

FLORIDA DIVISION OF WORKERS' COMPENSATION

Submitter Instructions Creating a Florida WC SSL/FTP Account

Scope and Purpose:

This document is intended as a guide to walk the submitter through the process of setting up a Secure Socket Layer/File Transfer Protocol (SSL/FTP) account with Florida's Division of Workers' Compensation. The SSL/FTP accounts are used for transmitting electronic medical, claims and proof of coverage transactions. Using the SSL/FTP accounts is a Health Insurance Portability and Accountability Act (HIPAA) compliant transmission vehicle utilizing signed digital certificates and 128-bit encryption technology.

Selecting and Installing a SSL/FTP Client Software Program:

These instructions are tailored to the WS-FTP Pro software program, **version 9.0**, on a Microsoft Windows platform. If a different SSL/FTP software program has been selected, either because there is already a SSL/FTP program established, or because there is a different operating system involved, please make sure that the SSL/FTP program selected can utilize one of the following certificate negotiation methods: AUTH SSL, AUTH TLS-P, AUTH TLS, AUTH TLS-C. **For a complete list of SSL/FTP Programs that run on a variety of platforms, refer to the following web site:**

http://www.ford-hutchinson.com/~fh-1-pfh/ftps-ext_col.html

Creating a Private Key (.key) file, Self-Signed Certificate (.crt) file, and a Certificate Signing Request (.csr) file:

The objective of this section is to generate an Encryption Key (.key) file, a self-signed Digital Certificate (.crt) file, and a Certificate Signing Request (.csr) file. The Certificate Signing Request file is then sent (e-mailed) to the Division of Workers' Compensation to be authenticated and signed. The division will send (e-mail) the signed certificate file (.crt) back so that it may be installed and used for connecting to the division's SSL/FTP Server. These steps will need to be performed only once at initial set-up.

Steps using WS-FTP Pro:

1. Run WS-FTP Pro, and close the "Site Manager" dialog box that pops up for connecting to profiles.
2. Select on the "Options" button at the top of the screen, and click on the tree-view item "Client Certificates" under the "SSL" branch.
3. Click on the "Create" button to start the process of creating a new certificate request.
4. In the "Certificate Name" field, enter your FTP userid (six-character Submitter ID - mtpNNN). Note: If you are a new Submitter, contact the division to receive your FTP userid.
5. For the "Expiration Date" field, simply enter some date that is 20 years into the future.
6. For the "Pass Phrase" field, make up a password or pass-phrase (multiple words separated by spaces). This does not have to be the same as your FTP account password (although it can be if you wish). Do not lose this password, however, as it is your "private" encryption keys; do not provide this password to us or anyone else outside your organization.
7. Type the passphrase over again in the "Confirm Passphrase" field.
8. Click the "Next" button to proceed to the next window.
9. Enter the "City" and two-letter abbreviation for your "State", and "US" in the Country in the requested fields. Click the "Next" button.

Submitter Instructions Creating a Florida WC SSL/FTP Account

10. For the “Common Name” field, enter the URL of your company’s web site. If your company does not have a web site, enter your name in this field (First + Last).
11. Enter your e-mail address in the “E-mail” field. (required)
12. For the “Organization” field, enter your company’s name.
13. For the “Unit” field, enter the name of your department within your company. If you do not have a department name, please enter “EDI” for the unit name. Click the “Next” button.
14. Click on the “Finish” button. You will receive a confirmation pop-up message if it was successful. Click on the “OK” button of the pop-up confirmation message to close this window.



15. This will create three files in the “C:\Documents and Settings\your_computer_login_ID\Application Data\IpSwitch\WS_FTP\SSL\Certs” directory; Self-signed Certificate file (.crt), Private Key File (.key), and a Certificate Signing Request File (.csr).
16. You will now be returned to the list of the Client Certificates, where you should see your new mtpNNN certificate listed.
17. Click OK, and then exit the WS-FTP Pro program.
18. Using your e-mail software, attach the Certificate Signing Request (.csr) file to an e-mail message and send it to Pi-Ching Huang at Pi-Ching.Huang@myfloridacfo.com or Theresa Pugh at Theresa.Pugh@myfloridacfo.com.
19. Our SSL/FTP account managers will authenticate your identity, digitally sign your certificate request, and e-mail you back a signed certificate file (.crt) for you to use (see steps below).

