



# Secure File Transfer Protocol (SFTP) Data Submission Users' Manual

Version 1.9

## Document Change History

Version Number	Date	Page(s) Affected	Description
1.0	June 2012		Initial version
1.1	March 2013		Formatting updates
1.2	May 2014		Formatting and contents updates
1.3	August 2014		Content updates
1.4	February 2015		Content updates
1.5	February 2017		Content updates
1.6	July 2017		Content updates
1.7	September 2019		Add Nursing Home
1.8	December 2020		Removed PSO Profile Information
1.9	January 2023		Add Diagnostic Safety

## Table of Contents

Chapter 1 Introduction.....	3
Objectives .....	3
Intended Audience.....	3
Program Overview .....	3
SFTP Data Submission Overview .....	3
Manual Scope .....	4
Chapter 2 Prerequisites.....	5
Pre-Registration .....	5
Registration.....	5
Chapter 3 File Formats .....	7
Conventional Submission .....	7
SFTP Submission Batch.....	7
XML Files.....	7
ZIP Files.....	9
Manifest File.....	10
Alternate Data Submission Format.....	12
SFTP Submission Batch.....	12
Simple XML and DSV .....	12
Chapter 4 Submitting Files .....	13
SFTP Client .....	13
Automation of Submissions .....	13
Public Key Authentication (PKA) Setup .....	13
File Upload Process .....	15
Chapter 5 Account Management.....	20
Technical Support.....	20
Account Termination .....	20

# Chapter 1 Introduction

## Objectives

The primary objective of this document is to provide users technical information for using the Secure File Transmission Protocol (SFTP) to submit data to the Patient Safety Organization Privacy Protection Center (PSOPPC).

## Intended Audience

The intended audiences for this manual are software developers, technical architects and leads involved in submitting formatted data to the Patient Safety Organization Privacy Protection Center (PSOPPC).

## Program Overview

The Agency for Healthcare Research and Quality (AHRQ) coordinates the development of Common Formats for patient safety concern reporting and analysis. This activity is authorized by the Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act). A major goal of the legislation is to provide for the improvement of patient safety and to reduce the incidence of events that adversely affect patient safety.

For additional information on Patient Safety Organizations (PSOs), the Patient Safety Act, and the Patient Safety Rule, please see AHRQ's PSO website: <http://www.pso.ahrq.gov/>

## SFTP Data Submission Overview

In order to support the Patient Safety Act, the Patient Safety Organization Privacy Protection Center (PSOPPC) established an import processor that allows Patient Safety Organizations and/or their vendors to submit patient safety Data in the AHRQ Common Formats through the PSOPPC website. The website functionality allows an authorized user to input a list of Extensible Markup Language (XML) or ZIP files to upload to the import processor. However, there are some disadvantages to using the existing web interface.

The web interface does not readily support automation. For security purposes, the website requires two-factor authentication, which requires user intervention. The website is also limited to 50 files for each submission due to the need to maintain 508 compliance.

The PSOPPC has implemented a Secure File Transfer Protocol (SFTP) solution as an alternative to the web interface for data submission. The goals of this solution are to:

- Accommodate a larger volume of submissions
- Accommodate PSOs with varying information technology (IT) skill sets. Many FTP clients are available at little or no cost
- Provide a solution that could be automated by the PSOs and software vendors

## Manual Scope

This manual presents the information needed to establish an SFTP account, properly format a submission batch for transfer, setup the secure FTP public key authentication (PKA) and upload to the secure FTP site. The steps involved in operationalizing this interface are as follows:

- Contact the PSOPPC Help Desk to request a SFTP account
- Complete the SFTP System Standard Operating Procedure Agreement
- Format files for submission
- Setup PKA and submit public key to the PSOPPC Help Desk
- Upload files
- Log in to the PSOPPC website or call the web service to review submission results

## Chapter 2 Prerequisites

### Pre-Registration

Many of the prerequisites for submitting through the SFTP system are the same as those for submitting through the website. The following prerequisites should be in place before registering to submit through the SFTP system:

#### Account Prerequisites

##### If submitting as a PSO:

- A valid PSO Data Use Agreement (DUA) has been executed with the PSOPPC
- At least one user that holds a Level 3 account

##### If submitting as a PSO Vendor:

- Your organization has been registered as a PSO Vendor with the PSOPPC
- At least one user holds a Level 3 account
- Your organization has been authorized by a PSO to submit on the PSO's behalf
- The PSO on whose behalf you are submitting data has an executed PSO Data Use Agreement

#### Technical Prerequisites

- The PSO or PSO Vendor must be able to construct Patient Safety Data Files in accordance with their relevant specification
- The PSO or PSO Vendor must have an Internet connection
- The PSO or PSO Vendor must have a SFTP client capable of FTP over Secure Shell (SSH).

### Registration

In order to submit using the SFTP system, a PSO or PSO Vendor will need to register for an account. You may contact the PSOPPC Help Desk at [support@psoppc.org](mailto:support@psoppc.org), or by calling 877-571-7712. The PSOPPC Help Desk will process your request and verify the necessary prerequisites.

