Enable file logging:** Logs connection information to a log file. Select the check box to **Enable file logging**.
- **Folder to store log files in:** Select the folder where log files are stored. The log file name will be the name of the site with a .log extension. Click **Change Folder** to browse to a different folder.

General Options

- **Truncate log file on each connect:** When enabled, clears out the log file each time you connect to the server.

Detailed Options

- **Log informational messages:** When enabled, log informational messages will log significant non-error events where no user action is required.
- **Log verbose information:** When enabled, detailed information including the type of message, text of the message, the cause of the condition leading to the message, and any recommended action will be logged. You can enable verbose logging to help troubleshoot technical problems.
- **Log file I/O information:** When enabled, all file system calls to the drive will be logged, these include reads/writes/creates/closes, etc.
- **Log protocol traffic to server:** When enabled, protocol traffic to the server will be logged.
- **Log detailed protocol traffic to server:** When enabled, detailed information about protocol traffic to the server will be logged; including the date and time of the request, the number of bytes sent, and the action taken. Detailed protocol logging may be helpful to detect suspicious activity or certain hacking attempts.
- **Log debug information:** When enabled, the debug log file contains status and error messages useful for diagnosing errors and debugging.

Program Popup Window Errors Settings

Use the **Program Popup Window Errors Settings** dialog to configure the pop-up window to display file transfer status, serious errors, and synchronization status. The Pop-up window will display messages near the taskbar tray. To access this tab, select **File > Program Settings**. On the **Program Settings** menu tree, click **Popup Window**.

Enable Popup Window: Use the check box to enable the pop-up window for file transfer status and error information.

Popup Settings: Click **Popup Settings** to configure the appearance of the pop-up window and display options.

Program Backup Files Settings

Use the **Program Backup Files Settings** dialog to configure where backup files are stored if an upload failure occurs. WebDrive will create a backup of a file when an upload failure occurs so that you do not lose changes to documents. This is only done for DAV & FTP server types. SFTP & GroupDrive® use block file I/O and do not generally upload entire files. To access this dialog tab, select **File > Program Settings**. On the **Program Settings** menu tree, click **Backup Files**. Use the check box to enable **Backup files if upload fails**. Click **Select Folder** to browse to a folder.

Program Certificate Management

Use the **Program Certificate Management** dialog to configure and manage SSL certificates. To access this dialog tab, select **File > Program Settings**. On the **Program Settings** menu tree, click **Certificate Management**.

Use the browse "... " button to browse to the Certificate Store Folder; by default this folder is located under **My Documents**.

Click **Certificate Manager** to launch the WebDrive **Certificate Manager**. The **Certificate Manager** allows you to import and manage certificates.

Certificate Manager Options:

Delete: Deletes the selected certificate from the **Certificate store**.

Export: Allows you to export the selected certificate.

Sign CSR: Displays WebDrive's **Certificate Signing Wizard**, which allows you to sign a certificate request.

Properties: Displays certificate properties.

Create: Allows you to create a new certificate.

Import: Allows you to import a certificate into the **Certificate Store** to be used when connecting to a secure site.

If you would like more information about configuring and managing SSL Certificates, please see the [WebDrive Public Key Certificate-based Authentication Quick Start Guide](#).

Program Host Key Management

Use the **Program Host Key Management** dialog to configure SSH Host Keys for use with SFTP servers. To access this dialog tab, select **File > Program Settings**. On the **Program Settings** menu tree, click **Hostkey Management**.

Use the browse "... " button to browse to the Host Key Folder; by default this folder is located under **My Documents**.

Click **Host Key Manager** to launch the WebDrive **Host Key Manager**. The **Host Key Manager** allows you to import and manage host keys.

Host Key Manager Options:

Delete: Deletes the selected host key.

Export: Allows you to export the selected host key.

Properties: Displays host key properties.

Create: Allows you to create a host key.

Import: Allows you to import a host key into the host key store; to be used when connecting to a secure site.

If you would like more information about Host Key Authentication, please see the [WebDrive Host Key Authentication Quick Start Guide](#).

Advanced Topics

Amazon S3

Setting up the Site Manager for Amazon S3

WebDrive's Site Manager is used to add or edit site information, change program settings, and configure WebDrive. Sample sites may appear on the Site Manager after installation. You can edit or delete these sample sites.

Mapping a drive to an Amazon server:

1. Launch the *WebDrive Site Manager*.
2. Click the **New Site** button.
3. Follow the prompts in the Site Wizard to create a new site.
4. Click the **Connect** button.

