TOC

Welcome to WebDrive 2018! **4**

What is WebDrive? 4

Where do I get Started? 4

I Need More Help! 5

Quick Start 5

Installation Notes 6

Activation 7

Contact Us 7

Administrator 8

Sites 14

Buckets 17

Folders 18

Setting up a custom S3 site 18

Amazon S3 Access Control Lists 18

Displaying the ACL Dialog 18

Editing the ACL 18

Overwrites & Renames 19

Program Settings Overview **20**

Settings 20

Transparency 24

Duration 24

File Transfer 24

Cache Settings 29

Backup **33**

File Transfer Manager 34

Properties Overview **35**

General Host Settings 35
Connection Settings 36
Server 38
Security 39
Advanced 39
Advanced Options 40
Basic File Settings 43
Cache Settings 51
Features **55**
WebDrive Site Manager 55
Collaboration 55
Security Features 55
Offline Access 55
File Transfer Manager 55
Legacy Support 56
Internet Enable any Application 56
Advanced Features 56
FIPS Compliance 57
WebDrive Menu 58
WebDrive with an NT Service 60
Example 1 60
Example 2 61
Automating Connections and Disconnections 61
Command Line Parameters 61
Registry Settings 63
Setup Options 65
Scripting or Batch Files 67
UNC 67

WebDrive with Windows NT 68

Help **70**

FAQ 70

Report Issues 72

Contact Us 73

System Requirements 73

Welcome to WebDrive 2018!

What is WebDrive?

WebDrive is a proprietary file transfer software engineered to connect you to all of your files, wherever they are, in the simplest and most secure way possible.

WebDrive allows you to connect to FTP, WebDAV, SFTP, Amazon-S3, GoogleDrive, Dropbox FrontPage, and other file servers using a LAN or Internet connection. You can then map a Network Drive to the server and treat the FTP/DAV/FrontPage Server as if it were a hard disk on your system.

Drag and drop files or copy files to and from the server using Windows Explorer; or use familiar DOS commands such as copy and xcopy. WebDrive FTP or HTTP enables any application instantly by integrating the server site into the Windows file system.

WebDrive uses industry standard Transport Layer Security (TLS 1.2) and SFTP to ensure secure transmission of your files.

WebDrive can provide S/Key password encryption so passwords can't be read during transmission.

WebDrive supports WebDAV protocol, which allows you to lock files, change the files, and then release the locks to allow other users to review and update the information.

Where do I get Started?

Once you've downloaded WebDrive from **WebDrive.com**, take some time to:

- Get started by Launching WebDrive
- Familiarize yourself with the Administrator
- Learn to Sites

- Take a look at WebDrive's **Features**
- See our important **Installation Notes**

Or skip to our **Getting Start** Quick Guide.

I Need More Help!

Can't find what you need in this help? Check out our open knowledge base, or submit a ticket if you have a support subscription, **at our support desk**.

Quick Start

Launch WebDrive

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

> If you started with a **trial** version and would like to access the **full product**, see our topic on **Activation**.

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.

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.

> See our topic on the **Tray Icon**.

Connect Sites

To set up a connection to a server, create a site profile by clicking on the new server toolbar button. This will launch the site wizard, which will allow you to setup a new connection.

> See our topic on **Sites**.

Once you have successfully connected to a remote server, an Explorer window will launch to allow you to navigate the newly mapped drive and access your files.

To manually connect a site, enter the WebDrive console and either double-click an unconnected site profile or right-click and select Connect from the context menu.

Disconnect Sites

To manually disconnect a site, enter the WebDrive console and either double-click a connected site profile or right-click and select Disconnect from the context menu.

Import/Export Sites

If you have previously configured a site profile and would like to import it to get the site set up more quickly:

1. Create a site profile using the correct protocol.
2. Right-click the site in the administrator and select Import Site Profile from the context menu.
3. Type or browse for the file path to your saved site profile.

You can also export a copy of your configuration settings:

1. Right-click the site in the administrator and select Export Site Profile from the context menu.
2. Type or browse to the location where you want the file to be stored.

Access Files

Once you are connected to the server, you can navigate the site with Explorer or a DOS command prompt. Copy files with the copy keyboard shortcut 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 disconnect from the site manager by right clicking on the connection and selecting disconnect.

Installation Notes

To **install** WebDrive, you must be logged on with the user account that has administrative rights. Once installed, you can use WebDrive from any user account.

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

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

Activation

To activate WebDrive and convert it from a trial version into a full version:

1. Enter your registration code on the Activation dialog. To access the Activation dialog, display the App Settings dialog and select "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:

1. Uninstall WebDrive to deactivate the license.
2. Reinstall WebDrive on the other computer, and reactivate using the same registration code.

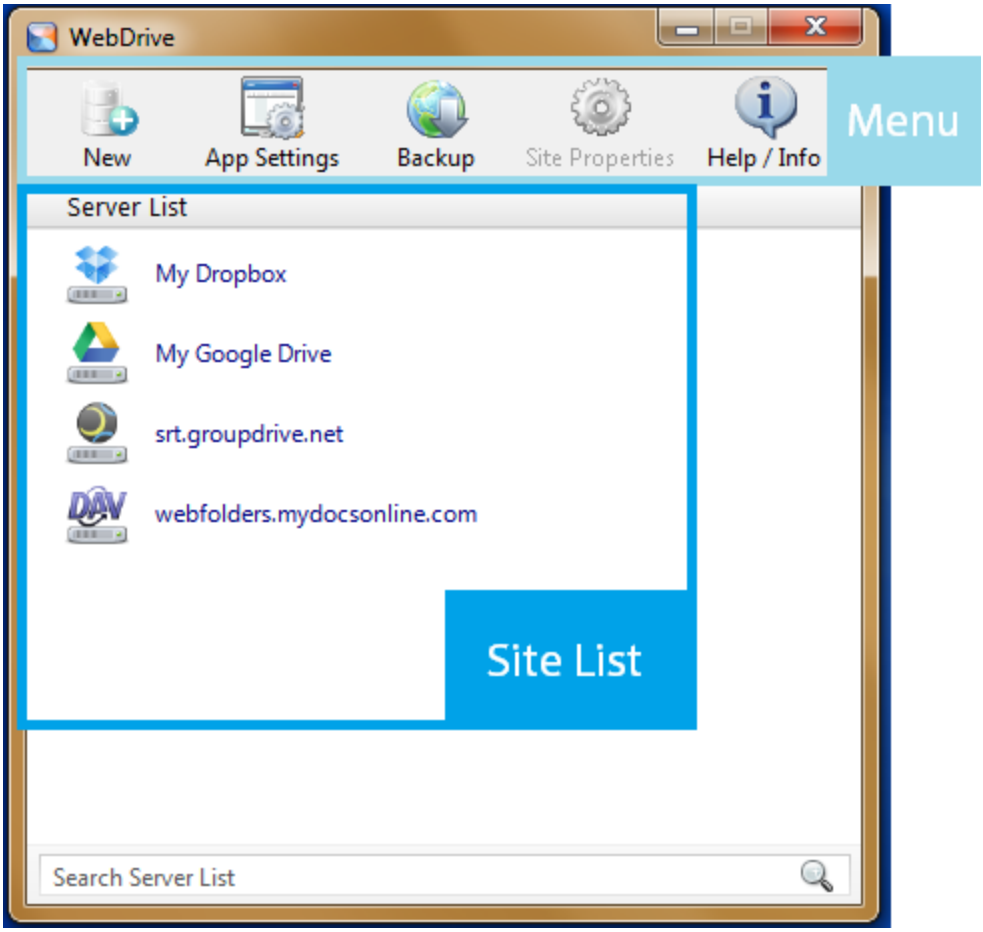
Contact Us

South River Technologies is headquartered in Annapolis, Maryland. We are also conveniently located just 2,461 miles from the heart of Silicon Valley.

Corporate Headquarters Address	South River Technologies 1910 Towne Centre Blvd Suite 250 Annapolis, Maryland 21401 USA
Toll-Free	1-866-861-9483
Main	443-603-0290
Fax	410-266-1191
Website	www.webdrive.com
Email	sales@southrivertech.com
Support Inquiries	support.southrivertech.com

Administrator

When you launch WebDrive, you will see the administrator window. Take some time to explore your administrator console. From this window, you can view and configure administrator and site settings and back up your sites.



For more information on the Site List, see our topic on **Sites**.

Menu Bar

The **Menu** bar, also known as the toolbar, gives you access to the most important WebDrive functions.

New: This launches the **Site Wizard**, which will take you through the steps to connect to a remote file repository.

