Setting up an SFTP Connection

Thank you for choosing to team up with Shipt.

Security is of utmost importance to us, especially when it comes to sharing files with our valued partners. SFTP is our preferred connection method at Shipt for transmitting catalog feeds.

Setting things up usually takes around 1 hour, but don't worry – your Partner Success Manager will be right there with you, ready to lend a hand if anything comes up along the way. We appreciate your trust in us for a secure and successful collaboration. Cheers to a smooth integration!

Required Information to Connect

1. **Username**
   To be shared by Shipt
2. **SSH Key Pair**
   To be generated by you
3. **Shipt Hostname (DNS)**
   sftp.partner.shipt.com
4. **Port**
   22

Process Overview

1. Add Shipt IP address to your firewall allowlist
2. Generate SSH key pair and share public key with Shipt. Upon receipt, Shipt provisions a username
3. Connect and send test product and inventory data files via SFTP for review
4. Set up recurring data feed upon Shipt file spec confirmation

Steps for Getting Set Up

Step 1: Add Shipt's IP address to your allowlist

To prevent potential networking issues, please add Shipt's IP address `35.238.218.241` to your firewall's allowlist. You are not required to share your own IP addresses with Shipt for this SFTP setup and configuration.

Step 2: Generate an SSH key pair

You can generate a new key pair on your local machine in a command prompt such as Terminal. You will then share the public key with your Partner Success manager. Shipt will provide a username for your new account.

Generating a new SSH Key Pair:

1. Open Terminal.
2. Paste the text below, replacing the example company with your company name. This will create a new SSH key using your company name as a label.

```
ssh-keygen -t rsa -b 4096 -C "your_company_name"
```

3. The command will prompt you to "Enter a file path in which to save the key". (Ex: /home/YOU/.ssh/id_rsa) You can hit enter to accept the default location. Please note that if you have created SSH Keys before, ssh-keygen may re-write another key. Shipt recommends updating the file path to end in **/id_shipt** instead of **/id_rsa** to rename the file to **id_shipt**.

```
/home/YOU/.ssh/id_shipt
```

4. The command will prompt you to enter a passphrase. The passphrase is not required and you must hit enter twice if you do not want one.

These steps will generate two keys in the path you chose in step 3. If you used the recommended path, the private key file will be called **id_shipt** and the public key **id_shipt.pub.** You may safely share the public key (.pub file) with Shipt over email as it does not contain sensitive information. At no point should you share the private key outside of your organization as it will be used for authenticating the connection.

Note: Shipt only accepts keys in Open SSH format. This means that public keys start with "**ssh-rsa"** and not "**BEGIN SSH2 PUBLIC KEY".**

If you are using Windows and/or PuTTy, please click this link

Step 3: Test Connection and submit files

Follow the steps outlined in the Shipt documentation to ensure that the data files are set up according to required specification.

To access the Shipt remote host server, you can connect using any client or directly through the command line interface (CLI) if you provide the correct username and private key for connection.

For Linux/Unix operating systems, popular clients include Cyberduck and FileZilla, while WinSCP is commonly utilized by Windows users.

Each user will directly connect to their root directory, meaning the file path for connection will be: `/`

Run the following command if connecting via CLI:

```
sftp -i path/to/private/key/file YOUR-USERNAME@sftp.partner.shipt.com
```

The first time connecting, you will receive a warning about connecting to an unknown server. It will provide a host fingerprint and ask if you want to trust this host. Click yes to accept. When you connect successfully, you should see the **sftp>** prompt. Some useful commands include:

Command	Function
cd	Change the directory on the remote host
ls (or dir)	List the contents of the current directory on the remote host
exit (or quit)	Close the connection to the remote host and exit SFTP
get filename	Copy a file from the remote host to the local computer
help (or ?)	Get help on the use of SFTP commands
put filename	Copy a file from the local computer to the remote host
pwd	Show the present working directory on the remote host
rm	Delete a file on the remote host
lcd	Change the directory on the local computer
lls	List the contents of the current directory on the local computer
lpwd	Show the present working directory on the local computer

Step 4: Create a recurring data feed

After Shipt confirms the receipt of the test files, you may start a recurring feed for catalog data ingestion. Congratulations! A new secure file transfer pipeline is now set up with Shipt via SFTP.

FAQ

What should be my folder path for this remote location?

Users will automatically connect to their respective directories, implying a connection to the root (/). The structure of your folders in the remote location is at your discretion, with full permissions granted for creating, removing, and managing folders.

Why am I being prompted for a password? Do I need one?

No, a password is not necessary as you are using a private key for authentication. It's important to clarify that the *password* for connecting to your SFTP remote directory is different from the *passphrase* used to set up your private key. The *passphrase* is an additional security layer to your key. A *password* is used as an alternative way of authenticating.

This error message may arise from various reasons, including:

- An incorrect path for the provided private key file
- Inadequate permissions for the public key file, hindering system/server validation of ownership (the key file should have read/write permissions)
- Incorrectly specified SFTP username
- Networking issues (doublecheck your firewall)

I am using a client to connect, and despite following all outlined steps, I still encounter a connection error. Is there anything I should double-check?

Confirm that you are using the latest version of your selected client; utilizing an outdated release may not be supported by the SFTP protocol.

I am using WinSCP to connect and I have an OpenSSH key. It says a PPK format is required, how do I change the key format?

Follow the instructions outlined here.