

# FL Division of Workers' Compensation

## SSL/FTP Connectivity Troubleshooting Guide

To communicate with our SSL/FTP Server, port 21 must be used for the initial certificate exchange and logon. In addition, ports 1024 thru 2000 must be opened for outgoing requests from the client computers. When the client computers go into passive mode for data transfer (used during file transfer, and for returning directory listings), our SSL/FTP Server sends the port numbers to be used, and then the client computer can connect to our SSL/FTP Server on these requested ports. The port numbers are issued dynamically by our server, depending upon current load, number of users, and actual transfers currently taking place, etc. Please note that it is only the outgoing traffic that requires these high port numbers opened. If routers are programmed correctly, this should not expose these ports to external Internet hackers. Furthermore, if there is a concern regarding internal employees having access to connect to other computers on the Internet, using these high port numbers for activity that may be considered a security risk, the following two additional measures may be taken:

1. Limit the outgoing destination server available for these high port numbers (by IP restriction) to only to connect to the division's SSL/FTP Server (sslftp.fldfs.com @ 158.229.250.201).
2. Limit the computers (and thus employees) within the organization that have these high port numbers open by segment or IP Address of the specific computers.

The following is a log of a successful SSL/FTP Session where the following high level events occur:

- An FTP Connection is established over port 21
- A Certificate is exchanged / verified with the host computer
- A UserID & Password are authenticated
- A directory listing is returned for the user's home directory
- The current directory is changed (CWD)
- A file is transferred
- The user logs off

A detailed explanation of the log entries follows this log printout:

```
[2004.06.24 15:13:57.876] Connecting to 158.229.250.201:21
[2004.06.24 15:13:57.906] Connected to 158.229.250.201:21 in 0.020028 seconds, waiting for Server
Response
[2004.06.24 15:13:57.906] Initializing SSL Session ...
[2004.06.24 15:13:57.916] 220 SSLFTP X2 WS_FTP Server 5.0.4 (3078219534)
[2004.06.24 15:13:57.936] AUTH SSL
[2004.06.24 15:13:58.447] 234 SSL enabled and waiting for negotiation
[2004.06.24 15:13:58.617] SSL Session Started.
[2004.06.24 15:13:58.637] Host type (1): WS_FTP Server
[2004.06.24 15:13:58.637] XAUT 2 <@::C362<15:C:5=;?58C95;775:C:5=;?;4D:5=<@5:D>9;
[2004.06.24 15:13:58.647] 230 user logged in
[2004.06.24 15:13:58.647] Host type (1): WS_FTP Server
[2004.06.24 15:13:58.647] PBSZ 0
```

# FL Division of Workers' Compensation

## SSL/FTP Connectivity Troubleshooting Guide

[2004.06.24 15:13:58.657] 200 PBSZ=0  
[2004.06.24 15:13:58.657] PROT P  
[2004.06.24 15:13:58.667] 200 PRIVATE data channel protection level set  
[2004.06.24 15:13:58.667] Sending "FEAT" command to determine what features this server supports.  
[2004.06.24 15:13:58.667] FEAT  
[2004.06.24 15:13:58.677] 211-Extensions supported  
[2004.06.24 15:13:58.677] SIZE  
[2004.06.24 15:13:58.677] MDTM  
[2004.06.24 15:13:58.677] MLST size\*;type\*;perm\*;create\*;modify\*;  
[2004.06.24 15:13:58.677] LANG EN\*  
[2004.06.24 15:13:58.677] REST STREAM  
[2004.06.24 15:13:58.677] TVFS  
[2004.06.24 15:13:58.677] UTF8  
[2004.06.24 15:13:58.677] AUTH SSL;TLS-P;  
[2004.06.24 15:13:58.677] PBSZ  
[2004.06.24 15:13:58.677] PROT C;P;  
[2004.06.24 15:13:58.677] 211 end  
[2004.06.24 15:13:58.677] Finished interpreting "FEAT" response.  
[2004.06.24 15:13:58.677] Sending the FEAT command is optional. It can be disabled in the site options of the profile.  
[2004.06.24 15:13:58.677] PWD  
[2004.06.24 15:13:58.687] 257 "/users/mtp158" is current directory  
[2004.06.24 15:13:58.687] TYPE A  
[2004.06.24 15:13:58.697] 200 Type set to ASCII.  
[2004.06.24 15:13:58.697] PASV  
[2004.06.24 15:13:58.737] 227 Entering Passive Mode (158.229.250.201:5,218).  
[2004.06.24 15:13:58.737] connecting data channel to 158.229.250.201:5,218(1498)  
[2004.06.24 15:13:58.747] data channel connected to 158.229.250.201:5,218(1498)  
[2004.06.24 15:13:58.747] MLSD  
[2004.06.24 15:13:58.767] 150 Opening ASCII data connection for directory listing  
[2004.06.24 15:13:58.817] # transferred 1451 bytes in < 0.001 seconds, 11335.938 Kbps (1416.992 Kbps), transfer succeeded.  
[2004.06.24 15:13:58.907] 226 transfer complete  
Starting request  
[2004.06.25 08:47:49.228] CWD incoming  
[2004.06.25 08:47:49.258] 250 CWD incoming  
[2004.06.25 08:47:49.258] PWD  
[2004.06.25 08:47:49.499] 257 "/users/admin4ftp/incoming" is current directory  
[2004.06.25 08:47:49.499] PASV  
[2004.06.25 08:47:49.509] 227 Entering Passive Mode (158.229.250.201:6,18).  
[2004.06.25 08:47:49.509] connecting data channel to 158.229.250.201:6,18(1554)  
[2004.06.25 08:47:49.529] data channel connected to 158.229.250.201:6,18(1554)  
[2004.06.25 08:47:49.529] MLSD

