

NJ Department of Health

Secure File Transfer with Public Key Authentication

Revised July 2014

Overview

The New Jersey Department of Health maintains an Internet-accessible SFTP/SSH2 server for secure drop off and pickup of data files. Upon authentication with a public key which you provide in advance, your SFTP client connects to a private directory. Both manual and automated transfers are supported. The retriever should delete the files after a successful download.

Technical Requirements

We use SFTP (SSH File Transfer Protocol), **not** FTPS (FTP over SSL/TLS). For us to create your account, you must generate a public/private SSH keypair, using `ssh-keygen` or similar on Linux, or PuTTYgen, Bitvise SSH Client, Core FTP LE, etc. on Windows (see example how-to below). You will email us the **public** key, and our server will use it to confirm your identity each time you connect. Your computers, whether test or production, must all use the same matching **private** key for authentication. Your SFTP/SSH client software must support

- SSH2 keypair, with RSA or DSA/DSS algorithm (**not** SSL cert or PGP key),
- Export of public key in SSH2 or OpenSSH format, and
- AES (Advanced Encryption Standard) encryption.

Testing Your Network Connection

Your network must permit an outbound connection on TCP port 7700 to **dohsftp.nj.gov** from the machine(s) you will use for file transfer. You will be unable to “ping” our server. Instead, enter **telnet dohsftp.nj.gov 7700** at a command or shell prompt. A text window should open starting with "SSH-2.0..." If it does not, please notify your network support staff. **Note:** In Windows 7, you must first click Start, search for “Turn Windows features on or off” and turn on “Telnet Client.” Windows Vista also requires enabling the telnet program before this test.

Planning Your Transfer Process

We recommend that your process, manual or automated, follow steps similar to the following:

1. Accumulate a batch of data (one large or many small files)
2. Open just one SFTP session to the dohsftp.nj.gov server
3. Upload the file(s) to the appropriate folder (if uploading)
4. Download and delete any files you are receiving (if downloading)
5. Log out from the server, closing the SFTP connection
6. Wait (typically **at least** an hour or two) and repeat these steps

Note: script examples are available upon request as a starting point for automation.

Testing SFTP Login and Client Software

In your SFTP client software, enter **dohsftp.nj.gov** for host or server, **7700** for port, and (for connection test only) **trysftp** as both username and password. Verify that our server key (also known as “host key”) fingerprint begins with **65:0b:ca** and ends with **18:74:2f**. Consult your IT

support if needed to obtain and install a compatible SFTP client. A few cost-free examples are listed below; many other clients are available.

1. **Bitvise SSH Client** on Windows, free for up to four computers per organizational unit. SFTP/SSH only. GUI with integrated key management. Includes scriptable command line client and detailed help text. <http://www.bitvise.com/ssh-client-download>
2. **WinSCP** on Windows. Supports GUI-based key management via included tools from PuTTY, partially integrated. Can store config in text file. .NET/COM interface and script samples available. Free (donation optional). <http://winscp.net/eng/docs/introduction>
3. **Core FTP LE** on Windows. Multi-protocol, GUI and command line, includes key management. LE version is free at <http://www.coreftp.com/download.html>
4. **PuTTY** on Windows, separate programs for key generation, key-based authorization and SFTP, freeware at <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
5. **OpenSSH** on Unix/Linux, BSD-licensed freeware at <http://www.openssh.com>

How to Get Your Production Account

First, use your SSH/SFTP software to generate an SSH2 public key (2048-bit RSA preferred). As an example, here are steps for key generation using Bitvise SSH Client for Windows:

1. Download Bitvise SSH Client from <http://www.bitvise.com/ssh-client-download> and install on your computer. (The SSH Client is licensed free for up to four machines per organizational unit.)
2. Start the program. On the Login page click "User keypair manager." Then click "Generate New..." Leave the settings as they are, and click "Generate."
3. Once it's done—a few seconds—click anywhere on the line of new key data to highlight it. Then click "Export..." Leave the settings as they are, and click "Export" again. Name the file **YourOrganizationName.pubkey** (Replace "YourOrganizationName" with the actual name of your organization.)

Next, email the public key file to **data.connect@doh.state.nj.us** We will load it into our SFTP server and email you the new account credentials. The account will then be ready for your testing.

For issues with accounts, keys, transfer scripting, and connectivity, email:

data.connect@doh.state.nj.us or scott.weed@doh.state.nj.us

For other issues, including file content, data format and transfer schedules, please contact the staff of the NJ DOH program area that works with your data. For the Department's Electronic Laboratory Reporting (ELR) program, the contact email is NJELR.ADMIN@doh.state.nj.us

Cancer related diagnoses are handled separately from other reporting to NJDOH. For Cancer related Data Exchange and Laboratory (ePath) please contact NJSCRDAT@doh.state.nj.us , for Cancer Clinical Document Architecture (CCDA) Meaningful Use Stage 2 (MU2) please contact NJSCR.MU2@doh.state.nj.us