Name: The name of this site. You can also rename a site by using this edit box.

Site Address/URL: The URL to connect to. For Amazon S3 users there are two options: The first option is to use the URL **http://s3.amazonaws.com**, which should show all buckets that you have access to in the root folder; then you can navigate to the buckets and treat them as folders. The second option is to root your drive in a bucket by using the following syntax **http://s3.amazonaws.com/mybucket** where mybucket is the name of the bucket you wish to use.

NOTE: To connect securely, use **HTTPS**.

Server Type: Select **Amazon-S3**.

Drive: Select the drive letter to map to the server.

Connect at login/startup: Enable this option if you want the drive to be automatically connected to the server when you logon to your computer.

Anonymous/Public Logon: Amazon-S3 servers do not allow Anonymous/Public Logon via the WebDrive interface. To allow public access to a file object, you must supply the URL to the user.

Username & Password: For Amazon-S3 servers, type your Amazon Access Key in the username box and type your Secret Key in the password box.

Connect: Connect and map a drive to the selected server.

Connect Offline: Select this check box to connect offline. You must first make the file and folder objects that you want to connect to offline available for offline access. To make the file or folder object available, select the object and use the WebDrive right-click context menu to select make available offline. You can manage offline files and folders using the WebDrive right-click context menu.

Properties: Displays the Site Properties dialog.

Help: Launches WebDrive Help.

New Site: Launches the WebDrive Site Wizard.

New Folder: This button creates a new folder in the site list, and allows you to group and organize multiple sites into a folder.

Delete: This button deletes the selected site from the site list.

Clone Site: This button creates a duplicate/clone of the currently selected site and allows you to rename it. This is useful when you have a site configured with custom settings that you want to duplicate for another site.

Save Password: Stores the password internally so that it is automatically entered for you each time.

Exit: Closes the Site Manager dialog.

Adding Folders in Amazon-S3

If you are using Amazon-S3: Amazon S3 does not have a concept of folders, but WebDrive uses the S3 prefix/delimiter option to make it appear as folders with '/' as the delimiter. This allows you to create folders with WebDrive and put files into them.

Creating a New Folder in Amazon-S3

In Amazon-S3 there are no actual folders, only "buckets". WebDrive uses a special syntax to make the S3 buckets appear as folders.

To create a new folder using Amazon-S3 you must either use the DOS prompt to create a new folder at the root level, or you can use Explorer to create a new folder in one of the existing buckets at the root level.

To create a new folder using Explorer, simply right click the existing bucket, which appears as a WebDrive folder, and select New>Folder.

To create a new folder at the root level using the DOS prompt, open a command prompt and type **MKDIR**.

In Amazon-S3, all bucket names have to be unique among all users. So when you are using Amazon-S3 with WebDrive, all folder names must be unique as well. For example, if you try to name a new folder "Docs" or "New Folder", it won't work. To create a root level bucket (which then appears as a WebDrive folder), you must name the new folder something unique, such as "MyNewTestBucketJohn".

Renaming Folders

To rename a folder in Amazon-S3, right-click the folder and select **Rename**. Type the new name and press **Enter**.

Offline File Access

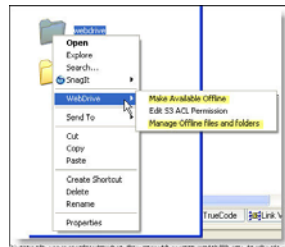
WebDrive allows you to access and work on documents offline. You do not need to be connected to the remote server; you can mark the documents as available for offline access and then synchronize your changes with the server the next time you connect to the remote server.

NOTE: To delete a file permanently you must be online to delete it.

Managing Offline File Access

You must first make the file and folder objects that you want to connect to offline available for offline access. To make the file or folder object available offline, select the file or folder and using the WebDrive right-click context menu, select **Make Available Offline**.

You can also use the WebDrive right-click context menu to remove a file's offline availability status. Select **Manage Offline files and folders**, and then select the file and click **Clear**.



When you want to connect in **Offline Mode**, launch the WebDrive Administrator program, and select **Connect Offline**. When you map a drive in offline mode; no connection to the server is established. Files that you marked *available for offline access* will be available to you. You will also be able to create new files and folders. You can synchronize your changes the next time you connect to the server.

If you would like to work offline after you have already connected online, you can use the WebDrive Site Monitor to go offline. To display the WebDrive Monitor, you can either double-click the WebDrive tray icon (found in the Windows taskbar) or you can right-click the WebDrive tray icon and select **Show Monitor**. To go offline, click **Site>Go Offline**.