If the necessary account prerequisites are in place, the PSOPPC Help Desk will forward the SFTP System Standard Operating Procedure Agreement. Complete this agreement and return it to the PSOPPC with the Authorized Official's signature.

The SFTP System Standard Operating Procedure Agreement provides all necessary information to establish the SFTP account for an organization.

- The PSOPPC will allow only the host designated by the organization to connect to the SFTP service. Section 4: Background will be filled out designating the PSO's/Vendor's host and Internet Protocol (IP) address, and will need to also contain the organization's system information.
- Addendum A of the SFTP System Standard Operating Procedure Agreement will document the relevant contact information.

- The Technical Contact should be an individual with the authority and knowledge for dealing with *network* connectivity issues
- The Security Contact should be an individual with the authority and knowledge to deal with *security incidents* at the organization
- If a PSO, the Authorizing Official is the individual on record with AHRQ as being the official for the PSO. If a PSO Vendor, the Authorizing Official is the individual designated when the PSO Vendor registered with the PSOPPC as a Vendor.
- The Data Submission Account is the organization's Level 3 Data Submission account that will be tied to the SFTP (FTP over SSH) account. This account will receive any email notifications as data submitted through SFTP is processed.

Once the agreement has been completed, the PSOPPC will authorize the designated host for access to the SFTP system. The PSOPPC Help Desk will then convey the steps to setup the Public Key Authentication (PKA) method ([see Chapter 4 Submitting Files](#)) to the Data Submission Account holder designated in the agreement.

## Chapter 3 File Formats

### Conventional Submission

#### SFTP Submission Batch

When performing a conventional submission (Clinical Document Architecture [CDA] XML Patient Safety Data), a complete SFTP submission batch consists of:

- One (1) or more XML and/or ZIP files
- Exactly one (1) manifest file

A SFTP submission batch may contain XML and/or ZIP files regarding CDA XML Patient Safety Data submissions. A SFTP submission batch may not mix the two submission types.

A SFTP submission batch may contain both Test and Production submissions. However, the XML files contained within a ZIP file must be all Test or all Production.

If the submitter is a PSO Vendor, the Vendor may submit for multiple PSOs in a single batch. However, the XML files contained within a ZIP file must all be for the same PSO.

The first 24 characters of each file name designate the SFTP submission batch to which the file belongs. The format Batch ID of the SFTP submission batch is as follows:

For CDA XML Patient Safety Data Submissions:

Hospital Common Formats:

PSE-<OrgID>-<YYYYMMDD>-<XXX>

Community Pharmacy Common Formats:

PSECP-<OrgID>-<YYYYMMDD>-<XXX>

Nursing Home Common Formats:

PSENH-<OrgID>-<YYYYMMDD>-<XXX>

Diagnostic Safety Common Formats:

PSEDS-<OrgID>-<YYYYMMDD>-<XXX>

OrgID: Organization ID of the PSO or PSO Vendor submitting. [P##### or V#####]

YYYY: Four digit year of the date of the batch file.

MM: Two digit month of the date of the batch file. Pad with a zero (0) (e.g. 01, not 1).

DD: Two digit day of the date of the batch file. Pad with a zero (0) (e.g. 01, not 1).

XXX: Three digit sequence number to designate different SFTP submission batches from the same date. Pad with a zero (0) (e.g. 001 not 1, or 012, not 12).

### XML Files

#### *XML File Contents*

The contents of an XML file must correspond to the established data submission formats. For CDA XML Patient Safety Data submissions, please see the technical specifications for the following AHRQ Common Formats:

[AHRQ Common Formats for Event Reporting](#)

January 2023

- [Common Formats – Hospital Version 2.0](#)
- [Common Formats – Hospital Version 1.2](#)
- [Common Formats – Community Pharmacy Version 1.0](#)
- [Common Formats – Nursing Home Version 1.0](#)
- [Common Formats – Diagnostic Safety Version 1.0](#)

### *XML File Names*

The format of the filename for the XML file is as follows:

For CDA XML Patient Safety Data Submissions:

Hospital Common Formats:

PSE-<OrgID>-<YYYYMMDD>-<XXX>[user selected portion].xml

Community Pharmacy Common Formats:

PSECP-<OrgID>-<YYYYMMDD>-<XXX>[user selected portion].xml

Nursing Home Common Formats:

PSENH-<OrgID>-<YYYYMMDD>-<XXX>[user selected portion].xml

Diagnostic Safety Common Formats:

PSEDS-<OrgID>-<YYYYMMDD>-<XXX>[user selected portion].xml

OrgID: Organization ID of the PSO or PSO Vendor submitting. [P##### or V#####]

YYYY: Four digit year of the date of the batch file.

MM: Two digit month of the date of the batch file. Pad with a zero (0) (e.g. 01, not 1).

DD: Two digit day of the date of the batch file. Pad with a zero (0) (e.g. 01, not 1).

XXX: Three digit sequence number to designate different SFTP submission batches from the same date. Pad with a zero (0) (e.g. 001 not 1, or 012, not 12).

- Filenames may not contain spaces.
- The total length of the filename may not exceed 40 characters (including delimiter and extension).
- The user selected portion of the filename may be 1 to 12 characters and must be unique within a specific SFTP submission batch.

