Joint Venture Hospital Laboratories

Secure File Transfer Protocol (SFTP) Secure Socket Shell (SSH) User's Guide for plmweb.jvhl.org

For Secure File Transfers via the Internet

Version 2.3
March 2018

Introduction

JVHL now provides secure file transfers over the Internet using SFTP/SSH version 2. This service is offered for those facilities that wish to utilize a scripted file transfer protocol. The SFTP/SSH service supports many commercially available clients and freeware clients. The site is part of a secure network connected to the backbone of the Internet, lending itself to a high level of availability and a sufficient amount of bandwidth for multiple file transfers at any given time.

Provided Services

JVHL will provide the following services via the SFTP/SSH site:

Submit encounter/claims data

Retrieve front-end processing reports (Approved Lines Report, Rejected Lines Report)

Retrieve payer remittance reports

Submit HEDIS result data

Retrieve HEDIS requests

A registration form will be sent and completed by the account requesting any of the above services. It will indicate which services are to be provided for that account. Any account requesting both HEDIS and claims servicing, will receive two unique account logons to avoid confusion and limit the possibility of error Claims data is processed every business day. Claim reports are available for retrieval every Friday.

Account Procurement

JVHL members interested in obtaining an account will need to complete the registration form and return it to the proper approval authority indicated on the form. An additional requirement is for a copy of the Business Associate Agreement to be on file with JVHL to ensure compliance with current HIPAA Privacy and Security standards. If a JVHL member wishes to use a test account in order to evaluate the site, please call one of the contacts listed at the end of this document.

HIPAA

Great emphasis is placed on providing a system that is not only usable, but also is compliant with HIPAA Security and Privacy standards. Accounts are not established until authorized individuals sign the proper Business Associates Agreement and JVHLWeb Authorization Request Form and return it to the appropriate JVHL contact. All traffic in and out of the SFTP/SSH site is encrypted.

JVHL member authentication is verified through a unique ID and password, along with the member's public SSH key. The public SSH key will need to be generated by the JVHL member and sent prior to account creation. In order for a successful login to take place, the JVHL member will need the username, password, and the SSH key pair (of which the public key sent is part of). JVHL members cannot see other members' files, either in the upload or download directories. If any JVHL member believes their password or public key has been compromised, they should contact JVHL immediately so new credentials can be generated.

File Naming Convention

A file naming convention is not necessary with the SFTP/SSH site. All files are automatically renamed upon receipt. All files being sent or received are logged. Those being received are logged with the original name and the name generated upon receipt for tracking purposes. JVHL does request that files not be zipped before being sent. Certain file extensions will not be accepted. Attempts to send files with these extensions will result in upload failures. Examples are: *.exe, *.msi, *.bat, *.mp3, etc. If you are sending a file that is being denied, then the extension is probably not accepted. Please contact JVHL for verification of the extension you are using.

File Back up

It is recommended to make a copy of transferred file(s) immediately upon receipt for back up purposes at your site.

It is the responsibility of the "owner" of a file to retain back up files for a reasonable length of time, until the destination party has the file verified and backed up at their site. In the event the destination party does not receive the file in its entirety, or the file is destroyed prior to complete back up, the file may be requested for transfer again.

For example: JVHL will retain back up on files going from JVHL to outside users. The outside users will retain back up on files coming into JVHL.

Hardware/Software Requirements

In order to successfully complete a SSH connection, the JVHL member will need to have a computer with a SSH client that supports the following:

SFTP/SSH version 2 (version 1 is not acceptable)
A valid username and password (assigned by JVHL)
A valid SSH key pair (generated by the JVHL member using the client or other)

Below is a list of clients tested by JVHL:

CuteFTP Professional	www.globalscape.com
WS_FTP Professional 2006	www.ipswitch.com
Putty (pscp or psftp using puttygen to create SSH keys)	www.openssh.com/windows.html

These clients were tested because of their popularity and ease of use. Putty is the only freeware option tested and some guidance will be given below. The commercial clients have good documentation in the help files for creating a session, generating keys, and exporting keys. Search for SSH or SFTP in the help files. Many, many clients are available and can certainly work as long as they satisfy above criteria. Some clients provide for the ability to encrypt just the authentication, just the data transfers, or both. PLEASE ensure all traffic is encrypted (commercial clients generally do this by default).

