



SECURE FILE TRANSFER



USER MANUAL

V. 4.3

TABLE of CONTENTS

Preface	<i>i</i>
Technical Assistance.....	i
What is Secure File Transfer?.....	i
Account Support.....	ii
Version	iii
Trademarks	iii
License Information.....	iii
Copyright.....	iii
The SFT Service comprises of three parts:	iv
Encryption	iv
Customer Notification LISTSERV	v
System Availability and Maintenance Window.....	vi
Maintenance Hours.....	vi
File Size Limitations	vi
File Naming Conventions.....	vii
File Retention Policy.....	vii
Transfer Log Retention Policy	vii
Conventions.....	<i>viii</i>
Chapter 1.....	<i>1</i>
Log in to Your Account	1
Using a Web Browser.....	1
Overview of the SFT User Directory Screen	3
Chapter 2.....	<i>4</i>
Passwords	4
Changing a Password.....	4
Using a Web Browser	4
Using Axway SecureClient™	6
Chapter 3.....	<i>7</i>
Upload Files.....	7
Using a Web Browser	7
Chapter 4.....	<i>8</i>
Download Files	8
Using a Web Browser.....	8
Internet Explorer	9
Firefox.....	10
Chapter 5.....	<i>12</i>
Delete Files.....	12
Using a Web Browser	12
Chapter 6.....	<i>13</i>
Log out of Your Account.....	13
Using a Web Browser	13
Chapter 7.....	<i>14</i>
Client Software.....	14
Configure a Connection using Axway SecureClient™	15
Defining an HTTPS connection	16

Defining an SFTP connection	19
Using a 3 rd -party Client.....	23
Auth TLS Connection.....	23
Other Protocols	24
Using 3 rd -party Command Line Clients.....	26
Examples of uploading a file with pscp.exe.....	26
Examples of uploading a file with psftp.exe.....	28
Chapter 8.....	29
Certificate Authentication	29
Appendix A	30
Technical Specifications	30
Operating System (OS) Requirements.....	30
Web Browser Requirements	30
Permission Requirements for Web Browser	30
SecureTransport™ Clients.....	30
FTP and HTTP clients	30
SSH clients	30
Appendix B	31
Support and References	31
Document Library	31
OTech Service Desk	31
SFT Staff Responsibilities	31
Customer Responsibilities	31
SFT Staff and Customer Shared Responsibilities	31
Internet Explorer (IE v8, 9) Security Alert Box.....	32
Installing a newer SSL Certificate -- Internet Explorer (IE) Issue	34
Appendix C.....	35
Automating Password Change Over FTPS.....	35
Syntax.....	35
Lesson: How to Base64 Encode.....	36
Base64 Utilities.....	36
Web-based (Browser).....	36
Linux	36
Linux/UNIX Compile from Source.....	36
Perl module	36
Windows.....	37
Changing the Password	37
Using cURL.....	37
MoveIT Freely Batch	38
Appendix D	39
Self-Provisioned Certificate Authentication	39
Create the SSH Key Pair	39
Create a .ssh folder	39
Upload the public key file.....	40
Note the Response Files	40
Glossary.....	42
Abbreviations, Acronyms, and Terms to Know	42
Quick Start.....	45
Using the Web Browser.....	45

Technical Assistance

For assistance with your user account or questions regarding the Secure File Transfer Service, please contact your Delegated Administrator(s). Use the space below to record your Delegated Administrator contact information:

Delegated Administrator 1:

Delegated Administrator 2:

Name: _____

Name: _____

Phone: _____

Phone: _____

Email: _____

Email: _____

What is Secure File Transfer?

Secure File Transfer (SFT), a service offering hosted by the California Technology Agency, Office of Technology Services (OTech), provides a cost-effective, fast, reliable and secure method of transmitting files to and from state agencies, counties and cities and any external business partners. SFT features automatic e-mail notification, includes a high-availability infrastructure to ensure continued accessibility, and provides industry standard encryption of data in transit and at rest on our pass-through storage (or customer purchased SAN).

Secure File Transfer uses the industry leading product, SecureTransport™ from the Axway Corporation (formerly Tumbleweed Communications). SFT provides multiple secure protocols and full regulatory compliance (HIPAA, HITECH, FIPS, GLBA, SOX, PCI, etc...) for managed file transfers. Axway Corporation is positioned as a leader in Gartner Managed File Transfer Magic Quadrant.

Secure File Transfer is also known in the industry as Managed File Transfer. Managed File Transfer is replacing VPN connections (IPSec tunnels), magnetic tape, tape couriers and tape storage solutions, paper and postal service delivery, CD and DVD packaging processes, flash drives, standard FTP, and other non-managed or unsecured methods of exchanging information in file-based formats.

What SFT is not? Secure File Transfer is not a data storage service or solution. However, SFT can utilize customer-purchased storage to create transfer/storage solutions to meet any need.

Real world meaning... move sensitive data files from any Internet-connected client (or OTech-hosted server) to any other server securely with user and file management controls and reporting tools, all wrapped with regulatory-compliant assurance!

Account Support

Your department Delegated Administrators (DA) are responsible for your account support including locked account resets, creation of new accounts, configuring accounts (email notification, for example) usage reporting, and support of client software.

You will request support from your Delegated Administrator(s), not from the OTech Service Desk. If you forget your password, your account has expired, or your account is locked, you must contact your Delegated Administrator. Only your Delegated Administrator is allowed to reset your password.

OTech Service Desk personnel are instructed to refer password resets and account unlock requests from SFT end users to the customer's Delegated Administrator.

OTech SFT staff will accept requests for SFT support only from customer Delegated Administrators.

Version

This manual explains the User functionality as it pertains to version 4.9.2 of the SecureTransport™ (ST) software from Axway Corporation (formerly Tumbleweed Communications).

Date	Version	Description	Author
02/2009 thru 09/2010	v. 2.0	Comprehensive rewrite. Updated all text to (ST) version 4.8.1, layout changes to match service documents, content updated. Extensive re-wording.	Kevin Paddock
09/2010 02/2011	v. 3.0 v. 3.1	ST version 4.8.1. Modern document design (Puneh Moasser).	Kevin Paddock Puneh Moasser Mauria Hirning Jimmy Choi
09/2011	v. 4.1	ST version 4.9.2	Kevin Paddock Jimmy Choi Puneh Moasser
07/2012	v. 4.2	Appendix C – Automating Password Change Over FTPS	Kevin Paddock Jimmy Choi Puneh Moasser
02/2013	v.4.3	Appendix D – Self-Provisioned Client Certificates	Kevin Paddock Puneh Moasser

Trademarks

Any names of other companies, products, or services may be the property of their respective owners and the Office of Technology Services, State of California uses these trademarks for training purposes only.

License Information

The Office of Technology Services, State of California authorizes the use of this document for training purposes and it may be copied in whole or in part for use by its customers. Any partial or whole copies must include the California Technology Agency, Office of Technology Services logo.

Copyright

©2013 California Technology Agency, Office of Technology Services, State of California. Portions ©2007 Axway Corporation (formerly Tumbleweed Communications).

The SFT Service comprises of three parts:

- A Software Client (Web Browser or other File Transfer Client that supports secure protocols)
- Edge Servers
- Backend Servers

All SFT file transfers, including those sent to or from customer agencies connected to CGEN (formerly CSGNet), pass through an Edge server via the Internet. Only the Edge servers are exposed to the Internet in the DMZ. All file processing is performed and all storage is located on (or attached to) the backend servers which are behind the OTech “trusted-tier” firewalls. At no time does data reside on the Edge servers.

Encryption

Secure File Transfer provides two methods of encryption: 1) encryption in transit and 2) encryption at rest.

Each method uses an industry standard algorithm and is fully compliant with all Federal, State, and local laws as well as California State Administrative Manual and other State rules and requirements.

Encryption in Transit: SSL and SSH provide the standard encryption solution for data passing through the network. When a customer connects to SFT using a supported web browser or a secure client, the server enforces an SSL or SSH connection. The connection is protected by means of a VeriSign certificate.

Encryption at Rest (repository encryption): Secure File Transfer includes encryption at rest. Data stored on the Secure File Transfer data storage location is encrypted using Triple Data Encryption Standard (3DES). When data is sent to Secure File Transfer, it is decrypted in active memory then re-encrypted in active memory using 3DES before writing to disk. Therefore, at no time does the service cache files, write temporary files, or save other sensitive data in an unencrypted format.

Customer Notification *LISTSERV*

OTech offers notification of SFT “news”, system maintenance, upgrades and planned outages to all SFT customer Delegated Administrators and interested parties.

To sign up, send an e-mail to LISTSERV@listserv.state.ca.gov

Put only the following information in the **message body**:

SUBSCRIBE [space] OTech_SFT [space] *YourFirstName* [space] *YourLastName*

example: If your name is James Taylor, in the message body put

SUBSCRIBE OTech_SFT James Taylor

To unsubscribe put the following in the **message body**:

UNSUBSCRIBE OTech_SFT James Taylor

You don't need to put any text on the Subject line. If you want to enroll a large number of email addresses, submit a Service Ticket (service.desk@state.ca.gov) with an attached text file in this format (one contact per line): *emailaddress@yourdept.ca.gov* *FullName*

System Availability and Maintenance Window

The SFT service runs 24/7, 365 days a year.

- ◆ California Technology Agency Tier III Data Center
- ◆ Fully redundant, high availability architecture
- ◆ Fully supported by OTech with 24/7 vendor support
- ◆ Layered Security Architecture

The network infrastructure at the Office of Technology Services runs at speeds of 1GB or faster. Customer connection speeds may vary depending on throughput capabilities at customer locations, bandwidth usage, and number of concurrent users.

Maintenance Hours

The SFT Maintenance Window is every **Sunday** from **8:00 pm to 12:00 am (midnight)**. Customers with transfer jobs scheduled during this time are advised to reschedule them in the event of a scheduled outage.

In addition, OTech offers notification of SFT system maintenance, upgrades and planned outages to all SFT Delegated Administrators through LISTSERV (see above). We notify all SFT LISTSERV subscribers of system maintenance that could impact file transfers and will make every effort to send notices at least 10 calendar days prior to the scheduled down-time.

OTech network maintenance could also affect SFT file transfer operations. Customers are advised to note ENEWS LISTSERV e-mail messages from the CIOENewsAdministrator. Contact the OTech Service Desk (service.desk@state.ca.gov) if you wish to receive these OTech customer notifications.

File Size Limitations

Files uploaded using a web browser are limited to 2GB in size (a limitation of all current web browsers). This limit does not apply to browser **downloads**. Files of any size can be transferred with the Axway SecureClient™ or other 3rd-party clients (FileZilla, CoreFTP, WSFTP, etc). The only limit to file size is the remaining storage available in the SFT shared SAN pool. However, if your requirements include very large files (10GB or larger), your organization may be directed to purchase OTech storage and dedicate it to your file transfer needs.

File Naming Conventions

Do not use the following Windows illegal characters in the names of files that originate on mainframe or Unix/Linux systems:

: (colon)

\ (backslash)

? (question mark)

(space) – yes, this IS a legal character, but don't use it in any SFT account, file or business unit name anyway.

You will not be able to download or delete such files using the Microsoft Internet Explorer browser. Mozilla Firefox browser can be used; however, Firefox will replace the illegal characters with a legal underscore before saving the file.

File Retention Policy

The Secure File Transfer (SFT) service provides temporary file storage for file transfer. SFT is a file transfer service not a data storage service or solution. The SFT service file retention policy stipulates that each file transferred to SFT, and not deleted by the recipient or automated application, will be retained on the system for a period of 14 days. Customers requesting no retention period will need to purchase dedicate SAN storage. For retention period requests in excess of 14 days may need to purchase storage at the current OTech storage rates.

Transfer Log Retention Policy

Every transfer into and out of the SFT system generates a file transfer log entry which is retained on the SFT system for a period of 1 year. The transfer log entry ensures audit ability and compliance with government regulations such as HIPAA, HITECH, SOX, GLBA, PCI, FIPS and others. The system also generates an MDN (Message Disposition Notification) for each transfer.

CONVENTIONS

Convention	Description	Example
Screen names, dialog boxes	<i>Italic Blue</i>	<i>Expired Account</i> screen
Field Names	Bold Pink	From the Protocol drop-down menu
Menu Items and Tabs	Bold Purple	From the top menu Tools > Site Manager
Column Headers	<u>Underline</u>	In the <u>Files</u> section
Button Names	Quotation marks " "	"Change Password" button
Green	Identifies values to be entered by the user	Select " HTTPS " from drop-down
Left-Click	By default, all click actions are single, left-mouse clicks.	Click "OK".
[Key Name]	Keyboard key to press	[Enter]
Right-Click	Identifies actions that require the right mouse button instead of the left mouse button.	<i>Right-click</i> on the file name.
	Identifies tips and notes.	
	Identifies cautionary alerts.	
	Identifies Advanced User information	
	End of chapter	

Log in to Your Account

Using a Web Browser

1. Open a web browser.
 Navigate to: <https://sft.ca.gov>
 (The web browser uses HTTPS secure protocol.)

Please refer to [Appendix A](#) for web browser requirements.

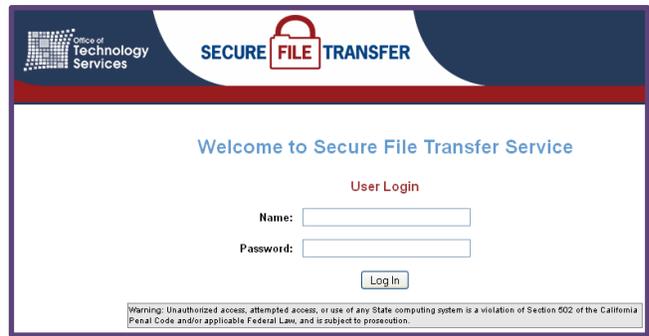
If using Internet Explorer, you may see this "Choose a digital certificate" prompt. If so, click "OK" to proceed.

To suppress this alert on subsequent logons, please see [Appendix B](#).



Certificate prompt

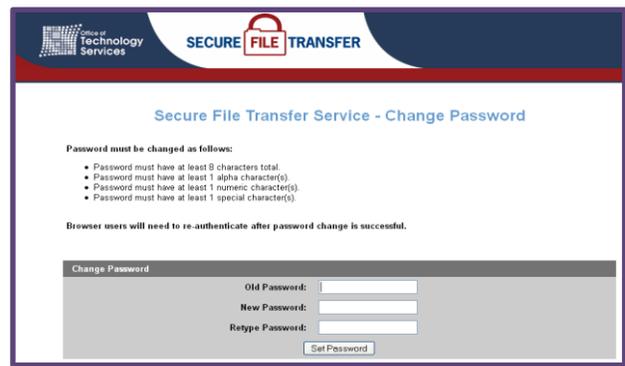
2. At **Log In** screen, enter your **Username** and **Password**, then click the "Log In" button or press [Enter].