Example:

PSE-P1024-20120220-001-File1.XML and PSE-P1024-20120220-001-File2.XML would be allowed and indicates two different files in the same SFTP submission batch.

PSE-P1024-20120220-001-File1.XML and PSE-P1024-20120220-002-File1.XML would be allowed and indicates two files with the same name but in different SFTP submission batches.

PSE-P1024-20120220-001-File1.XML and PSE-P1024-20120220-001-File1.XML would not be allowed as the second submission would overwrite the first submission.

### *XML File Size*

A single XML file may not exceed 80 megabytes.

## ZIP Files

### ZIP File Contents

A ZIP file may contain one or more XML files that correspond to the established formats.

The XML files within a ZIP file must be designated as Test or as Production for submission.

The XML files within a ZIP file must all be for the same PSO (primarily of concern to PSO Vendors).

The names of XML files contained within a ZIP file do not need to conform to the XML filename format given above. However, the filenames of XML files contained within a ZIP file may not exceed 40 characters (including delimiter and extension).

Note: Any files in a ZIP file that are not XML will not be processed and will be deleted from the system.

### ZIP File Names

The format of the filename for ZIP file is as follows:

For CDA XML Patient Safety Data Submissions:

Hospital Common Formats:

PSE-<OrgID>-<YYYYMMDD>-<XXX>[user selected portion].zip

Community Pharmacy Common Formats:

PSECP-<OrgID>-<YYYYMMDD>-<XXX>[user selected portion].zip

Nursing Home Common Formats:

PSENH-<OrgID>-<YYYYMMDD>-<XXX>[user selected portion].zip

Diagnostic Safety Common Formats:

PSEDS-<OrgID>-<YYYYMMDD>-<XXX>[user selected portion].zip

OrgID: Organization ID of the PSO or PSO Vendor submitting. [P##### or V#####]

YYYY: Four digit year of the date of the batch file.

MM: Two digit month of the date of the batch file. Pad with a zero (0) (e.g. 01, not 1).

DD: Two digit day of the date of the batch file. Pad with a zero (0) (e.g. 01, not 1).

XXX: Three digit sequence number to designate different SFTP submission batches from the same date. Pad with a zero (0) (e.g. 001 not 1, or 012, not 12).

- Filenames may not contain spaces
- The total length of the filename may not exceed 40 characters (including delimiter and extension)
- The user selected portion of the filename may be 1 to 12 characters and must be unique within a specific SFTP submission batch.

Example:

PSE-P1024-20120220-001-File1.zip and PSE-P1024-20120220-001-File2.zip would be allowed and indicates two different files in the same SFTP submission batch.

PSE-P1024-20120220-001-File1.zip and PSE-P1024-20120220-002-File1.zip would be allowed and indicates two files with the same name but in different SFTP submission batches.

PSE-P1024-20120220-001-File1.zip and PSE-P1024-20120220-001-File1.zip would not be allowed as the second submission would overwrite the first submission.

### *ZIP File Size*

A single ZIP file may not exceed 300 megabytes.

## **Manifest File**

The manifest file serves as the packing slip for a CDA XML Patient Safety Data SFTP batch submission. It allows the PSOPPC to ensure that all files intended for a batch have been received. The manifest file also provides additional information necessary to properly process and ensure the integrity of the batch submission. There may only be one (1) manifest file for each SFTP submission batch.

### *Manifest File Contents*

The manifest file is a comma separated value file (.csv), and as such does not contain quotes. Each row contains the information regarding one file in the submission and takes the following format:

<PSOID>,<Test/Production Flag>,<File Name>,<Number of XMLs>

**PSOID:** AHRQ Assigned PSO ID associated with the file. If the submitter is a PSO, this should be that PSO's ID. If the submitter is a PSO Vendor, the PSOID will vary depending on which PSO the PSO Vendor is submitting for.

**Test/Production Flag:** A flag value denoting how to treat the file submission. One of two values:

T – Treat the file submission as a test submission. The file will be processed and a report generated. However, the data will not be stored. When applied to a ZIP file, all XML files within that ZIP file will be treated as a test submission.

P – Treat the file submission as a production submission. The file will be processed and a report generated. If the data passes processing, it will be stored in the database. When applied to a ZIP file, all XML files within that ZIP file will be treated as a production submission.

**File Name:** The name of an XML or ZIP file that is part of the submission. The name must follow the established format.

Number of XML Files: If the submission file is an XML file, this number should be 1. If the submission file is a ZIP file, this number should be the count of XML files contained within the ZIP file.

Example:

P1024,T,PSE-1024-20120220-001-File1.XML,1  
P1024,P,PSE-1024-20120220-001-File2.ZIP,6

The example shows a manifest file with a test submission for a single XML file and a production submission of a ZIP file that contains six (6) XML files.

### *Manifest File Names*

Manifest files will always be named after the 24 character batch ID.

