CBM ARCHIVES, LLC.
THE COMPLETE DOCUMENT MANAGEMENT SOLUTION

Agency Instructions for Submitting and Receiving Store & Forward (S&F) Transactions via S/FTP

EFT received from agencies must be encrypted with their DPS assigned crypto key.

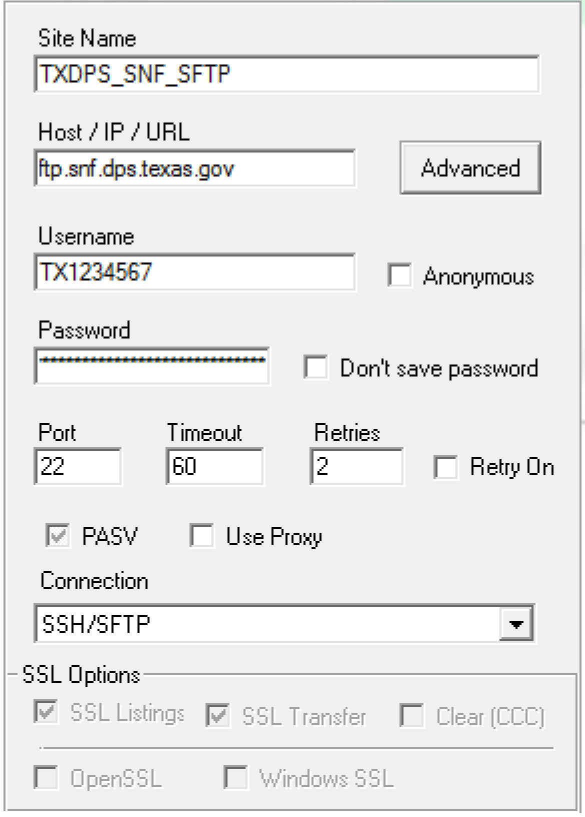
There are two different protocols for transferring EBTS files to and from the Texas Department of Public Safety Store and Forward – Secure File Transfer Protocol SFTP, and File Transfer Protocol (SFTP). Since most Internet browsers do not support SFTP, it's highly recommended to use an SFTP client. The client used is a matter of personal preference and any of these clients should work just fine: CoreFTP, WinFTP, CuteFTP, FileZilla, or WinSCP.

Secure FTP

A secure alternative to FTP is Secure FTP (SFTP). An SFTP client must be used to connect to an SFTP server. Although Microsoft does not provide an SFTP client with its Windows operating systems, most FTP clients include an option to connect using SFTP.

To start an SFTP session connecting to DPS's S&F SFTP Server, follow these instructions:

1. Configure your SFTP client to connect to ftp.snf.dps.texas.gov. Depending on the client used, the configuration screens may vary in appearance.



Site Name: TXDPS_SNF_SFTP
Host / IP / URL: ftp.snf.dps.texas.gov
Username: TX1234567   □ Anonymous
Password: ******************************   □ Don't save password
Port: 22   Timeout: 60   Retries: 2   □ Retry On
☑ PASV   □ Use Proxy
Connection: SSH/SFTP
SSL Options
☑ SSL Listings   ☑ SSL Transfer   □ Clear (CCC)
□ OpenSSL   □ Windows SSL

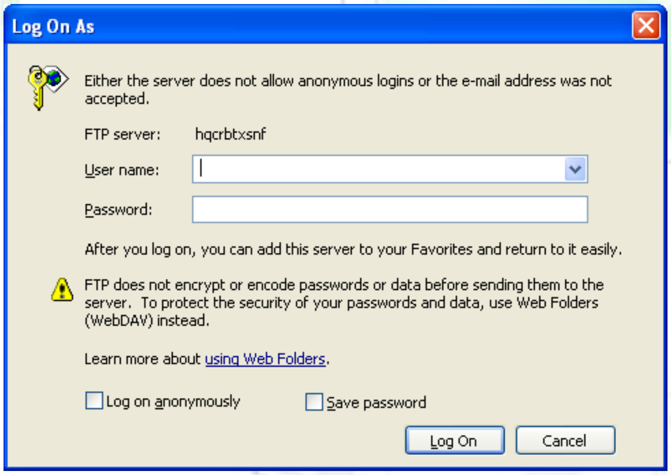
2. Use port 22
3. Enter Username and Password
4. Select SSH/SFTP (not SSL) as the connection protocol.

First time you connect with SFTP you should see a confirmation that your client is connecting to SFTP server with rsa key fingerprint ssh-rsa 3f:4b:a4:ae:4f:7c:b0:dd:”52:20:00:73:9e:da:36:6c. If connecting using the command line, use the above ssh-rsa key. For WinSCP command-line options, see http://winscp.net/eng/docs/commandline.

FTP

If for some reason SFTP isn’t an available option, a less secure FTP is available. Although the files are encrypted regardless of the file transfer method used, your user ID and password are transmitted in clear text when using FTP. To start an FTP session using Internet Explorer and to connect to DPS’s S&F FTP Server, follow these instructions:

1. From Windows click on the Start menu, then click on RUN
2. Type ftp://ftp.snf.dps.texas.gov
3. A screen should appear asking for logon credentials. (Supplied by DPS)



Log On As

Either the server does not allow anonymous logins or the e-mail address was not accepted.