Log In screen

3. All new (and reset) accounts use the temporary Initial Default Password provided to you by your Delegated Administrator. Use the Initial Default Password to log in for the first time or after a password reset.

When you see this screen, you **must** change your password.

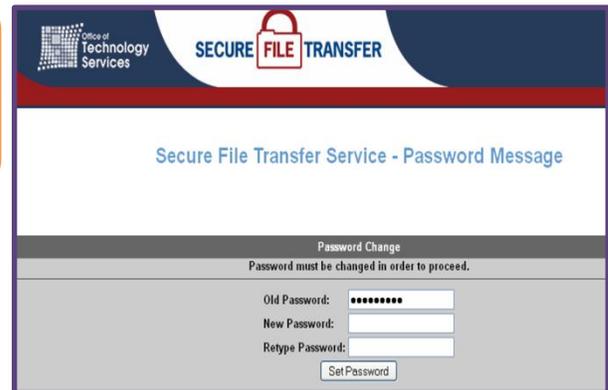


Change Password screen

Log in to Your Account

NOTE: If you fail to change the Initial Default Password within 90 days, your account will lock..

This screen will display when you attempt to log in.

The screenshot shows the 'Secure File Transfer Service - Password Message' page. At the top, there is a header with the 'Office of Technology Services' logo and the 'SECURE FILE TRANSFER' text. Below the header, the main content area is titled 'Secure File Transfer Service - Password Message'. Underneath, there is a section titled 'Password Change' with the instruction 'Password must be changed in order to proceed.' This section contains three input fields: 'Old Password:' (with a masked password), 'New Password:', and 'Retype Password:'. A 'Set Password' button is located at the bottom of the form.

Expired Password screen

If your account is locked, you will need to ask your Delegated Administrator to unlock it. Then follow steps 1 and 2 of this chapter.

4. Upon successful login, your SFT User Directory page appears which allows you to perform file upload, download and other operations.

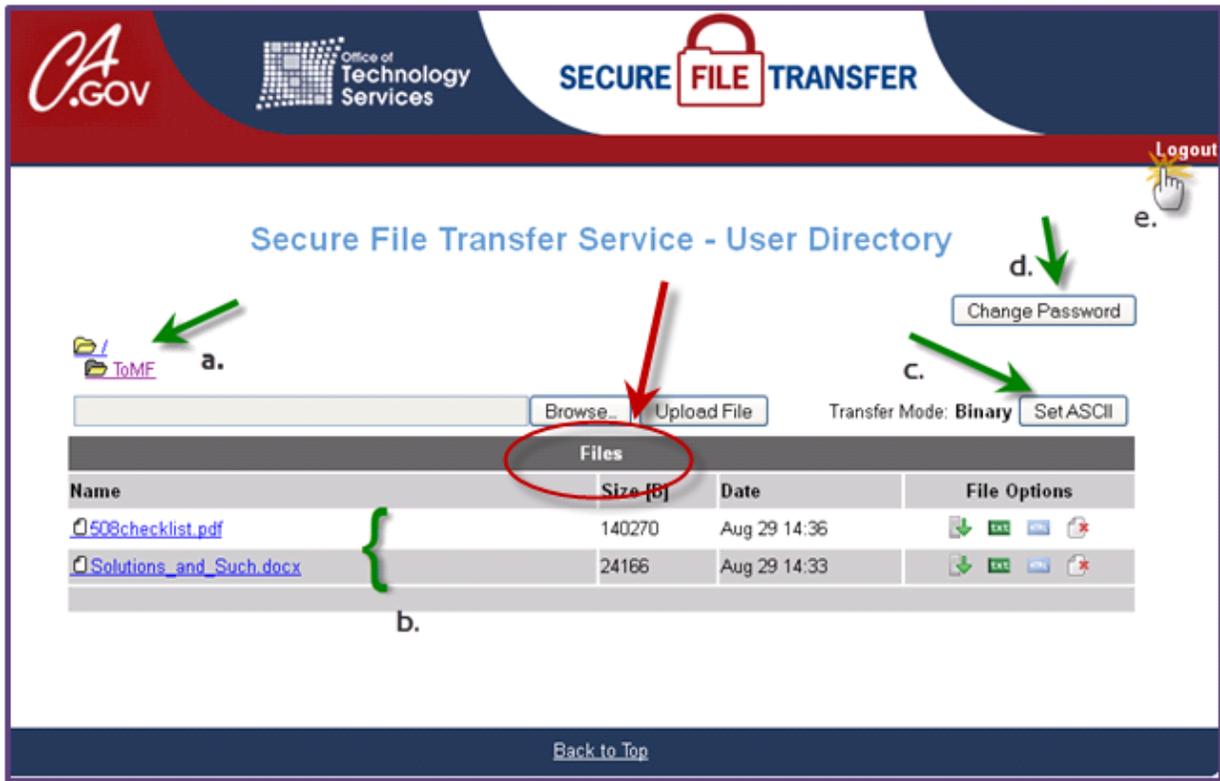


Your SFT session will time out after 15 minutes of inactivity.

| Continued on next page |

Log in to Your Account

Overview of the SFT User Directory Screen



SFT *User Directory* screen

- a. All users have a root or home folder. Your Delegated Administrator may have created additional folders/subdirectories for you and these will appear under the root folder. Note: you cannot create subfolders using the web browser. However, you can create subfolders with 3rd-party secure client software. See Appendix A.
- b. Click on the root folder (or another if you see any). All uploaded files in the folder you clicked on are listed under the dark grey banner named Files.
- c. Toggle between Binary (default) and ASCII for "upload" and "download" transfer mode. If you don't know what this does, leave it set to Binary.

d. "Change Password" button.

e. "Logout" button.

Note the File Options Column. The chapters ahead describe these functions in detail.

Passwords

The Password Policy includes the following syntactical requirements:

- ✓ The password must contain at least 8 characters.
- ✓ At least one of the characters must be a number.
- ✓ At least one of the characters must be a symbol (for example: !@#\$%).
- ✓ At least one of the characters must be an UPPERCASE alpha character.

SFT accounts used for process automation can also be configured for certificate authentication with or without interactive passkey requirements (see Chapter 8). Certificate authentication allows for secure account access without a password. Passwords must be changed at or before the mandatory 90-day period. Authentication certificates are valid for up to two years. If you want to authenticate with a certificate, contact your delegated administrator or, if you want to self-provision your own authentication certificate, see Appendix D in this document.

An account password expires after 90 days and must be changed at or before expiration.

Forgotten password, expired or locked account? Contact your Delegated Administrator.

Do not contact the OTech Service Desk. Neither OTech nor SFT staff are allowed to reset SFT customer passwords.

Changing a Password

The ONLY supported ways for you, the user account owner, to change your password are by using a Web Browser or the Axway SecureClient™ (sold separately).

UPDATE: For advanced users... You can now change your password by using a 3rd-party client, with the FTPS protocol (See Appendix C)

Using a Web Browser

1. Log in to your SFT account using a web browser (Chapter 1), the *User Directory* screen will display.



SFT *User Directory* screen

Passwords

Changing a Password Using a Web Browser (cont'd)

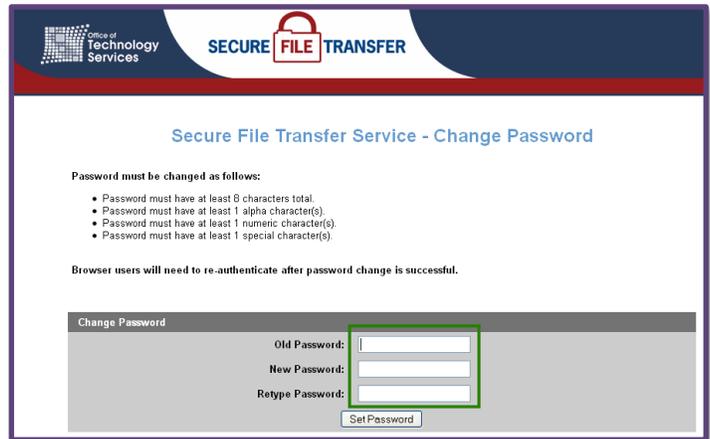
2. Click the "Change Password" button.

The *Change Password* screen will display.

3. Fill in the fields as indicated.

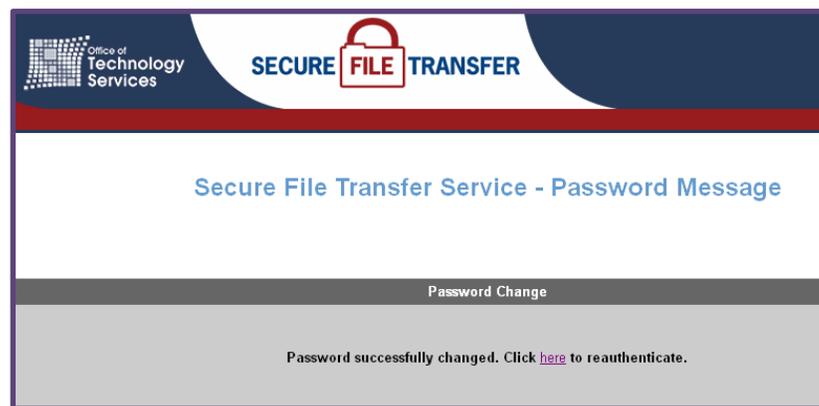
Click the "Set Password" button.

If the **New Password** field and the **Retype Password** field do not match, an error message will appear. Try again.



Change Password screen

When the password has been successfully changed, the *Confirmation* screen will display.



Successful Password Changed screen

If the account password you just changed is used in any automated processes or scripts, you must also change the password in the code or configurations setting of your automated system.

To eliminate the need to update passwords for automated systems, consider using client certificate authentication. To learn more about certificate authentication please see Chapter 8. Your Delegated Administrator will help you set this up for your account.

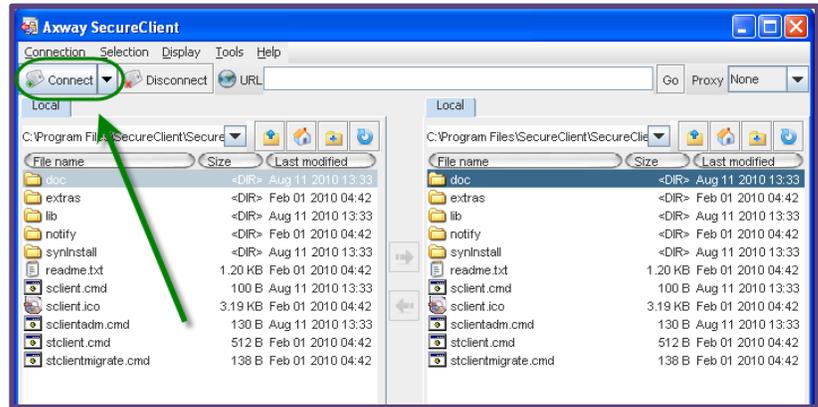
Passwords

Changing a Password Using Axway SecureClient™

With the Axway SecureClient™, you can change your password on demand using the HTTPS protocol.

Open the SecureClient™ program.
(This is an optional third-party client available for a fee from the SFT Service team.)

1. Click on the "Connect" button or select from the top menu **Connection > Connect**.

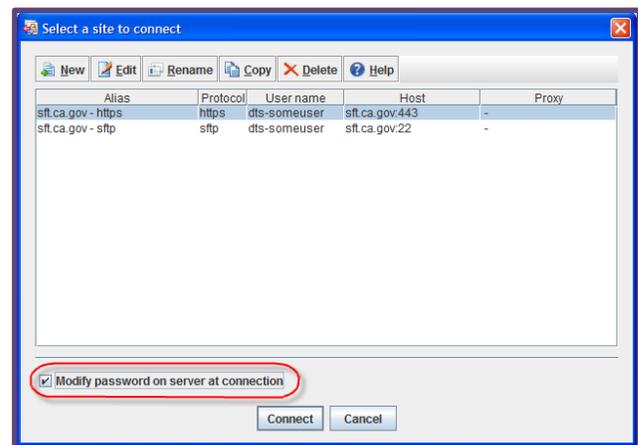


SecureClient™ | Main window

2. *Select a site to connect* window will pop up.

Check the field **Modify password on server at connection** by clicking inside its check box.

If more than one site connection is listed, verify the correct HTTPS connection is selected, highlighted blue (as shown in screen shot). To choose another connection within the list, simply click once on the line of the HTTPS connection you wish to change the password.



SecureClient™ | Select a site to connect

3. *Enter the password for the FTP user* window will pop up. Fill in all three fields...

PASSWORD: your old SFT account password

NEW PASSWORD: new password *

CONFIRM NEW PASSWORD: Re-enter new password



SecureClient™ | Enter a Password... window

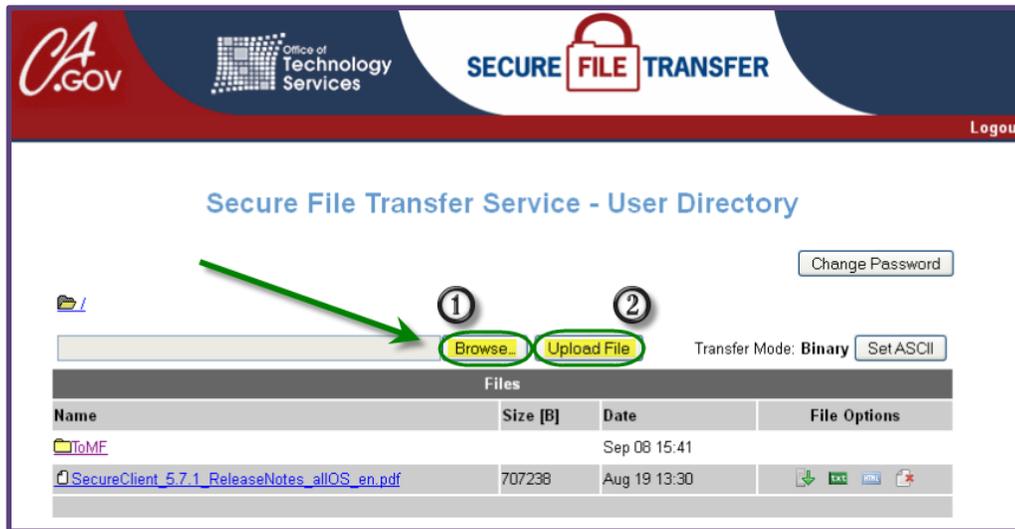
Click "OK".