The format of the file name for manifest file is as follows:

For CDA XML Patient Safety Data Submissions:

Hospital Common Formats:

PSE-<OrgID>-<YYYYMMDD>-<XXX>.csv

Community Pharmacy Common Formats:

PSECP-<OrgID>-<YYYYMMDD>-<XXX>.csv

Nursing Home Common Formats:

PSNH-<OrgID>-<YYYYMMDD>-<XXX>.csv

Diagnostic Safety Common Formats:

PSEDS-<OrgID>-<YYYYMMDD>-<XXX>.csv

Example:

PSE-P1024-20120220-001.csv

### *Manifest File Size*

A single manifest file may not exceed 80 megabytes.



Avoid confusion regarding which organization ID to use. The name of the manifest file should always contain the organization ID of the submitter. The rows of the manifest file should always contain the organization ID of the PSO associated with the file. If the submitter is a PSO, these should be the same. If the submitter is a PSO Vendor, file names should contain the Vendor's organization ID and the manifest file should contain the PSO's organization ID.

## Alternate Data Submission Format

### SFTP Submission Batch

When submitting Patient Safety Data in the Alternate Data Submission specified file formats, a SFTP submission batch consists of one (1) ZIP file that will contain one (1) of the following file formats:

- Simple XML
- DSV (Delimiter-separated values)

A SFTP submission batch can only contain Patient Safety Data in simple XML or DSV file format.

A SFTP submission batch may only contain simple XML or DSV formatted files. A SFTP submission batch may not mix the two file formats.

A SFTP submission batch must contain either all Test or all Production submissions. Test and Production submissions cannot be mixed together within the batch.

A SFTP submission batch must identify the AHRQ Common Format setting and version, for example, Community Pharmacy Version 1.0.

If a PSO Vendor is submitting for multiple PSOs, the Vendor must submit a separate batch for each PSO.

### Simple XML and DSV

#### *Simple XML and DSV Contents*

The contents of the simple XML or DSV file must correspond to the following AHRQ Common Formats:

- Common Formats – Hospital Version 2.0
- Common Formats – Hospital Version 1.2
- Common Formats – Community Pharmacy Version 1.0
- Common Formats – Nursing Home Version 1.0
- Common Formats – Diagnostic Safety Version 1.0

Please refer to the following guides for further information on file naming convention, and how to develop and implement the simple XML or DSV file formats:

- [Hospital Version 2.0 Alternate Data Submission Users' Guide](#)
- [Hospital Version 1.2 Alternate Data Submission Users' Guide](#)
- [Community Pharmacy Version 1.0 Alternate Data Submission Users' Guide](#)
- [Nursing Home Version 1.0 Alternate Data Submission Users' Guide](#)
- [Diagnostic Safety Version 1.0 Alternate Data Submission Users' Guide](#)

## Chapter 4 Submitting Files

### SFTP Client

A SFTP client capable of FTP over SSH (not FTP over SSL) is required to connect to the PSOPPC SFTP system. PSOPPC does not endorse any particular client. The following list is provided as a reference of readily available SFTP clients. PSOs and PSO Vendors will need to make an independent assessment of which SFTP client will meet its needs.

- FileZilla client -- <http://filezilla-project.org/>
- WinSCP -- <http://winscp.net/eng/index.php>
- PuTTY, PSFTP - <http://www.chiark.greenend.org.uk/~sgtatham/putty/>
- OpenSSH -- <http://www.openssh.com/>

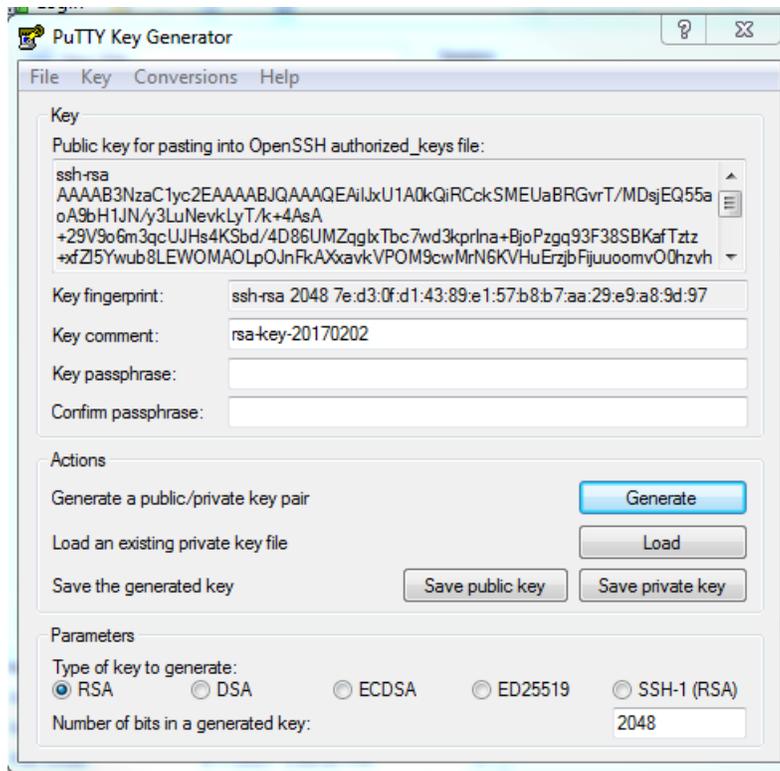
### Automation of Submissions

Due to the variety of systems supported by PSOs and PSO Vendors, the specifics for automating submissions are outside the scope of the PSOPPC. Each PSO or PSO Vendor will need to determine which automation mechanism will best suit its needs. The PSOPPC has implemented a standard SFTP interface that should support a variety of automation mechanisms, as well as allow for manual upload of submissions.

