2018

HIPAA Compliance for WebDrive and Cornerstone MFT

Instructions for achieving HIPAA compliance with WebDrive and Cornerstone MFT Server software.

QuickStart Guide

© 2018 South River Technologies, Inc.
All Rights Reserved

HIPAA Compliance QuickStart

WebDrive and Cornerstone MFT work together to satisfy the security standards mandated by HIPAA. Follow this simple guide to set up a HIPAA-compliant file transfer system. Once you have installed Cornerstone MFT Server, you will have access to a variety of features to secure your information. Configuring your Cornerstone and WebDrive clients according to this QuickStart will render you compliant with the following HIPAA mandates:

- **Security Management**
- **Information Access Limitation**
- **Termination Procedures**

Configuring Cornerstone MFT Server

Refer to the online guides to install Cornerstone MFT Server, found at http://webdrive.com/product-support/cornerstone-mft/. With Cornerstone installed, implement HIPAA-compliant server settings by selecting the following configurations while following the wizard-driven setup:

- **Timeout** — Via the Connections page, adjust the "Idle Connection Time-out" to set the number of minutes an account can be idle before it is logged out.
- **Disable Account** — Select the Connections Advanced tab on the Connections page and enable the "Disable account after" option. Enter the number of incorrect password entries a user will be allowed before being locked out.
- **Password Encryption** — Expand Users and select a user; from the "Password Type" dropdown menu, select OPT S/Key MD4 or S/Key MD5.
- **Lock Users in Home Directory** — Check "Lock User(s) in Home Directory" in Files/Directories on the server level. This denies users access to directories other than their own.
- **Disable Anonymous Access** — At the Server level, under the FTP tab, uncheck "Allow Anonymous Access" to require all users to logon with their username and password.
- **SFTP** — At the Server level, select Security, open the FTPS/SSL tab, and check "Enable SSL/TLS access on this server."
- **Require Connections to be Secure** — At the Server level, select Security and the FTPS/SSL tab. Check "Require all FTP connections from clients to be secure," directing the server to refuse non-encrypted communication attempts.
- **Up to 512-bit TLS/SSL security** — At the Server level, select Security and open the SFTP/SSH tab. Check the "Enable SFTP (SSH's Secure File Transfer Protocol) on this server" option and select the bit level you prefer in the Cipher preferences menu. The security can be adjusted down to 128-bit (faster, less secure) or up to 512-bit (slower, more secure). The current industry standard is 256-bit.
- **Permissions** — Create Groups or Users to grant permissions on a group or user basis.

- **Logging** — Enable Logging to file on the Logging tab. The log will produce an audit trail displaying the user id, the date, the time of activity, and the activity performed. This will satisfy HIPAA's mandate for Internal Audit capabilities.
- **Force Complex Password Rules** — At the Users level of the tree view, on the User General tab, enable "Force Complex Password Rules" and select OTP S/Key MD4 from the Password Type dropdown menu. Users will be required to select a password at least 8 characters long, with at least one each of an uppercase letter, lowercase letter, digit 0-9, and non-alphanumerical character (!, #, $, ^, etc.).
- **Termination** — Disable the user's account by de-selecting "Account enabled" on the User General tab. The user will be immediately ejected from the system. The user's account can also be set to expire on a set date on the General tab by selecting "Expiration Date" and specifying a date. Delete the user by right clicking the user's name from the left-hand menu and selecting Delete.

Configuring WebDrive

WebDrive offers HIPAA-compliant secure access and collaboration without requiring users to learn a new application. Install WebDrive on all computers with access to patient data on the server. To install WebDrive, see the general configuration guide found on the South River Technologies website at http://webdrive.com/product-support/webdrive/.

SFTP

To set up a server, you will select a server profile. Each profile has different security standards. SFTP servers are preferred for HIPAA compliance, as they meet all of the requirements by default. This protocol is fast, preserves the security of the server's firewall by creating fewer openings during file transfer, and allows more advanced password coding, including support for the use of SSH host keys.

FTPS

If you choose to connect through FTPS, WebDrive will need to be configured to meet HIPAA regulations. Create a new site by clicking the New button at the top left of the WebDrive window and change the following settings:

1. Select "TLS v.1.0 'Auth TLS'" or "TLS v1.0 Implicit" from the Security Type dropdown menu.
2. Check that "Secure data channel (PROT P)" is enabled.
3. Click the "Advanced Settings" button, navigated to FTP Settings under General Settings in the new window, and select either "S/Key MD4" or "S/Key MD5" and from the Password Encode dropdown menu.

WebDrive Requirements

Supported Operating Systems

WebDrive is supported on both the 32- and 64-bit editions of Windows.

- Windows Vista
- Windows 7
- Windows 8
- Windows 10
- Windows Server 2016, all editions
- Windows Server 2012-R2 editions
- Windows Server 2012, all editions
- Windows Server 2008-R2, all editions
- Windows Server 2008, all editions

Minimum Hardware Requirements

- Pentium® class processor or better
- 4GB of RAM is required; 8GB of RAM is recommended
- Minimum 100MB of free disk space for product and cacheing
- Minimum SVGA (800x600) resolution

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