2018

SafeNet® eTokens with WebDrive

Using WebDrive to leverage SSL Certificates stored on hardware-based eTokens such as the SafeNet® eToken PRO.

QuickStart Guide

SafeNet® eTokens

WebDrive supports secure sharing using SafeNet eTokens over any SSL connection, including FTP/S, HTTP/S, and WebDAV/S, using third party SSL certificates.

Under the hood, WebDrive's SSL features rely on Microsoft's CryptoAPI engine, which is included in all versions of Windows supported by WebDrive. With the appropriate token-specific Cryptographic Service Provider (CSP) installed, WebDrive can interact with hardware-based tokens containing SSL certificates through Microsoft's CryptoAPI.

The benefit of using hardware-based tokens is that the private key is secured physically on the device and cannot be accessed directly. Keeping the private key 'in the black' ensures the integrity of the certificate and is a requirement for certain installations.

2 Factor Authentication Requirements

Supported Hardware Tokens

- SafeNet eToken PRO - 32K
- SafeNet eToken PRO - 64K
- SafeNet eToken PRO - 72K

Minimum Hardware Requirements

- USB slot for eToken

Minimum Software Requirements

- SafeNet Authentication Client v8.1 or Later

Configuring Webdrive for SafeNet® eToken Support

The following instructions will guide you through the process of installing the SafeNet Authentication Client (SAC) and testing to ensure WebDrive can access the certificate information on your eToken.

To use SafeNet eTokens with WebDrive, you must first install SAC v8.1 or later on the computer. Please contact SafeNet for a copy of the SAC. Once installed, the SAC client icon will appear in the system tray at the bottom right of your screen.

Configuring WebDrive to use an eToken

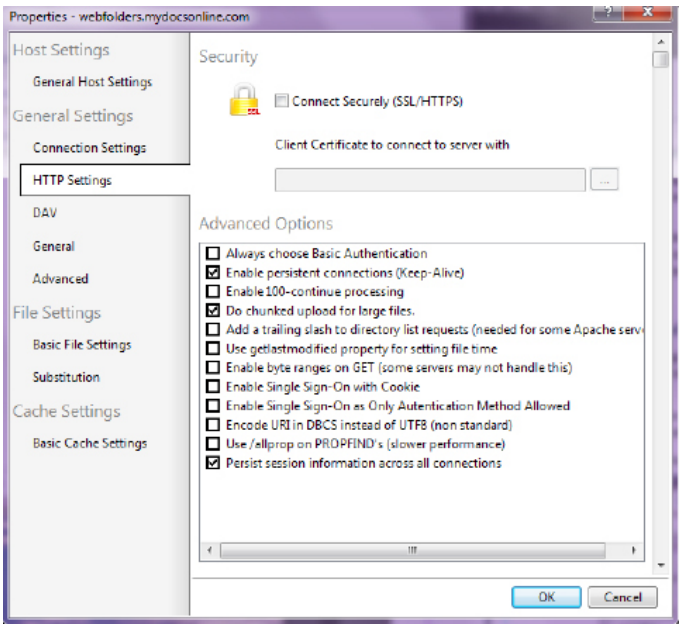
Before you get started: You must be working at the physical computer on which WebDrive is installed, with your eToken inserted in an available USB slot. **This process will not work through Microsoft's Remote Desktop.**

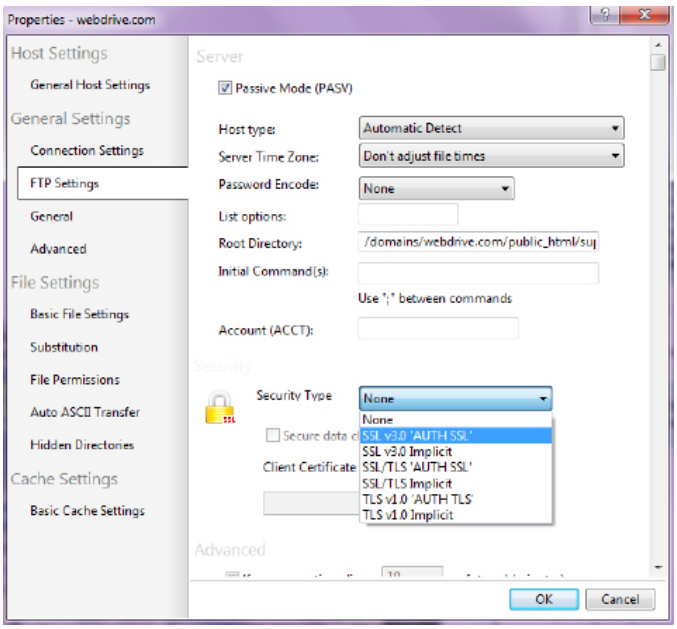
1. Launch WebDrive and either add a new site or select a server which utilizes an SSL connection (FTP over SSL, HTTPS, or WebDAV) which will be using the certificate stored on the eToken.