### Public Key Authentication (PKA) Setup

The following setup steps are using PuTTY with the WinSCP client on the Windows operating system. If using the WinSCP client, PuTTYgen (key generation utility) is already available within the client.

1. Open the PuTTY Key Generator (On the “Login” window, select “Tools”, and then select “Run PuTTYgen”).
2. For key parameters, select SSH-2 RSA or SSH-2 DSA and a value of 2048. (Under “Parameters” select RSA or DSA, and then set the value in the “Number of bits in a generated key” field to 2048.)
3. Generate the public/private key pair. (Under “Actions”, select “Generate” and then, when prompted, use your mouse (or trackpad) to move your cursor around the blank area located under “Key” (this generates randomness used to create your key pair)).

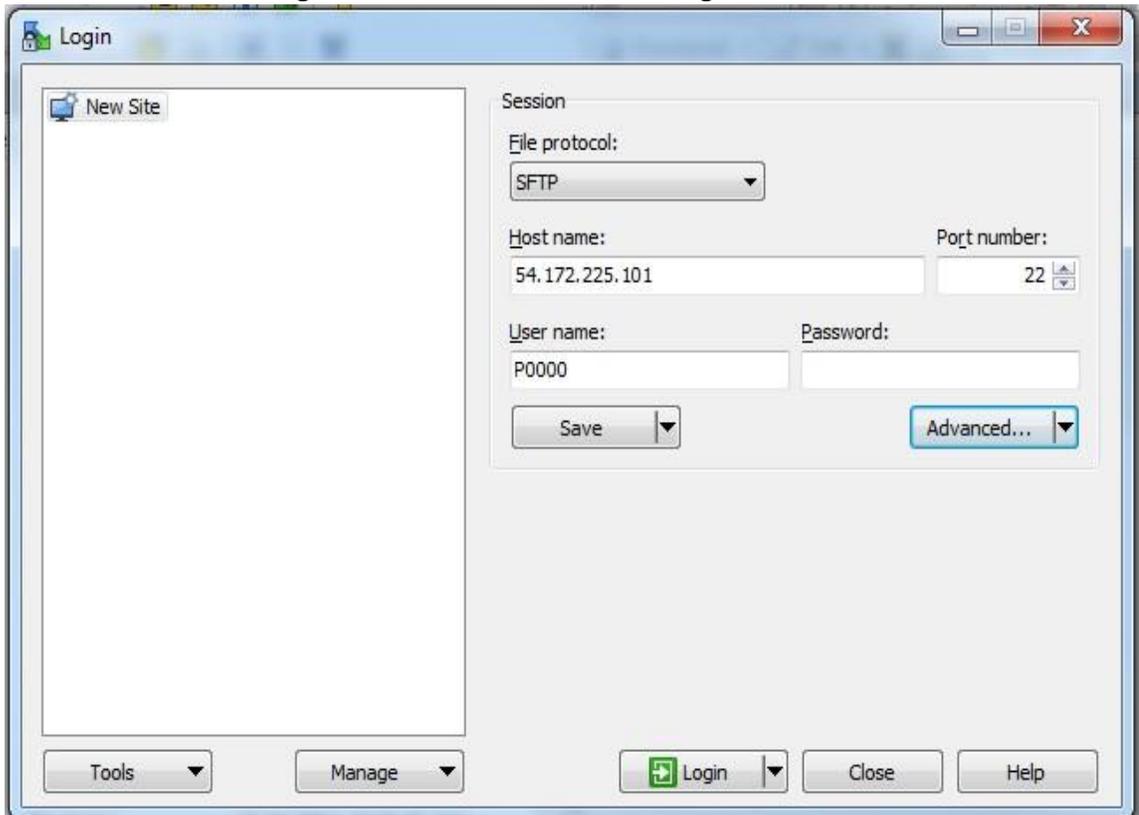


4. Choose a key passphrase to passphrase protect the private key (enter in the “Key passphrase” and “Confirm passphrase” text boxes).
5. Create a folder on the machine to save the public and private keys.
6. Save the public key to the machine using a name that is associated with your PSOPPC SFTP account (i.e., PSOPPC\_OrgName\_PublicKey). Under “Actions”, next to “Save the generated key”, select “Save public key”. Name the file, select a location on your machine, and select “Save”.)
7. Save the private key to the machine using a name that is associated with your SFTP account. (Under “Actions”, next to “Save the generated key”, select “Save private key”. Keep the “Save as type” set to PuTTY Private Key Files (\*.ppk) when saving to the machine.
8. Send the public key to the PSOPPC Help Desk at [support@psoppc.org](mailto:support@psoppc.org).
9. The PSOPPC Help Desk will send a notification when the PKA is setup for your account. (Once setup is complete, the file upload process can begin using the SFTP client).