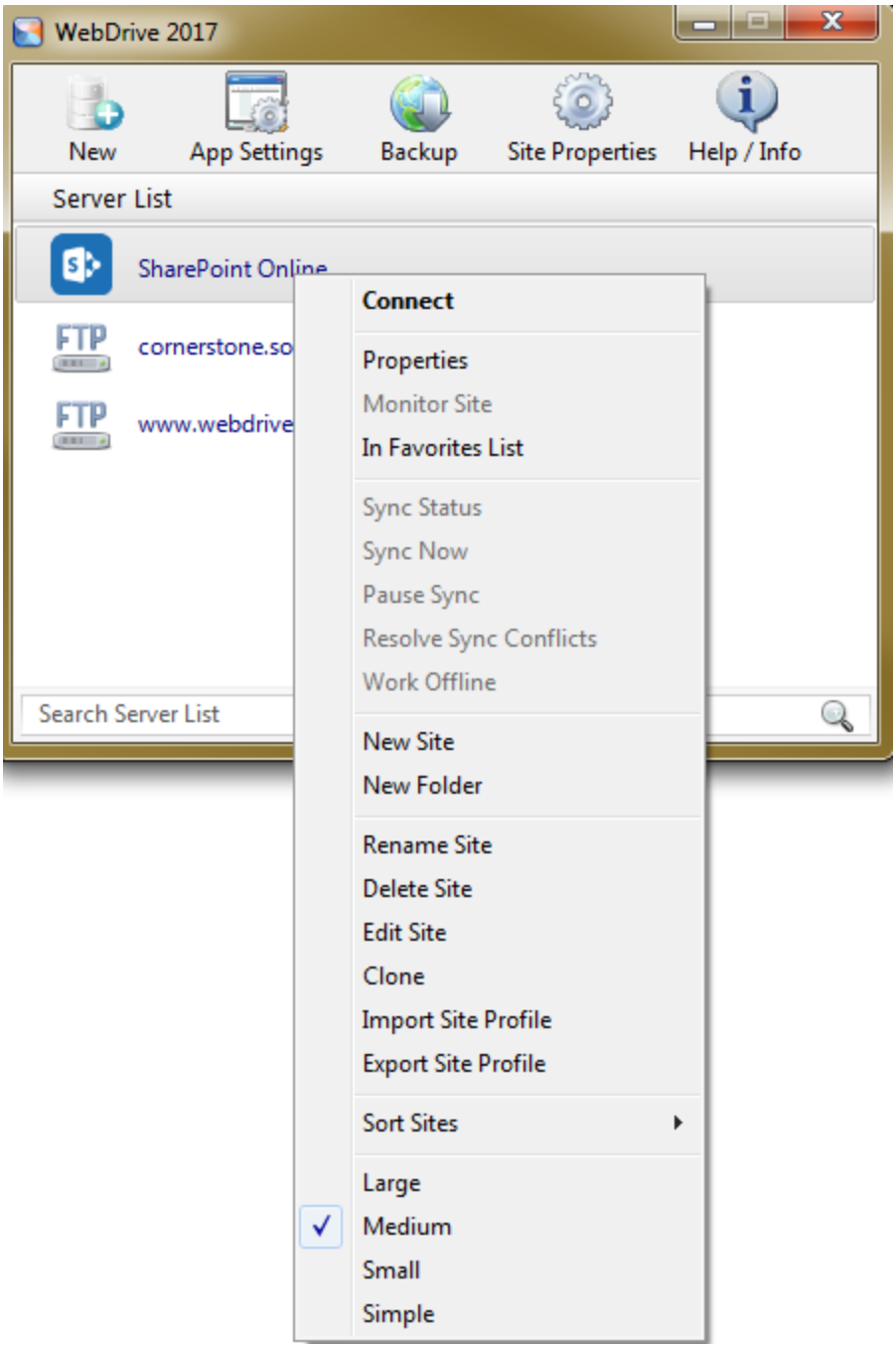
App Settings: This opens a **Program Settings** dialogue, which allows you to configure WebDrive-wide settings.

Backup: This opens the **File Transfer Manager**, which contains a list of current backups which you can then edit. You can also create or schedule new backups, or synchronize with the remote server.

Site Properties: This brings up a **Properties** dialogue with configuration options specific to the site selected in the WebDrive administrator.

Help/Info: You are **here**! Can't find what you need in the topics? Check out or **FAQ**, or visit our online **Knowledge Base**.

Context Menu (Right-click Menu)



Connect/Disconnect: This will connect to a site if you are currently disconnected, or disconnect if you are connected. When disconnected, you will not be able to see current directories. You can set files for caching in offline mode, however. You may need to disconnect and reconnect to a site if you make changes to the site profile settings.

Properties: This will open the Properties Setting window, where you can adjust the settings for this site profile.

Monitor Site: This option opens the WebDrive **Monitor** and shows the recent connection and logging information for this site in easily-readable format.

In Favorites List: Toggle setting to add this connection to your list of Favorites. Favorites are accessible through the right-click menu on the system tray icon. This is a quick way to access Favorite connections via the system tray icon.

Sync Status: This option only shows when the site profile is not connected. Otherwise it will provide the current status of any ongoing sync. When everything is up-to-date with the server, this will say Sync Complete.

Sync Now: Initiates an immediate sync between WebDrive and the server. This is useful if a user is not seeing file updates.

Pause Sync: Pauses an ongoing update. This is useful if the sync is taking too long or using too many resources, or if a user needs to go offline and wants to complete the update later.

Resolve Sync Conflicts: Choose which version of a file to keep when the local and server files are out of sync. For instance, if a local file has the same name as a file on the server. Also, when returning to online mode after working offline, cached files may have been updated by another user in the meantime. WebDrive will work through these conflicts by asking if the user would like to keep their version, the old version, or both.

Work Offline: When the site is connected, you can cause the site profile to go into offline mode. Your cache and sync settings will determine which files are available when in offline mode. These files will not be live, so adjust your settings to account for overwriting previous changes.

New Site: Launch the New Site Wizard, to create a new site profile.

New Folder: Create a new folder, where you can place site profiles for organization purposes.

Rename Site: Give the site profile a different name, for easy cataloging.

Delete Site: Delete the selected site profile. You will lose all settings unless

Edit Site: Opens the Site Wizard to allow you to change the settings of the site profile, including protocol used.

Clone: Create another site profile that is an exact copy of the one selected.

Import Site Profile: This will allow you to take a pre-existing site profile's settings and apply it to a new site profile in WebDrive.

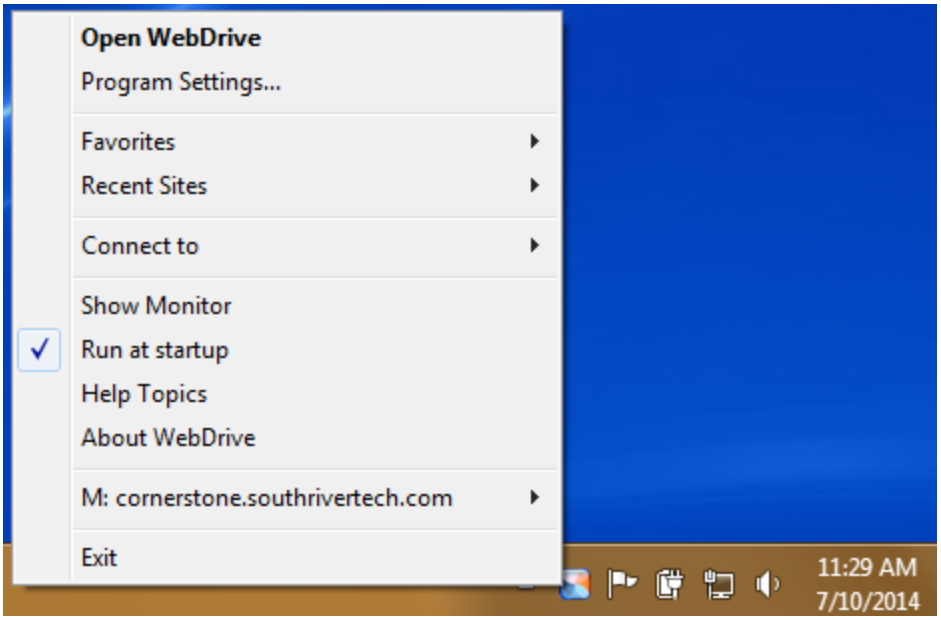
Export Site Profile: This will save the settings for this site profile so that it can be transferred to another WebDrive.

Sort Sites: This will rearrange the order of your site profiles in the WebDrive administrator alphabetically, if chosen. If None is selected, the order will remain the same, with new sites added to the end as they are created.

Large/Medium/Small/Simple: Adjust the size and style of the icons as displayed in the WebDrive administrator.

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.

Favorite Sites: Within the WebDrive Administrator, right-click a site and select In Favorites List. This will add this site to a quick list you can access by right-clicking the WebDrive Tray Icon and hovering over the Favorites menu item. To remove a site from this list, clear the whole list from the same Tray Icon menu, or right-click on the site you would like to unfavorite in the administrator and deselect In Favorites List.

Recent Sites: Displays a list of site profiles most recently connected.

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, which allows you to open an up-to-the-second list of ongoing transfers on your active connections.

> See our topic on the WebDrive **WebDrive Monitor**.

Run at Startup - Selecting this option enables the tray icon to launch WebDrive at desktop login.

Help Topics - Launches WebDrive Help files (you are here).

About WebDrive - Provides you with the Program Version Number, Registration Code, License Type, Product Registration Date, Upgrade Status, and Registration Status.

Exit: Closes the WebDrive administrator and disconnects all sites.

WebDrive Monitor

The monitor feature of WebDrive allows you to view ongoing activity on your sites. Open the monitor window in one of two ways:

1. Right-click the WebDrive tray icon found in the Windows taskbar. Select Show Monitor.

> See our topic on the **Tray Icon**.

2. Select the site in the Server List and right-click to bring up the context menu. Select Monitor Site.

Once launched, the Monitor dialogue will show an ongoing feed of activity between the client and the server. To display a dropdown menu of Monitor options, click the Site button.

Open Explorer: Launches a Microsoft Explorer window.

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.

Sync Now: Performs immediate synchronization to the server.

Work Offline/Go Online: Toggle online or offline work. While offline, the connection for this site will be terminated, but you can access cached files.

> See the our topic on **Cache Settings**.

Log:

Clear Log: Click this button to clear the Monitor's log events listing.

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.

Launching WebDrive

After installing the WebDrive software, you will notice a tray icon located in your Windows task bar tray area.

Launch WebDrive

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.

See our topic on the **Tray Icon**.

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.

Sites

What is a site?

A **site** is the term WebDrive uses to refer to a connection to a file repository, usually a server. The site profile contains all configurations set for a specific connection, many of which can be changed by using the Site Properties menu button.