(* must meet password policy requirements, see [page 4](#))

Upload Files

Using a Web Browser

1. Log in (Chapter 1). The *User Directory* screen is displayed.



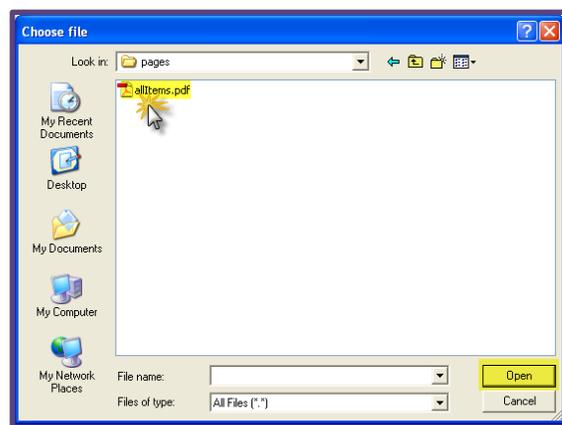
User Directory screen

Unless you have a specific reason for changing the transfer mode, leave it set to “Binary”.

Only one file may be selected at a time. If you need to upload more than one at a time, use a 3rd-party client. (Refer to [Appendix A](#) for compatible clients).

2. **a.** Click the “Browse” button (1) to open the *File Upload* dialog box.

b. In the dialog box, locate and select the file to be uploaded by clicking on its name, then click the “Open” button. You can also simply double-click the file name.



File Upload dialog box

3. Initiate the upload by clicking on the “Upload File” button (2) on the *User Directory* screen. A progress window may appear. Please wait until the screen refreshes before doing any other work. If email notification is enabled, you’ll get a message indicating success or failure.

Download Files

Using a Web Browser

“Download” a file can refer to several actions. You can “Open” which allows you to view the file on your screen or you can “Save” the file to your local machine. Internet Explorer and Firefox use different names for their dialog boxes, but the end result is either opening or saving the file. In both cases, the file *must* first be downloaded to your computer, then opened or saved. If you choose to open the file, you need to make sure you have the appropriate software (like MS Word or Acrobat Reader) on your system to open and view it.

1. Log in ([Chapter 1](#)). The *User Directory* screen is displayed.
2. From the *User Directory* screen, in the *Files* section, locate the file to download. If you have many files listed, you may need to scroll down.

Note: Your file(s) may not be in the top level folder.  You may need to “drill down” to a specific folder. In this example, the file to be downloaded is in the subfolder ToMF.  ToMF

Unless you have a specific reason for changing the transfer mode, leave it set to “Binary”.

3. Initiate the download by clicking one of the following:
 - the “file name” link
 - the Download icon under the File Options column, on the same row as the file name.



Name	Size [B]	Date	File Options
508checklist.pdf	140270	Aug 29 14:36	   
Solutions_Std_Such.docx	24166	Aug 29 14:33	   

File list for the folder ToMF

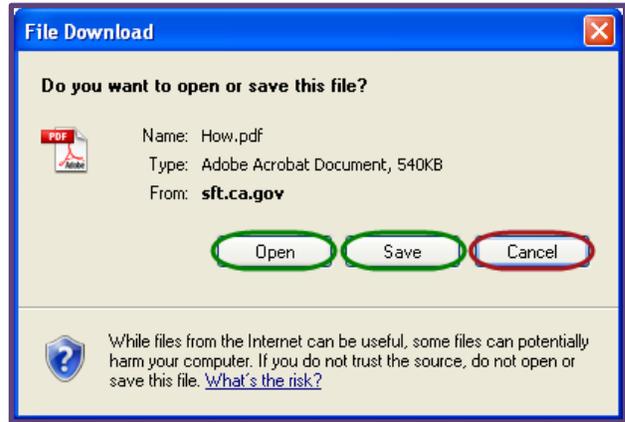
Step 4 - Internet Explorer - continued on next page
 Step 4 - Firefox- go to [page 10](#)

Download Files

Using a Web Browser (cont'd) Internet Explorer

4. A *File Download* dialog box will appear.

- Click "Open" to view the file.
- Click the "Save" button to open the *Save As* dialog box.
- Click the "Cancel" button to terminate this current download request.

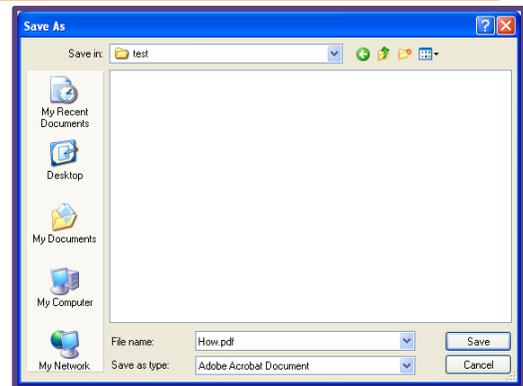


File Download dialog box - Internet Explorer

Note: If your account has email notification enabled, you may receive the successful download notice even if you click "Cancel". Reason: browsers start downloading to a temp folder immediately. The file may already be fully downloaded before you select the Save location.

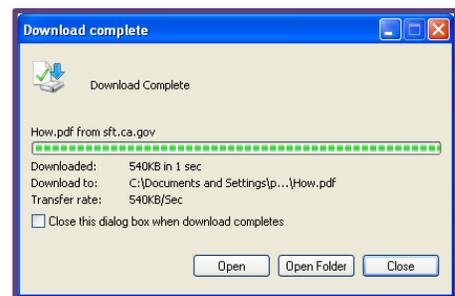
Within the *Save As* dialog box, you can choose the download location. You may also rename the file at this point by typing the new name in the **File name** field.

Click the "Save" button. The download duration will vary depending on file size, connection bandwidth, and the number of concurrent users.



Save As dialog box

When the file has downloaded successfully, a pop-up box will appear. You can now select the "Open" button to open the file, assuming you have the program on your system that can open the file. By clicking "Open Folder" button, the system will open the containing folder where your file resides. If you click "Close", the "Download Complete" window closes.



Download complete dialog box

Download Files

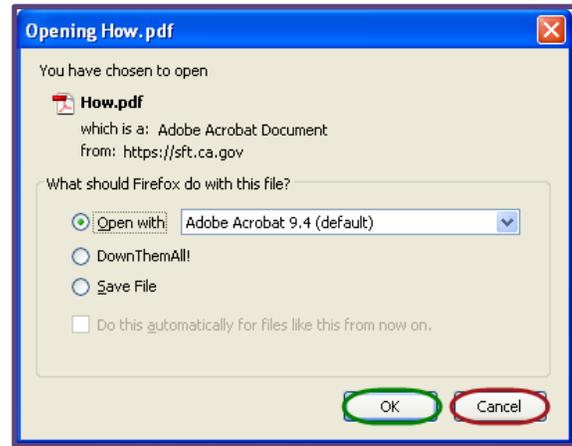
Using a Web Browser (cont'd)

Firefox

- An *Opening [file name]* dialog box will appear. If you click "Cancel" the box will be dismissed.

Note: If your Delegated Administrator has turned on email notification for you, you will receive the download email notification even if you click "Cancel".

Click inside the appropriate circle to mark your selection, and then click "OK".



File download dialog box - Firefox

If you select "Open With"



you can open the file with the displayed default program, or you can select which program to use by clicking on the drop-down arrow and choosing "Other..."

Adobe Acrobat 9.3 (default)

Adobe Acrobat 9.3 (default)

Other...

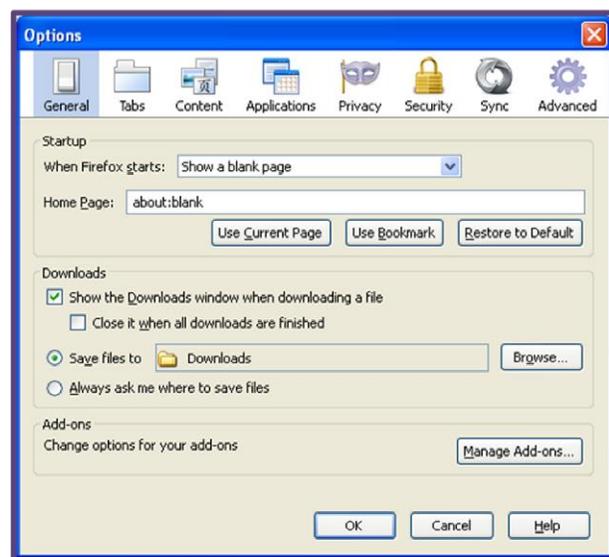
If you select "Save File",



depending on your Firefox browser settings, you may or may not see a dialog box asking for a location to save your file.

depending on your Firefox browser

To review your download settings in Firefox, you can select from the main tool bar **Tools > Options ... General** tab. You can see how Firefox is handling downloads and where it is saving files.



Firefox **General** tab under **Tools > Options**

Download Files

Using a Web Browser (cont'd)

Note: If your account has e-mail notification enabled, you will receive an e-mail for each upload and download success or failure. Contact your delegated administrator for questions about setting up (or removing) email notification.



Please download your files as soon as possible. Files have a **14 day retention policy** on the SFT servers.

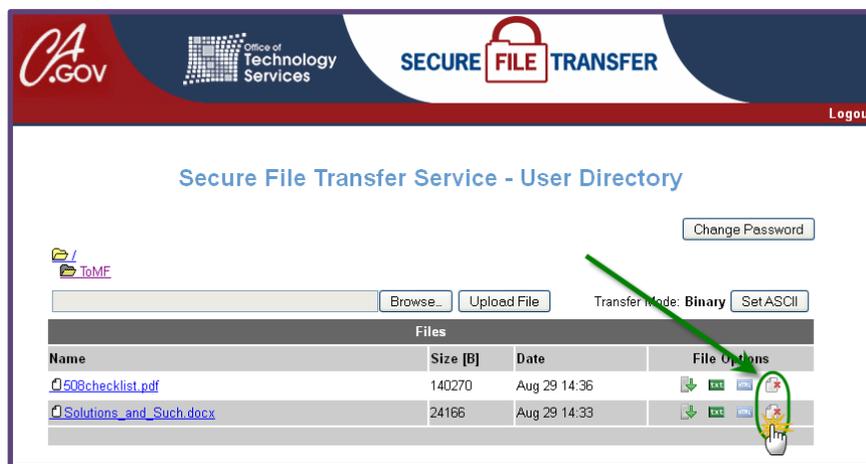
File storage is provided on a temporary basis. If your use of SFT requires either a longer retention period or permanent storage, contact your Delegated Administrator.

Delete Files

Using a Web Browser

1. Log in to your account. On the *User Directory* screen, under the Files header, locate the file to be deleted. If the name is not displayed on the screen, scroll down in the window until the file name appears.

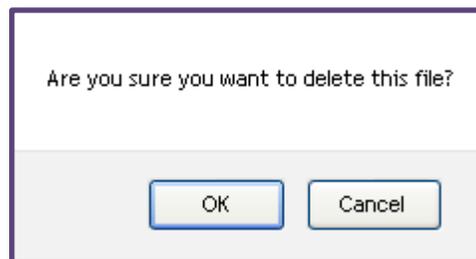
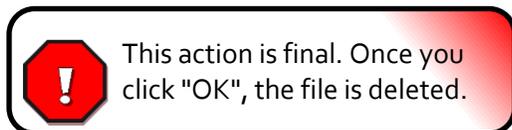
2. Under the File Options column, on the same row as the file name, click the "Delete" icon .



User Directory screen

3. A confirmation prompt will appear.

Click "OK" to confirm the file you wish to delete.



File Delete Confirmation prompt

The *User Directory* screen will return to focus and the file is removed. If you accidentally delete a file, contact your delegated administrator to have the file sent to you again.

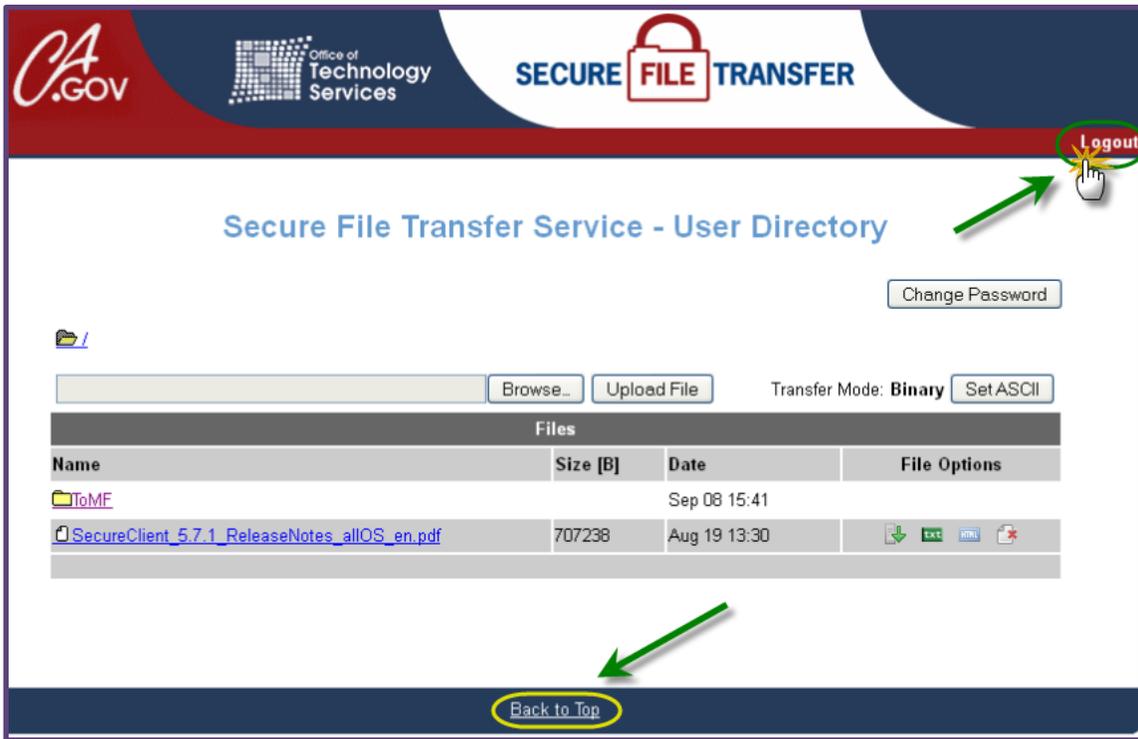
Log out of Your Account

Using a Web Browser

 If your SFT session has no activity for 15 minutes, it will time out automatically.

