Welcome to Segra's FTP Feed Service Setup Guide. This guide should be followed to ensure your connection to the FTP servers is setup securely.

The table and sections below show the information needed to connect successfully to the Segra FTP Host.

FTP Information Table

	FTP Information
FTP Host	ftp.invoice.segra.com
FTP Port	22
Protocol	SFTP
Authentication Method	SSH Key
File Retention Period	12 Months

FILE RETENTION PERIOD

Please be aware ftp.invoice.segra.com will have a file retention policy that will remove files monthly that are older than 12 months. This policy will help maintain the server's performance and availability for delivering files to our customers. If you wish to keep a longer history, please save files older than 12 months to a location of your choice outside of the FTP site.

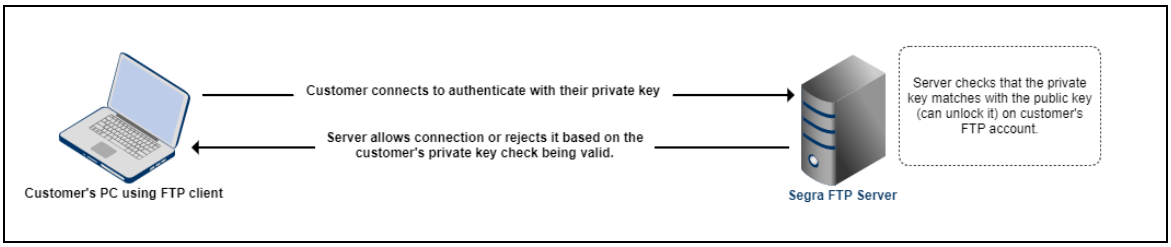
SSH KEY AUTHENTIFICATION

What is SSH Key Authentication?

SSH key authentication is when a key pair is used for authentication instead of using a password. The SSH key pair consists of the two key files below.

- Public Key - Think of this file as a lock for your FTP account. It will be copied to the FTP server and configured as the lock on your FTP account.
- Private Key - Think of this file as the key for the lock. It will be used by your connection to identify you and unlock your FTP account (login) so you can access your files.

You will set your private key in your SSH/FTP client connection used to access to your FTP account. The below diagram gives a simplistic view of how this process works.



Why is Segra using SSH Key Authentication?

SSH Key Authentication is more secure than using passwords. Password authentication has many issues from the password being weak, being cracked with brute force attacks or simply someone guessing it. The list of issues using passwords can go on. When using SSH keys, the only way someone would be able to authenticate to your FTP account is if they have a copy of your private key file. It's in the best interest for Segra and you (the customer) to use SSH key authentication to protect the server and its files from unauthorized access.

How to use SSH Key Authentication

The SSH keys pair files must be created by you. The reason for this is to so you as the customer are the only one who has the key to unlock your account. No one at Segra should ever have your private key.

Need-to-Know

- Never share your private key with anyone who should not have it.
- Never email your private key even if it is someone who needs it.
- Keep your private key in a safe location that is backed up and is not accessible by anyone not authorized to have it.
- Segra personal will NEVER ask you for your private key. If they do, tell them no and report it to Segra.
- If you believe someone unauthorized may have got access to your private key, contact Segra support as soon as possible to set up a new key.

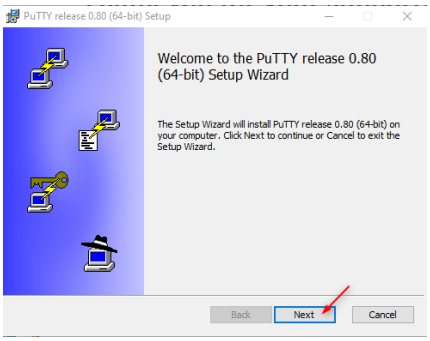
CREATE PUBLIC AND PRIVATE SSH KEYS

You can create SSH keys using several methods and tools. In this guide we will use a tool called Putty that can be downloaded for Windows using this link: https://www.puttygen.com/download-putty#PuTTY_for_windows. You can download the 32bit version if you're not sure if you have a 64bit PC.

