

Secure FTP with ELMNet

Secure FTP – What Is It?

Secure FTP (SFTP) is a file transmission technique that allows schools and Members to send files to and from ELM without having to exchange public encryption keys or pre-encrypt the file before sending. SFTP is a “right now” kind of transmission – it either completes successfully or you see that there is an error. When it completes successfully, the file has been copied to the other system (either yours or ELM’s) and is readable by the system. If being copied to ELM, ELM does not need to decrypt the file (decryption

can introduce processing errors or delays). If the file is being copied to your system, you can open and use the file immediately.

You can think of SFTP as FTP with automatic encryption.

There is a lot of technology “under the hood” that handles the encryption for you so you don’t have to be aware of it or get involved with encryption directly. We’ve included technical information about file transfer protocols at the end of this document.

Authentication, access to the SFTP mailbox, can be programmed as either a manual or automated process. Authentication options include using a user id/password combination or user id/public key to gain access to the mailbox via ELM’s SFTP server. The ability to use a public key will depend on the functionality within a specific SFTP application.

INTERFACE

SFTP for Free (Using a Shareware Client)

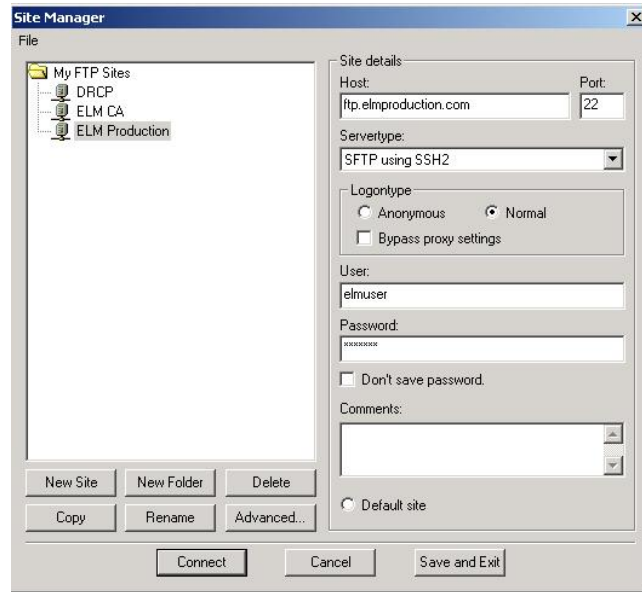
FileZilla is a “shareware” Secure FTP program that provides a straightforward and easy-to-use user interface for sending and receiving encrypted files. Shareware programs are distributed without paid maintenance and often without support. Only users authorized to install free, open-source software should continue with this section. If your security policies prohibit you from using this type of software – software without a paid-for license – please skip to the next section.

Note: ELM Resources does not endorse or recommend FileZilla in particular. We have used it with success but do not warrant it for use by others and take no responsibility for your particular use of this free product.

1. Go the FileZilla website at <http://filezilla.sourceforge.net>. Click on **Download** on the left side of the page and it will take you to a download screen for the latest

version of FileZilla. Proceed to download the FileZilla client, remembering where you direct the file to be saved. Once the download is complete, run the FileZilla installation.

2. In the general settings window of the FileZilla installation program, choose **Do Not Use Secure Mode** and **Use XML File** and complete the client installation.
3. Open the FileZilla client program. Under **File**, choose **Site Manager**.



4. Click on the **New Site** button and fill in the appropriate **Site Details**.
 - a. For testing, use ftp.elmtest.com.
For production, use ftp.elmproduction.com .
 - b. Put **22** in the Port field. **IMPORTANT!**
 - c. Choose **SFTP using SSH2** under **Servertype**. **IMPORTANT!**
 - d. Choose **Normal** for Log-on Type.
 - e. The User and Password will be the same as that used on the ELM Website when logging in to the ELM Web SLI. Your password is case-sensitive.
 - f. If allowed by your security rules, ensure the **Don't save password** checkbox remains **un-checked** – let it remember your password. Otherwise, check the checkbox and enter your connection password each time you go to connect to ELMNet.
5. Next, click the **Advanced** button in the Site Manager window and that will bring up a new dialogue box titled **Advanced Site settings**. In the Default local directory field, click on the browse button (the three dots on a gray button to the right of the field). Select the local file directory where you keep your files for ELM.

In the Default remote directory field enter `\mailbox\` followed by the name of your ELM mailbox (i.e. `\mailbox\ELM`).

Now, in the Passive transfer mode settings choose the button **Use default**. Click **OK**. Click **Save and Exit**.

6. Click the **Connect** button and you should see FileZilla process the secure log-on and display the directory structure of your destination SFTP site. Be patient, it may take a few moments for the destination site directories to be displayed.
 - a. The initial remote connection will be made to the Mailbox Directory which lists mailboxes alphabetically. Locate and click on your mailbox.