1. On the screen, locate the word "Logout"  in the upper right corner.

If the "Logout" link is not displayed, click the "Back to Top" link, located at the bottom of all screens. 



User Directory screen

2. Click on "Logout" to end your SFT session.

Client Software



Please see your Delegated Administrator for organization's policy, installation, usage, and support of client software.

Accessing your SFT account files through the ubiquitous web browser is intuitive and easy to use. But the SFT web access offers limited functionality. If the web-based user experience lacks the features you need, consider using one of the many open source, freeware or fee-based software clients or a command-line utility. These application software tools often provide many features required for more advanced file access and manipulation such as the ability to transfer or delete multiple files in one operation, drag and drop file movement and folder create, rename and delete functions.

Axway SecureClient™ allows for batch processing, scripting, and scheduled tasks as well as those mentioned above. It can run as a Windows service for unattended transfers even while logged out. It also allows you to update an expired password.

Please refer to [Appendix A](#) for a list of compatible client software



The first-time SFT account login must be completed **using a web browser** because you will be prompted to change the temporary or expired password.

If you have not yet logged in using a web browser ([Chapter 1](#)), do so now before attempting to log in with another client.

The Axway SecureClient™ can be purchased from OTech at the price listed in the Rate Sheet posted on OTech's web site (www.otech.ca.gov). With a completed billing Service Request (SR), you will receive a "single-seat" license key that allows for perpetual use and all upgrades.

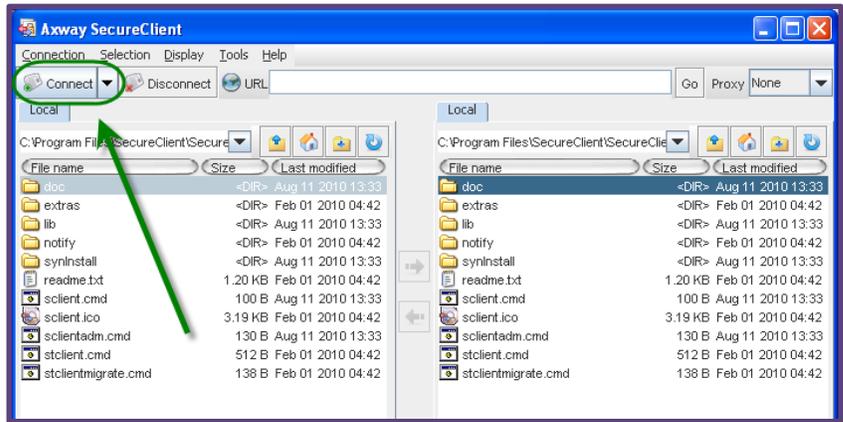
Refer to Appendix B for download location. SFT staff will provide installation and configuration support for SecureClient™. For other clients, you, your delegated administrator or your IT shop must provide the client software and support.

For Axway SecureClient™ support requests, submit a request to the OTech Service Desk.

Client Software

Configure a Connection using Axway SecureClient™

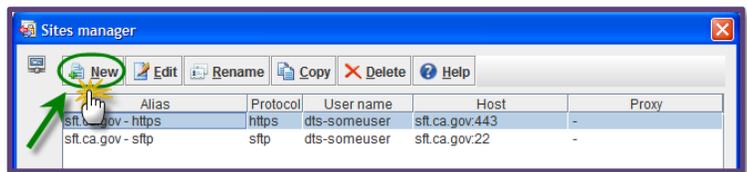
1. Open the SecureClient™ program.



SecureClient™ | Main window

2. Click on the “Connect” button or select from the top menu
Tools > Site Manager

3. From this window, you have many actions to choose from.

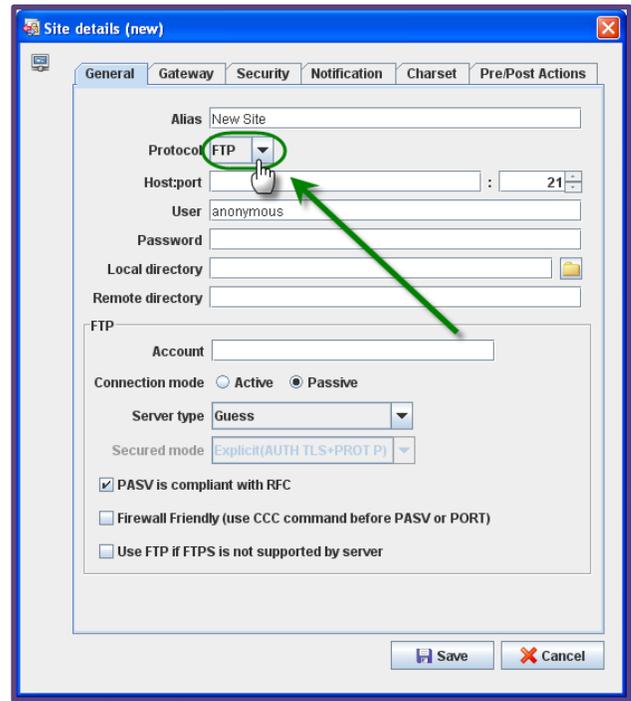


SecureClient™ | Tools > Site Manager

Click on the “New” button to create a new connection.

A *Site Details (new)* window will pop-up. You will need to change the values of some fields and enter information into others under two of the tabs **General** and **Security**.

4. From the **Protocol** drop-down menu, “FTP” by default, select your protocol. Choosing protocol “HTTP” will bring up the fields needed to define a HTTPS connection and “SFTP” will bring up the fields needed for a SFTP connection.



SecureClient™ | Site details (new) pop-up > **General** tab default view

Settings for HTTPS go to [page 16](#).
Settings for SFTP go to [page 19](#).

Client Software

Configure a Connection using Axway SecureClient™ (cont'd) Defining an HTTPS connection

5. a. Under the **General** tab, locate the **Protocol** drop-down menu, "FTP" by default, select "**HTTP**".

Once you make the selection of "HTTP", the fields in this window will change.

- b. Fill in the following values:

ALIAS: create a connection name as to identify this site within SecureClient™

PROTOCOL: Keep at **HTTP**

HOST: **sft.ca.gov**

PORT: **443**

USER: your **SFT user account name**

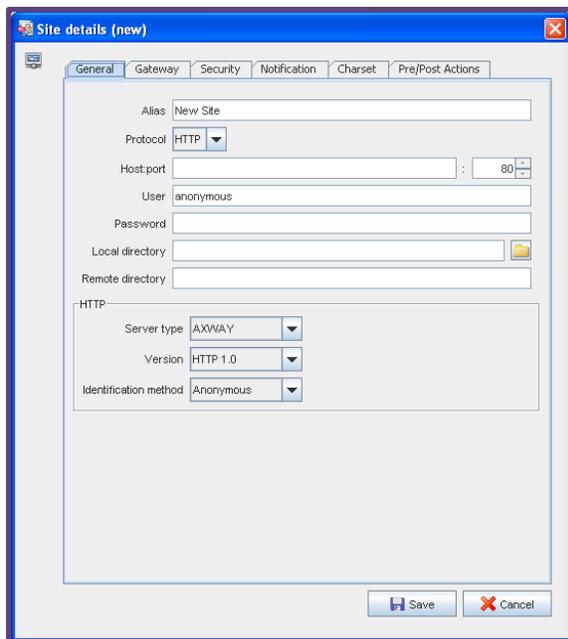
PASSWORD: your **SFT user account password**

SERVER TYPE: From the drop-down menu, choose **SecureTransport**

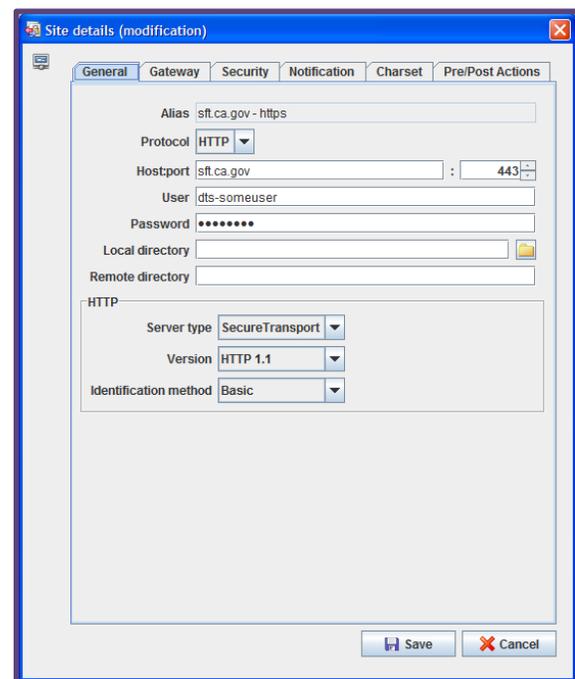
VERSION: From the drop-down menu, choose **HTTP 1.1**

IDENTIFICATION METHOD: From the drop-down menu, choose **Basic**

| Continued on next page |



SecureClient™ | Defining an HTTPS site >
General tab at start-up



SecureClient™ | Defining an HTTPS site >
General tab filled in

Client Software

Configure a Connection using Axway SecureClient™ (cont'd)

Defining an HTTPS connection (cont'd)

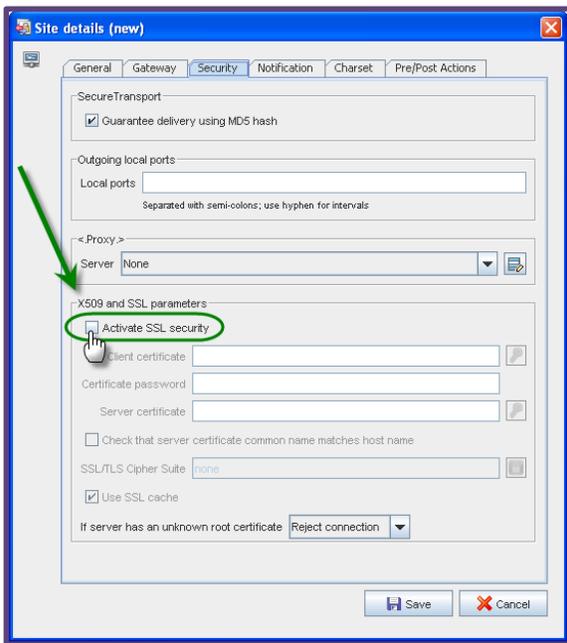
c. Next, click on the **Security** tab.
The fields in this window will be related to the choice of HTTP protocol.

If the fields under the **Security** tab do not look like this screen shot, go back to the **General** tab and verify that HTTP is the selected protocol.

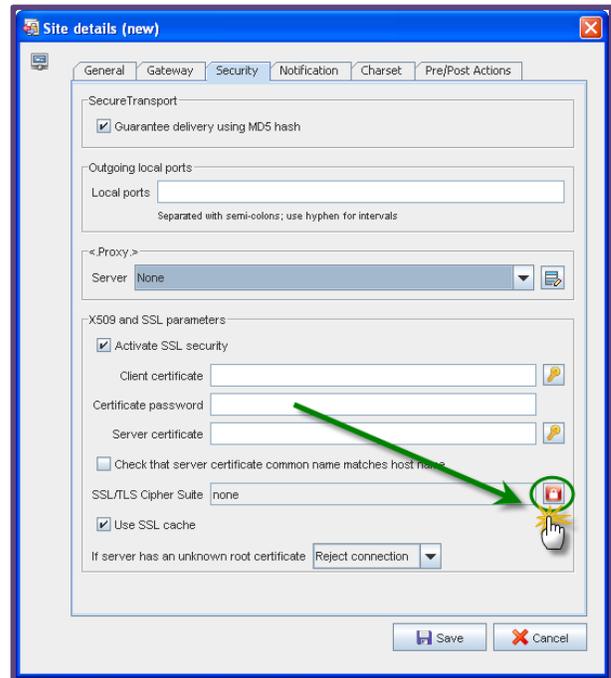
d. Click inside the check box **Activate SSL Security**.
The remaining fields of "X509 and SSL parameters" will become available fields.

e. Notice the **SSL/TLS Cipher Suite** field states "none".
Click on the orange lock icon. 

| Continued on next page |



SecureClient™ | Defining an HTTPS site >
Security tab at start-up



SecureClient™ | Defining an HTTPS site >
Security tab with X509 check box filled

Client Software

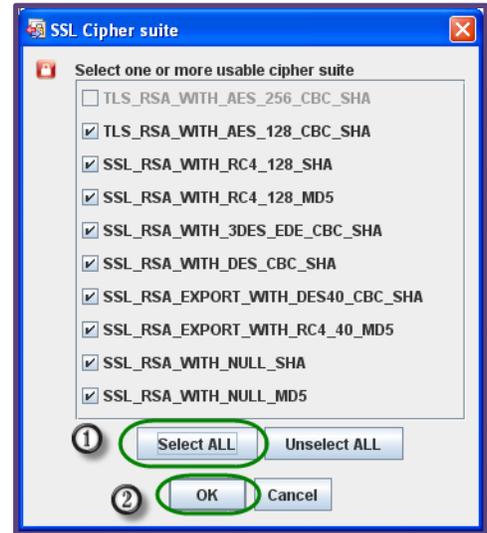
Configure a Connection using Axway SecureClient™ (cont'd)

Defining an HTTPS connection (cont'd)

f. After clicking on the orange lock, an *SSL Cipher suite* window will pop up.

All the check boxes available need to be checked. The quickest way to do this is to click on the button "Select All".

Then click "OK".



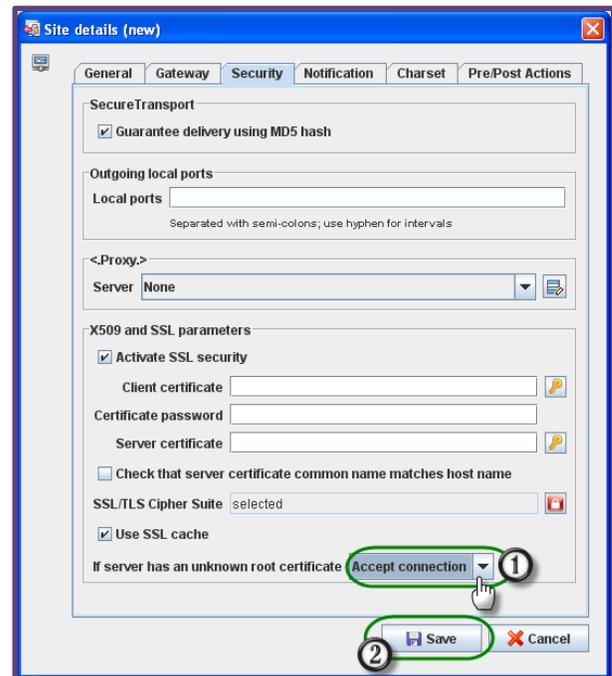
SecureClient™ | Defining an HTTPS site > *SSL Cipher suite* pop-up dialog box

g. You will be returned to the **Security** tab.