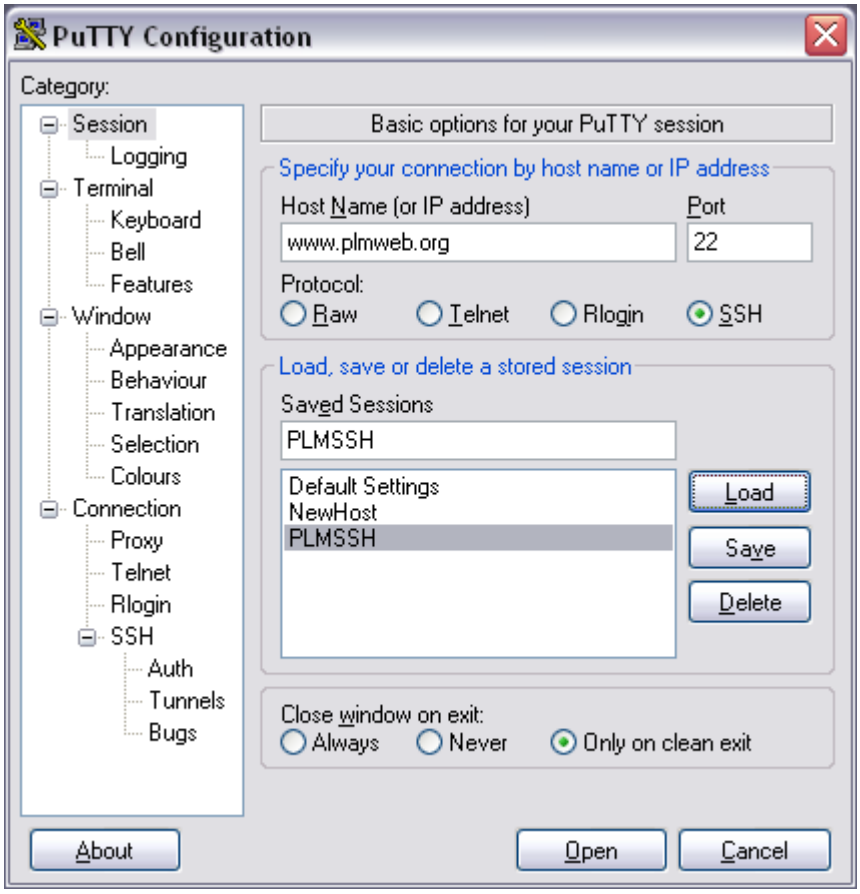
Putty:

Download the following:

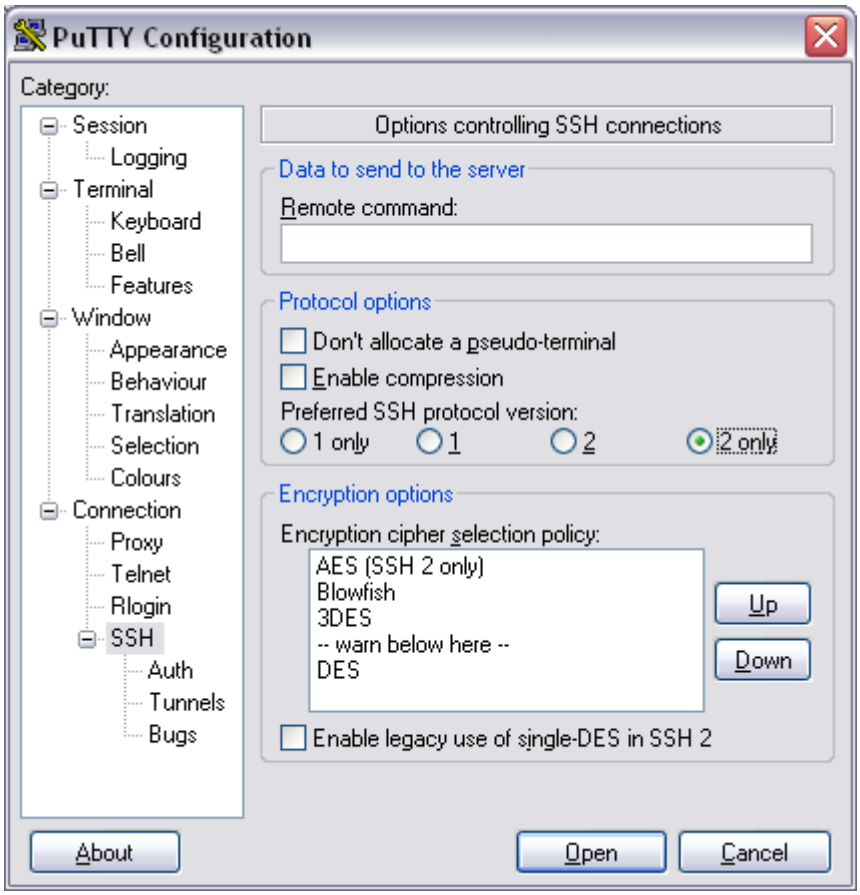
pscp.exe
psftp.exe
puttygen.exe
putty.exe

Puttygen.exe is used to create a SSH key pair. Execute the application and select SSH2 DSA with a 1024 bit key , then select "Generate" to create a key. Move your mouse as instructed during the generation. Enter a "passphrase" for the key and then save the public and private key (make sure the private key and "passphrase" are kept in a safe place). Send the public key to JVHL.