# FL Division of Workers' Compensation

## SSL/FTP Connectivity Troubleshooting Guide

[2004.06.25 08:47:49.539] 150 Opening ASCII data connection for directory listing  
[2004.06.25 08:47:49.589] # transferred 157 bytes in < 0.001 seconds, 1226.563 Kbps ( 153.320 Kbps), transfer succeeded.  
[2004.06.25 08:47:49.699] 226 transfer complete  
[2004.06.24 15:14:21.750] TYPE I  
[2004.06.24 15:14:21.770] 200 Type set to IMAGE.  
[2004.06.24 15:14:21.770] PASV  
[2004.06.24 15:14:21.780] 227 Entering Passive Mode (158.229.250.201,5,219).  
[2004.06.24 15:14:21.780] connecting data channel to 158.229.250.201:5,219(1499)  
[2004.06.24 15:14:24.805] data channel connected to 158.229.250.201:5,219(1499)  
[2004.06.24 15:14:24.805] STOR fields.txt  
[2004.06.24 15:14:24.815] 150 Opening BINARY data connection for fields.txt  
[2004.06.24 15:14:25.035] 226 transfer complete  
[2004.06.24 15:14:25.035] # transferred 5383 bytes in 0.010 seconds, 4199.422 Kbps (524.928 Kbps), transfer succeeded.  
Transfer request completed with status: Finished  
[2004.06.24 15:14:25.045] TYPE A  
[2004.06.24 15:14:25.055] 200 Type set to ASCII.  
[2004.06.24 15:14:25.055] PASV  
[2004.06.24 15:14:25.065] 227 Entering Passive Mode (158.229.250.201,5,220).  
[2004.06.24 15:14:25.065] connecting data channel to 158.229.250.201:5,220(1500)  
[2004.06.24 15:14:25.085] data channel connected to 158.229.250.201:5,220(1500)  
[2004.06.24 15:14:25.085] MLSD  
[2004.06.24 15:14:25.105] 150 Opening ASCII data connection for directory listing  
[2004.06.24 15:14:25.165] # transferred 1539 bytes in 0.010 seconds, 1200.615 Kbps (150.077 Kbps), transfer succeeded.  
[2004.06.24 15:14:25.315] 226 transfer complete  
[2004.06.24 15:14:27.729] QUIT  
[2004.06.24 15:14:27.739] 221 Good-Bye  
[2004.06.24 15:14:27.739] Connection closed. Ready for next connection.

