FL EDI SECURE FTP CONNECTIVITY TROUBLESHOOTING GUIDE

This troubleshooting guide covers secure file transfers using the SFTP file transfer protocols for Claims, POC, and Medical EDI transmissions.

SFTP (Secure File Transfer Protocol)

SFTP uses the SSH (Secure SHell) protocol for both command and data connections:

The client must support and use RSA keys with a key length of 2048-bits and the AES encryption algorithm with a 256-bit key length in order to use the SFTP protocol.

How SSH works:

A key pair is created by the client. The key pair consists of a public key, which you give to FL, and a private key, which you keep secret. The keys are mathematically related so that data encrypted by the public key can be decrypted by the private key and data encrypted by the private key can be decrypted by the public key. At logon, the server sends the client a "challenge", a message encrypted by the public key tied to the user's account. The client decrypts the message using its private key then re-encrypts the message using the server's public key. If the message matches the server's challenge and the user's FTP password is also correct, the user is authenticated. All subsequent data exchanges (file transfers) will be encrypted using a session key, a one-time-use password that is securely exchanged using the public/private key pairs.

To communicate with FL's FTP server using the SFTP protocol outgoing requests must be permitted on the following port:

- Port 22 (SSH) – port 22 will be used for the entire communication session.

Please note: This port only need to be available for **outgoing** connections (connections originating from inside your organization). If routers/firewalls are configured correctly, this should not create security vulnerabilities or expose your organization to hackers. If you are concerned with your employees being able to connect to other computers on the internet, or believe this activity will create a security risk, you can take the following measures to restrict connections:

1) Only permit outgoing connections on port 22 to FL's FTP server.

    a. Permit outgoing TCP connections from any internal host to FL's FTP server (158.229.250.41) when the TCP port = 22 (SSH).

2) Only permit outgoing connections on these port numbers to FL's FTP server from a specific IP address or subnet in your organization.

    a. Permit outgoing TCP connections from select internal host(s) (single IP or subnet) to FL's FTP server (158.229.250.41) when the TCP port = 22 (FTP Command).

The following is a log of a successful SFTP Session where the following high level events occur:

- An SFTP connection is established over port 22
- A User ID, Password, and RSA Key Pair are authenticated
- The current directory is changed (CWD)
- A directory listing is returned
- A file is transferred
- The user logs off

Log from Successful SFTP Tile Transfer

Command issued from command prompt:

```
wsftppro -s local:c:\users\humelsinem\Desktop\S000000050A49-20121210-
103412P.TXT -d SSH:/incoming/S000000050A49-20121210-103412P.TXT -binary
```

Creating SSH Connection on port 22:
Finding Host dwcftp.fldfs.com ...
[2012.12.10 10:36:30.687] Connecting to 172.17.200.17:22
[2012.12.10 10:36:30.691] Connected to 172.17.200.17:22 in 0.004000 seconds, Waiting for Server Response
[2012.12.10 10:36:30.696] Server Welcome: SSH-2.0-1.82_sshlib GlobalSCAPE
[2012.12.10 10:36:30.696] Client Version: SSH-2.0-WS_FTP-12.3-0

Server Creates a Challenge:
[2012.12.10 10:36:30.699] KexInitPacket (Server): no kex guess present
[2012.12.10 10:36:30.699] KexAlgorithms

Challenge Created by Client:
[2012.12.10 10:36:31.051] KexInitPacket (Client): no kex guess present
[2012.12.10 10:36:31.051] KexAlgorithms

Key Exchange Protocols Supported:

[2012.12.10 10:36:31.051] diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
[2012.12.10 10:36:31.051] 00: diffie-hellman-group-exchange-sha1
[2012.12.10 10:36:31.051] 01: diffie-hellman-group1-sha1

Key Types Supported:

[2012.12.10 10:36:31.051] ServerHostKeyAlgorithms
[2012.12.10 10:36:31.051] ssh-dss,ssh-rsa
[2012.12.10 10:36:31.051] 00: ssh-dss
[2012.12.10 10:36:31.051] 01: ssh-rsa

Encryption Algorithms Supported by Client:

(algorithms are numbered in order of preference with the lowest number being the highest priority)