See our **Properties Overview**.

Managing Sites

WebDrive's main administrator console is used to add or edit site information.

For more information on the administration console or menu options, see our topic on the **Administrator**.

Server List: The administrator displays a list of all site profiles you've configured. This includes all different protocol types, indicated by the icons to the left of each site.

Search Server List: You can filter the list of sites displayed by entering a search string in the search window located at the bottom of the site manager window. If any site name has the string you entered it will be displayed in the list, to cancel the search click the close button located to the right of the search edit window.

Double-click on any site in the WebDrive Administrator's list to connect to the remote server. You can also right-click a site and select "Connect" from the menu.

To **edit** a site profile that has already been defined, right-click the site in the list and select "Properties" from the menu. If you want to re-run the New Site Wizard to configure base settings, select "Edit Site" from the menu.

You can organize your sites into **folders**. To create a new folder, right click in the site manager and select "New Folder" from the menu. Then drag and drop the sites you want to store into the folder.

Import/Export Sites

If you have previously configured a site profile and would like to import it to get the site set up more quickly:

1. Create a site profile using the correct protocol.
2. Right-click the site in the administrator and select Import Site Profile from the context menu.
3. Type or browse for the file path to your saved site profile.

You can also export a copy of your configuration settings:

1. Right-click the site in the administrator and select Export Site Profile from the context menu.
2. Type or browse to the location where you want the file to be stored.

Connectors

WebDrive includes protocols for transferring to offsite data or a Cornerstone server.

- FTP/S
- SFTP
- HTTP/S
- WebDAV

WebDrive also has these proprietary connectors:

- Amazon S3
- Amazon Cloud Drive
- Box.com
- Dropbox
- Google Drive
- OneDrive
- OneDrive for Business
- Sharepoint (via WebDAV)
- Sharepoint Online/Office 360

For more information on the settings specific to these connectors, see the **General Host Settings** topic.

Site Wizard

The site wizard will walk you through the process of creating a connection to a remote file repository. After a site has been created, you will be able to upload and download files from your WebDriveclient freely, according to your permissions.

1. Select your server protocol type. WebDrive supports HTTP, WebDAV, FTP, and SFTP, and connects to Google Drive, DropBox, Amazon S3, Amazon Cloud Drive, FrontPage servers, OneDrive and OneDrive Business, Box.com, SharePoint, and Cornerstone MFT.
2. You'll need to enter login credentials for each type of protocol, each of which require different information. You should be able to get this information from your network administrator.
3. Enter a unique name for the site. This is for identification purposes and can be anything you'd like.
4. Select a unique drive letter to map this site to. Never assign multiple site profiles to the same drive letter. If you would like this site to connect automatically when your desktop loads, enable Connect at login/startup.

Note: WebDrive now allows you to root to a specific folder with the **SharePoint Online** connector by simply entering the URL. You do not need to enter extra path/subfolder information in the URL when initially connecting. For more information, see the **General Host Settings** topic.

Import/Export Sites

If you have previously configured a site profile and would like to import it to get the site set up more quickly:

1. Create a site profile using the correct protocol.
2. Right-click the site in the administrator and select Import Site Profile from the context menu.
3. Type or browse for the file path to your saved site profile.

You can also export a copy of your configuration settings:

1. Right-click the site in the administrator and select Export Site Profile from the context menu.
2. Type or browse to the location where you want the file to be stored.

Amazon S3

The easiest way to connect to your Amazon S3 Simple Storage account is to create a new Site in WebDrive and select "Connect by Service Type" in the new Site Wizard.

When you do this the URL is automatically selected and all you need to enter is your Amazon Access Key and Secret Key. You can also create a standard site and enter the URL for amazon storage your-self if you would like.

Note: When using **Amazon S3** as your connector, **Multi-User cache settings** will not function correctly because the directory's modified-time metadata will not be updated by Amazon. Therefore, files will fall out of sync, and users may interfere with each other's alterations on a common file.

Solution: If you are not using **Single User mode**, you will need to navigate to the Basic Cache Settings tab of the Properties for your S3 site and set your mode to **Custom** and enable **Expire cached files after (x) seconds** and **Expire cached listing after (x) seconds**.

Buckets

The Amazon S3 simple storage service will store all your files in Buckets. Bucket names are unique across the entire S3 storage space so choose your names carefully as many common things you would like to use to call a bucket is already taken. By default when you map a drive to your S3 account you will see all your buckets at the root level of the drive. If you wish to root your drive on a specific bucket then you can select the bucket to root your drive on with the Site properties/S3 dialog tab.

Folders

Unlike most file systems the S3 storage model does not have a concept of folders, all files are stored in a top level bucket and you can not have sub buckets. Most S3 clients will make the S3 service appear to support buckets by using folder place holders. Some clients will append $folder$ to a filename to denote a placeholder for a folder. Other clients may append a trailing slash '/' to denote a folder.

WebDrive will support either method, so it will be compatible with other S3 clients.

Setting up a custom S3 site

If you choose to setup your own S3 account without using the "Connect by Service Type" option then you will need to enter the URL yourself, the proper URL to use is **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. Enter your access key in the username field and your Secret Access Key in the password field.

Amazon S3 Access Control Lists

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:

1. An Owner grant - which defines the permissions the owner of the object has.
2. Authenticated Users - which are all Amazon S3 storage users that have an account with S3.
3. Public - which means any anonymous user that you have provided the URL to.
4. Email-ID - which is 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.

Program Settings Overview

Reach the Program Settings dialogue by clicking the App Settings menu button. From here, you can configure your WebDrive administrator's global functions. These fall into two sections: **General** and **Cache** settings.

Many of these options will be inherited at the site profile level. Feel free to configure these on an individual basis.

Settings are divided into two categories of tabs on the left-hand side of the window: **General** and **Cache**.

> For more information on site-specific configuration, see our **Properties Overview**.

Settings

The Program General Settings dialog allows you to customize various program options.

To access this dialogue, click your App Settings menu button. Under General, the Settings tab should already be selected.

Basic Settings

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

Open Site Manager on system startup: The WebDrive administrator will launch automatically when the desktop is loaded.

Open Explorer in Folder View mode: 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 monitor after connecting: When selected, the Drive Monitor dialog will be displayed after connecting to the server.

> See our topic on the WebDrive's **WebDrive Monitor**.

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.

Remember Site Manager Window Position: When the administrator is closed and reopened, it will appear in the same place on your screen as it was in when it was closed.

Import & Export

Use the export/import feature to save both site profile and program settings to a .reg file that can be imported on other machines. This is also useful for backing up your settings if you need to uninstall WebDrive.

Export Settings: Clicking this will launch a form box for you to enter a file to which you would like to export your WebDrive site settings. You can decide if you would like to include the site database and user settings from WebDrive.

Import Settings: Clicking this will launch a form box for you to enter a file path from which you would like to retrieve site settings for WebDrive to use.

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.

Disable shell column handlers while connected: 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 (improves performance of MS Office): 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.

Use Windows to restore drives at login instead of WebDrive: Maps drives at startup with WebDrive instead of using persistent drive connections, which sometimes conflict with wireless Internet connections.

UI Style: Change the layout of the WebDrive application to reflect past versions of the software.

Configure Default Site Settings: Brings up a dialogue in which you can select the settings you would like to be set automatically when you create a site using a certain protocol. When you create a new site it will inherit all settings from the pre-defined site. This overrides the installed WebDrive defaults.

License Information

Check for update: Click this button to immediately check if there is a newer version of WebDrive available for download. WebDrive will check for updates on its own at regular intervals.

Help File: You are here! You can also follow the links provided to the WebDrive Product Page or the Knowledge Base for additional information.

Copy Program Info to Clipboard: Adds information about the WebDrive product you are currently running to your clipboard, which can then be pasted in any text editor. This information includes the version number, 32- or 64-bit version, operating system it is currently running in, registration code, license type, and purchase date.

Activate License: Click this button to activate your software by entering your registration code you received during purchase.

See also our topic on **Activation**.

Logging

WebDrive can be configured to log a variety of data in order to track the functionality of the software. This information can be used to perform debugging, and will often be requested by our **support team** if a ticket is submitted.

Log Settings

Log connection information to a file: Logs connection information to a log file.

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.

Folder to store log files in: Enter a path (or browse) to the folder you would like your logs to be stored in. This should be a local folder, so log files will be accessible to send for troubleshooting purposes.

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

View Logs: Immediately brings up your logs for this site.

Log 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.

File Transfer

This tab contains configuration options concerning the transfer process of files to and from your remote servers.

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

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

See our topic on **Transparency**.

Backup files if upload fails: When enabled and a file upload fails a copy of the file is placed into the specified backup folder.

Popup Settings

These settings will change the overall look of the transfer window that appears while files are being exchanged.

Transparency

How transparent should the popup window be? Changes the window frame to opaque or clear, depending on your preference.

Duration

How long should the window appear? The window will stay on screen for the amount of time specified.

How long should the window fade-in last? The window will appear slowly, going from clear to opaque, over the course of the time set.

How long should the window fade-out last? The window will disappear slowly, going from opaque to clear, in the time set.

File Transfer

Display File Transfer Popup Window: Enabled by default. When disabled, no window will appear while files are being exchanged with the server. You can also specify the size of files at which you would like a popup to appear. This way, the smaller, faster file transfers will happen with little to no interruption of the desktop.

Don't display for transfers by File Transfer Manager: The File Transfer Manager handles backups of WebDrive files. By default, a window does not display to notify users that these backups are in progress.

Security

Certificate Store Folder

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.

See our topic on the **Certificate Manager**.