FTP server: hqcrbtxsnf

User name:

Password:

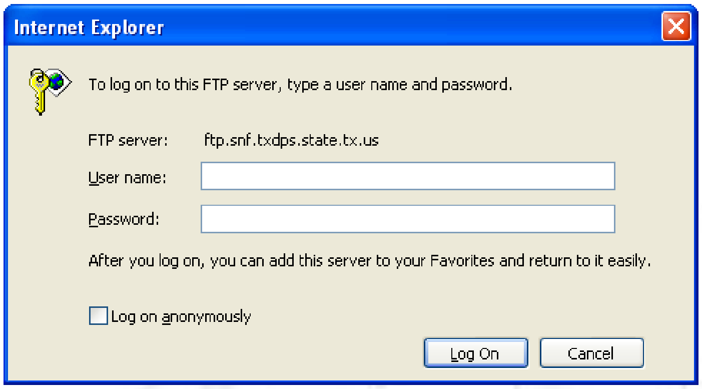
After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.

Learn more about using Web Folders.

□ Log on anonymously □ Save password

Depending on the version of Internet Explorer, the logon screen may look somewhat different.



To log on to this FTP server, type a user name and password.

FTP server: ftp.snf.txdps.state.tx.us

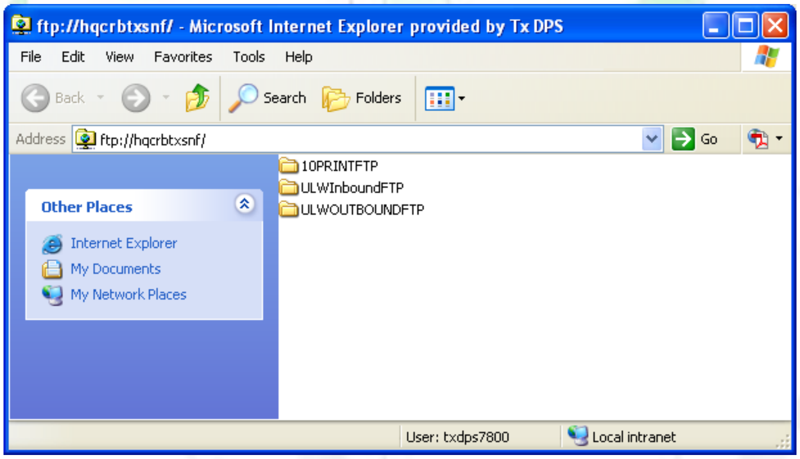
User name:

Password:

After you log on, you can add this server to your Favorites and return to it easily.

☐ Log on anonymously

4. Since anonymous access is not allowed, a valid user name and password is required to access the FTP server. <u>The User name will always be the agency's ORI.</u> Enter the required information, and click Log on. Once authenticated, the directories for the S&F files will be displayed.

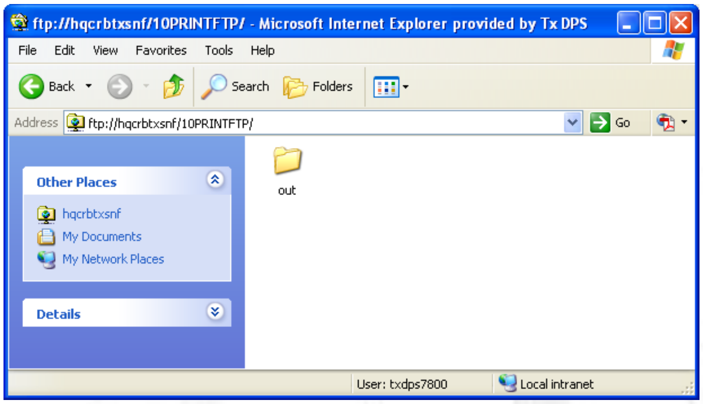


Address: ftp://hqcrbtxsnf/

10PRINTFTP
ULWInboundFTP
ULWOUTBOUNDFTP

User: txdps7800

5. Copy the encrypted files from your local computer to the appropriate S&F directories. Note: the response files will be placed in the "out" directory of each of the directories show above. Each ORI will have the above listed directories, regardless of whether or not the agency uses all three. Note: If unable to copy files to the FTP folder, try first selecting "Open FTP Site in Windows Explorer" under the "Page" tab at the top right hand corner of Internet Explorer versions 8.0 and above.



6. To view the encrypted response files, open the “out” directory located under the directory drop point. Copy the file(s) to your local computer and decrypt the file. In this example the “out” directory is under the 10PrintFTP directory. Each drop point has its own Out directory.

   You will need the crypto software with your assigned DPS crypto key in order to decrypt the files.

Note: Each of these sub directories will have an **out** directory where response files will be placed. It is the responsibility of the agencies to drop the file into the appropriate directories. Otherwise, S&F will reject the files and put a text file with a date time stamp in the **out** directory. The contents of the text file will contain an error message. Error messages will also be generated for files that fail to decrypt or fail to insert into our SQL server tables.

It is the responsibility of the agencies to manage their FTP folders. Files older than 90 days are automatically deleted.