Synchronization Settings

Use the **Site General Dialog Tab** to configure synchronization settings. To access Site General dialog tab, launch the WebDrive Site Manager and then click **Properties**. On the Properties menu tree, click **General**.

Synchronize Offline files at Connect time: Select this check box to synchronize all files marked as *Offline* with the server when you connect.

Synchronize Offline files at Disconnect time: Select this check box to synchronize all files marked as *Offline* with the server when you disconnect.

Amazon S3 Access Control List (ACL)

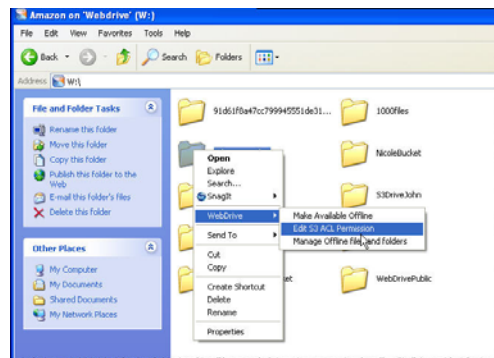
The **Access Control List (ACL)** is used to define other users' access permissions for your file and folder objects. The Access Permissions that you set using the ACL determine what a user can and cannot do with your file and folder objects. For example, you can set permissions on a file object to let one user read the contents of a file (read access) and let another user make changes to the file (write access). In Amazon S3 you will first add grants to objects and then set the permissions for the grant.

There are 4 types of grants:

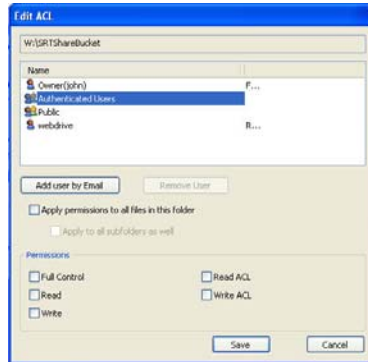
- **Owner** - defines the permissions the owner of the object has.
- **Authenticated Users** –all Amazon S3 storage users that have an account with S3.
- **Public** – any anonymous user that you have provided the URL to.
- **Email-ID** – an email address of specific S3 customers that have S3 accounts, not general public emails. The email given must match exactly the email address the S3 user signed up with and can only match one user account.

Displaying the ACL Dialog

To display the ACL dialog, right-click on a file in Explorer, and select **WebDrive>Edit S3 ACL Permission** from the context menu.



Editing the ACL



- To add a new user by email ID, click on the **Add User by Email** box to enter the email address.
- To remove a user, select the user and click **Remove User**.
- When selected, the **Apply permissions to all files in this folder** check box will apply the rights selected here to all file objects in the folder.
- When selected, the **Apply to all subfolders as well** check box will apply the rights selected here to all subfolders inside the folder. When you enable this option, a progress dialog box will be displayed.
- To select specific permissions on each grant, select the grantee in the list box, then select the various permissions. Click **Save** to write the ACL to the S3 server.

The permissions are as follows:

- **Full Control** – all permissions
- **Read** – read access to the object
- **Write** – write access to the object
- **Read ACL** – able to read the ACL for the object
- **Write ACL** – able to write the ACL for the object

Overwrites & Renames

The default setting on overwrites and renames is Preserve S3 ACLs on overwrites and renames. This setting is located under Properties>Connection>HTTP Settings. When enabled, WebDrive will preserve a file's Access Control List (ACL) when a user overwrites or renames a file.

Caching Options

Caching Explained

In order to provide quicker directory browsing and file editing, WebDrive caches both directory listings and files that are accessed on the server.

Caching Files

Some applications require that a file be cached on the local computer so that the application can access the file, for example, Word or MediaPlayer. Protocols like FTP and WebDAV do not provide for random file access, i.e., the capability to seek to a location within a file and read or write a small byte-range of data. However, Windows applications expect to be able to perform random access on a file. Therefore, when WebDrive receives a request from the file system to read a section of a file, it will download the entire file into the cache so that the Windows application will have full access to its contents.

Caching Directory Listings

It is usually advantageous for WebDrive to cache a directory listing so that when a user is browsing in Explorer and clicks on a folder, WebDrive can first check the cache and return the file listing from the cache before downloading a listing from the server, which can be a lengthy operation.

Caching Issues

One issue that can arise with caching is what happens if the file in the cache is out of date with what is on the server. Once a directory listing is cached by WebDrive, depending on your cache mode, you may not be able to see files in a folder that were uploaded by another user. Also, a file that was previously cached may be out of date if another user edited the file on the server. This is where the various caching modes of WebDrive can address these concerns.