Host Key Folder

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

> See our topic on the **Host Key Manager**.

Host Key Manager

The Host Key Manager allows you to alter your host key settings, which apply to SSH connections. Host key settings can be configured from either the App Settings, Security tab or the Site Properties, SFTP Settings tab (if the selected site uses the SFTP protocol).

> See also our topic on **SFTP Settings**.

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.

Certificate Manager

The Certificate Manager dialogue allows you to access, create, and update certificates for use with SSL connections.

Certificate List: Displays a list of currently available certificates. Choose from the list to delete, export, view properties, or sign or update your CSR.

Delete: Removes this certificate from the list.

Export: Saves this certificate to another folder location.

Sign CSR: If you have a self-sign certificate, sign it before applying it to a connection.

Properties: View the properties of this certificate.

Create: Use WebDrive's built-in certificate algorithm to generate a new certificate, which can then be either self-signed or sent to a certificate authority.

Import: Navigate to a certificate saved in another folder to apply it to your site.

Update CSR: Apply a new signature to an old certificate.

Close: Exit this window to return to the main WebDrive menu.

Proxy HTTP

Proxy Type: Select the type of proxy server that you have using the dropdown 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. 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. 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.

Proxy FTP

Proxy Type: Select the type of logon required for your firewall using the dropdown 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.

Proxy Options

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.

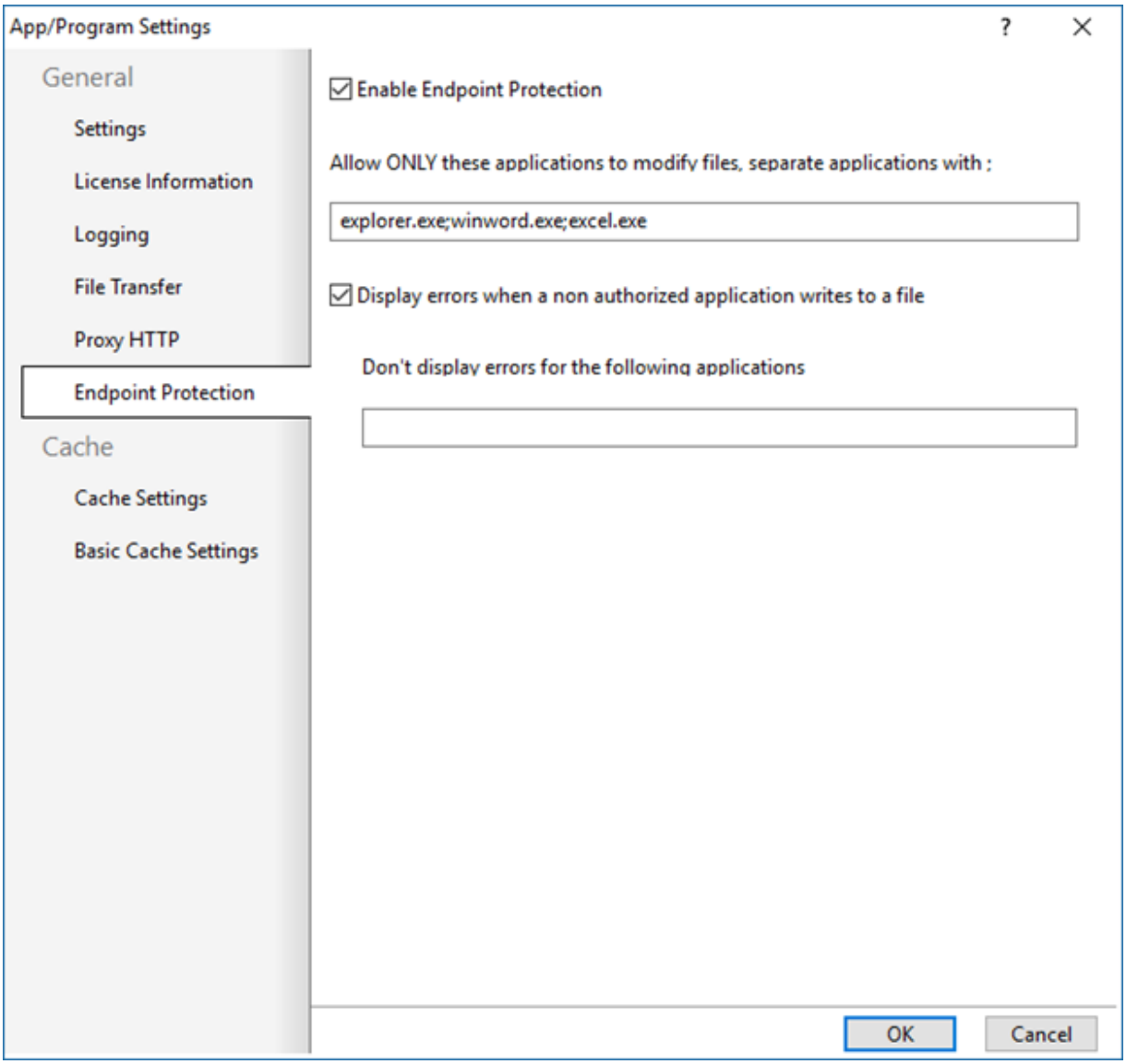
Port: Enter the port number for your firewall. The default port is 21. For SOCKS Servers, use port 1080.

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

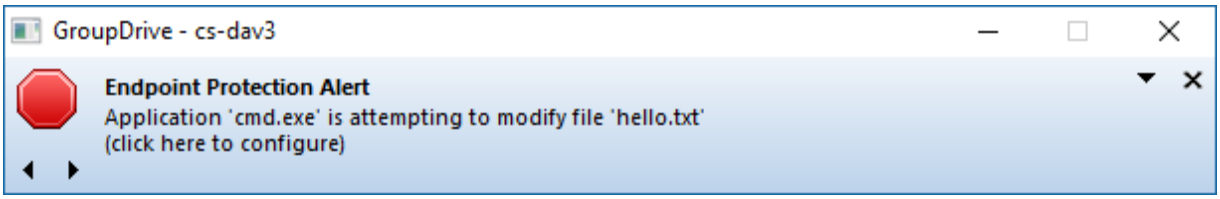
Proxy server password: Enter the password for your proxy server, if required.

Endpoint Protection

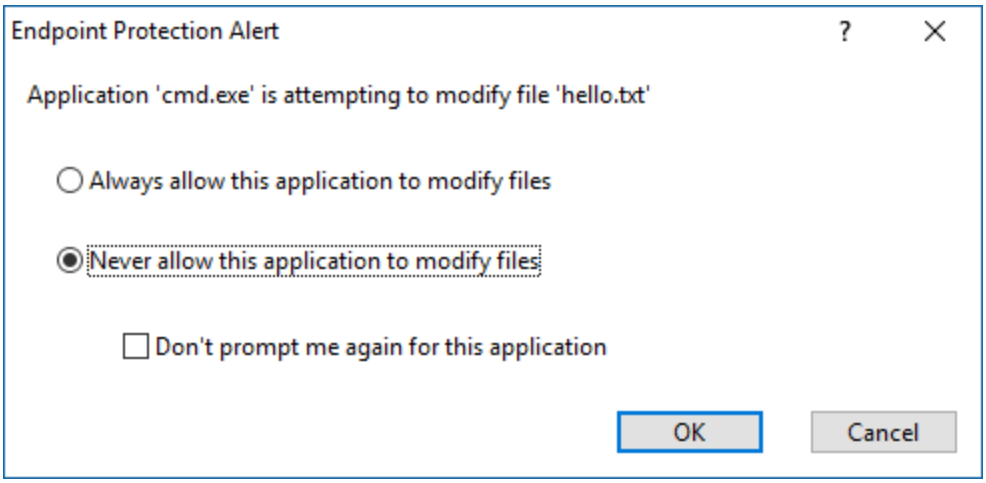
The endpoint protection feature protects your server from unauthorized applications creating or modify files on the server. When enabled, only applications you approve are allowed to create or modify files on the server. Enable the endpoint protection feature from either the App Settings or Site Properties dialog.



When enabled, only applications specified in the ‘Allow’ white list are permitted to write to files on the server. If any application that isn't on this list attempts to alter or create a file, this error will display:



If the user clicks on the window, the configure dialog below will be displayed:



From here the user can:

Always allow this application to modify files: The application will immediately be allowed to modify files. The user will not be prompted again, and the application will have full access to the drive.

Never allow this application to modify files: The application will continue to be denied access to the drive.

Don't prompt me again for this application: Controls whether or not the alert message is displayed when this application attempts to modify files on the drive.

Applications in the 'Don't display errors …' list not will not be allowed to write to files; however, no error window will be displayed.

Cache Settings

From the Program Settings window, in the Cache Settings tab, you can override the global application cache settings with this dialog.

Cache Folder Location: Specify a path to the folder you would like your cached data to be stored in.

Currently in Use (All sites): This is the total amount of space on your hard disk WebDrive is currently using to store data.

Clear Cache: Click to immediately flush all temporary data from the cache.

See also our topic on **Basic Cache Settings** at the site level, or our **Caching Overview** topic for more general information.

Basic Cache Settings

WebDrive can be configured to cache data (store it temporarily to a local file) in order to speed performance or allow you to work offline.

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 at a regular interval (for example, every ten seconds). 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.

Inherit global cache settings: This option only exists at the site level. When enabled, this site will inherit the cache settings applied at the program level; access these in the administrator via the App Settings button.

See our **Cache Overview** topic for more information.

Cache Mode

Single User Mode: This is the default setting and is intended to provide the best performance. It assumes that cached files and directory listings will not be modified by another user. WebDrive will not validate the cached files with the server using the files' last modified time.