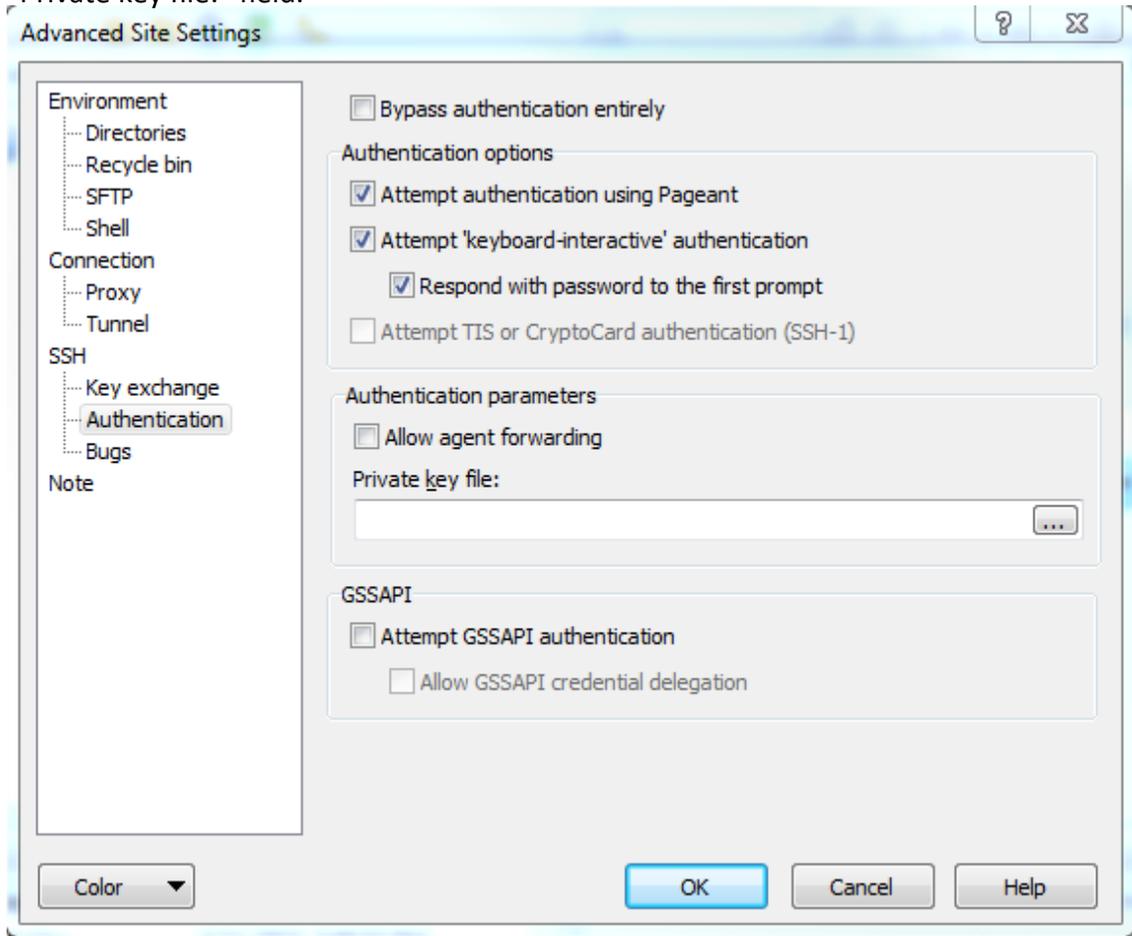
## File Upload Process

The following illustrates manually uploading a file using the WinSCP tool under the Windows operating system.