### **Detailed breakdown of SSL/FTP Log, with important comments included:**

#### **Original FTP Connection: (Port 21)**

[2004.06.24 15:13:57.876] Connecting to 158.229.250.201:21  
[2004.06.24 15:13:57.906] Connected to 158.229.250.201:21 in 0.020028 seconds, Waiting for Server Response

#### **Host SSL/FTP going into forced SSL mode and requesting client certificate (234): (Port 21)**

[2004.06.24 15:13:57.906] Initializing SSL Session ...  
[2004.06.24 15:13:57.916] 220 SSLFTP X2 WS\_FTP Server 4.0.2 (834488424)  
[2004.06.24 15:13:57.936] AUTH SSL  
[2004.06.24 15:13:58.447] 234 SSL enabled and waiting for negotiation

# FL Division of Workers' Compensation

## SSL/FTP Connectivity Troubleshooting Guide

### **Host accepts clients SSL Certificate and starts 128-bit encrypted session: (Port 21)**

[2004.06.24 15:13:58.617] SSL Session Started.  
[2004.06.24 15:13:58.637] Host type (1): WS\_FTP Server

### **UserID & Password sent across encrypted channel: (Port 21)**

[2004.06.24 15:13:58.637] XAUT 2 <@::C362<15:C:5=;?58C95;775:C:5=;?;4D:5=<@5:D>9;

### **Host successfully authenticates UserID & Password: (Port 21)**

[2004.06.24 15:13:58.647] 230 user logged in

### **Client interrogates host to see what kind of host it is, and what features it supports: (Port 21)**

[2004.06.24 15:13:58.647] Host type (I): WS\_FTP Server  
[2004.06.24 15:13:58.647] PBSZ 0  
[2004.06.24 15:13:58.657] 200 PBSZ=0  
[2004.06.24 15:13:58.657] PROT P  
[2004.06.24 15:13:58.667] 200 PRIVATE data channel protection level set  
[2004.06.24 15:13:58.667] Sending "FEAT" command to determine what features this server supports.  
[2004.06.24 15:13:58.667] FEAT  
[2004.06.24 15:13:58.677] 211-Extensions supported  
[2004.06.24 15:13:58.677] SIZE  
[2004.06.24 15:13:58.677] MDTM  
[2004.06.24 15:13:58.677] MLST size\*;type\*;perm\*;create\*;modify\*;  
[2004.06.24 15:13:58.677] LANG EN\*  
[2004.06.24 15:13:58.677] REST STREAM  
[2004.06.24 15:13:58.677] TVFS  
[2004.06.24 15:13:58.677] UTF8  
[2004.06.24 15:13:58.677] AUTH SSL;TLS-P;  
[2004.06.24 15:13:58.677] PBSZ  
[2004.06.24 15:13:58.677] PROT C;P;  
[2004.06.24 15:13:58.677] 211 end  
[2004.06.24 15:13:58.677] Finished interpreting "FEAT" response.  
[2004.06.24 15:13:58.677] Sending the FEAT command is optional. It can be disabled in the site options of the profile.

### **Notice how the client is automatically placed in their home directory: (Port 21)**

Note: The accounts are actually locked into the home directory as well.

[2004.06.24 15:13:58.677] PWD  
[2004.06.24 15:13:58.687] 257 "/users/mtp158" is current directory

### **ASCII mode is requested by the client in preparation for directory listing xfer: (Port 21)**

[2004.06.24 15:13:58.687] TYPE A  
[2004.06.24 15:13:58.697] 200 Type set to ASCII.

# FL Division of Workers' Compensation

## SSL/FTP Connectivity Troubleshooting Guide

### **Client software enters Passive mode in preparation for directory listing xfer: (Port 21)**

[2004.06.24 15:13:58.697] PASV

[2004.06.24 15:13:58.737] 227 Entering Passive Mode (158.229.250.201,5,218).

### **Host instructs client to use port 1498 for the directory listing xfer, and directory list is sent: (Port 1498)**

Note: Passive mode is how the host computer tells the client which high data port numbers to use for data transfers. Data transfers include both directory listings and actual file transfers (uploads OR downloads). Passive mode is required for using the division's SSL/FTP server because the division's SSL/FTP server is located behind a firewall. The range of high data port numbers that are used for the division's server is 1024 – 2000. Ensure that the router is set up to allow outgoing connections on this range of port numbers for the client computer.

[2004.06.24 15:13:58.737] connecting data channel to 158.229.250.201:5,218(1498)

[2004.06.24 15:13:58.747] data channel connected to 158.229.250.201:5,218(1498)

[2004.06.24 15:13:58.747] MLSD

[2004.06.24 15:13:58.767] 150 Opening ASCII data connection for directory listing

[2004.06.24 15:13:58.817] # transferred 1451 bytes in < 0.001 seconds, 11335.938 Kbps (1416.992 Kbps), transfer succeeded.