Multi-user mode: This mode will validate cached files with the server to keep them up to date. If a cached file has been modified by another user it will be purged from the cache and replaced with the most recent version. DAV & SFTP servers allow WebDrive to easily access 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 to allow applications that perform random access to the file data to work. But the next time the application opens the file, it will download a fresh copy from the server.

Note: When using **Amazon S3** as your connector, **Multi-User cache settings** will not function correctly because the directory's modified-time metadata will not be updated by Amazon. Therefore, files will fall out of sync, and users may interfere with each other's alterations on a common file.

Solution: If you are not using **Single User mode**, you will need to navigate to the Basic Cache Settings tab of the Properties for your S3 site and set your mode to **Custom** and enable **Expire cached files after (x) seconds** and **Expire cached listing after (x) seconds**.

Cache Options

Cache Files: When enabled, your files will be stored in the cache folder for faster access. These files will be available in offline mode as well.

Validate Cache Files: Validates that a cached file is up to date by checking the modified time of the cache file against 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. 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: When enabled, your directory listings will be stored in the cache folder for faster directory and file access. These directories will be available in offline mode as well.

Validate Cached Directory Listings: Validates that a cached directory listing is up to date by checking the modified time of the cache file against 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. The files will then 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.

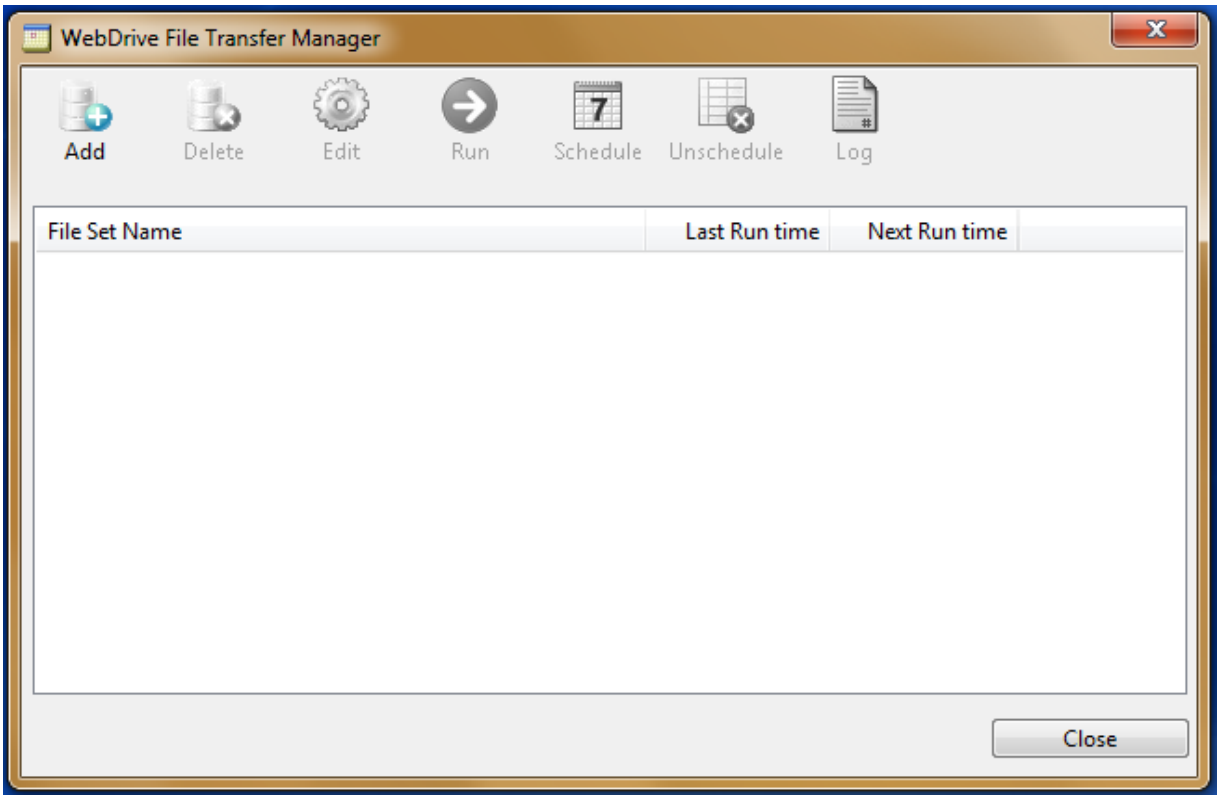
Enable Asynchronous Mode: This feature can greatly improve editing and overall performance of a mapped drive by allowing WebDrive to delete, rename, and create asynchronously, which allows for quick editing of files locally. Changes made to the drive will synchronize automatically with the server a few seconds after modification in the local cache. This provides an overall performance improvement and responsiveness to the drive.

Cache Limit: This specifies a maximum amount of space WebDrive can use to store temporary files. Lower limits will require WebDriveto retrieve files from the server more often, which may result in slower performance.

Clear Cache: Immediately empty the cache. Temporary data will be lost and refreshed with the most recent data from the server on an as-needed basis.

Backup

Clicking the Backup button in the top toolbar of the administrator will launch the WebDrive File Transfer Manager. This feature can be used to back up or synchronize remote folders or entire websites.



Use the File Transfer Manager to:

- Perform full or incremental backups from 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 time

Click Add or the File Set Name to launch the File Transfer Wizard. You can also delete, edit, and run transfers here.

See our topic on the **File Transfer Manager**.

File Transfer Manager

The File Transfer Wizard will lead you through the process of setting up one of three types of transfers:

- Upload/Backup
- Download/Restore
- Synchronize

Choose which of these managed file transfers you would like to configure and click next. You will need to select a destination folder or site profile you would like to retrieve file copies from or transfer them to.

Click Next and select your preferences:

Full vs. Incremental Transfer: A full backup transfers every file and folder to the destination. If the file already exists, it will be replaced with a new copy. An incremental backup transfers only the files and folders that have been modified.

Preserve source path structure: Keep the original directory structure in place when transferring files. Folders and files will be placed into the folders they were in on the server.

Delete source file after copy: After the transfer to the destination is complete, the original file(s) will be deleted.

Select the site profile to use for this transfer: Choose a configured site profile from WebDrive to use for the transferred data.

Select remote folder for transferred files: Choose what location the backup files should be copied to.

Synchronize

1. Select the folder that will be matched. Click Next and select the site profile you want to work with and the folder you'd like the synched data to save to.
2. Pre-determine decisions for WebDrive to make in case it encounters duplicate files. Click Next.
3. After selecting one of these options, click Next and select a name for this backup, to identify it if you have multiple backups.
4. Decide if you'd like to have it **Run Now** (back up immediately), and whether you'd like WebDrive to display a progress dialogue while the backup is in progress.
5. Click Finish when you're done. Your new backup should appear in the File Transfer Manager list.

For more information on backing up server information, see our topic on **Backup**.

Properties Overview

To reach Site Properties in the WebDrive administrator, either select the Site Properties menu button or right-click a site profile and select properties.

> See our overview of **Sites**.

When you configure properties, selected options will only affect one site profile at a time. The configuration options you see will be tailored to the protocol of the selected site.

To see specific configurations for each protocol type, see these topics:

- DAV
- HTTP Settings
- FTP Settings
- SFTP Settings

> For WebDrive-wide configuration options, see our topic on **Program Settings**.

> To create site profiles with a pre-determined set of configuration options, see **Settings**.

General Host Settings

This dialog allows you to edit the server host settings for a site and alter the url, or username/password. The contents of this dialog will vary slightly depending on the server protocol type.

Site Information

Site Name: This name can be changed to differentiate between multiple sites of the same protocol.

Drive Letter: Assign a unique drive letter to each site.

Connect at login/startup: If enabled, WebDrive will automatically connect to this site when the desktop loads.

Always prompt for login credentials: Enable to require the user to enter login credentials every time WebDrive connects to this site. This is the most secure setting for computers shared by multiple users.

Protocol-Specific Options

Dav/HTTP, FTP, and SFTP Host Settings

Url/Address: Type the web address of the server you need to connect to to.

Username: Enter the login name associated with this server.

Password: Enter the password associated with the login name.

Save Password: Choose to save your password if you would like to connect to this server without reentering your credentials.

Amazon S3 Host Settings

Url/Address: Type the web address of the server you need to connect to to.

Access Key ID: Enter the access key provided by Amazon.

Secret Access Key: Enter the secret access key provided by Amazon.

Root Bucket: Select a root bucket to access. Amazon buckets include different sets of files, similarly to a directory.

Google Drive, DropBox, and OneDrive Host Settings

Google Drive, DropBox, and OneDrive will require you to login via a browser. Clicking the login button in the WebDrive applet will bring you to a login and acceptance page, where you must give permission for WebDrive to access your files.

SharePoint Online Host Settings

A special rooting option lets you open to a specific location for your root folder in your SharePoint Online configuration. Click the checkbox for "Root Drive on this folder" and either type or click on the button to choose what folder to root to. The URL does not need to include subfolders/paths for the initial connection.

Connection Settings

Use default port: When checked, WebDrive will connect to the server via the default port for the connection's protocol. Uncheck to specify a new port if the server receives information on a different port.

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

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.

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.

Set initial state to Offline: WebDrive will not connect to this site when it launches. Files will not be synced and cannot be uploaded or downloaded until the site is connected.

When connection to Internet or Server is lost: Select a response. WebDrive can either automatically go into offline mode, open a window to inform you that it must go into offline mode, or keep trying to connect. In offline mode, files will not be synced and cannot be uploaded or downloaded from the remote server, but cached files will be accessible. Repeated attempts to connect to the server may degrade performance.