[2012.12.10 10:36:31.051] CsEncryptionAlgorithms
[2012.12.10 10:36:31.051] aes256-cbc,3des-cbc,aes128-cbc,aes192-cbc,blowfish-cbc
[2012.12.10 10:36:31.051] 00: aes256-cbc
[2012.12.10 10:36:31.051] 01: 3des-cbc
[2012.12.10 10:36:31.051] 02: aes128-cbc
[2012.12.10 10:36:31.051] 03: aes192-cbc
[2012.12.10 10:36:31.051] 04: blowfish-cbc

Encryption Algorithms Supported by Server:

(algorithms are numbered in order of preference with the lowest number being the highest priority)

[2012.12.10 10:36:31.051] ScEncryptionAlgorithms
[2012.12.10 10:36:31.051] aes256-cbc,3des-cbc,aes128-cbc,aes192-cbc,blowfish-cbc
[2012.12.10 10:36:31.051] 00: aes256-cbc
[2012.12.10 10:36:31.051] 01: 3des-cbc
[2012.12.10 10:36:31.051] 02: aes128-cbc
[2012.12.10 10:36:31.051] 03: aes192-cbc
[2012.12.10 10:36:31.051] 04: blowfish-cbc

Hashing Algorithms Supported by Client:

(algorithms are numbered in order of preference with the lowest number being the highest priority)

[2012.12.10 10:36:31.051] CsMACAlgorithms
[2012.12.10 10:36:31.051] hmac-md5,hmac-sha1,hmac-ripemd160
[2012.12.10 10:36:31.051] 00: hmac-md5
[2012.12.10 10:36:31.051] 01: hmac-sha1
[2012.12.10 10:36:31.051] 02: hmac-ripemd160

Hashing Algorithms Supported by Server:

(algorithms are numbered in order of preference with the lowest number being the highest priority)

[2012.12.10 10:36:31.051] ScMACAlgorithms
[2012.12.10 10:36:31.051] hmac-md5,hmac-sha1,hmac-ripemd160
[2012.12.10 10:36:31.051] 00: hmac-md5
[2012.12.10 10:36:31.051] 01: hmac-sha1
[2012.12.10 10:36:31.051] 02: hmac-ripemd160

Compression Algorithms Supported by Client:
(algorithms are numbered in order of preference with the lowest number being the highest priority)

[2012.12.10 10:36:31.051] CsCompressionAlgorithms
[2012.12.10 10:36:31.051] zlib,none
[2012.12.10 10:36:31.051] 00: zlib
[2012.12.10 10:36:31.051] 01: none

Compression Algorithms Supported by Server:
(algorithms are numbered in order of preference with the lowest number being the highest priority)

[2012.12.10 10:36:31.051] ScCompressionAlgorithms
[2012.12.10 10:36:31.051] zlib,none
[2012.12.10 10:36:31.051] 00: zlib
[2012.12.10 10:36:31.051] 01: none

Initiating Key Exchange:
[2012.12.10 10:36:31.051] >SSH2_MSG_KEXINIT (330)

Stating Agreed Upon Algorithms:
[2012.12.10 10:36:31.051] SSH Transport agreed algorithms

Agreed Algorithm to Exchange (symmetric) Encryption Keys:
[2012.12.10 10:36:31.051] Purpose: key agreement Algo: diffie-hellman-group-exchange-sha1

Agreed Key Type is RSA-type:
[2012.12.10 10:36:31.051] Purpose: server host key Algo: ssh-rsa

Agreed Encryption Algorithm is AES-256 bit:
[2012.12.10 10:36:31.051] Purpose: encryption cs Algo: aes256-cbc
[2012.12.10 10:36:31.051] Purpose: encryption sc Algo: aes256-cbc

Agreed Hashing Algorithm is MD5:
[2012.12.10 10:36:31.051] Purpose: MAC cs Algo: hmac-md5

[2012.12.10 10:36:31.051] Purpose: MAC sc Algo: hmac-md5

Agreed Compression Algorithm is zlib:

[2012.12.10 10:36:31.051] Purpose: compression cs Algo: zlib
[2012.12.10 10:36:31.051] Purpose: compression sc Algo: zlib

Key Exchange:

[2012.12.10 10:36:31.080] >SSH2_MSG_KEX_DH_GEX_INIT (261)

[2012.12.10 10:36:31.120] SSH Server Host Key Size 277 bytes
[2012.12.10 10:36:31.120] SSH Signature Size 256 bytes
[2012.12.10 10:36:31.168] RSA Signature Verified
[2012.12.10 10:36:31.168] Session Keys Created
[2012.12.10 10:36:31.168] Ciphers Created
[2012.12.10 10:36:31.168] >SSH2_MSG_NEWKEYS (1)
[2012.12.10 10:36:31.168] New Client->Server ciphers in place.
[2012.12.10 10:36:31.168] New Server->Client ciphers in place.
[2012.12.10 10:36:31.168] Completed SSH Key Exchange. New Keys in place.