[2004.06.24 15:13:58.907] 226 transfer complete

### **Client changes directory to the incoming folder in the client home directory: (Port 21)**

Starting request

[2004.06.25 08:47:49.228] CWD incoming

[2004.06.25 08:47:49.258] 250 CWD incoming

[2004.06.25 08:47:49.258] PWD

[2004.06.25 08:47:49.499] 257 "/users/admin4ftp/incoming" is current directory

### **A new directory listing must be requested and sent because the division has changed directories: (Port 1554)**

Note: Port 1554 is selected by the server for the directory listing transfer.

[2004.06.25 08:47:49.499] PASV

[2004.06.25 08:47:49.509] 227 Entering Passive Mode (158.229.250.201,6,18).

[2004.06.25 08:47:49.509] connecting data channel to 158.229.250.201:6,18(1554)

[2004.06.25 08:47:49.529] data channel connected to 158.229.250.201:6,18(1554)

[2004.06.25 08:47:49.529] MLSD

[2004.06.25 08:47:49.539] 150 Opening ASCII data connection for directory listing

[2004.06.25 08:47:49.589] # transferred 157 bytes in < 0.001 seconds, 1226.563 Kbps ( 153.320 Kbps), transfer succeeded.

[2004.06.25 08:47:49.699] 226 transfer complete

### **Transfer Mode is set to Binary (I) in preparation to upload data file: (Port 21)**

[2004.06.24 15:14:21.750] TYPE I

[2004.06.24 15:14:21.770] 200 Type set to IMAGE.

# FL Division of Workers' Compensation

## SSL/FTP Connectivity Troubleshooting Guide

### **Client goes into Passive mode in preparation for file transfer: (Port 1499)**

Note: High port number 1499 is selected by the host for the transfer.

[2004.06.24 15:14:21.770] PASV

[2004.06.24 15:14:21.780] 227 Entering Passive Mode (158.229.250.201,5,219).

[2004.06.24 15:14:21.780] connecting data channel to 158.229.250.201:5,219(1499)

[2004.06.24 15:14:24.805] data channel connected to 158.229.250.201:5,219(1499)

### **Client software initiates the actual file transfer (upload) of a file called fields.txt: (Port 1499)**

[2004.06.24 15:14:24.805] STOR fields.txt

[2004.06.24 15:14:24.815] 150 Opening BINARY data connection for fields.txt

[2004.06.24 15:14:25.035] 226 transfer complete

[2004.06.24 15:14:25.035] # transferred 5383 bytes in 0.010 seconds, 4199.422 Kbps (524.928 Kbps), transfer succeeded.

Transfer request completed with status: Finished

### **Another directory listing is requested, because of the uploaded file changing the contents: (Port 21)**

Note: Client switches back to ASCII transfer mode in preparation for directory listing xfer.

[2004.06.24 15:14:25.045] TYPE A

[2004.06.24 15:14:25.055] 200 Type set to ASCII.

### **Client goes into Passive mode in preparation for directory listing transfer: (Port 1500)**

Note: High port number 1500 is selected by the host for the transfer.

[2004.06.24 15:14:25.055] PASV

[2004.06.24 15:14:25.065] 227 Entering Passive Mode (207,156,46,139,5,220).

[2004.06.24 15:14:25.065] connecting data channel to 158.229.250.201:5,220(1500)

[2004.06.24 15:14:25.085] data channel connected to 158.229.250.201:5,220(1500)

[2004.06.24 15:14:25.085] MLSD

[2004.06.24 15:14:25.105] 150 Opening ASCII data connection for directory listing

[2004.06.24 15:14:25.165] # transferred 1539 bytes in 0.010 seconds, 1200.615 Kbps (150.077 Kbps), transfer succeeded.

[2004.06.24 15:14:25.315] 226 transfer complete

### **Client computer logs out of the SSL/FTP Session: (Port 21)**

[2004.06.24 15:14:27.729] QUIT

[2004.06.24 15:14:27.739] 221 Good-Bye

[2004.06.24 15:14:27.739] Connection closed. Ready for next connection.