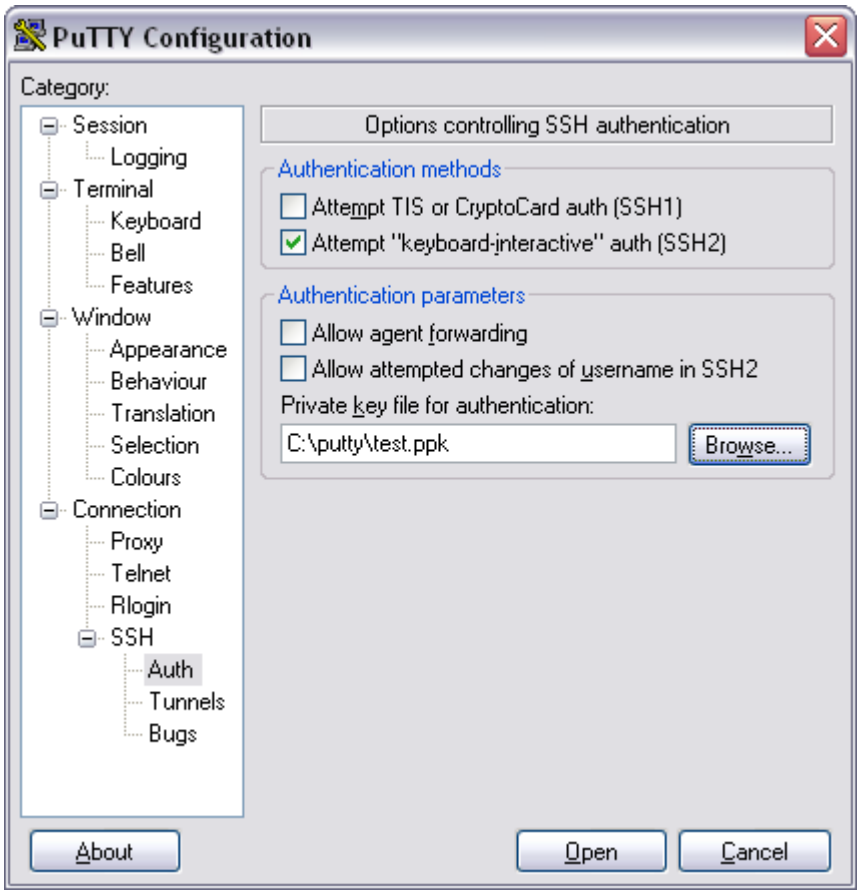
Putty.exe can be used to add connections. Below I have added the session PLMSSH.



Now set the SSH settings.



Now select the key you generated (test.ppk is the key file I created and saved).



Close the putty.exe application. Use the pscp.exe or psftp.exe applications to make the SSH connection and transfer files. Psftp.exe is more interactive and can be executed by double clicking on it. Type "open plmssh" to make a connection (plmssh comes from the entry created in putty.exe, this could be any name you chose to enter). Pscp.exe is a command line tool. This has to be executed from a command prompt (like MS-DOS). You can use the following to send and receive files:

The first command uploads a single file and the second uploads multiple files to the SSH site. The third command downloads files from the SSH site. The *fileextension* could be a ".txt" or ".zip" for instance and the *username* is the username given by JVHL for the account. PLMSSH is the name I gave to the connection created using putty.exe.

Pscp –v *filename* *username*@plmssh:
Pscp –v *.*fileextension* *username*@plmssh:
Pscp –v *username*@plmssh: /download/*.* .

Contacts and Areas of Specialty

IT Director

Rob Ramey
support@jvhl.org
(248) 594-0998 x202

Change Summary

This section describes the differences between the current guide and previous guide(s).

Date	Version	Description
11/5/2015	2.0	Reformatted the companion guide and also updated contact information
2/9/2016	2.1	Updated contact information
4/20/2017	2.2	Updated logo
3/26/2018	2.3	Updated logo

Review History
7/14/2011 - RRAMEY