Validating a cache file

When enabled, WebDrive “validates” files/listings in the cache by keeping track of a “files modified time”. When WebDrive downloads a directory listing or file into the cache, it records the modified time as reported by the server at the time it was downloaded. Then, when the files are accessed by the user in an application or Explorer, WebDrive will check with the server in real-time to see if the files modified time matches the cached version's files modified time. If the modified times match, then WebDrive will use the cached version and access will be quick. If the modified time does NOT match, then WebDrive will discard the cached version and download a new file or directory listing from the server so that it provides up-to-date information to the user.

Cache Modes

Single-User – In Single-User mode, WebDrive will act as if you are the only user accessing the server. This means that once a directory listing or file is cached, WebDrive will assume that the file is up to date. If a remote user uploads a new file to a folder on the server that was already cached by WebDrive, then the WebDrive user browsing the server in Explorer will not see the file unless they manually flush the cache. This cache mode provides the best performance and is the default mode selected after installation.

Multi-User – In Multi-User mode, WebDrive will “validate” files and listings that are cached with the server when they are accessed on the local system. This ensures that you are always seeing up-to-date directory listings and files. The drawback to this mode is that the validating process does take some time; however, it is fairly efficient, especially for SFTP and HTTP protocols. If you are using FTP, this cache mode can be problematic because most FTP servers do not have a way of reporting the modified time for a single file listing.

Custom – In Custom mode, you can fine-tune how and when files are validated with the server. The option **Expire cached files after (X) seconds** can be used when your server is unable to determine or report a files modified time. When this option is enabled, WebDrive will simply assume that after X seconds have passed, a cache file will be considered invalid and a new one will be downloaded from the server. This setting should only be used for FTP servers or special circumstances where determining the files modified time is not possible.

None – If you select **None** as your cache mode, files will always be downloaded from the server when accessed. A file in the cache will not be considered valid. When enabled, this mode is very slow and not recommended. In order to provide random access to applications, WebDrive must still cache files; however, once the application closes the file it will be marked invalid in the cache and downloaded again on the next access.

Frequently Asked Caching Questions

Q: Why can't I see a file that was added by another user?

A: You are probably using single-user cache mode. You can either switch to multi-user mode or manually flush the cache. You can use the WebDrive tray icon to manually flush the cache or you can use Explorer. To manually flush the cache in Explorer, right-click on a drive and select **Flush Cache** from the WebDrive context menu.

Q: Why does WebDrive download the entire file?

A: FTP/HTTP protocols do not provide for random file access, so WebDrive must cache the file. When **Block I/O** mode is enabled, SFTP provides random access.

Q: Why do files start downloading on their own while browsing in Explorer?

A: WebDrive never caches a file or folder listing on its own, an application is requesting to read the file or browse the folder. This often happens in Explorer by shell extensions known as *column handlers* or *icon handlers*. For example, it may be trying to extract an icon, or generate a thumbnail image of a JPEG. To minimize this, you can configure WebDrive to disable column handlers and icon handlers. See the *Program Settings* and *Site Properties* dialogs for details.

Q: I have disabled caching; why is it so slow?

A: When caching is not enabled, WebDrive is constantly downloading directory listings from the server while you are browsing in Explorer. If you would like to disable caching in WebDrive, it is best to keep **directory listing** caching enabled and only disable **files** caching.

Automating Connections/Disconnections

WebDrive allows you to map a network drive to a site in the following ways:

- From the **Application window** - select **Make a connection persistent**.
- From the **Site Manager** - select **Connect at login/startup**.
- **Program Command Line Options** - The application will accept a connection name as a parameter and perform the connection.

***NOTE:** This can be useful when you wish to automate a connection using a batch file. The connection name must be in quotes. For example **WebDrive.exe /s:"Microsoft"**. To disconnect you can specify the **drive letter** and **/d**, for example **WebDrive.exe X: /d** will disconnect **drive X:**.*

To disconnect a drive, you can use the **WebDrive.exe** command line option listed above, or enter the command **use X: /d** where **X:** is the drive letter you wish to disconnect.

Command Line Parameters

Each command line parameter is optional. If a parameter is omitted then the existing value will be used.

If the site name specified in the command line parameter does not exist, then a new site will be created in the registry. In this case, you will need to specify enough parameters to complete a valid connection, such as user name, password, and URL.