Connection Settings

Use default port: When checked, WebDrive will connect to the server via the default port for the connection's protocol. Uncheck to specify a new port if the server receives information on a different port.

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

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.

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.

Set initial state to Offline: WebDrive will not connect to this site when it launches. Files will not be synced and cannot be uploaded or downloaded until the site is connected.

When connection to Internet or Server is lost: Select a response. WebDrive can either automatically go into offline mode, open a window to inform you that it must go into offline mode, or keep trying to connect. In offline mode, files will not be synced and cannot be uploaded or downloaded from the remote server, but cached files will be accessible. Repeated attempts to connect to the server may degrade performance.

Protocol-Specific Settings

Different tabs will appear under General Settings in the Site Properties dialogue, depending on the type of protocol your site connects with. WebDrive supports a variety of protocols, including FTP, SFTP, HTTP, and WebDAV. WebDrive also connects to cloud-based file storage systems like Google Drive, DropBox, and Amazon S3.

> For more information on Google Drive, Dropbox, and Amazon connector configurations, see **General Host Settings**.

> For more specific information on the Amazon S3 connector, see **Buckets**.

For General Settings page info pertaining to the different protocols, see these topics:

- FTP Settings
- DAV
- HTTP Settings
- SFTP Settings

FTP Settings

> **Note:** This is a protocol-specific tab with configurations that will only be available if your site profile uses the **FTP** protocol.

Server

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

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 which 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 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. The directory is case sensitive for FTP.

Initial command: Allows you to enter custom FTP commands to perform after logon.

You must use a semi-colon (;) between commands.

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

Security

Security Type: Select the SSL method to connect securely to the FTP server.

Secure Data Channel: Secures the FTP data channel.

Client Certificate to connect with: Select the SSL certificate to connect to your server with if the server requires one.

Advanced

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.

SFTP Settings

> **Note:** This is a protocol-specific tab with configurations that will only be available if your site profile uses the **SFTP** protocol.

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).

Folder Auto-mount list ; separated: This feature does not apply in most cases. Certain SFTP servers will only allow clients to directly open folders in a list.

Host Key: Select the host key to connect to the SFTP server with.

> See also our topic on the **Host Key Manager**.

HTTP Settings

> **Note:** This is a protocol-specific tab with configurations that will only be available if your site profile uses the **HTTP** protocol.

Connect Securely (SSL/HTTPS): Connect to your server using SSL, and optionally select a client certificate to connect with.

Advanced Options

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.

Use /allprop on PROPFINDS: This will return all information about a resource however this can severely degrade performance please don't enable unless necessary.

Persist session information across all connections: Uses the same cookies used during authentication on all subsequent connections.

DAV

> **Note:** This is a protocol-specific tab with configurations that will only be available if your site profile uses the **WebDAV**protocol.

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 feature is designed to be used with Microsoft Office applications like word and excel, other applications may not work.

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.

DAV Lock timeout (minutes): Allows you to configure a custom length of time before files that are DAV locked are released.

General

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.

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

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.

Windows NT Service Access

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 topic on using **WebDrive with an NT Service**.

Basic File Settings

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.

General 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: Enable this option to cache and combine small writes by applications into larger writes. Some applications issue very small writes of say 1 byte at a time for example, even when writing a very large file. Enabling this setting can greatly increase performance for these applications.

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

Disable Explorer icon handler to prevent file download: Prevents files from beingdownloaded 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. This is only available for servers that support block I/O, for example, SFTP and Cornerstone MFT.

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 folder's 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, WebDrivewill 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

> **Note:** These options will only be visible in the properties sections of FTP connections.

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.

Keep the following files in Cache Only: This allows you to specify a list of file types to be treated as "Local Only," meaning they will remain in cache and never be uploaded to the server.

Basic File Settings

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.

General 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: Enable this option to cache and combine small writes by applications into larger writes. Some applications issue very small writes of say 1 byte at a time for example, even when writing a very large file. Enabling this setting can greatly increase performance for these applications.

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

Disable Explorer icon handler to prevent file download: Prevents files from beingdownloaded 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. This is only available for servers that support block I/O, for example, SFTP and Cornerstone MFT.

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 folder's 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, WebDrivewill 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

> **Note:** These options will only be visible in the properties sections of FTP connections.

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.

Keep the following files in Cache Only: This allows you to specify a list of file types to be treated as "Local Only," meaning they will remain in cache and never be uploaded to the server.

Substitution

Use the Substitution dialog 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 substituted using ASCII code in a string that is formatted as **wdxyNNwdxz**, 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.

Note: This feature is **only** used to translate filenames before uploading them to the server, once uploaded they will have the substituded filename characters and will display in explorer that way which can lead to confusion. This setting is meant for legacy main frame servers and it's use is limited.

File Permissions

Use the File Permissions dialog tab to configure Unix file permissions for new files or directories.

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.

Auto ASCII Transfer

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

Use the 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.

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.

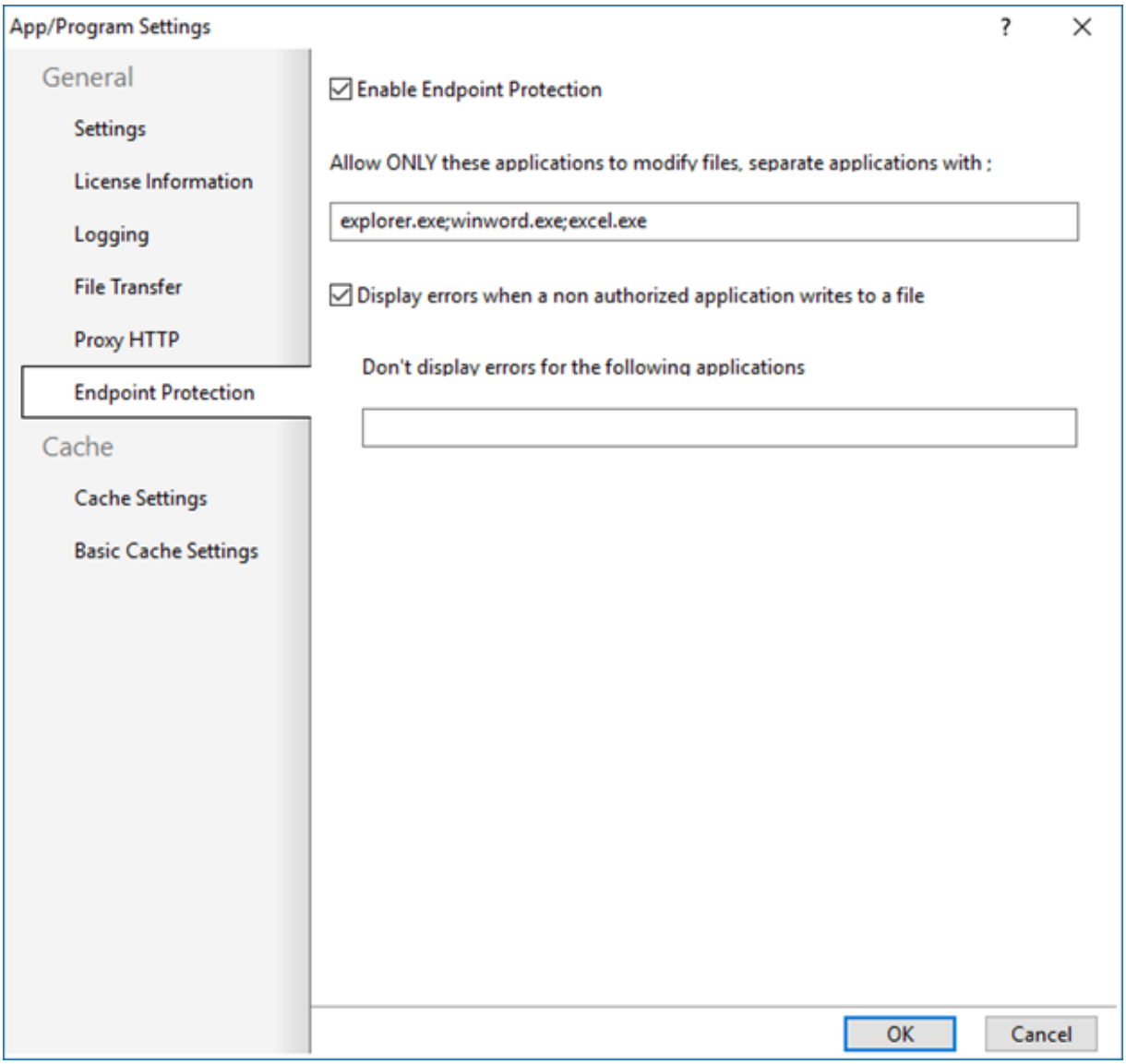
To view hidden directories:

1. Select Enable Hidden Directories on the File Settings tab of the Site Properties window
2. Add hidden directory names to the list
3. Type a full file specification to the hidden subdirectory

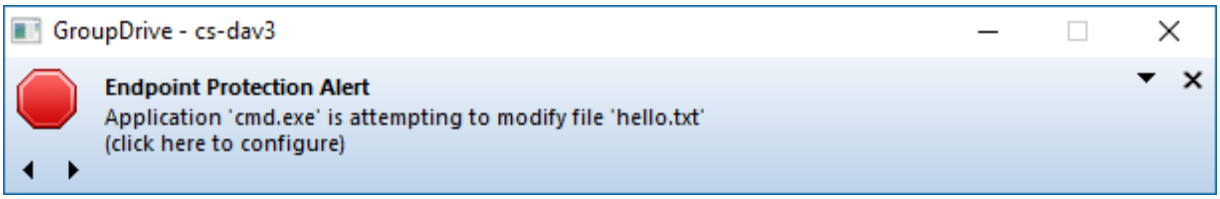
For example, to add a hidden folder under the folder named subdir, add it as / subdir/myhiddendir.