Requesting a SSL/FTP User account from the Florida Division of Workers’ Compensation:

At this point an FTP userid and password has been established. The userid will be the six-digit Submitter ID. If both medical and claims data are transmitted to the division, then two different SSL/FTP accounts will need to be established. Eventually, these accounts may be merged or combined, but for now they must both be maintained.

If both medical and claims data are transmitted, only one SSL Certificate signed and configured on your system will be required, even though there are two different SSL/FTP accounts. The software will use the same certificate for both SSL/FTP accounts.

Upon receiving the e-mail containing the Certificate Signing Request (.csr) File, the division will process the request and e-mail the signed certificate (.crt) file back after activating the SSL/FTP account. The filename for the signed certificate file sent back will have the same name as the .csr File sent to the division, but with “_Signed” added to the filename. For example, if a Certificate Signing Request File called “MTP125.csr” is sent, then a “MTP125_Signed.crt” file will be returned.

Submitter Instructions Creating a Florida WC SSL/FTP Account

Receiving and configuring the Signed Certificate (.crt) File from the Division of Workers' Compensation:

Once the e-mail from the division's SSL/FTP account manager containing the Signed Certificate (.crt) file is received, save the file and configure the SSL/FTP Software Program to use the signed certificate for secure file transfers.

Steps using WS-FTP Pro:

1. From the e-mail, save the attached Signed Certificate File (.crt) to the "C:\Program Files\WS_FTP Pro" directory. This can be accomplished in most e-mail programs by right clicking on the attachment icon and selecting "Save As," then navigating to the desired directory. NOTE: Sometimes, due to e-mail virus protection, we may have to send the signed certificate to you with a .txt filename extension added to the end of the filename (i.e. – mtp143.crt.txt). If this is the case, trim off the .txt as you are saving the file to make it a .crt filename extension (i.e. – mtp143.crt).
2. Run WS-FTP Pro, and close the Site Manager dialog box that pops up connecting to profiles.
3. Click the "Options" button at the top of the screen, and click on the tree-view item "Client Certificates" under the "SSL" branch.
4. Click on the "Import" button.
5. Click on the "Browse" button in the lower right corner, and navigate to the C:\Program Files\WS_FTP Pro" directory to select the signed certificate file (mtpNNN_Signed.crt), and click the "Open" button after selecting it. This will place the signed certificate filename into the "Public Key File" box. NOTE: This may be a little confusing, because it is actually a CERTIFICATE to be selected at this prompt. Select the signed certificate for this step (not the key file).
6. Click on the "Next" button to proceed to the next window.
7. To select the "Private Key File", click on the "Browse" button in the lower right corner, and navigate to the C:\Documents and Settings\Your Username\Application Data\Ipswitch\WS_FTP\SSL\Certs directory, and select your mtpNNN.key file, and then click the "Open" button.
8. Click the "Next" button to proceed to the next window.
9. Enter your pass phrase in the "Password" field.
10. Click the "Next" button to proceed to the next window.
11. For the "Certificate Name", enter your Submitter ID followed by an underscore "_" and the word "Signed". For example: mtp143_Signed
12. Click the "Next" button to proceed to the next window.
13. Click "Finish" to finish importing the Signed SSL Certificate.
14. Click "OK" close the Settings window.
15. Exit WS FTP Pro.

Creating a new connection Profile to connect to the Division of Workers' Compensation SSL/FTP Site:

The objective of this section is to configure the SSL/FTP software with the division's SSL/FTP site address, and specifically configure the connection profile to use SSL encryption for the connection and data channels.