If a parameter value contains a space, you will need to enclose it in quotes, for example, **/s:"site name"**

- **/s:"sitename"** (The site name you wish to connect to; if this site does not exist then a new one will be created.)
- **/u:username** (The user name to use for connecting to the site.)
- **/p:password** (The password to use for connecting to the site.)
- **/url:url** (The URL to connect to.)
- **/pr:protocol** (FTP=0, WebDAV=1, FrontPage=2, GroupDrive=3, SFTP=4. For a FTP connection enter **/pr:0**)
- **/d:driveletter** (the drive letter to map to the site, for example **/d:W**)
- **/nosaveuserinfo** (When specified, the username/password are not recorded in the registry.)
- **/exp** (Launch an Explorer window after connecting to server.)
- **/service** (Map the drive in the **LocalSystem** process context rather than the current user's context. This allows system services like IIS to access the mapped drive.)

- **/ntservicecontext** (Tells WebDrive that the drive is being mapped by a different NT user than the one that created the specified site on the command line. WebDrive will then search the WebDrive site database for all users for the specified site. The first site found will be used.)
- **/lock:<filename>** (Takes out a DAV lock on the specified file; be sure to include the drive name, for example, **w:\hello.txt**)
- **/unlock:<filename>** (Removes a DAV lock on the specified file.)
- **/lockinfo:<filename>** (Displays lock information on the specified file.)
- **/cacheflush:<drivename>** (Flushes the file and directory cache. For example, WebDrive **/cacheflush:W:**)
- **/cacheflushfiles:<drivename>** (Flushes **file cache** only.)
- **/cacheflushdir:<drivename>** (Flushes the **directory listing** cache only.)
- **/flushandwait:<drivename>** (Flushes all files that are in the **delay close queue** and waits for them to upload to the server if needed. This is useful in scripting scenarios when before disconnecting the drive you need to flush files and wait, or during a script where you need to wait for an operation to complete on WebDrive before accessing the files on the server using a different access method.)
- **/online:<drivename>** (Switch to online mode, for example **/online:W:**)
- **/offline:<drivename>** (Switch to offline mode, for example **/offline:W:**)
- **/synch:<drivename>** (Perform a synchronization option on the specified drive.)
- **/job:"jobname"** (Run the specified file transfer manager job to perform a backup or synchronization task.)
- **/batch** (Suppress dialog prompts for some commands if an error occurs.)

Scripting or Batch Files

WebDrive can be used in a **batch file** to open a connection, copy files back and forth between the client and server, and then disconnect. The following batch file is an example of how to do this. This assumes that WebDrive was installed into the default directory of **c:\program files\webdrive**.

Windows Example:

```
ECHO "Running FTP batch file!"
start /wait /D"c:\program files\webdrive" webdrive.exe /s:"Microsoft"
copy x:\dirmap.txt c:\
start /wait /D"c:\program files\webdrive" webdrive.exe X: /d
```

Registry Settings

WebDrive stores its settings and connection database in the Windows registry. This makes it easy to export these settings into a registry file that can be quickly imported on another computer. The settings can be exported using WebDrive from the **File** Menu; or by using *regedit*.

Program Settings

The WebDrive program settings are stored under the registry key **HKEY_CURRENT_USER\Software\South River Technologies\WebDrive**. You can export this registry key and import it onto another computer so that WebDrive will be configured the same as on the PC that you exported from.

Site Database

The WebDrive site database is stored under the registry key **HKEY_CURRENT_USER\Software\South River Technologies\WebDrive\Connections**. Each site has its own key under this key which contains site settings such as site URL, site type, etc.

Automatic Setup of Registry Settings

You can manually import registry settings for WebDrive, or you can use WebDrive's automatic import feature to push settings to each user on a system, or to all users on multiple systems. This may be useful for system administrators who need to push out configuration updates to end user machines and have the updates applied without visiting each machine. There are two ways to take advantage of this feature. The first method is to set the registry key

HKEY_LOCAL_MACHINE\SOFTWARE\South River Technologies\WebDrive\RegImportFile to the name of the file you wish to import. This file can be either local to the machine or on a network drive/UNC location. Alternately you can place a file named **userdefaults.reg** in the program installation folder. (The default location is **C:\Program File\WebDrive** but the parameter **InstallDir** may be used to change this.) The file should initially be created by an export of the properly configured WebDrive program registry settings. Install WebDrive on a target system, define all the sites needed, configure all the application settings, and then export the registry keys to a **userdefaults.reg file**. The **userdefaults.reg file** can be edited with a text editor to customize as needed.