Requesting the SFTP Service:

[2012.12.10 10:36:31.168] >SSH2_MSG_SERVICE_REQUEST (17)
[2012.12.10 10:36:31.172] SSH2_MSG_SERVICE_ACCEPT (48)

Trying Password Authentication:

[2012.12.10 10:36:31.172] Trying authentication method: "password"
[2012.12.10 10:36:31.172] >SSH2_MSG_USERAUTH_REQUEST (64)
[2012.12.10 10:36:31.172] SSH2_MSG_USERAUTH_BANNER (80)

Authentication Resulted in Partial Success (FL requires two-part authentication – the password was correct):

[2012.12.10 10:36:31.175] SSH2_MSG_USERAUTH_FAILURE (32)
[2012.12.10 10:36:31.175] Authentication Method password(4) resulted in Partial Success

Trying Public Key Authentication:

[2012.12.10 10:36:31.175] Trying authentication method: "publickey"
[2012.12.10 10:36:32.196] Loaded key Pair "000000050", types(public,private): "RSA","RSA"
[2012.12.10 10:36:32.196] Key pair algorithm type: "ssh-rsa"
[2012.12.10 10:36:32.215] >SSH2_MSG_USERAUTH_REQUEST (615)

Two-Part Authentication Success (public key + password was correct for the username provided):

[2012.12.10 10:36:32.221] SSH2_MSG_USERAUTH_SUCCESS (16)
[2012.12.10 10:36:32.221] User Authenticated OK!

[2012.12.10 10:36:32.221] Completed SSH User Authentication.

Opening SFTP Connection:

[2012.12.10 10:36:32.221] >SSH2_MSG_CHANNEL_OPEN (24)
[2012.12.10 10:36:32.223] SSH2_MSG_CHANNEL_OPEN_CONFIRMATION (32)
[2012.12.10 10:36:32.223] SSH Channel confirmed open: LocalID:(0760a2ce) ServerID(00000000) ServerMaxPacket(35840) ServerWindow(33554432)
[2012.12.10 10:36:32.223] >SSH2_MSG_CHANNEL_REQUEST (27)
[2012.12.10 10:36:32.228] SSH2_MSG_CHANNEL_SUCCESS (32)
[2012.12.10 10:36:32.228] Started subsystem "sftp" on channel 0760a2ce
[2012.12.10 10:36:32.228] >SSH2_MSG_DISCONNECT #4 (5)
[2012.12.10 10:36:32.228] >SSH2_MSG_CHANNEL_DATA (18)
[2012.12.10 10:36:32.231] SSH2_MSG_CHANNEL_DATA (32)
[2012.12.10 10:36:32.231] <SSH_FXP_VERSION #3 (5)
[2012.12.10 10:36:32.231] SFTP Protocol Version 3 OK
[2012.12.10 10:36:32.231] >SSH_FXP_REALPATH #3294 (10)
[2012.12.10 10:36:32.231] >SSH2_MSG_CHANNEL_DATA (23)
[2012.12.10 10:36:32.266] SSH2_MSG_CHANNEL_DATA (48)
[2012.12.10 10:36:32.266] <SSH_FXP_NAME #3294 (23)
[2012.12.10 10:36:32.266] sftp protocol initialized

Changing Directory to [/incoming]:

[2012.12.10 10:36:32.267] Changing remote directory to "/incoming"
[2012.12.10 10:36:32.267] >SSH_FXP_OPENDIR #1110 (18)
[2012.12.10 10:36:32.267] >SSH2_MSG_CHANNEL_DATA (31)
[2012.12.10 10:36:32.276] SSH2_MSG_CHANNEL_DATA (32)
[2012.12.10 10:36:32.276] <SSH_FXP_HANDLE #1110 (10)
[2012.12.10 10:36:32.276] >SSH_FXP_CLOSE #1929 (10)
[2012.12.10 10:36:32.276] >SSH2_MSG_CHANNEL_DATA (23)
[2012.12.10 10:36:32.279] SSH2_MSG_CHANNEL_DATA (48)
[2012.12.10 10:36:32.279] <SSH_FXP_STATUS #1929 (21)