Endpoint Protection

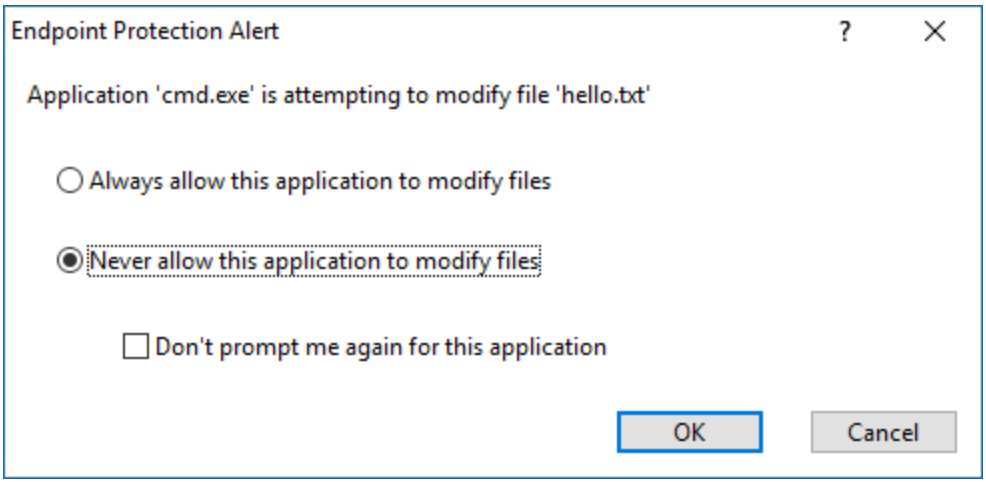
The endpoint protection feature protects your server from unauthorized applications creating or modify files on the server. When enabled, only applications you approve are allowed to create or modify files on the server. Enable the endpoint protection feature from either the App Settings or Site Properties dialog.



When enabled, only applications specified in the ‘Allow’ white list are permitted to write to files on the server. If any application that isn't on this list attempts to alter or create a file, this error will display:



If the user clicks on the window, the configure dialog below will be displayed:



From here the user can:

Always allow this application to modify files: The application will immediately be allowed to modify files. The user will not be prompted again, and the application will have full access to the drive.

Never allow this application to modify files: The application will continue to be denied access to the drive.

Don't prompt me again for this application: Controls whether or not the alert message is displayed when this application attempts to modify files on the drive.

Applications in the 'Don't display errors …' list not will not be allowed to write to files; however, no error window will be displayed.

Cache Settings

From the Program Settings window, in the Cache Settings tab, you can override the global application cache settings with this dialog.

Cache Folder Location: Specify a path to the folder you would like your cached data to be stored in.

Currently in Use (All sites): This is the total amount of space on your hard disk WebDrive is currently using to store data.

Clear Cache: Click to immediately flush all temporary data from the cache.

See also our topic on **Basic Cache Settings** at the site level, or our **Caching Overview** topic for more general information.

Basic Cache Settings

WebDrive can be configured to cache data (store it temporarily to a local file) in order to speed performance or allow you to work offline.

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 at a regular interval (for example, every ten seconds). 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.

Inherit global cache settings: This option only exists at the site level. When enabled, this site will inherit the cache settings applied at the program level; access these in the administrator via the App Settings button.

See our **Cache Overview** topic for more information.

Cache Mode

Single User Mode: This is the default setting and is intended to provide the best performance. It assumes that cached files and directory listings will not be modified by another user. WebDrive will not validate the cached files with the server using the files' last modified time.

Multi-user mode: This mode will validate cached files with the server to keep them up to date. If a cached file has been modified by another user it will be purged from the cache and replaced with the most recent version. DAV & SFTP servers allow WebDrive to easily access 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 to allow applications that perform random access to the file data to work. But the next time the application opens the file, it will download a fresh copy from the server.

Note: When using **Amazon S3** as your connector, **Multi-User cache settings** will not function correctly because the directory's modified-time metadata will not be updated by Amazon. Therefore, files will fall out of sync, and users may interfere with each other's alterations on a common file.

Solution: If you are not using **Single User mode**, you will need to navigate to the Basic Cache Settings tab of the Properties for your S3 site and set your mode to **Custom** and enable **Expire cached files after (x) seconds** and **Expire cached listing after (x) seconds**.

Cache Options

Cache Files: When enabled, your files will be stored in the cache folder for faster access. These files will be available in offline mode as well.

Validate Cache Files: Validates that a cached file is up to date by checking the modified time of the cache file against 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. 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: When enabled, your directory listings will be stored in the cache folder for faster directory and file access. These directories will be available in offline mode as well.

Validate Cached Directory Listings: Validates that a cached directory listing is up to date by checking the modified time of the cache file against 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. The files will then 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.

Enable Asynchronous Mode: This feature can greatly improve editing and overall performance of a mapped drive by allowing WebDrive to delete, rename, and create asynchronously, which allows for quick editing of files locally. Changes made to the drive will synchronize automatically with the server a few seconds after modification in the local cache. This provides an overall performance improvement and responsiveness to the drive.

Cache Limit: This specifies a maximum amount of space WebDrive can use to store temporary files. Lower limits will require WebDriveto retrieve files from the server more often, which may result in slower performance.

Clear Cache: Immediately empty the cache. Temporary data will be lost and refreshed with the most recent data from the server on an as-needed basis.

Features

WebDrive Site Manager

Use WebDrive's Site Manager to define your servers and to map your servers to drive letters. Type your server's URL, type your Username and Password, and click Connect to map the selected drive letter to your server.

You can also use Site Manager to map unique drive letters to different directories that are located on the same server. This provides easy access to frequently updated directories.

Collaboration

WebDrive supports Web-Based Distributed Authoring and Versioning protocol (WebDAV). When you map a drive letter to any WebDAV compliant Web server, WebDrive allows you to lock files, modify them, and then release the locks so that others can review and update the files. WebDrive users can maintain data integrity by using WebDAV locking concepts.

Security Features

WebDrive provides built-in support for the industry standard SSL protocol. When used in conjunction with secure Web servers, WebDrive opens an encrypted tunnel between the client computer and the remote server to allow secure transmission of critical data over the Internet. WebDrive can be used as an efficient alternative to an expensive and complicated corporate VPN. Install the WebDrive Client and an SSL enabled server and WebDrive can function as your company VPN. WebDrive also supports SSL certificates and SSH host keys.

Offline 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.

File Transfer Manager

The WebDrive File Transfer Manager can be used to perform full or incremental backups and synchronization between files and folders on your local computer to your server. You can schedule backup jobs to run at specific times or on demand.

Legacy Support

WebDrive allows you to map a drive to your server and access it like a local drive. You can use a DOS-Prompt for commands (such as copy, xcopy, mkdir, dir, move, etc). As Internet usage grows, DOS based and other legacy applications quickly become antiquated because of the inability to access data over the Internet. WebDrive breathes new life into these applications by providing DOS based Internet file access. Still using WordPerfect for DOS? Not a problem. Using WebDrive, you can map any available network drive letter to a remote server over your corporate Intranet or over the Internet, then use WordPerfect for DOS to access those files using the mapped drive.

Internet Enable any Application

Instantly Internet enable any application. Use WebDrive to manipulate files on your server using your favorite applications.

For example, you can use Microsoft Backup to create backups of your Web site by simply selecting the drive letter to be backed up.

Advanced Features

SSL: Supports Secure Sockets Layer protocol and SSL certificates.

WebDAV: Supports Web-Based Distributed Authoring and Versioning protocol.

SFTP: Supports SSH host keys and provides secure connections to SFTP/SSH servers. Provides read-only directory attribute support for SFTP servers.

S/KEY Password Encryption: Supports MD4 & MD5 password encryption for supported FTP servers.

Firewall/Proxy server: Supports a variety of proxy servers and firewalls, including Microsoft ISA Server , SOCKS v4.3 and SOCKS v5, and Raptor/Symantec Enterprise Firewall (gwpasswd).

Microsoft FrontPage: Supports connections to any Web site running Microsoft FrontPage extensions.

Foreign Languages: Supports Far East languages such as Japanese and Chinese using DBCS.

Caching: Supports caching for both file and directory listings. You control the amount of disk space to be used for the cache and whether to cache files, directory listings, or both.

FTP: Supports resume interrupted download.

UNIX: Supports file attributes through an Explorer shell extension as well as a command line utility.

ASCII/Binary: Supports options to transfer files in mode based on file extension.

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 web-site:

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

FIPS SSL

WebDrive uses the FIPS compliant Microsoft SSL engine.

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 and currently connected**.
2. Right-click and hover over the WebDrive option.

Depending on whether you select the entire drive, a folder, or a file, the context menu should contain the following options:

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

Work 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 connected.

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.

Lock File: Only available for DAV connections. This will prevent other users from altering the file while you have it open. Closing the file will automatically unlock it.

Unlock File: Only available for DAV connections. This will make the file available for others to alter it. Closing the file will automatically unlock it.

See also our topic on **Lock DAV Files**.

Copy URL to Clipboard: Automatically copies the file's URL path, which can be used to locate the file online if your server has a WebUI.

Sync Now: Immediately synchronizes your files with the server.

Disconnect: Disconnects this site from the server.

Manage Offline files and folders: See a list of files marked for work offline. Remove them from the list to keep them from being cached..

Lock DAV Files

> **Note:** This feature is only available for DAV connections.

You can **lock** or **unlock** a drive, folder, or file and **examine** the lock status of a file via a shell interface.