WebDrive's main program interface offers a **registry export** function under the **File** menu. This is useful for IT administrators that may have to install WebDrive on many different machines but would like to have all the sites and settings predefined.

Keep in mind that you may not want all settings exported and imported. Some registry settings, such as cache folder, etc., are often tied to **My Documents**, and these settings may change from system to system. You can use a text editor to edit the **.reg** file and remove any settings that contain a path in them, or if you wish to use the same path for all users, you do not need to change these settings.

This registry file will typically contain settings that are stored under the **HKEY_CURRENT_USER** key; however, other keys can also be imported as long as they conform to the **regedit** file format. The file must be in ASCII format, not Unicode format. The file is imported when WebDrive is used by each NT user on the system. A recorded time stamp is used to determine if changes have been made to the **userdefaults.reg** file since the last execution of the program. If the time stamp of the file is more recent than the recorded time stamp, the **userdefaults.reg** file is imported. This is useful to propagate information to all NT users on the system after the install has been completed. If you use the registry setting **RegImportFile** to specify a registry file on a network drive or UNC path, it then becomes very easy to replicate settings to all your users, simply edit the global **userdefaults.reg** file and the next time the user runs WebDrive it will import the new settings.

Settings that are imported are overlaid on top of any existing settings for WebDrive; however, there is a special action that you can place in the registry file so that WebDrive will delete the existing site database and use the new one. To do this, place the following line early in the registry file, before any settings. Place it in a comment field exactly as shown:

```
;wdAction=Overwrite
```

Using Regedit

Windows ships with a registry utility named **regedit.exe**.

To run **regedit**:

1. Select the **Start** menu.
2. Select **Run**.
3. Type **regedit**.
4. Click **OK**.
5. Select the **key** you wish to export.
6. Select the **Registry menu**.
7. Select **Export Registry File**.

NOTE: To import a registry file you can use **regedit** or simply execute the registry file.

UNC - Universal Naming Convention

WebDrive® has limited support for UNC. Universal Naming Convention is a name format used to refer to files on a network share. For example: instead of `c:\dir1\dir2\file.txt`, UNC follows the format `\\servername\share\dir1\dir2\file.txt`.

To refer to a UNC file in WebDrive, you would replace **server name** with **WebDrive** and **share** with the **site name** that you defined in WebDrive.

You can refer to files in UNC fashion as long as the connection to the server is already established; for example, if you are connecting to the connection Microsoft (ftp.microsoft.com), with drive letter X:. To do a **dir** using UNC from a DOS prompt, you can type the command

DIR \\WebDrive\Microsoft. To map a file you can type [\\WebDrive\Microsoft\dirmap.txt](#).

NOTE: If you are using Windows Server 2003 (or any later version) or a terminal server, then the UNC name will also contain the currently logged on user. For example, using a site name of "MySite" and a currently logged on user with a name of "john", the UNC name would have the following format: `\\WebDrive-john\MySite`. Therefore, the generic syntax is: `\\Server-ntusername\SiteName`

To disable adding the NT username to the server name behavior, edit the following registry key: `HKEY_LOCAL_MACHINE\Software\South River Technologies\WebDrive\DisableTerminalServer`. Set this value to **1**.

Setup Options

WebDrive® Installer

The WebDrive installation program is a Windows installer MSI file that is wrapped with an InstallShield 11.0 bootstrap loader. For most situations you can simply run the setup package. However, for advanced users it is possible to unpackage the setup program and extract the MSI file so that it can be customized if you are familiar with MSI files and packages and transforms. IT administrators are familiar with MSI files because MSI files are useful for doing remote and unattended installations for network users. There are many ways to customize MSI installs. We will include a few of the basic options for customizing the installer. For more information on editing MSI files and creating transforms, see Microsoft's Orca MSI editor <http://support.microsoft.com/kb/255905/EN-US/>

Unpacking the Setup

You may want to unpack the WebDrive setup package to get access to the Windows installer MSI file or modify the installation process. The easiest way to get an unpackaged version of the setup program is to obtain a CD or ZIP version from [South River Technologies](#). Alternatively, you can unpack the setup package by running the setup in *Administrator* mode. You can use the `/a` command line option to do this, for example, `webdrive.exe/a` In Administrator mode the install will unpack the setup package to a directory that you choose; it will *not* install the program on the target system. However, when you unpack using Administrator mode, this version will not have the setup.exe bootstrap loader, which is required unless you are planning on using **MSIEXEC** to launch the setup.