Next, for the field **If server has unknown root certificate**, from the drop-down menu, choose "Accept Connection".

h. Click "Save".

Connection is defined.



SecureClient™ | Defining an HTTPS site > **Security** tab filled out

Client Software

Configure a Connection using Axway SecureClient™ (cont'd)

Defining an SFTP connection

4. a. Under the **General** tab, locate the **Protocol** drop-down menu, "FTP" selected by default, select "**SFTP**".

Once you make the selection of "SFTP", the fields in this window will change.

- b. Fill in the following values:

ALIAS: create a connection name as to identify this site within SecureClient™

PROTOCOL: Keep at **SFTP**

HOST: **sft.ca.gov**

PORT: **22** ♦

USER: **your SFT user account name**

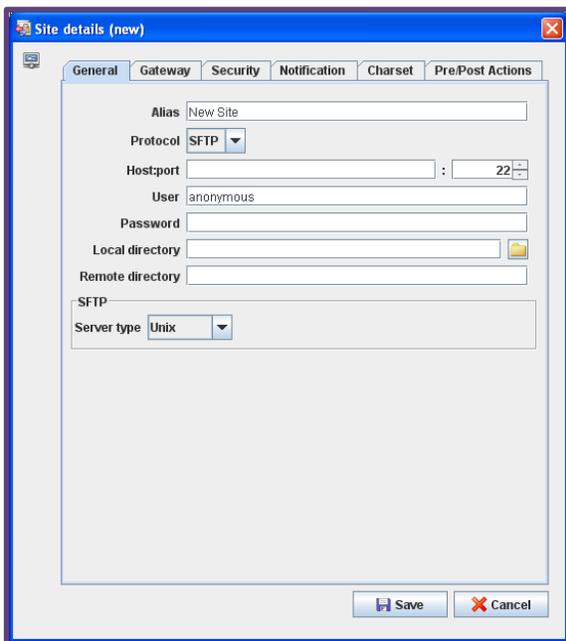
PASSWORD: **your SFT user account password** OR

if using certificate authentication, this field will be left blank.

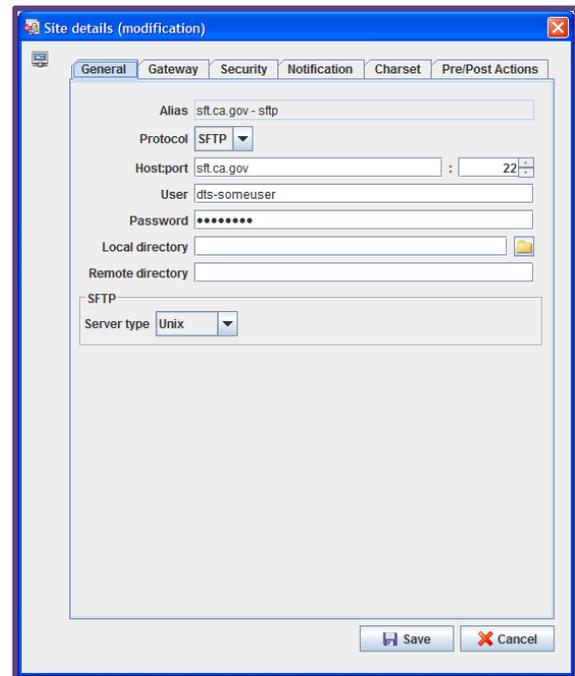
◆ **NOTE:** If you use SSH (SFTP) protocol, it is highly recommended that you use certificate authentication instead of a password, especially if you are using an automated process.

For additional information, please refer to Chapter 8 ([Certificate Authentication](#)).

| Continued on next page |



SecureClient™ | Defining an SFTP site >
General tab at start-up



SecureClient™ | Defining an SFTP site >
General tab filled in

Client Software

Configure a Connection using Axway SecureClient™ (cont'd)

Defining an SFTP connection (cont'd)

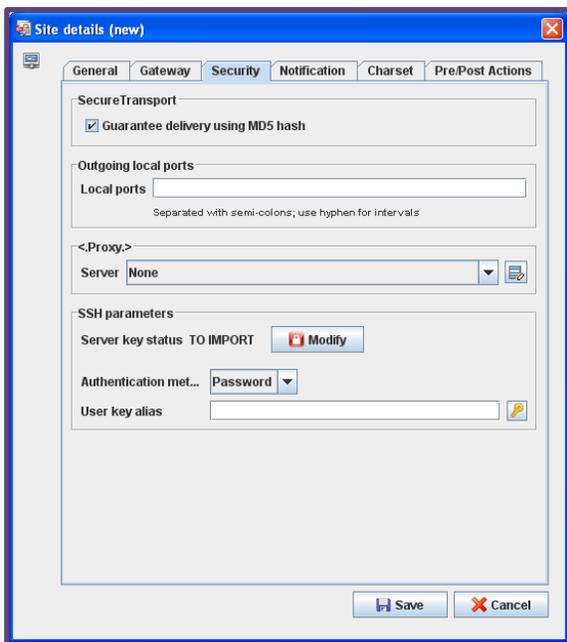
- c. Under the **Security** tab, within the SSH parameters area, locate the field **Authentication met**, select **"Key"** from the drop-down menu.

- d. Click on the "Key" icon.

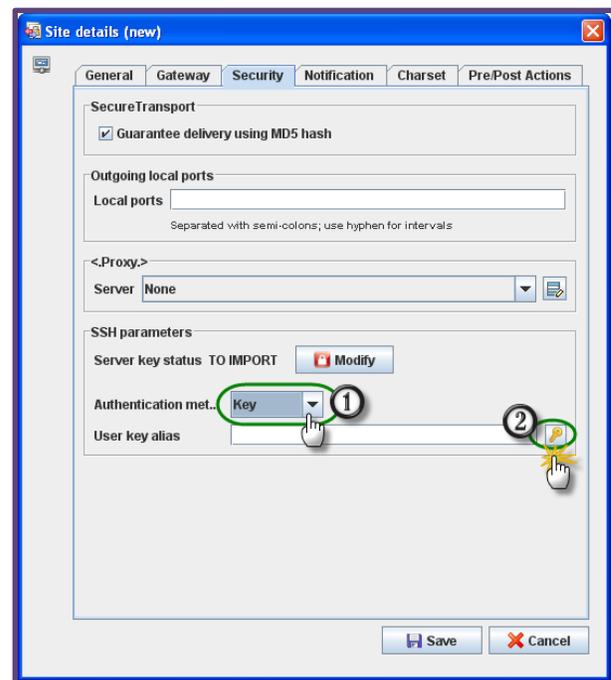


If the fields under the **Security** tab do not look like this screen shot, go back to the **General** tab and verify that SFTP is the selected protocol.

| Continued on next page |



SecureClient™ | Defining an SFTP site >
Security tab at start-up



SecureClient™ | Defining an SFTP site >
Security tab ... Choosing the Key

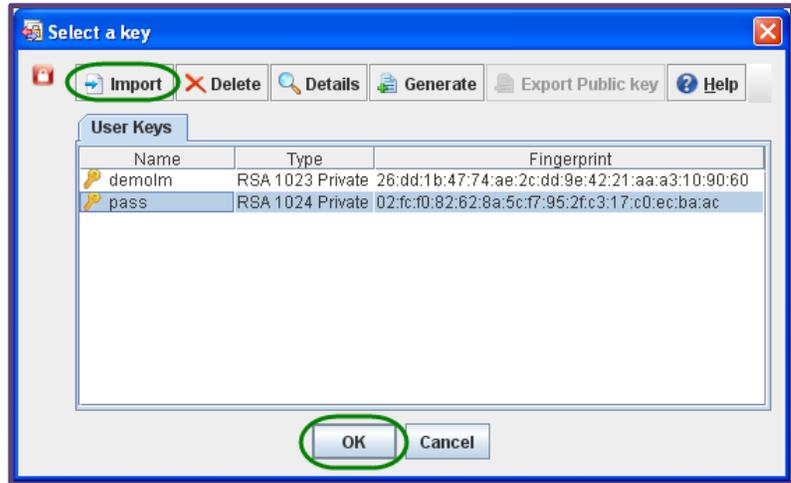
Client Software

Configure a Connection using Axway SecureClient™ (cont'd)

Defining an SFTP connection (cont'd)

e. In the *Select a key* pop-up window, select the private key that pairs with the public key previously e-mailed to your Delegated Administrator.

If the existing private key you wish to use has already been imported, click on the key's line to highlight the name, then click "OK".



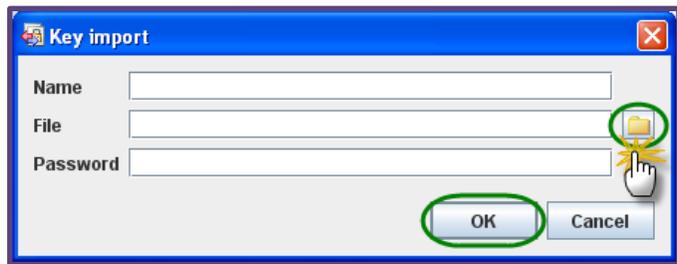
Select a key window

OR

If the private key you wish to use is not listed under available User Keys, click the "Import" button.

The *Key import* window will appear. Give this key a name of your choosing.

Then click the "Folder" icon  to browse and find the private key you wish to import. Lastly, if the private key was protected with a passphrase during the export, enter that passphrase here.



Key import window

Click "OK" to save your settings for this key.

You will return to *Select a key* window.

Click on the line of your newly created key to highlight it. Click "OK".

| Continued on next page |

Client Software

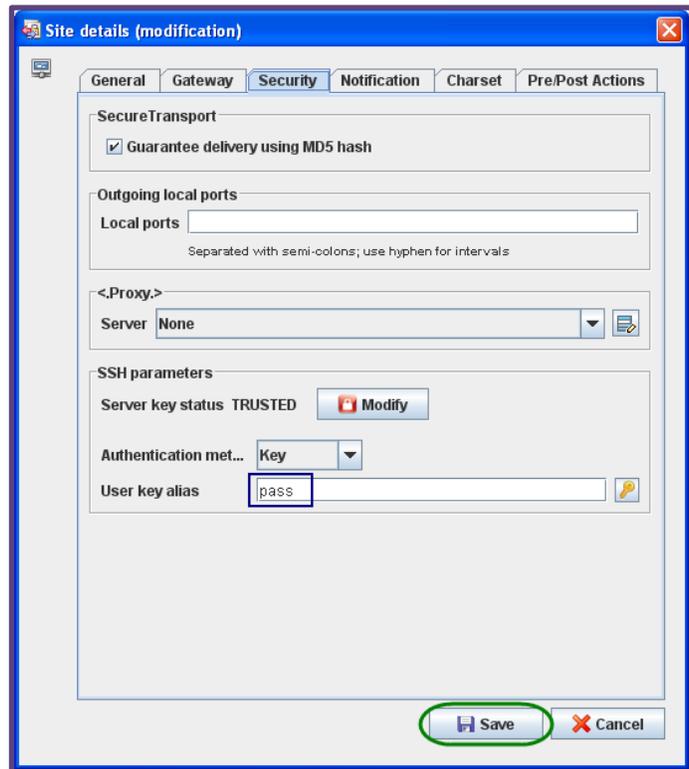
Configure a Connection using Axway SecureClient™ (cont'd)

Defining an SFTP connection (cont'd)

f. The **User key alias** field will now populate with the name of the key you just selected.

g. Click "Save".

Connection is defined.



SecureClient™ | Defining an SFTP site >
Security tab filled in

Client Software

Using a 3rd-party Client

For instructional purposes, this manual will use the CoreFTP 2.1 LE product to demonstrate the process of configuring a 3rd party SFTP client. If using one of the other clients, you may use these instructions as a guide, but we recommend reading the product documentation for configuring connections.

1. Launch the client application.

Auth TLS Connection...

2. Fill in the appropriate values in the following fields...

SITE NAME: create a name

HOST/IP/URL: sft.ca.gov

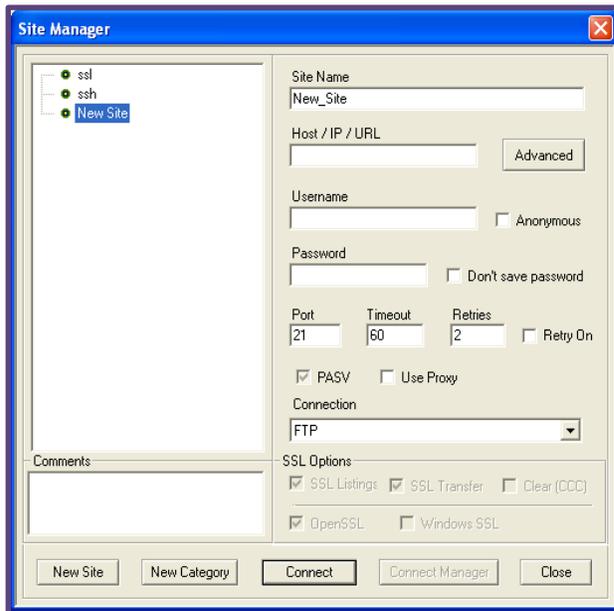
USERNAME: your SFT account name

PASSWORD: your SFT password

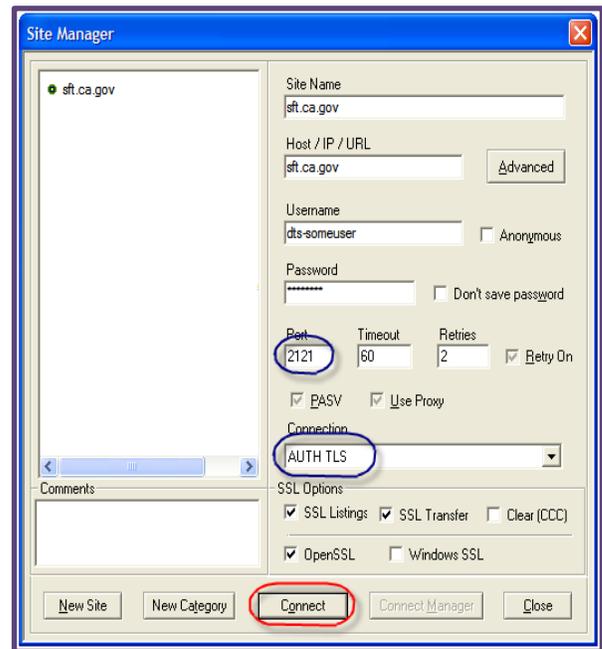
PORT: 2121

CONNECTION (FROM THE DROP-DOWN MENU): AUTH TLS

| Continued on next page |



Site Manager default dialog box



Site Manager dialog box > define a new Auth TLS connection/site > filled in

Client Software

Using a 3rd-party Client (cont'd) Other Protocols

You may also configure the client to use either SSH or FTPS.