Once locked, only the owner of the lock on a file can access it, which serves to prevent others from altering the file and creating unsynchronized copies.

To access the Lock interface:

1. Open an Explorer window and right-click a connected DAV drive, folder, or file.
2. Next, either hover over the WebDrive option and select Lock or Unlock, or select Properties, and then select the Lock tab.

When you are finished with the file, you can either unlock the file manually, or close the file to automatically unlock it.

Permissions and Attributes

The Permissions Property tab allows you to examine and change file attributes for files on an FTP or SFTP server.

> **Note:** This feature is only available on UNIX SFTP Servers and FTP Servers that support the CHMOD FTP extension.

This feature can be handy when working with CGI and Perl scripts where you need to set the execute and write privileges.

To display permissions:

1. Using Explorer, select the file you wish to examine and right-click it.
2. Select Properties from the menu.
3. Select the Security tab.
4. A list of permissions for this file will be displayed. Click Edit to alter the permissions.

To display attributes:

1. Using Explorer, select the appropriate file and right-click it.
2. Select the General tab and select the attributes you want. The CHMOD value will be calculated automatically.
3. Click the OK or Apply button to send the CHMOD command to the server.

WebDrive with an NT Service

You can use drives mapped by WebDrive in NT services; however, there are several issues to 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, user-name/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.

Automating Connections and Disconnections

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

1. From the Application window: Select **Make a connection persistent**.
2. From the Site Manager: Select **Connect at login/startup**.
3. Program Command Line Options: The application will accept a connection name as a parameter and perform the connection.
   This is useful for:
   - Automating a connection using a batch file. The connection name must be in quotes. For example **WebDrive.exe /s:"Microsoft"**.
   - Automate a disconnect by specifying 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, 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, Cornerstone MFT=3 , SFTP=4. For a FTP connection enter /pr:0
- **/ d: driveletter**
  the drive letter to map to the site, for example / d:X
- **/ 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.

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**.

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

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

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.

1. 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.
2. 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 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 need 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 sys-

tem. 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. The next time the user runs WebDrive, the new settings will be imported. Imported settings are overlaid on any existing settings for WebDrive; however, there is a special action that you can place in the registry file to cause WebDrive to 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
```

Setup Options

WebDrive Installer

The WebDrive installation program is a Windows installer MSI file 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 often familiar with MSI files because they are useful for 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 here. For more information on editing MSI files and creating transforms, see Microsoft's Orca MSI editor: **http://msdn.microsoft.com/en-us/library/aa370557(v=vs.85).aspx**.

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. You can unpack the setup package by running the setup in Administrator mode. You can use the **/a** command line option to do this (ie, **webdrive.exe /a**).

In Administrator mode the install will unpack the setup package to a directory of your choice; 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 Windows 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 to prevent the user interface from displaying, you can use the following command line parameters for the main setup executable:

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

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) and 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; keeps the user interface from displaying.
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-E="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"
```

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:"Micros
                      @if not exist X:\  (
                      echo COULD NOT CONNECT
                      goto END
                      )
                      copy x:\dirmap.txt %TEMP%
                      start /wait /D"c:\program files\webdrive" webdrive.exe X: /d
               :END
```

UNC

WebDrive has limited support for Universal Naming Convention (UNC), which 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 **\\server-name\share\dir1\dir2\file.txt** format.

To refer to a UNC file in WebDrive, you would replace the server name with WebDrive and share with the site name 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:

Say you are connecting to the connection Microsoft (ftp.microsoft.com), with drive letter **X:**. To do a **dir** using UNC from a CMD 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 the **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.

For more information, see our QuickStart on **UNCs**.

WebDrive with Windows NT

You can use drives that are mapped by WebDrive in NT services. However, keep several things in mind.

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:

Say you're logged onto 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, a DOS prompt, or applications you run under the same NT session you created drive W: with. However, by default, most **NT services do not run under a normal NT user account**; instead, they 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 W: drive 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.

Enabling NT Services to Access WebDrive mapped drives

Example 1 is the less complicated of the two examples.

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.

Note: You may also want to enable the companion setting **Connect drive at system startup** , which will map the drive letter when the computer boots, without the need to log onto 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** as well as 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.

Note: When using command line options from an NT service, user context is vital. 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", 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 in which you defined the site information, there shouldn't be a problem.

If you want to use the command line option to map a drive and still use the drive by a service, add the command line parameter **/ ntservicecontext** . This will allow you to use a standard WebDrive site created under a logged-in NT user, as well as map the drive in another context.

Help

Having a problem with WebDrive? We have answers.

Explore the help topics included with your software or provided online to learn more about WebDrive. If you can't find the information here, you may find answers in our **Knowledge Base**. Clients with active maintenance can also submit tickets here for assistance with specific issues.

FAQ

Common Questions

Is there a way to view a list of the computers that are activated on my registration code? Can I deactivate computers online?

Yes. We have a Customer Activation Portal that will enable you to review your current activations on a given registration code.

You can log into the Activation Portal using your software registration code and the email address that was used to register the software. Please contact our Support Team if you do not know the registered email address for your license.

The address of the customer portal is **http://activate.southrivertech.com/CIS/Default.aspx**

Upon successful entry into the portal, the basic information about your software license is displayed. This includes the order number, the purchase date and the description of the product purchased.

Using the Portal you have the ability to view your current activations, download the list of activations in XML format, deactivate one (or all) computer activations, edit the customer registration information for the registration code, and manage any SRT email mailing list subscriptions.

How do I create log files for debugging?

Instructions for generating and sending over a debug log file (WebDrive for Windows):

1. Disconnect the mapped drive in WebDrive (if it is currently connected).
2. Go to App Settings --> Cache Settings and choose to "Clear Cache."
3. Go to App Settings --> Logging and enable all logging options (check all boxes).
4. Connect the mapped drive in WebDrive.
5. Reproduce the issue.

6. Disconnect the mapped drive in WebDrive.
7. Go to App Settings --> Logging --> View Logs and attach the resulting log file to this email.

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.

There is a gray "X" where the file icon would be. How can I remove it?

Click the site you would like to change, then select Site Properties and Basic File Settings. Uncheck the box beside **Disable Explorer icon handler to prevent file download**.

The icon overlay is a result of the setting Properties > File > **Disable Explorer icon handler to prevent file download**. The overlay is associated with the offline attribute, which Windows uses to denote the fact that it can't pull down the icon information. This setting is enable in WebDrive by default in order to avoid uninitiated downloads of files simply to extract the icon information. Disabling this setting removes the icon overlay, but may result in increased and/or unintended file downloads.

How do I increase WebDrive's Storage Limit?

Open the registry editor and go to HKEY_CURRENT_USER\Software\South River Technologies\WebDrive\Connections\(Your Site Profile Name). Find QuotaMB and change the value to something greater, depending on how large you would like the limit to be.

Location Not Available

The likely cause for this issue is that Webdrive.exe is running as Administrator (elevated). The Session ID will not matchup with the Drive Letter being selected. It is important to ensure Webdrive.exe is not running as Admin when it is launched.

I can only open one PDF document at a time; how do I change this?

This is caused by an update that Adobe added recently. To work around this, please open Adobe Reader, go to Edit/Preferences/Security (Enhanced) and turn off "Enable protected mode at startup."

How can I configure Multiple Cloud Accounts (OneDrive, Google Drive, etc.)

You can set up multiple cloud accounts with the same service (i.e. two OneDrive accounts) or any number and combination of other cloud storage connectors. To do this, create your first account site profile as normal (for instance, if you need a OneDrive connection, set up a OneDrive account via their website). Then, open an Internet browser, log into the same account, and log back out. Then, create a OneDrive site profile in WebDrive using the same credentials. Create another OneDrive (or other cloud service) account, log in and out, and enter those credentials as a site profile in WebDrive. By entering

the credentials for each different account, you can connect to any number of them. You can continue this for any additional site profiles to be created; be sure to log in through a browser and then log out for each one.

Caching Questions

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

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.

Also, see **There is a gray "X" where the file icon would be. How can I remove it?** in the Common Questions section above.

I have disabled caching; why is it so slow?

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.

Note: Some anti-virus software may have issues with WebDrive when the anti-virus software attempts to perform real-time scanning on files in the WebDrive Cache Folder. Most anti-virus software has an option to exclude specific folders from their scan, if you experience hanging issues please add the WebDrive cache folder to the exclusion list in your anti-virus or anti-malware software.

Report Issues

Reporting Problems

To report a problem, visit the **WebDrive support page**. If the answers aren't in the product help, explore the Knowledge Base and submit a ticket if necessary.

Please furnish our Support Engineers with the following information:

- The Windows platform that you are running
- The WebDrive version you are using
- The URL of the server that you were using when the problem occurred
- A detailed description of the problem

Include file name and complete sub-directory name if applicable. Attach a copy of the log file to your e-mail.

To find pertinent information specific to your version of this product, go to the License Information tab under App Settings, General Settings and click **Copy Program Info to Clipboard**.

Contact Us

South River Technologies is headquartered in Annapolis, Maryland. We are also conveniently located just 2,461 miles from the heart of Silicon Valley.

Corporate Headquarters Address	South River Technologies 1910 Towne Centre Blvd Suite 250 Annapolis, Maryland 21401 USA
Toll-Free	1-866-861-9483
Main	443-603-0290
Fax	410-266-1191
Website	www.webdrive.com
Email	sales@southrivertech.com
Support Inquiries	support.southrivertech.com

System Requirements

Make sure your system has been updated with the most recent service packs.

Operating System	Windows Vista (32-bit & 64-bit) Windows Server 2008 (32-bit & 64-bit) Windows 7 (32-bit & 64-bit) Windows 8 (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

No other TCP/IP stacks are currently supported.