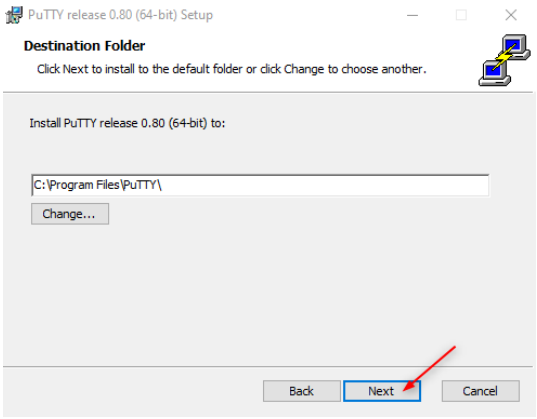
Install PuTTYgen Application (After Downloading)

Step 1
Double click on the Putty installer msi file you downloaded from their site.

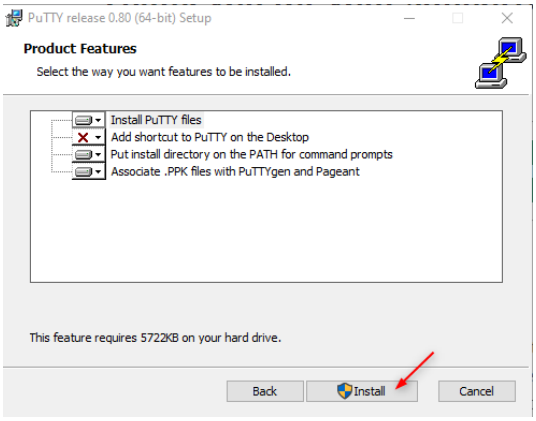
Step 2
Click "Next" on the Setup window.



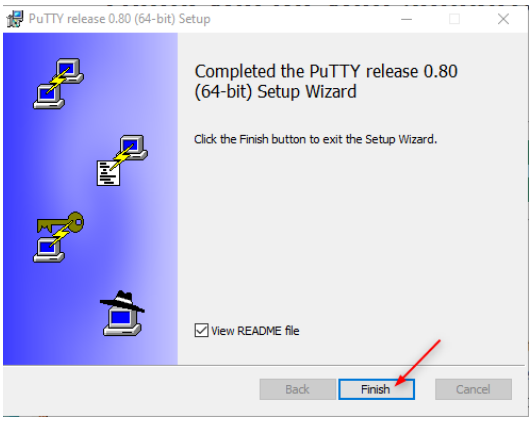
Step 3
Click "Next" on the Destination Folder window.



Step 4
Click "Install" on the Product Features window.

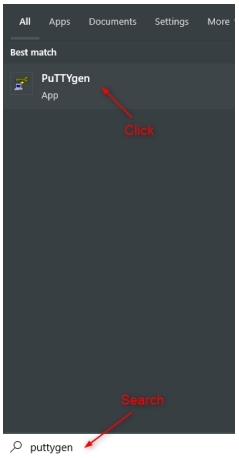


Step 5
Click "Finished" on the completed install window.

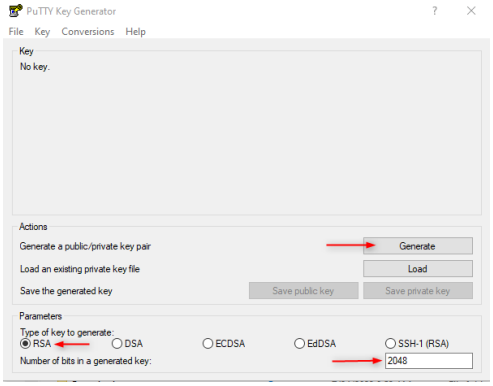


Generate Keys using PuTTYgen

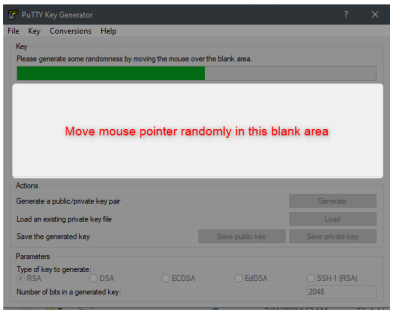
Step 1
Click on the Windows start button on your desktop taskbar and search for "PuTTYgen".