From the **Connection** drop-down menu select:

- **SSH (SFTP)**: Port: **22** ♦
- **FTPS**: Port: **2121** (ports 5000-5899 must be opened outbound for passive mode transfers.)

◆ **NOTE:** If you use SSH (SFTP) protocol, it is highly recommended that you use certificate authentication instead of a password, especially if you are using an automated process

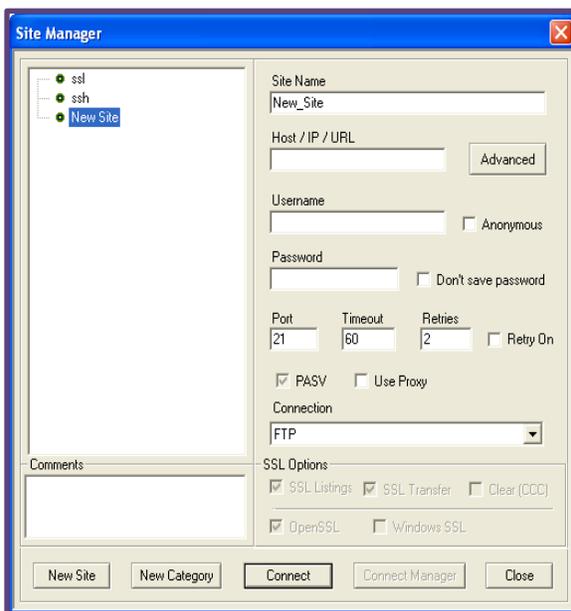
For additional information, please refer to Chapter 8 ([Certificate Authentication](#)).

NOTE: No matter what client you use, no matter the protocol, the PASV option must be selected. If there is no check mark in its box, please check it.

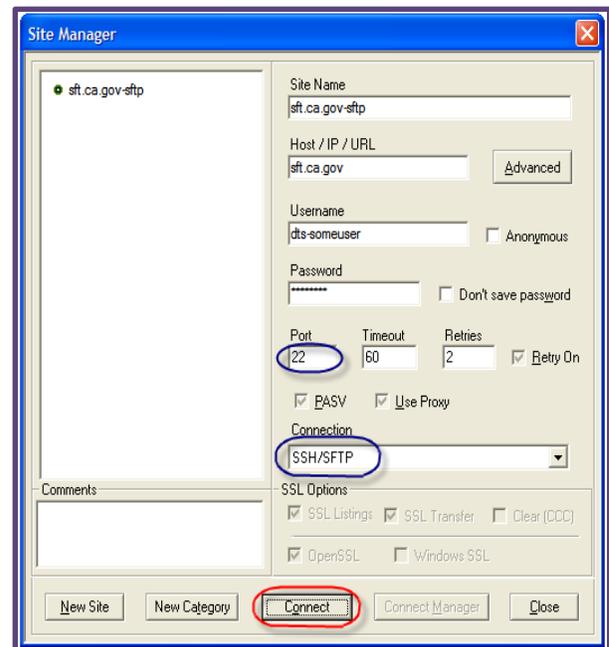
Should you have an initial connection failure, please go back and confirm the PASV setting.

3. Click the "Connect" button.

| Continued on next page |



Site Manager default dialog box



Site Manager dialog box > define a new SSH connection/site > filled in

Client Software

Using a 3rd-party Client (cont'd)

- After clicking the "Connect" button, the *Certificate Information* pop-up box appears.

Notice the **Organization**, **Common Name**, and **Unit** field values.

If the values in these fields do not match those in the screen shot below, something is wrong, do not accept the certificate. Click "Cancel", do not proceed any further, and contact your Delegated Administrator immediately



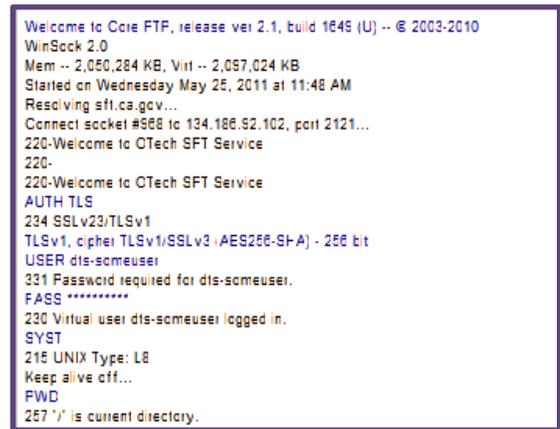
Certificate Information pop-up

- Click "Always Accept".
If you click "Accept Once", you will have to repeat these steps on your next log in.

- The *Site Manager* dialog box will disappear

If you connected successfully, your SFT account folders will now populate the *Remote View* window (by default the right-side window).

If there was a connection failure, there will be an entry in the *Session Log* window (the upper-left window).



Session Log window

Client Software

Using 3rd-party Command Line Clients

You can also use the command line with some third party clients like CoreFTP (refer to its manual for command line parameters and usage). The PuTTY suite includes two useful command line tools that work with SFT... pscp.exe and psftp.exe. See the online PuTTY documentation for all the command switches and parameters.

Examples of uploading a file with pscp.exe

Upload C:\testfiles\testfile.txt to SFT:

```
pscp C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:
```

```
C:\>pscp C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:
SSH server: Password Authentication
Using keyboard-interactive authentication.
Password:
testfile.txt           | 0 kB |   0.0 kB/s | ETA: 00:00:00 | 100%
```

Upload C:\testfiles\testfile.txt to SFT as a new filename "new_filename.txt":

```
pscp C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:new_filename.txt
```

```
C:\>pscp C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:new_filename.txt
SSH server: Password Authentication
Using keyboard-interactive authentication.
Password:
testfile.txt           | 0 kB |   0.0 kB/s | ETA: 00:00:00 | 100%
```

Upload C:\testfiles\testfile.txt to SFT to remote directory "ToMF":

```
pscp C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:ToMF/
```

```
C:\>pscp C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:ToMF/
SSH server: Password Authentication
Using keyboard-interactive authentication.
Password:
testfile.txt           | 0 kB |   0.0 kB/s | ETA: 00:00:00 | 100%
```

Upload testfile.txt and specify password in command using "-pw":

(replace the ***** with your actual password)

```
pscp -pw ***** C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:
```

| Continued on next page |

Client Software

Using 3rd-party Command Line Clients (cont'd)

Examples of uploading a file with pscp.exe (cont'd)

Upload testfile.txt and specify PuTTY private key in command using "-i":

```
pscp -i C:\putty\dts-someuser_ssh_key.ppk C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:
```

```
C:\>pscp -i C:\putty\dts-someuser_ssh_key.ppk C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:
testfile.txt           | 0 kB | 0.0 kB/s | ETA: 00:00:00 | 100%
```

Upload testfile.txt but output debug information (verbose) using "-v":

```
pscp -v C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:
```

```
C:\>pscp -v C:\testfiles\testfile.txt dts-someuser@sft.ca.gov:
Looking up host "sft.ca.gov"
Connecting to 134.186.92.102 port 22
Server version: SSH-2.0-SSHD
We claim version: SSH-2.0-PuTTY_Release_0.60
Using SSH protocol version 2
Doing Diffie-Hellman group exchange
Doing Diffie-Hellman key exchange with hash SHA-1
Host key fingerprint is:
ssh-rsa 2048 c7:a0:7d:bd:80:f6:7a:f1:44:17:3f:a3:b3:f4:7e:52
Initialised AES-256 CBC client->server encryption
Initialised HMAC-SHA1 client->server MAC algorithm
Initialised AES-256 CBC server->client encryption
Initialised HMAC-SHA1 server->client MAC algorithm
Using username "dts-someuser".
OTech SFT SSH connected.
SSH server: Password Authentication
Using keyboard-interactive authentication.
Password:
Access granted
Opened channel for session
Started a shell/command
Using SFTP
Connected to sft.ca.gov

Sending file testfile.txt, size=4
testfile.txt           | 0 kB | 0.0 kB/s | ETA: 00:00:00 | 100%
Sent EOF message
Disconnected: All channels closed
```

| Continued on next page |

Client Software

Using 3rd-party Command Line Clients *(cont'd)*

Examples of uploading a file with psftp.exe

SFTP login with interactive password:

```
psftp dts-someuser@sft.ca.gov
```

SFTP login with password in command using "-pw":

(replace the ***** with your actual password)

```
psftp -pw ***** dts-someuser@sft.dts.ca.gov
```

```
C:\>psftp dts-someuser@sft.ca.gov
Using username "dts-someuser".
OTech SFT SSH connected.
SSH server: Password Authentication
Using keyboard-interactive authentication.
Password:
Remote working directory is /
psftp> bye
```

SFTP login and specify PuTTY private key using "-i":

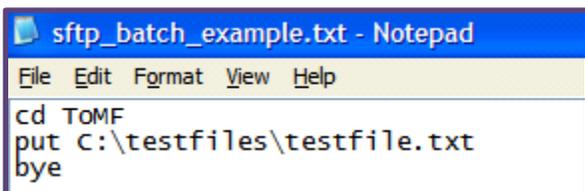
```
psftp -i C:\putty\dts-someuser_ssh_key.ppk dts-someuser@sft.ca.gov
```

```
C:\>psftp -i C:\putty\dts-someuser_ssh_key.ppk dts-someuser@sft.ca.gov
Using username "dts-someuser".
OTech SFT SSH connected.
Remote working directory is /
psftp> bye
```

SFTP using batch file and PuTTY private key (completely automated!) using "-b" and "-i" to upload testfile.txt to remote "ToMF" directory:

```
psftp -i C:\putty\dts-someuser_ssh_key.ppk -b C:\sftp_batch_example.txt dts-someuser@sft.ca.gov
```

C:\sftp_batch_example.txt looks like:



```
sftp_batch_example.txt - Notepad
File Edit Format View Help
cd ToMF
put C:\testfiles\testfile.txt
bye
```

Certificate Authentication

Client Certificate Authentication eliminates the username and password prompt when securely logging in to the SFT system. Automated file transfers need not use parameter driven scripts that contain a username and password if an X.509 or SSH key is used instead. SFT supports two-factor authentication: enable both client certificate authentication AND password authentication for the user account.

To enable Client Certificate Authentication please contact your Delegated Administrator or see Appendix D in this manual.

There are several advantages to using certificates (vs. passwords).

1. You do not need to remember another password. (But a new certificate will need to be generated before the current certificate expires. SFT supports authentication certificates that are valid for up to two years.)
2. You cannot be locked out due to a set-number of failed login attempts.
3. You will not be required to change your password every 90 days. Your password will still expire after 90 days, but your account access using the cert will work for 2 years.
4. Since you do not need to be at a terminal to type a password, you can automate file transfers (to an extent).



NOTE: If you use SSH (SFTP) protocol, it is highly recommended that you use certificate authentication instead of a password, especially if you are using an automated process (scripts, batch-file driven, scheduled jobs ...)

You will generate a SSH key pair and install the private key into the client software certificate store on your computer and upload the public key to a special folder in your SFT user account.

See [Appendix D](#) for information on implementing client certificate authentication.

NOTE: If you replace a certificate with a newer one and are using Internet Explorer, you may need to clear the SSL cache for the new certificate to be recognized. See [Appendix B](#).

Technical Specifications

Operating System (OS) Requirements

Windows, Mac, Linux/UNIX, Mainframe

(The client/web browser will determine the specifics of the OS)

Web Browser Requirements

Internet Explorer® 7 and 8 only, FireFox® 3.x – 6.x

Permission Requirements for Web Browser

Ability to save cookies (session management)

JavaScript enabled

SecureTransport™ Clients

SecureClient™ 5.5 (or later) - OTech is an authorized reseller of this product.

SecureTransport Command Line (FDX) Client, version 4.5.1, 4.5.2

FTP and HTTP clients

cURL 7.19 (HTTPS only)

CuteFTP Professional 8.3.2

FileZilla 3.0.0

Igloo FTP Professional 3.9

IBM Mainframe client

Ipswitch WS_FTP Server 7.1

LFTP 3.7.14

SmartFTP Client 3.0

SSH clients

FileZilla 3.0.0 (and later)

PuTTY 0.60 (pscp.exe and psftp.exe)

SecureFile Transfer SCP and SFTP (shipped with Solaris 10)

Tectia Client 5.3

Tectia Client 6.0.7

VanDyke SecureFX 6.2.1

WinSCP 4.1.9

Support and References



User account holders request support from their Delegated Administrator(s), not from the OTech Service Desk or SFT staff. OTech Service Desk personnel are instructed to refer password resets and account unlock requests from end users to the customer's Delegated Administrator. SFT staff will accept requests for SFT support only from customer Delegated Administrators.

Document Library

This User Manual, Quick Start Guide and other SFT documentation can be found here: http://getsft.ca.gov/sft_resources.asp. The OTech Service Catalog (<http://www.servicecatalog.dts.ca.gov/sft/sft.asp>) is another reference for SFT information.

OTech Service Desk

(916) 464-4311 or service.desk@state.ca.gov

SFT Staff Responsibilities

Customer Configuration Settings

Based on your requirements and resources, SFT staff can recommend a file transfer client. Depending on your client's file transfer protocol (FTPS, SFTP, or HTTPS), your organization may need to adjust network configuration (firewall) settings to provide connectivity for that protocol.

Customer Responsibilities

Operations and Systems Security

Customers are responsible for the integrity of their internal networks and local data.

SFT User Administration

Customer Delegated Administrators are responsible for the administration of their SFT user IDs and passwords. To implement certificate-based authentication, users may contact their Delegated Administrator or follow the steps in [Appendix D](#).

Desktop Systems

Customers have full responsibility for all file transfer client installation and configuration. This includes, but not limited to, the operating system, the browser version, and client licenses.

SFT Staff and Customer Shared Responsibilities

File Transfer Support Issues

SFT staff and the customer's delegated administrators will work together to resolve any file transfer issues.

Support and References

Internet Explorer (IE v8, 9) Security Alert Box



Security prompt

How to avoid the "Choose a digital certificate" prompt that is encountered when you log into your SFT account using Internet Explorer.