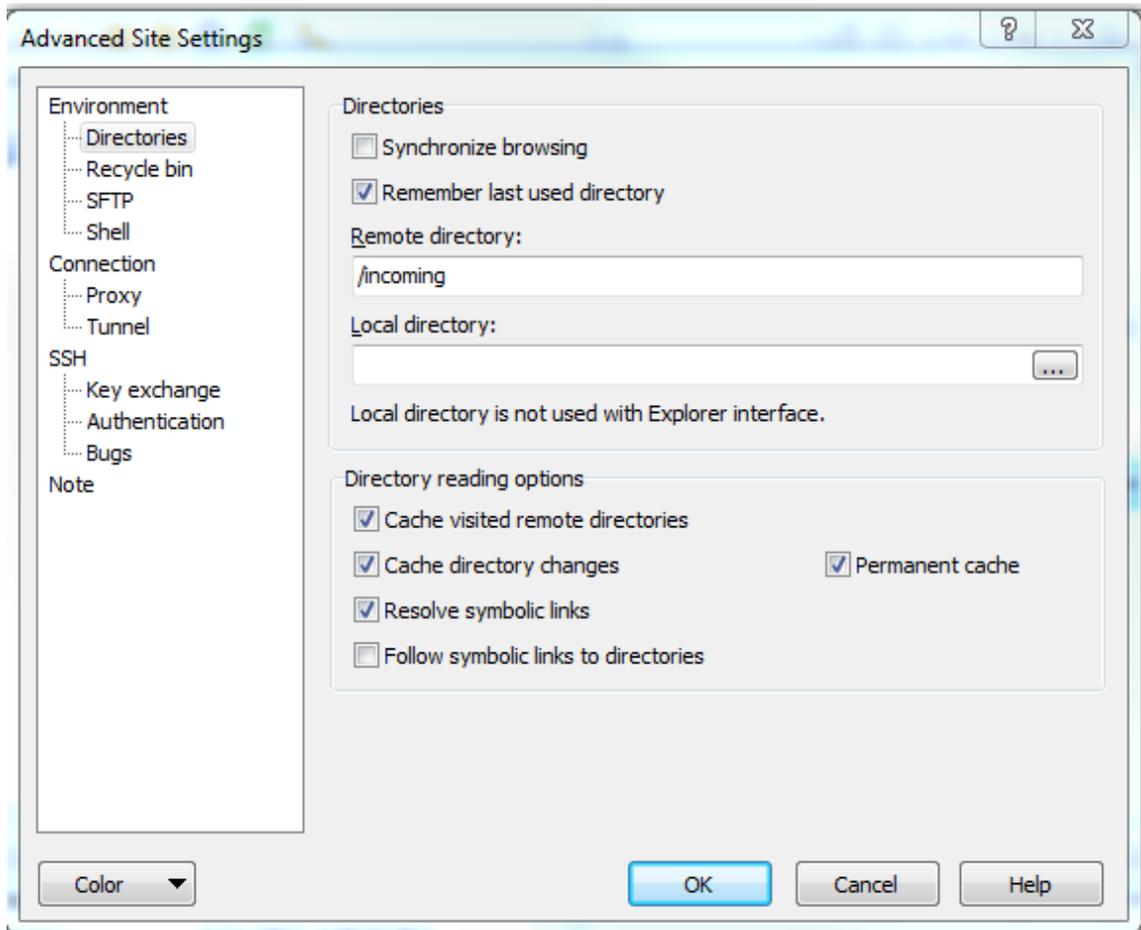
1. Start WinSCP and use SFTP as File protocol, "54.172.225.101" as the Host name, 22 as the Port number and your PSO ID or Vendor ID as the User name. Then, select the "Advanced" button to go to the "Advanced Site Settings" window:



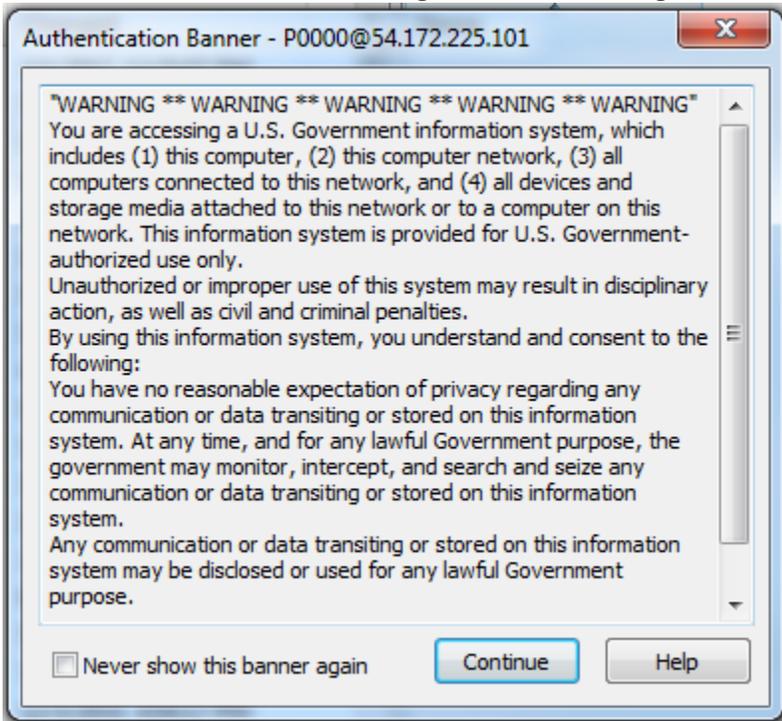
2. In the “Advanced Site Settings” window select “Authentication” in the left navigation menu under “SSH”. Under “Authentication Parameters” apply your private key file in the “Private key file:” field.