Remote Site: /mailbox/						
Filename ▲	Filesize	Filetype	Date	Time	Pe	
..						
AAA		File Folder	06/07/...	12:59		
AACC		File Folder	06/07/...	13:00		
AADA		File Folder	06/07/...	13:00		
AADANY		File Folder	06/07/...	13:00		
AAMU		File Folder	06/07/...	13:00		
AASC		File Folder	06/07/...	13:00		
ABC		File Folder	09/08/...	12:02		
ABS		File Folder	06/07/...	13:01		

7. Once a remote SFTP connection is made, you can transfer files simply by dragging and dropping in the customary Windows manner.

Remote Site: /mailbox/ELM/						
Filename ▲	Filesize	Filetype	Date	Time	Permissions	
..						
DELETED		File Folder	06/07/...	15:07		
INBOX		File Folder	06/07/...	15:07		
OUTBOX		File Folder	06/07/...	15:07		

NOTE: The first time you use FileZilla, you will receive a popup dialogue box that asks you if you want to continue the connection with the server you have reached. The server identifies itself (in the popup message) using a “fingerprint” – a series of letter/digit pairs. The letter/digit pairs below are unique to ELM’s systems – you will only get these specific codes from ELM systems. You should ensure that the fingerprints in the warning message are the same as one of the fingerprints listed below. You will only see this popup message the first time you connect and will not see it in any subsequent SFTP sessions.

The ELM “SFTP RSA key fingerprints” are:

ftp.elmtest.com
 e0:67:b0:b0:71:05:23:f9:b2:76:af:6c:34:86:c9:12

ftp.elmproduction.com
 80:6c:de:09:33:96:d3:84:dd:a7:77:fb:f1:24:47:55

File Transmission Directions

Receiving Files from ELMNet:

1. Open a Secure FTP connection and log in.
2. Navigate to your mailbox. The mailbox directory consists of the Inbox, Deleted, Outbox, and Transferred directories. You only have access to the Inbox, Deleted, and Outbox directories. The Transferred directory is for ELM's use.
3. Navigate to your mailbox Inbox directory.
4. Download copies of the files you wish to receive from the Inbox.
5. Upload copies of the downloaded files to the Deleted directory.
6. Delete remote copies of the files you've downloaded.

Sending Files to ELMNet:

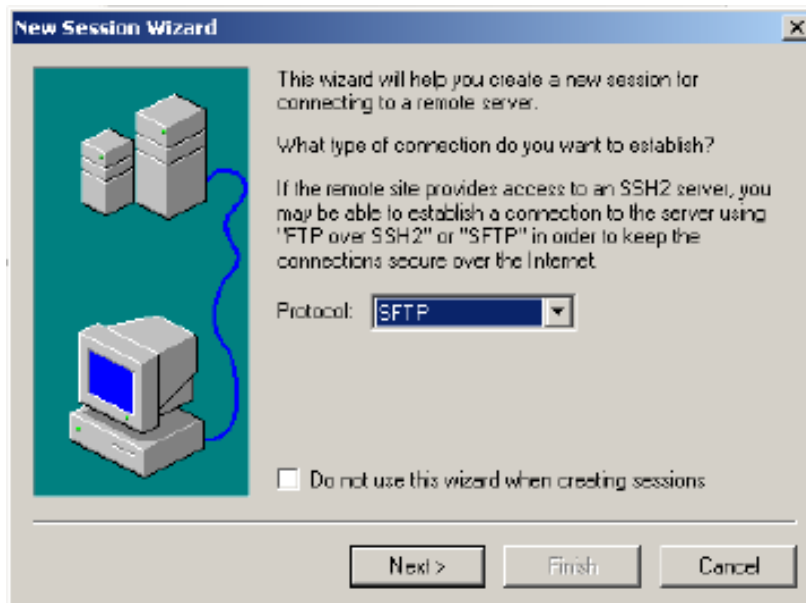
1. Open a SECURE FTP connection and log in.
2. Navigate to your mailbox.
3. Navigate to your mailbox Outbox directory.
4. When sending an application send or change file to ELMNet, the file will be put in the Outbox, so ELMNet can pick it up and process it. The naming convention for sending files is MMDDYY##.sis for appsend files and MMDDYY##.clc for change files (if applicable). The sequence number should increment by one for each file sent for that specific day.

SFTP with Commercial Software (Using a Commercial Client)

SecureFX is a commercial Secure FTP program that provides a straightforward and easy-to-use user interface for sending and receiving encrypted files. Only users who purchase this software or download it for evaluation should continue with this section. If you cannot purchase software, please go back to the prior section. ELM does not support, sell, or resell VanDyke Software products.

Note: ELM Resources does not endorse or recommend SecureFX in particular. We have used it with success but do not warrant it for use by others and take no responsibility for your particular use of this commercial product.