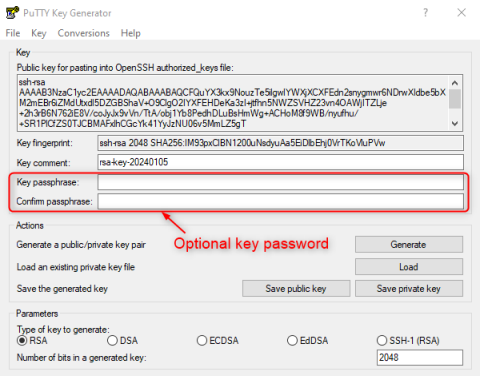
Step 2
Make sure the "RSA" parameter is selected and the "Number of bits generated for the key" value is 2048. Next, you can click on the "Generate" button to start the key creation.



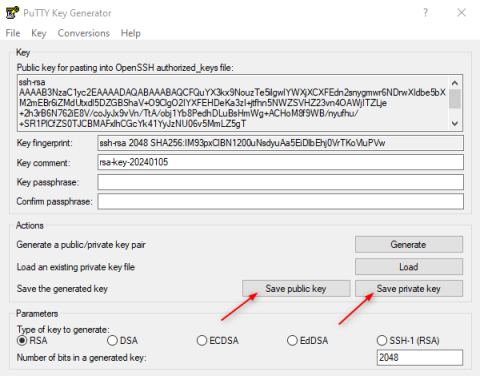
During the key generation, follow the instructions to move your mouse pointer randomly within the blank area of the window to help generate a more random key based on your mouse pointer locations.



Step 3 (Optional)
You can set a key password if you want on the generated key results window. This is not required and is optional. By doing this, it will require you to enter a password when you authenticate with your private key. This is useful if someone unauthorized gets a copy of your key. They won't be able to use it without this password. If you do decide to use a password, do know that Segra does NOT have the ability to reset your private key password if its lost. You will need to generate a new key if lost.



Step 4
Click on the "Save public key" and "Save private key" button to save your key files on your computer. Its recommended you backup your private key in a safe location that cannot be accessed by unauthorized users.



Step 5
Send the public key file via the form on the landing page where this document was downloaded (QR code below) or to billingsupport@segra.com. **Do NOT send Segra your private SSH key file**. Remember, this is your key that only you should have. If you send the private key by accident, then you will need to generate a new key.

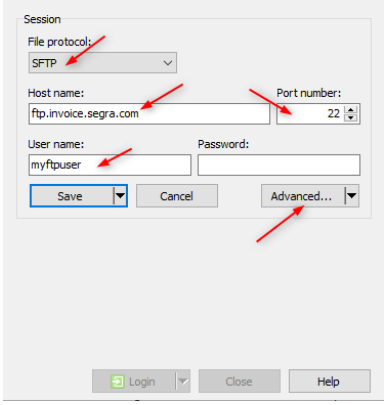
While submitting your public key, you will also be asked for the following information:

1. First and Last Name
2. Email
3. Phone
4. Company
5. Account Number
6. FTP Username Requested
7. Public SSH Key
    a. Type of FTP Feed (Select all types that apply)
    b. Call Detail Records
    c. Data Records
    d. Invoice Data Records
8. File Type (Select all that apply)
    a. CSV
    b. PDF

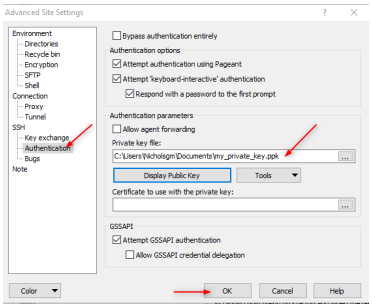
Connecting to Segra FTP using your SSH Private Key

You can connect to your FTP account using your private key after Segra has configured your public key to your account. You will receive an email notification once the account has been set up. Use an FTP client of your choosing. In the examples below, we will be using WinSCP.

Step 1
Set up your connection to the new FTP host ftp.invoice.segra.com, using Port number 22, File protocol SFTP and your FTP Username login. Click on "Advanced" button.



Step 2
On the advance settings, go to "SSH→Authentication" in the left menu and set the "private key file" path to save on your PC. Click "OK" to close window.



Step 3
On the connection window, click "Save" to save your changes and then click "Login" to connect to the SFTP server using your private key.