Once you have customized the unpackaged version of the setup, you can either run it as is or you can repack it into a self extracting single executable file. You can use XP's built in utility **iexpress.exe** to create a self extracting executable, or WinZip, or any other third party utility.

Silent Install

To run the standard installer in silent mode so that no user interface is displayed, you can use the following command line parameters for the main setup executable:

```
Setup.exe /s /v"/qn REBOOT="ReallySupress""
```

The `/v` parameter passes information that follows to the MSIEXEC program, `/qn` suppresses the UI. The **REBOOT="ReallySupress"** option disables a reboot that may occur if this is an upgrade and files were in use at the time of installation. For full details on MSIEXEC command line options please refer to the Windows installer documentation.

Using MSIEXEC

The WebDrive MSI file can be run directly by using **MSIEXEC** instead of using the **setup.exe** bootstrap loader. However, it is more complex because the parameters for performing a clean install (installing WebDrive on a system that is has never been installed on) or performing an upgrade are different.

Installing on a clean system:

```
msiexec /i Webdrive.msi
```

Installing an upgrade:

```
msiexec /i Webdrive.msi REINSTALL=ALL REINSTALLMODE=vomus
```

Advanced Parameters for MSIEXEC:

Parameters	Description
/qn	Silent install; do not display user interface.
SETUPEXEDIR=c:\pathtomsi	Used to define the location of the MSI file; this is required if an appsetup.ini file is also located in the same folder as the MSI file and you want the setup to parse and process it.
REBOOT=ReallySupress	Suppress the reboot dialog at the end of installation. Reboot may still be required.
WDPROP_REGCODE="55-4341"	Pass a regcode to the install.
WDPROP_INSTALLOPTIONS="512"	Same as LicenseActivate=1 in an appsetup.ini file. This will activate WebDrive during the install using the specified regcode.

Example command line: msiexec /qn /i z:\temp\Webdrive.msi REINSTALL=ALL REINSTALLMODE=vomus SETUPEXEDIR=Z:\temp\ REBOOT=ReallySupress WDPROP_REGCODE="55-31" WDPROP_INSTALLOPTIONS="512"

Using WebDrive® from an NT Service

You can use drives that are mapped by WebDrive in NT services; however, there are several issues that you should be aware of. Normally when you map a drive letter to a server the drive letter can only be accessed by the NT user process that has mapped the drive.

For example:

You are logged on to the NT system with a user account of "john" and you map drive letter **W:** to any server. After mapping the drive you can use drive **W:** with Explorer, or a DOS prompt, or applications that you run under the same NT logon session that you created drive **W:** with. However, by default, most NT services do not run under a normal NT user account, but instead run under the **LocalSystem** account. This **LocalSystem** account is a built-in NT account that is not associated with a normal NT user account. Since the NT service is run under a different NT process, it cannot see or access the drive **W:** that you mapped from the NT user account "john".

The site database for WebDrive is stored in the registry under the key **HKEY_CURRENT_USER\Software\South River Technologies\WebDrive\Connections**. Each NT user will have a site database under the user's specific **HKEY_USER** tree.

There is more than one way to enable NT services to access WebDrive mapped drives. (Of our two examples, Example 1 is less complicated.)

Example 1

Enable the **Allow services to access mapped drive** setting on the site properties/advanced dialog tab. When this setting is enabled and you connect to the site, the drive will be mapped under the NT **LocalSystem** account rather than the currently logged on NT user account. This enables services to access the mapped drive, either by drive letter or UNC (Universal Naming Convention) format. If you are using this setting you may also want to enable the companion setting **Connect drive at system startup** so that when the computer boots it will map the drive letter without having to log on to the NT system. This is useful for unattended server operation. When you enable the setting **Allow services to access mapped drive**, WebDrive stores the site information under **HKEY_LOCAL_MACHINE** in addition to the **HKEY_CURRENT_USER** tree. This allows the service to access the registry settings without having the NT user context.