1. Go the VanDyke website at <http://www.vandyke.com>. Click on **Download** toward the top of the page and it will take you to a download screen for the latest version of SecureFX. Proceed to download the SecureFX client, remembering where you direct the file to be saved. Once the download is complete, run the SecureFX installation.
2. Open the SecureFX client, and from the **File** menu, click **Connect**.
3. In the **Connect** window, click on the **New Session** icon and it will bring up the New Session Wizard. Choose **SFTP** for the protocol, and fill in the appropriate SFTP site address in the next window. For testing, log on to <ftp.elmtest.com> or <ftp.elmimp.com> (as directed by ELM staff). For production, log on to <ftp.elmproduction.com>. Click **Next**, and use the appropriate user name and password.



4. When the remote site comes up on your screen, you can tile the **local** and **remote** windows by going to the **Window** menu and choosing **Tile Horizontally** or **Tile Vertically**.

5. Transfer files by dragging and dropping folders and files in the standard Windows method.
6. To set the initial local and remote directories for an ftp site, click on **File** and then **Connect**. Right click on the ftp site and choose **Properties**. You will be able to set the initial local and remote directories in this window. The local directory is the directory where you keep your files to send to ELM. The remote directory is your ELM Mailbox directory. In the remote directory window enter “\mailbox” followed by the name of your ELM mailbox directory name (i.e. \mailbox\ELM).

☞ **NOTE:** The first time you use SecureFX, you will receive a popup dialogue box that asks you if you want to continue the connection with the server you have reached. The server identifies itself (in the popup message) using a “fingerprint” – a series of letter/digit pairs. The letter/digit pairs below are unique to ELM’s systems – you will only get these specific codes from ELM systems. You should ensure that the fingerprints in the warning message are the same as one of the fingerprints listed below. You will only see this popup message the first time you connect and will not see it in any subsequent SFTP sessions.

The ELM “SFTP RSA key fingerprints” are:

ftp.elmtest.com

e0:67:b0:b0:71:05:23:f9:b2:76:af:6c:34:86:c9:12

ftp.elmproduction.com

80:6c:de:09:33:96:d3:84:dd:a7:77:fb:f1:24:47:55

How Does SFTP Work?

SFTP encrypts the entire file transfer in a single secure channel. By contrast, using a standard FTP client over an SSH port encrypts only the control channel. Standard FTP uses separate network (TCP) connections for control and data. Although control traffic may be forwarded over secure shell (SSH1), file content must be transferred outside Secure Shell over an unprotected data connection where it is vulnerable.

SFTP is a robust method of secure file transfer.

SFTP leverages Secure Shell for authenticated and encrypted file transfer. SFTP does not use port forwarding, but instead operates as a subsystem integrated with SSH2. The

SFTP protocol consists of remote file system commands like open and read; these commands are tunneled directly through the existing Secure Shell session. SFTP is not constrained by the multi-connection architecture of SSH1, but rather encrypts every bit of data including usernames, passwords and file data exchanged between an SFTP client and server.

Files are automatically encrypted/decrypted using Secure Shell (SSH) login. The entire session, including the transmission of the password, is encrypted. The encrypted session is moderated by an SFTP server, and the clients are capable of transmitting, receiving, and processing the encryption/decryption algorithm utilizing SSH over Port 22.

Not All Secure FTP Solutions Are the Same

ELM’s use of “FTP using SSH2” is one of a few ways to do secure FTP. Another technique uses a program called secure copy or “scp.” Scp uses Secure Shell version 1 (SSH1) to communicate between the client and the server, and the SSH1 server forwards unencrypted traffic to the FTP server. ELM does not use this because it is an outdated technology and is not as secure as FTP using SSH2. FTP using SSH2 adds an element to the data transfer called Message Identification Codes or MACs. These are used to ensure that the data sent was received accurately without alteration.

Another approach to secure FTP is to use the Secure Sockets Layer, SSL, as an addition to the FTP protocol. SSL is the technology used to encrypt web traffic for safe web browsing. It is used on merchant and banking web sites to protect visitor’s confidential information including credit card data and personal identification information. ELM does not support FTP using SSL.

The following table summarizes the different file transfer techniques and which ones are supported by ELM.

FTP Technique	Supported by ELM
File Transfer Protocol (FTP)	Yes *
File Transfer Protocol using SSL (FTPS)	No
Secure File Transfer Protocol using SSH1 (scp)	No
File Transfer Protocol using SSH2 (SFTP)	Yes
Secure Hyper Text Transfer Protocol (HTTPS) using SSL	Yes **

* Files must be pre-encrypted before being sent to ELM, typically with Pretty Good Privacy™ (PGP)

** Used interactively on the ELM Web site

Questions

Call ELM Priority Services at 866.524.8198

If you have questions about using Secure FTP, please contact the ELM Resources Priority Services Team at pss@elmresources.com, 866.524.8198