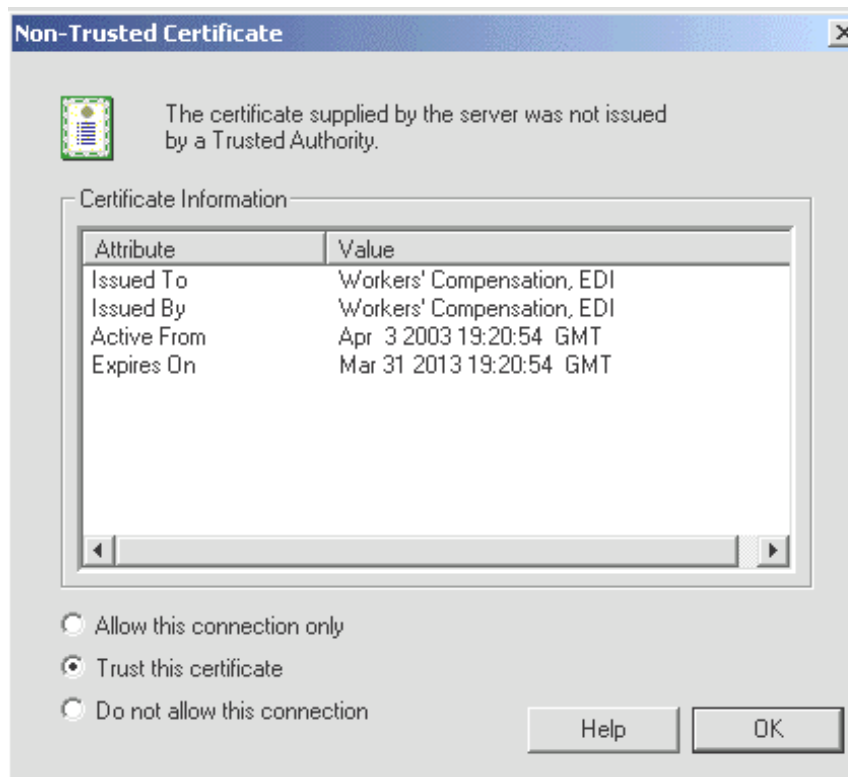
Submitter Instructions Creating a Florida WC SSL/FTP Account

Steps using WS-FTP Pro:

1. Run WS-FTP Pro.
2. Click on the “Create Site” button on the Site Manager dialog box.
3. A “Wizard” type user interface for creating the connection will appear.
4. Enter a name to give the connection, such as “FL WC SSL FTP Site”.
5. Click “Next”.
6. Enter sslftp.fldfs.com in the “Host Name or IP Address” field.
7. Click “Next”.
8. Enter the userid (six-digit Submitter ID), and the assigned FTP password.
9. Click “Next”.
10. Select Connection Type “FTP/SSL (AUTH SSL)”
11. Click “Next”
12. Un-check the “Connect to this Site” checkbox.
13. Click “Finish”. This will return to the connection dialog box.
14. Make sure the new connection profile is still selected and click on the “Edit” button.
15. Click on the “SSL” tree branch on the left side of the “Site Options” window.
16. Select your new signed Client Certificate in the dropdown box (i.e.: mtpNNN_Signed).
17. Check the box that reads “Use only 128 bit SSL for Secure Connections”.
18. Click “OK” to accept the changes to the connection profile.

Connecting to the Division of Workers’ Compensation SSL/FTP Site:

When connecting to the division’s SSL/FTP for the first time, the following confirmation message will appear:



Submitter Instructions Creating a Florida WC SSL/FTP Account

Select the “Trust this Certificate” option and click OK. This is saying that the self-signed certificate is accepted (accepting the division’s identity). The division is performing identity verifications before signing any certificates. This alleviates the need to pay a third party company to authenticate the certificate.

Upon connection, the following three subdirectories will be listed: incoming, outgoing, and badfiles. The subdirectories are to be used for the following purpose:

Use the **incoming** directory to place all incoming data files sent to the division.

PLEASE NOTE: DO NOT ZIP any files before transmitting them. The SSL/FTP connection is a 128-bit secured, encrypted channel, and the files do not need to be zipped.

Medical Claim Processing Reports will be placed in the **outgoing** directory. An e-mail notice will be sent when files are placed in this file for pick up. Delete the file(s) from the outgoing directory after retrieval. When the division’s system detects that an incoming file cannot be processed (i.e. – defective, empty, bad filename, etc.), an e-mail notice stating the problem and the file will be placed into the **badfiles** directory for further action. Delete the file from this directory after resolving the problem.

Programming notes:

The WS-FTP Pro software has a very powerful scripting language that allows automation of the connection and file transfers, should there be a need to automate.