Getting Directory Listing in [/incoming]:

[2012.12.10 10:36:32.279] Getting Dirlisting
[2012.12.10 10:36:32.279] >SSH_FXP_OPENDIR #1110 (18)
[2012.12.10 10:36:32.279] >SSH2_MSG_CHANNEL_DATA (31)
[2012.12.10 10:36:32.287] SSH2_MSG_CHANNEL_DATA (32)
[2012.12.10 10:36:32.287] <SSH_FXP_HANDLE #1110 (10)
[2012.12.10 10:36:32.288] >SSH_FXP_READDIR #3021 (10)
[2012.12.10 10:36:32.288] >SSH2_MSG_CHANNEL_DATA (23)
[2012.12.10 10:36:32.293] SSH2_MSG_CHANNEL_DATA (272)
[2012.12.10 10:36:32.293] <SSH_FXP_NAME #3021 (525)

[2012.12.10 10:36:32.293] >SSH_FXP_READDIR #3021 (10)
[2012.12.10 10:36:32.293] >SSH2_MSG_CHANNEL_DATA (23)
[2012.12.10 10:36:32.295] SSH2_MSG_CHANNEL_DATA (48)
[2012.12.10 10:36:32.295] <SSH_FXP_STATUS #3021 (22)
[2012.12.10 10:36:32.295] # transferred 529 bytes in 0.007 seconds, 604.571 kbps (75.571 kBps), transfer succeeded.
[2012.12.10 10:36:32.295] >SSH_FXP_CLOSE #1929 (10)

Transferring File from Local User's Desktop to [/incoming]:

[2012.12.10 10:36:32.295] >SSH2_MSG_CHANNEL_DATA (23)
[2012.12.10 10:36:32.297] SSH2_MSG_CHANNEL_DATA (32)
[2012.12.10 10:36:32.297] <SSH_FXP_STATUS #1929 (21)
[2012.12.10 10:36:32.304] Opening remote file **"/incoming/S000000050A49-20121210-103412P.TXT" for writing**
[2012.12.10 10:36:32.304] >SSH_FXP_OPEN #1383 (61)
[2012.12.10 10:36:32.304] >SSH2_MSG_CHANNEL_DATA (74)
[2012.12.10 10:36:32.315] SSH2_MSG_CHANNEL_DATA (32)
[2012.12.10 10:36:32.315] <SSH_FXP_HANDLE #1383 (10)
[2012.12.10 10:36:32.315] Uploading local file **"c:\users\humelsinem\Desktop\S000000050A49-20121210-103412P.TXT"**
[2012.12.10 10:36:32.315] SFTP Send File, Server window size: 33554432, Server packet size: 35800, 10 packets ahead
[2012.12.10 10:36:32.315] >SSH_FXP_WRITE #1234 (129)
[2012.12.10 10:36:32.315] >SSH2_MSG_CHANNEL_DATA (142)
[2012.12.10 10:36:32.320] SSH2_MSG_CHANNEL_DATA (32)
[2012.12.10 10:36:32.320] <SSH_FXP_STATUS #1234 (21)
[2012.12.10 10:36:32.320] # transferred 107 bytes in 0.005 seconds, 171.200 kbps (21.400 kBps), transfer succeeded.
[2012.12.10 10:36:32.320] >SSH_FXP_CLOSE #1929 (10)
[2012.12.10 10:36:32.320] >SSH2_MSG_CHANNEL_DATA (23)
[2012.12.10 10:36:32.352] SSH2_MSG_CHANNEL_DATA (32)
[2012.12.10 10:36:32.352] <SSH_FXP_STATUS #1929 (21)
Transfer request completed with status: Finished

Closing SFTP Connection:

[2012.12.10 10:36:32.356] Sending channel close message for channel 0760a2ce
[2012.12.10 10:36:32.356] >SSH2_MSG_CHANNEL_CLOSE (5)
[2012.12.10 10:36:32.356] SSH Transport closed.
[2012.12.10 10:36:32.356] Connection closed. Ready for next connection.