2. Right-click on the connection and select Properties. Depending on the type of connection, you will see different options.

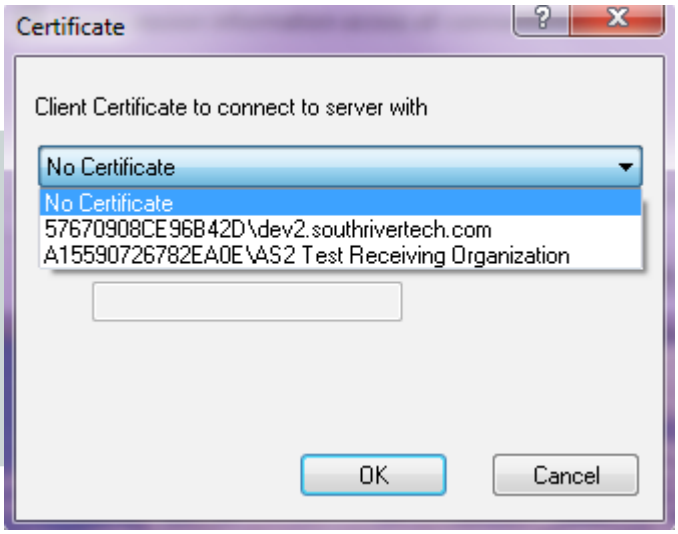
    - For an HTTP or WebDAV connection, click the HTTP Settings tab and enable "Connect Securely (SSL/HTTPS)".

    - For an FTP connection, change the Security Type to one of the SSL options and enable "Secure data chanel (PROT P)".





3. Click the "..." button beside the "Client Certificate to connect to server with" form. The default selection is No Certificate. Select the certificate that corresponds to your eToken from the drop-down menu.



NOTE: Since multiple eTokens can be present at any given time, and since the same certificate name can be used on multiple eTokens, WebDrive's Certificate Manager will prefix the eToken's unique container ID to the front of the certificate name. To view the unique container name, use the SAC utility and select the certificate to view its details.

4. Enter the password used to access the eToken and click OK, then click Okay in the properties window.

Back in the main WebDrive Administrator, test your connection by opening the newly-configured WebDrive site.

System Requirements

Supported Operating Systems

- Windows Server 2012, all editions, 32-bit and 64-bit
- Windows Server 2008-R2, all editions, 32-bit and 64-bit
- Windows Server 2008, all editions, 32-bit and 64-bit
- Windows Server 2003, all editions, 32-bit and 64-bit

Minimum Hardware Requirements

- 2 GHz Pentium® class processor
- 4GB of RAM is required; 8GB of RAM is recommended
- Minimum 100MB of free disk space for the application
- Minimum SVGA (800x600) resolution display is required to run the Administration console program.

Minimum Software Requirements

- Microsoft .NET Framework v2.0 is required
- Microsoft SQL Server 2005 or later is required
- Microsoft SQL Server Management Studio Express is recommended

About South River Technologies

South River Technologies (SRT) is an innovator in secure file management software. SRT software allows users to securely access, manage, and collaborate on files over the Internet, streamlining business processes to improve productivity. SRT's products enhance customers' existing applications by instantly enabling secure access and collaboration within those applications. More than 90,000 customers in 140 countries use SRT's software to make remote file access and collaboration more efficient for their customers, partners, and distributed workforce.

For more information, please visit www.southrivertech.com. South River Technologies, Cornerstone MFT, Titan FTP Server, WebDrive, and DMZedge Server are registered trademarks of South River Technologies, Inc. in the U.S. and other countries. Any information in this document about compatible products or services should not be construed in any way to suggest SRT endorsement of that product or service.

Contact Information

South River Technologies, Inc.
1910 Towne Centre Blvd
Suite 250
Annapolis, Maryland 21401
USA

Toll Free: 1-866-861-9483
Main: 443-603-0290
Fax: 410-266-1191
Corporate Web site: www.southrivertech.com
Online Support: www.srthelpdesk.com