1. In the IE browser, on the Menu Bar, click **Tools**.

At the bottom of this submenu, select **Internet Options**.



IE | Menu Bar | **Tools** > **Internet Options**

2. Under the **Security** tab, make sure *Internet* icon is selected.

Then click on "Custom level..."



Internet Options pop-up

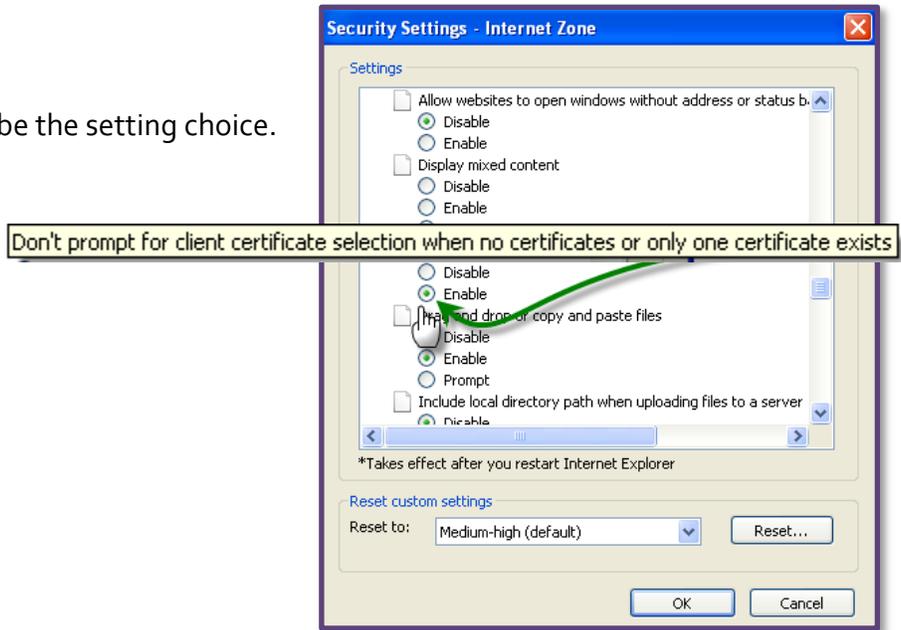
Support and References

Internet Explorer Security Alert Box (cont'd)

- The pop-up box Security-Settings – Internet Zone has a number of settings. Scroll down about half way until you reach

"Don't prompt for client certificate selection when no certificates or only one certificate exists"

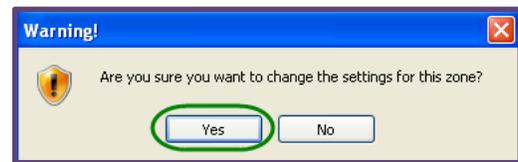
You want "Enabled" to be the setting choice.



Security-Settings-Internet Zone options

- Click "OK".

- You may see this warning box pop-up. Click "Yes".



Warning pop-up

- You will return to the initial *Internet Options* pop-up. Click "OK".

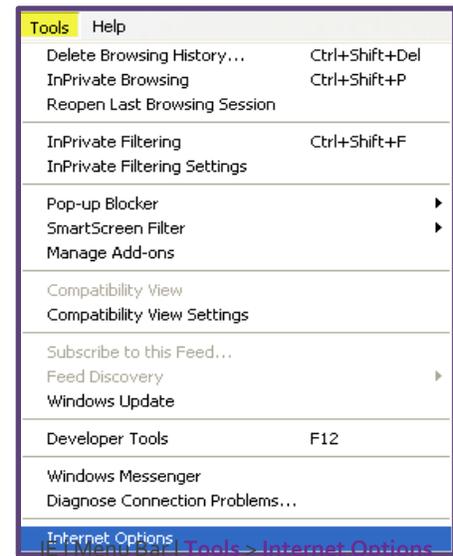
Support and References

Installing a newer SSL Certificate -- Internet Explorer (IE) Issue

If you are using an SSL Certificate to access your SFT account and using Internet Explorer as your browser **AND** you create a **new** SSL certificate, you will need to "Clear SSL state cache" within IE so this new certificate is recognized and used by Internet Explorer.

1. In the IE browser, on the Menu Bar, click **Tools**.

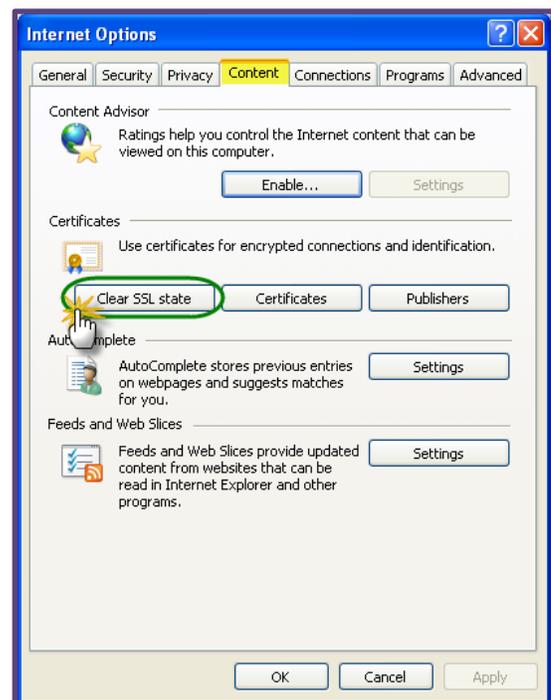
At the bottom of this submenu, select **Internet Options**.



2. Under the **Content** tab, click the button "Clear SSL state".
3. When the cache is fully cleared, you will see an alert box letting you know the action was successful.



4. You will see the initial **Internet Options** pop-up. Click "OK".



IE | Menu Bar | **Tools** > **Internet Options** > **Content**

Automating Password Change Over FTPS

NOTE: Target Audience

This feature is recommended for advanced users who wish to automate the process of changing their passwords through a script or program.

For less-technical users, the recommended way to change your password is by logging in with a web browser to <https://sft.ca.gov> and then clicking "Change Password". (See [Chapter 2](#))

Again, this option is only available over FTPS. In order to automate this process, you must use an FTPS client that supports scripting or batch files, as well as the FTP QUOTE or SITE commands.

Windows

- MoveIT Freely: <http://www.ipswitchft.com/products/moveitFreely/index.aspx>
- cURL: <http://curl.haxx.se/download.html>

UNIX/Linux

- cURL: <http://curl.haxx.se/download.html>

Mainframe (z/OS)

- Standard FTP program

SFT provides the ability to change your SFT account password over the FTPS protocol. This can be executed from any FTPS client that supports the FTP "SITE" command. Typically the "SITE" command must come after a "QUOTE" command or option.

Syntax

The syntax of the change password SITE command is:

```
ftp> SITE CHPWD <SFT_login_name> <base64-current-password> <base64-new-password>
```

Where:

- <SFT_login_name> is your SFT login name
- <base64-current-password> is your current password, Base64-encoded
- <base64-new-password> is your new password, Base64-encoded

Lesson: How to Base64 Encode

Base64 encoding converts any string or binary stream into a string of printable characters. SFT does not have this feature built-in, thus it is the end-user's responsibility to Base64 encode the passwords.

Further information on Base64 can be found on Wikipedia: <http://en.wikipedia.org/wiki/Base64>.

For example, let us assume we have an SFT user dts-someuser:

- Current password: MyOldP@55
- New password: N3wP@s5wOrd

After Base64 encoding these passwords:

- Base64 Current password: TX1PbGRQQDU1
- Base64 New password: TjN3UEBzNXdPcmQ=

Base64 Utilities

Web-based (Browser)

Several websites offer Base64 encoding. These were found by Googling "Base64 encoder":

- <http://www.string-functions.com/base64encode.aspx>
- <http://www.opinionatedgeek.com/dotnet/tools/base64encode/>
- <http://www.motobit.com/util/base64-decoder-encoder.asp>

Linux

Some Linux distributions include `/usr/bin/base64`. <http://linux.die.net/man/1/base64>

Linux/UNIX Compile from Source

Base64 can be compiled from a single C source file without the need for a Makefile. A compiler such as `gcc` is required. The source code is maintained on SourceForge and can be downloaded at <http://base64.sourceforge.net/b64.c>.

This command will compile this C file into a binary "base64" (-o = output file) using `gcc`:

```
$ gcc b64.c -o base64
```

Perl module

Base64 encoding is available in `MIME::Base64`, included in the Perl core (no installation required). See <http://perldoc.perl.org/MIME/Base64.html> for more details. This can be achieved using a Perl "one-liner":

```
# Password with @ character needs to be escaped (\) in Perl quoted-string
$ perl -MMIME::Base64 -e 'print encode_base64("MyOldP\@55")'
$ perl -MMIME::Base64 -e 'print encode_base64("N3wP\@s5wOrd")'
```

Windows

A command-line Base64 utility is available for Windows at <http://www.f2ko.de/programs.php?lang=en>

```

Base64 - Encode/Decode files using the Base64 algorithm.
Call: base64.exe [-options] <infile!-s> <outfile!-s>

Options:
  -d --decode           Decode base64 encoded file
  -e --encode          Encode file using the Base64 algorithm
  -h --help            Print this message
  -s --stdin/stdout    Read data from stdin/Write data to stdout
  -v --version         Print version number

Examples: base64 -e myfile.exe myfile.txt
          base64 -d myfile.txt myfile.exe

by Fatih Kodak
http://www.f2ko.de
    
```

DOS syntax to base64 using base64.exe without adding the extra carriage-return+line-feed (CRLF):
`echo.|set /P ="MyOldP@55" | base64.exe -e -s`

Would output:

`TX1PbGRQQDU1`

WARNING: BASE64 IS NOT ENCRYPTION!

Please note Base64 *does not encrypt* – it only converts the string to a different base. Decoding this string will show the password in its original cleartext form.

```

$ echo -n "MyOldP@55" | base64
TX1PbGRQQDU1
# Now we decode the password using the "-d" flag
$ echo -n "TX1PbGRQQDU1" | base64 -d
MyOldP@55
    
```

Changing the Password

Now that you have your current and new passwords Base64 encoded, you need to execute the command using your FTPS client. As with any FTPS command, you must first authenticate using your existing credentials.

Using cURL

cURL is an open-source command-line application available on almost any platform (Windows, Linux, UNIX, Mac OS X, z/OS) and for multiple protocols, FTPs included. cURL has full support of the FTPS "QUOTE" function which allows us to issue a change password line in a single cURL command.

cURL documentation and binaries can be found at <http://curl.haxx.se/>.

```
#!/bin/sh

oldpass='MyOldP@55'
newpass='N3wP@s5wOrd'
b64_oldpass=$(echo -n ${oldpass} | base64)
b64_newpass=$(echo -n ${newpass} | base64)

user='dts-someuser'
server='sft.ca.gov'
port=2121

curl --ssl-reqd -u ${user}:${oldpass} \
  --quote "SITE CHPWD ${user} ${b64_oldpass} ${b64_newpass}" \
  ftp://${server}:${port}

exit $?
```

MoveIT Freely Batch

To run MoveIT Freely's FTPS client and run a script:

```
ftps.exe -a -e:on -s:C:\ftps-script.txt
```

- **-a:** Use FTP Passive
- **-e:on:** Encrypt both control and data with AUTH TLS ("explicit")
- **-s:file** Run the script file

To change the dts-someuser's password from **MyOldP@55** to **N3wP@s5wOrd**, your C:\ftps-script.txt file would look like:

```
open sft.ca.gov 2121
dts-someuser
MyOldP@55
quote site chpwd dts-someuser TX1PbGRQQDU1 TjN3UEBzNXdPcmQ=
bye
```

For Windows, OTech recommends using a more robust scripting environment such as PowerShell (http://en.wikipedia.org/wiki/Windows_PowerShell) or Cygwin (<http://www.cygwin.com/>).

Self-Provisioned Certificate Authentication

SFT User account holders can “activate” certificate authentication themselves, possibly without Delegated Administrator assistance. Delegated Administrators, however, are responsible for identifying eligible users and providing support for this feature.

The process of activating certificate authentication requires the creation of file folders in your user account home folder. Since the web browser cannot be used to create folders, you must use a 3rd-party client. For this tutorial, we will use FileZilla. However, you can use any compatible secure FTP client. Follow these 4 steps:

- Step 1: Create the SSH key pair
- Step 2: Create the “.ssh” folder
- Step 3: Upload the public key into the .ssh folder
- Step 4: Note the response files created to indicate success or failure

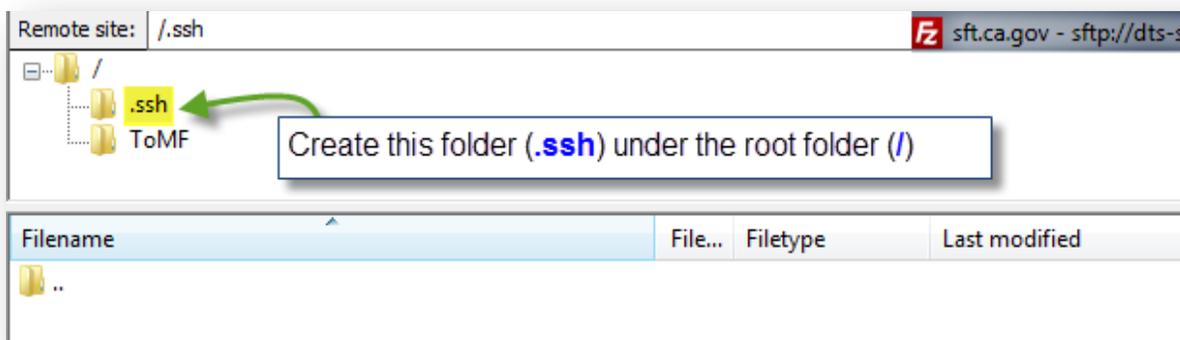
Create the SSH Key Pair

Generate the SSH key pairs saving the private and public keys to a folder on your PC. Key pairs can be generated on Windows PCs using the PuTTY software

Create a .ssh folder

Use your client to create a host connection to log in to your SFT user account at <https://sft.ca.gov>

- ⇒ Create directory named “.ssh” in your SFT root directory. Note the “dot” in front of the “ssh”. The quotes are NOT a part of the directory name.



