



**National Student Clearinghouse®**  
2300 Dulles Station Boulevard, Suite 300  
Herndon, Virginia 20171

703-742-4200  
[www.studentclearinghouse.org](http://www.studentclearinghouse.org)

© 2009 National Student Clearinghouse. All rights reserved.

---

## Secure FTP Automation

The National Student Clearinghouse supports Secure FTP in automated environments to safely and securely collect, store, manage, and distribute sensitive information between your organization and the Clearinghouse. Key features of this system are:

- Web browser interface - users can view logs of file and user activity and change passwords (as well as manually send and receive files).
- All files received by the Clearinghouse are securely stored using FIPS 140-2 validated AES encryption, the U.S. Federal encryption standard.
- Eliminates the need for encryption.

For automated environments, no cost/low cost Secure FTP clients can exchange files via encrypted FTP over SSH (SFTP) and FTP over SSL (FTPS) connections.

### **FTP over SSH (SFTP)**

- SFTP clients are typically found on UNIX/Linux systems and IBM OS/390 mainframes
- The Clearinghouse Secure FTP system works with a variety of third-party clients
  - Tested with OpenSSH, F-Secure, and SSH Communications SFTP clients on UNIX
  - Tested with F-Secure, PSFTP, and WinSCP SFTP clients on Windows
- Free client programs are available at <http://www.openssh.org>.

### **FTP over SSL (FTPS)**

- FTPS clients are commonly used on Windows systems and are native to IBM z/OS mainframes.
- The Clearinghouse Secure FTP system works with a variety of third-party FTP over SSL (Secure Sockets Layer) clients.
- The Clearinghouse recommends Implicit mode FTPS, which prevents malformed scripts from sending login credentials over the Internet in the clear. Passive mode transfers are required.
- A free Windows client (MOVEit Freely) is available at <http://www.stdnet.com>.

## Secure FTP Automation (cont'd)

### Example – FTP over SSH (SFTP)

SSH clients use TCP Port-22 to establish the connection with the server. Make sure that your firewall is configured to allow outbound traffic on Port-22 to [ftps.nslc.org](https://ftps.nslc.org).

Contact the Clearinghouse to obtain a userid and password for the Secure FTP system. Although SSH uses a public key signature in lieu of a password, you can still use your password to access the Secure FTP system interactively via a Web browser or a command line program.

The following example uses the SSH Tectia Client obtained from [www.ssh.com](http://www.ssh.com). The Tectia Client has a file transfer program named SFTP2, based on the SSH2 standard. The following steps are typical of those running on a Unix platform:

1. Enter the command: `sftp2 userid@ftps.nslc.org`

If this is the first time your host establishes a connection with [ftps.nslc.org](https://ftps.nslc.org), it will prompt you to create a host key file for [ftps.nslc.org](https://ftps.nslc.org). Create the key file. If you would like to confirm the key's signature, please contact the Clearinghouse.

2. If you do not already have a public/private keypair for SSH, create one using the command: `ssh-keygen2`.
3. Provide the Clearinghouse with your public key fingerprint. The Clearinghouse will add that to your user account on the Secure FTP system.
4. Create a batch file of FTP commands such as the following (`batch.file`):

```
open userid@ftps.nslc.org
put test.file
close
```

Note: you may send a test file, but please indicate in the contents and the name that it is a test file.

5. You can run the batch file with the following command: `sftp2 -B batch.file`.
6. For automated transfers, you can schedule this command to run at a particular time.

## Secure FTP Automation (cont'd)

### Example – FTP over SSL (FTPS)

FTP connections are established from the client to the server via **Explicit** or **Implicit control channels**. Explicit FTPS control connections take place on TCP port 21. Implicit FTPS control connections take place on TCP port 990.

Once the control channel is established, the client and server negotiate a port for either **PASSIVE** or **ACTIVE MODE** data transfers. ACTIVE mode transfers take place on TCP port 20. PASSIVE mode transfers take place on a TCP port in the range 3000 – 3010. “Regular” ftp typically uses ACTIVE mode, however, for SSL connections the Clearinghouse strongly recommends using PASSIVE MODE FTP transfers due to firewalls not being able to correctly route FTP traffic that has been encrypted via SSL.

Make sure that your firewall is configured with the following:

- Allow TCP Port-990 to ftps.nslc.org (control channel)
- Allow TCP Port range 3000-3010 to ftps.nslc.org (data channel)

Contact the Clearinghouse to obtain a userid and password for the Secure FTP system.

The following example uses a Windows command line program called MOVEit Freely, by Standards Networks ([www.stdnet.com](http://www.stdnet.com)). The program is named ftps.exe.

1. Open a Windows command window and change directory to the folder where ftps.exe is installed.
2. The ftps program can be run interactively from the command line or it can read commands from a file. The ftps command syntax is very similar to “regular” ftp. For the complete syntax, see the MOVEit Freely documentation or enter ftps /? from the command line.
3. For automated file transfers, create a batch file of FTP commands such as the following (batch.file):

```
userid  
password  
put test.file  
quit
```

Note: you may send a test file, but please indicate in the contents and the name that it is a test file.

## Secure FTP Automation (cont'd)

4. You can run the batch file with the following command:

```
ftps -a -e:implicit -s:batch.file ftps.nslc.org
```

The parameters are:

- a indicates Passive Mode transfers.
  - e:implicit indicates that both control and data channels are encrypted.
  - s:batch.file indicates that commands are to be read from a file.
5. For automated transfers, you can schedule this command to run at a particular time.

If you have questions or need additional information regarding Secure FTP, please contact Clearinghouse Customer Service at **703-742-4200** or email **[secureftp@nslc.org](mailto:secureftp@nslc.org)**.