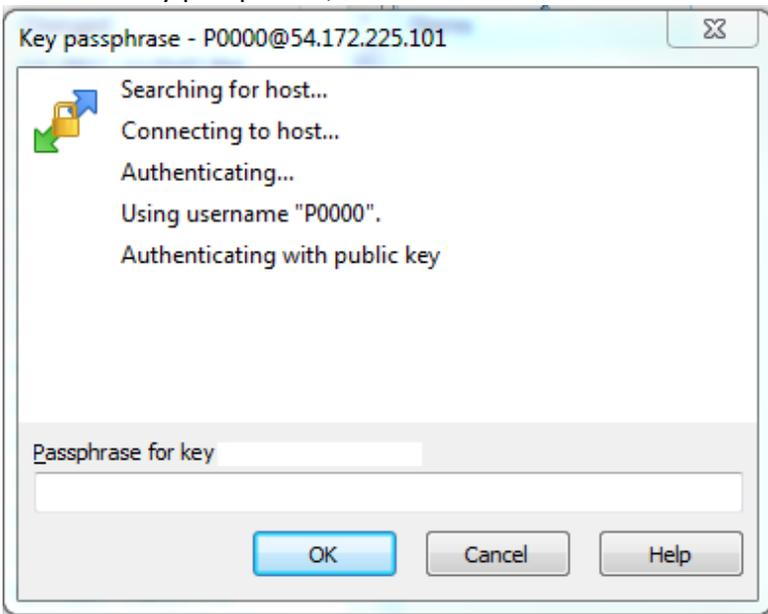
3. Now, select “Directories” under “Environment” in the left navigation menu. In the “Remote directory” field please specify the username/incoming (e.g. /incoming). Then select “OK” and then “Save.”



4. Click the "Continue" button to agree to the warning banner:



5. Enter the key passphrase, then select the "OK" button:



## 6. Upload the file(s) to the “incoming” folder.

The screenshot displays the WinSCP interface with two panes. The left pane shows the local file system at 'C:\Users\xiaoxin.hu\Documents'. The right pane shows the remote file system at '/incoming'. The status bar at the bottom indicates the local side has 0 B of 6,955 KiB in 0 of 18, and the remote side has 0 B of 130 KiB in 0 of 13.

Name	Ext	Size	Type	Changed
..			Parent directory	7/17/2014 4:20:33 PM
Custom Office Templa...			File folder	4/17/2014 4:34:29 PM
My Cert Key			File folder	5/19/2014 12:09:59 PM
My Music			File folder	4/16/2014 2:26:39 PM
My PaperPort Docume...			File folder	7/1/2014 6:20:31 PM
My Pictures			File folder	4/16/2014 2:26:39 PM
My Received Files			File folder	6/12/2014 3:38:37 PM
My Shapes			File folder	4/18/2014 8:09:08 AM
My Videos			File folder	4/16/2014 2:26:39 PM
Optimizer Pro			File folder	6/3/2014 4:45:26 PM
Outlook Files			File folder	5/7/2014 12:19:10 PM
sftp-1.0			File folder	5/31/2014 4:45:21 PM
application.properties		2,962 B	PROPERTIES File	5/31/2014 4:27:39 PM
Default.rdp		2,200 B	Remote Desktop C...	8/19/2014 9:37:04 AM
desktop.ini		402 B	Configuration setti...	5/17/2014 10:29:59 AM
Nuance Image Printer ...		0 B	File	7/8/2014 12:07:48 PM
PSOstats.sql		3,350 B	SQL File	5/20/2014 11:27:37 AM
sftp-1.0.jar		6,947 KiB	JAR File	5/31/2014 2:16:04 PM
velocity.log		0 B	LOG File	5/31/2014 4:50:58 PM

Name	Ext	Size	Changed	Right
..			8/18/2014 1:46:39 PM	rw-r-
PSE-P0000-20140812-001.csv.completed		39 B	8/18/2014 6:23:14 PM	rw-r-
PSE-P0000-20140812-001-.zip.completed		14,002 B	8/18/2014 6:22:46 PM	rw-r-
PSE-P0000-20140815-005.csv.completed		78 B	8/18/2014 6:10:56 PM	rw-r-
PSE-P0000-20140814-004.csv.completed		39 B	8/18/2014 6:04:18 PM	rw-r-
PSE-P0000-20140816-002.csv.completed		39 B	8/18/2014 6:00:47 PM	rw-r-
PSE-P0000-20140817-007.csv.completed		39 B	8/18/2014 5:57:14 PM	rw-r-
FTP-PSE-P0000-20140602-000-.xml.completed		19,746 B	8/18/2014 12:53:06 PM	rw-r-
PSE-P0000-20140818-001.csv.completed		37 B	8/18/2014 12:22:42 PM	rw-r-
PSE-P0000-20140818-001-.xml.completed		19,747 B	8/18/2014 12:19:00 PM	rw-r-
PSE-P0000-20140817-007-.xml.completed		19,747 B	8/18/2014 12:19:00 PM	rw-r-
PSE-P0000-20140816-002-.xml.completed		19,747 B	8/18/2014 12:19:00 PM	rw-r-
PSE-P0000-20140815-005-.xml.completed		19,747 B	8/18/2014 12:19:00 PM	rw-r-
PSE-P0000-20140814-004-.xml.completed		19,747 B	8/18/2014 12:19:00 PM	rw-r-

## Chapter 5 Account Management

### Technical Support

Any questions or issues regarding the SFTP account should be coordinated through the PSOPPC Help Desk, who can be reached at (866) 571-7712 or [support@psoppc.org](mailto:support@psoppc.org).

Common issues that can be resolved through the PSOPPC Help Desk:

- SFTP account setup
- Public Key Authentication (PKA) setup
- Account termination

### Account Termination

The SFTP account is setup for AHRQ listed PSO organizations and active Vendor organizations; upon PSO delisting or Vendor deactivation, the account will be terminated.