Upload the public key file

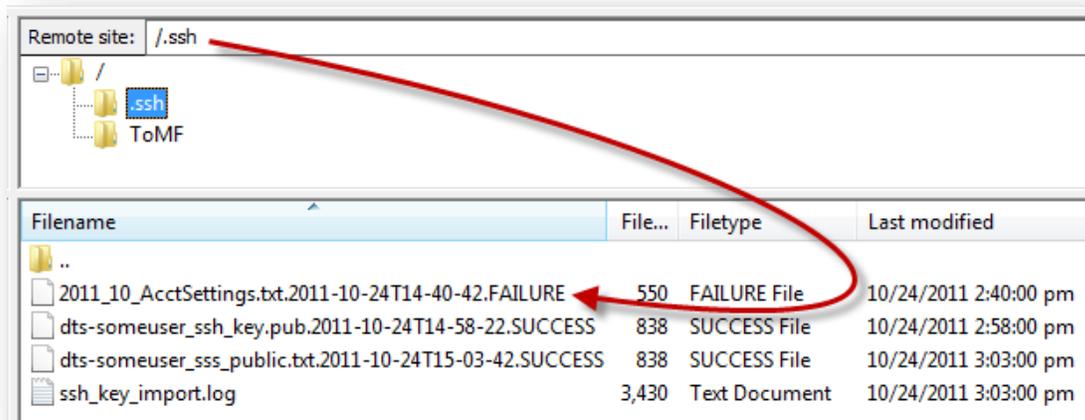
1. Navigate inside the .ssh directory.
2. Upload the file containing your SSH public key into the ".ssh" directory.

Note the Response Files

1. On success, the uploaded public key file will be renamed with the timestamp and ".SUCCESS". On failure, it will be renamed with the timestamp and ".FAILURE".
2. A log file named "ssh_key_import.log" is also created the first time a file is uploaded into the .ssh folder. See Examples below.

EXAMPLE 1: FAILURE

The sample file named "2011_10_AcctSettings.txt" was uploaded. It does not contain a valid SSH public key:



Filename	File...	Filetype	Last modified
..			
2011_10_AcctSettings.txt.2011-10-24T14-40-42.FAILURE	550	FAILURE File	10/24/2011 2:40:00 pm
dts-someuser_ssh_key.pub.2011-10-24T14-58-22.SUCCESS	838	SUCCESS File	10/24/2011 2:58:00 pm
dts-someuser_ssh_public.txt.2011-10-24T15-03-42.SUCCESS	838	SUCCESS File	10/24/2011 3:03:00 pm
ssh_key_import.log	3,430	Text Document	10/24/2011 3:03:00 pm

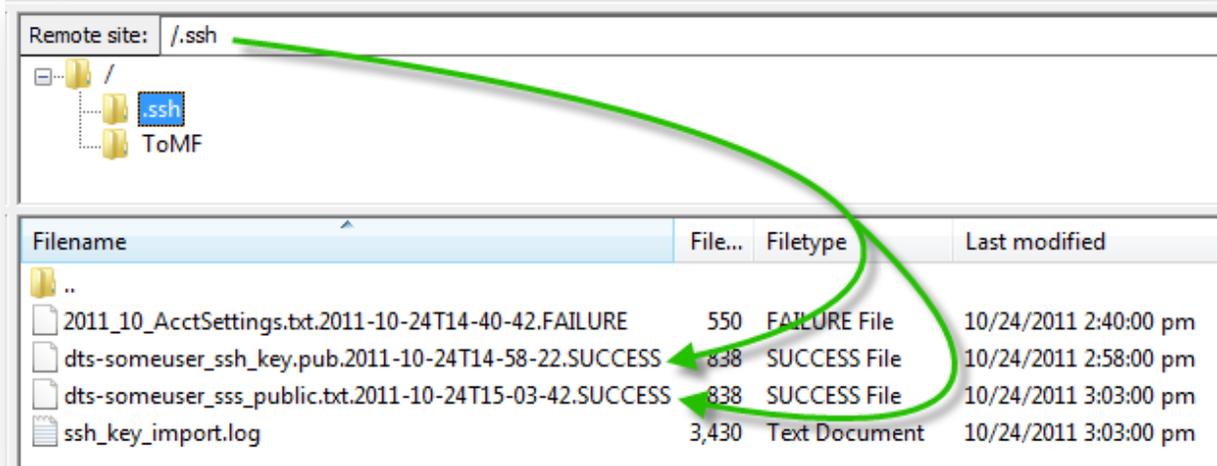
EXAMPLE 2: SUCCESS

- Saved as a default .pub file
- Saved as a file with an extension other than default.

```
dts-someuser_ssh_key.pub
----- BEGIN SSH2 PUBLIC KEY -----
Comment: "rsa-key-20110921"
AAAAB3NzaC1yc2EAAAABJQAAAIB3jxDxh
2FSPg6XDwxWZmXvEUTgJh1Q+r71TAHb2M
BFYQ57QybWyK9FhM6ke2VMshpOKXeWvbA
WSZF0w==
----- END SSH2 PUBLIC KEY -----
```

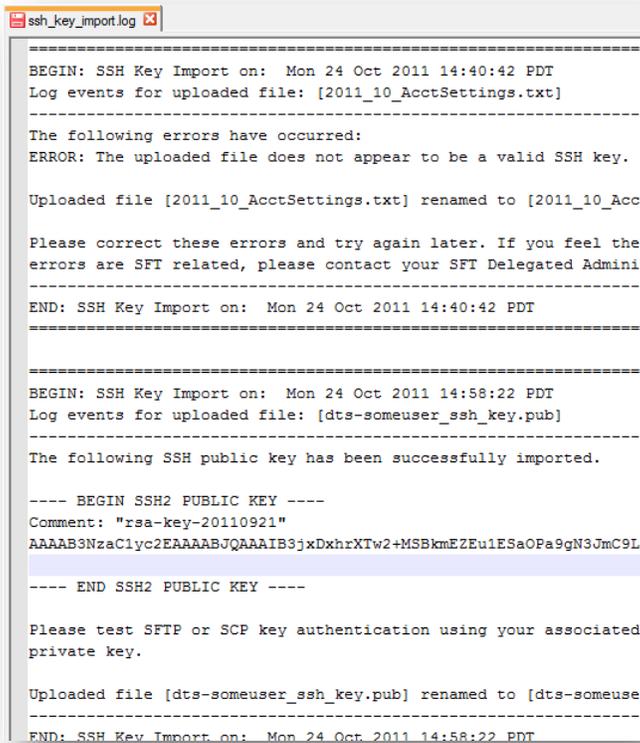
```
dts-someuser_ssh_public.txt
----- BEGIN SSH2 PUBLIC KEY -----
Comment: "rsa-key-20111024"
AAAAB3NzaC1yc2EAAAABJQAAAIEAg1Qtu
PZAoubMr+WUN8h845gSItN0gh1fBXERtg
pEp1qSiXBRF8wYjQIWMvX3xL3+jcM3HCE
MhQc1FM=
----- END SSH2 PUBLIC KEY -----
```

In these examples, public key file saved with a .pub extension and a .txt extension



Results of uploading dts-someuser_ssh_key.pub and dts-someuser_sss_public.txt

3. The status and logs are appended to a log file *ssh_key_import.log* in the ".ssh" directory.



Abbreviations, Acronyms, Terms to Know

3DES	Triple Data Encryption Standard: In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA) block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Because of the availability of increasing computational power, the key size of the original DES cipher was becoming subject to brute force attacks. Triple DES was designed to provide a relatively simple method of increasing the key size of DES to protect against such attacks, without designing a completely new block cipher algorithm.
ASCII	American Standard Code for Information Interchange: ASCII is a character-encoding scheme based on the ordering of the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that use text. Most modern character-encoding schemes are based on ASCII, though they support many more characters than did ASCII.
Auth SSL	Authorizing Secure Sockets Layer: A prompt within SFT to set up 3 rd -party client procedure.
GLBA	The Gramm–Leach–Bliley Act (GLB), also known as the Financial Services Modernization Act of 1999, enacted November 1999, is an act of the United States Congress signed into law by President Bill Clinton which repealed part of the Glass-Steagall Act of 1933, opening up the market among banking companies, securities companies and insurance companies.
CTA	California Technology Agency: A California cabinet-level agency that includes Office of Technology Services (OTech). The CTA was dissolved by legislation in 2012 (effective July 2013) and its functions and subdivisions moved under the new Government Operations Agency.
CD	Compact Disc: CDs are used to store files and can be shipped or distributed for file transfer.
DA	Delegated Administrator: The Secure File Transfer primary contact for users.
DVD	Digital Video Disk

FIPS	Federal Information Processing Standards: FIPS are publicly announced standards developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.).
FTP	File Transfer Protocol: FTP is a standard network protocol used to copy a file from one host to another over a TCP/IP-based network, such as the Internet. FTP is built on a client-server architecture and utilizes separate control and data connections between the client and server. FTP users may authenticate themselves using a clear-text sign-in protocol but can connect anonymously if the server is configured to allow it. The OTech SFT service does NOT support legacy FTP due to its lack of security in authentication and file transfer.
FTPS	FTP Secure and FTP-SSL: An extension to File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols
HIPAA	Health Insurance Portability and Accountability Act: HIPAA was enacted by the U.S. Congress in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers
HITECH	The Health Information Technology for Economic and Clinical Health (HITECH) Act. Addresses privacy and security concerns associated with the electronic transmission of health information.
HTTP	Hypertext Transfer Protocol: A networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.
HTTPS	Hypertext Transfer Protocol Secure: A combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network web server.
MDN	Message Disposition Notification: MDNs provide a notification of the "disposition" of a message - indicating, for example, whether it is read by a recipient, discarded before being read, etc. However for privacy reasons, and also for backward compatibility, requests for MDNs are entirely advisory in nature - i.e. recipients are free to ignore such requests. The format and usage MDNs are specified in RFC 3798.

OTech	Office of Technology Services: OTech is an office within the California Technology Agency in which the Secure File Transfer service is operated.
PCI	Payment Card Industry: PCI is in regard to federal compliance to services as funded by credit card.
PuTTY	PuTTY is a free and open source terminal emulator application which can act as a client for the SSH computing protocol among others, and as a serial console client. The name "PuTTY" has no definitive meaning, though 'tty' is the name for a terminal in the Unix tradition, usually held to be short for teletype.
SCP	Secure Copy Protocol (or Secure Copy Program): Network protocol that supports file transfers. Runs on port 22. Is tunneled through the Secure Shell (SSH) protocol to provide encryption and authentication. SCP protects the authenticity and confidentiality of the data in transit and the credentials used to authenticate. Has been superseded by the more comprehensive SFTP protocol, which is also based on SSH.
SFT	Secure File Transfer: In this document, refers to the OTech managed, shared service, Secure File Transfer.
SFTP	SSH File Transfer Protocol (sometimes called Secure File Transfer Protocol) is a network protocol that provides file access, file transfer, and file management functionality over any reliable data stream. An extension of the Secure Shell protocol (SSH) version 2.0. SPFT is most often used as subsystem of SSH protocol version 2.
SOX	Sarbanes–Oxley Act of 2002: Known as the 'Public Company Accounting Reform and Investor Protection Act' (in the Senate) and 'Corporate and Auditing Accountability and Responsibility Act' (in the House) and commonly called Sarbanes–Oxley, Sarbox or SOX, is a United States federal law enacted on July 30, 2002, which set new or enhanced standards for all U.S. public company boards, management and public accounting firms.
SSH	Secure Shell protocol: A network protocol that allows data to be exchanged using a secure channel between two networked devices. Used primarily on Linux and Unix based systems to access shell accounts.
SSL/TLS	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security for communications over networks such as the Internet. TLS and SSL encrypt the segments of network connections at the Application Layer to ensure secure end-to-end transit at the Transport Layer.
VPN	Virtual Private Network: A virtual private network (VPN) is a computer network that uses a public telecommunication infrastructure to provide remote offices or individual users with secure access to their organization's network.

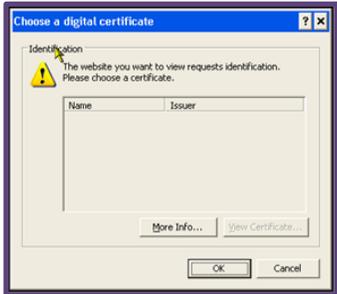
QUICK START

Using the Web Browser

1. Open a web browser.
 Navigate to: <https://sft.ca.gov>
 (The web browser uses HTTPS secure protocol.)

If using Internet Explorer, you may see this "Choose a digital certificate" prompt. If so, click "OK" to proceed.

To suppress this alert on subsequent logons, please see Appendix B in the User Manual.



Certificate prompt

2. At **Log In** screen, enter your **Username** and **Password**, then click the "Log In" button or press [Enter].

NOTE: After a limited number of failed login attempts, the account will be locked.



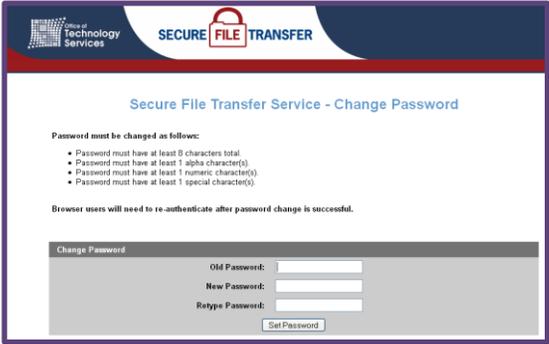
Log In screen

If this is your first time logging into the Secure File Transfer (SFT) system OR your password has been reset... proceed to Step 3.

Otherwise proceed to Step 4.

3. All new (and reset) accounts use a temporary password provided to you by your Delegated Administrator. Use this password to log in for the first time or after a password reset.

When you see this screen, you **must** change your password.



Change Password screen

| Continued on next page |

Using the Web Browser (cont'd)

NOTE: If you fail to change your temporary password within 90 days, your account will expire.

This screen will display when you attempt to log in.

If your account has expired, you will need to ask your Delegated Administrator to unlock it.

Expired Password screen

4. Upon successful login, the SFT *User Directory* screen appears which allows you to perform file upload, download and other operations.



After 15 minutes of inactivity, your SFT session will time out.

Overview of the SFT User Directory Screen

Name	Size [B]	Date	File Options
508checklist.pdf	140270	Aug 29 14:36	[Download] [View as Text] [View as HTML] [Delete]
Solutions_and_Such.docx	24166	Aug 29 14:33	[Download] [View as Text] [View as HTML] [Delete]

SFT *User Directory* screen

- All users have a root or home folder. Your Delegated Administrator may create additional folders for you and these will appear under the root folder.
- All uploaded files in that folder are listed under the dark gray banner named Files.
- Toggle between Binary (default) and ASCII for "upload" and "download" transfer mode.
- "Change Password" button.
- "Logout" button.