Example 2

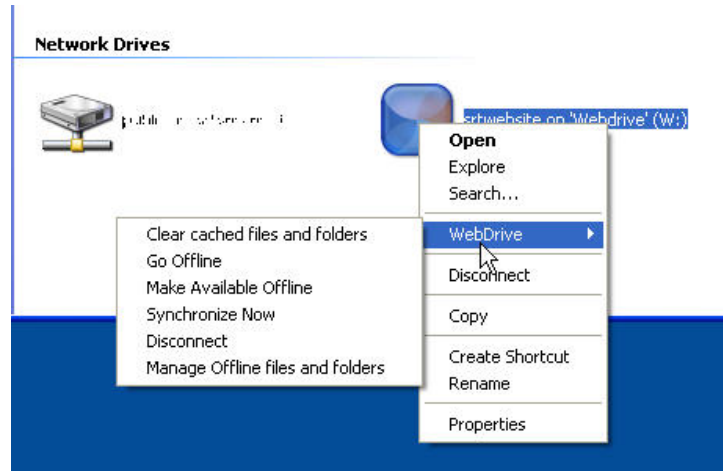
Map the drive from the NT service using [Command Line Parameters](#). This will map the drive in the NT context that the service is running in. One thing to keep in mind when using command line options from an NT service is the NT user context. WebDrive stores site information such as URL, username/password, etc., in the registry under **HKEY_CURRENT_USER**, which is different for each NT user account. Therefore, if you defined your WebDrive site information while logged onto the NT system under the NT user account of "john", then only processes logged in under the NT account "john" would have access to the site information. If the NT service is run under the same NT account where you defined the site information, there is no problem. If you want to use the command line option to map a drive and still use the drive by a service, then add the command line parameter **/ntservicecontext** which will allow you to use a standard WebDrive site that was created under a logged in NT user and additionally, map the drive in another context.

Shell Extensions

WebDrive Menu

WebDrive has a **shell extension** to provide a context menu for connected drives. To display the **context menu** from **Explorer**:

1. Select a drive, folder, or file that is mapped.
2. Right-click the mouse button and then Click **WebDrive**.



The context menu will only appear for drives, folders, and files that are currently mapped by WebDrive. The menu has the following options:

Clear cached files and folders: Removes the directory listings and files that are cached for the selected drive. It will not remove caches for other connections.

Go Offline: Work offline after you have already connected online. This option will disconnect you from the server. Files marked available for offline access will be available to you. You will also be able to create new files and folders. You can synchronize your changes the next time you connect to the server. To delete a file permanently you must be online to delete it.

Make Available Offline: Marks a file or folder as available for offline access. This will cause the file to be cached so that you can later access the file while not connected to the server.

Synchronize Now: Immediately synchronizes your files with the server.

Disconnect: Disconnects from the server.

Manage Offline files and folders: Remove a file's offline status.

Lock Property

The **Lock** tab dialog allows you to lock or unlock a drive, folder, or file and examine the lock status of a file. This is only available for DAV connections.

To access the **Lock Property** tab, right-click the drive, folder, or file and select **Properties**, and then select the **Lock** tab.

Cache Property

The **Cache Property** tab can be used to manage a drive that is mapped to a server. To display the **Cache Property Page**:

1. Select the drive icon from Explorer.
 2. Right-click on the drive to display the context menu.
 3. Select **Properties** from the menu and then select the **Cache** tab. The **Cache Property** tab will be displayed..
- **Clear Cache:** Removes the directory listings and files that are cached for the selected drive. It will not remove directory listings for other connections.
 - **Synchronize Now:** Immediately synchronizes files marked as **Offline** with the server. To delete a file permanently, you must be online to delete it.

Permissions Property

The **Permissions Property** tab allows you to examine and change file attributes for files that are on the FTP or SFTP server. This feature is only available on UNIX SFTP Servers and FTP Servers that support the [CHMOD](#) FTP extension.

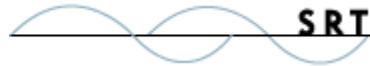
NOTE: *This feature can be useful when working with [CGI](#) and [PERL](#) scripts when you need to set the **execute** and **write** privileges.*

To display the Permissions Property tab:

1. Using **Explorer**, select the **file** you wish to examine.
2. Right-click on the **file**.
3. Select **Properties** from the menu. The **File Properties** page will be displayed.

To change the attributes for a file:

1. Select the **attributes** that you want, the CHMOD value will be calculated automatically.
2. Click the **OK** or **Apply** button to send the CHMOD command to the server.



File Transfer Manager

The WebDrive **File Transfer Manager** can be used to back up or synchronize remote folders or entire Web sites. To access the **File Transfer Manager**, launch the WebDrive **Site Manager**. On the **Utilities** menu, click **File Transfer Manager**. The WebDrive **File Transfer Manager** will launch. Click **New** or click the **File Set Name** to launch the **File Transfer Wizard**.

Use the File Transfer Manager to:

- Perform full or incremental backups for local files or folders to a server.
- Synchronize files and folders between your local computer and your server.
- Download files/folders from your server to your local computer.
- Schedule backup or synchronization jobs to run periodically or at specific times.

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.