samegoal

Set Up SFTP Connection

There are three parts to setting up an SFTP connection:

1. Generate a key pair
2. Install your public key
3. Verify you can connect

Generate a key pair

Generate a public/private key pair.

Steps *To set up a public/private key pair for Windows:*

1. Use WinSCP to generate a PPK-style public/private key pair.
2. Launch WinSCP. A login window will appear.
3. In this window, click **Tools** (bottom left) > **Run PuTTYgen**.
4. In the **PuTTY Key Generator** window:
    - Set **Type of keys to generate** to **RSA** if not set by default.
    - Click the **Generate** button. Generate randomness by moving the mouse over the blank area of the window while the key is being generated.
5. Once the key is generated, save your keys to a location on your local machine.
    1. Click the **Save public key** button. Recommended file name: **id_rsa.pub**
    2. Click the **Save private key** button. When prompted "Are you sure you want to save this key without a passphrase to protect it?" choose **Yes.** Recommended file name: **id_rsa.ppk**
6. **Public key for pasting into OpenSSH authorized_keys file** is displayed at the top of the window after keys are generated. Copy/paste this key into SameGoal (see next step to install your public key), or email it to your SameGoal representative.

Steps *To set up a public/private key pair for Mac or Linux:*

1. Use the ssh-keygen utility to generate an OpenSSH-style public/private key pair on the command line.
2. Open a terminal.
3. <user>@dev1:~$ ssh-keygen
4. Enter file in which to save the key (/home/<user>/.ssh/id_rsa): *Press enter to accept default location*
5. Enter passphrase (empty for no passphrase): *Press enter to leave passphrase empty*
6. Enter same passphrase again: *Press enter to leave passphrase empty*
7. Once your keys have been generated, they will be saved in your **~/.ssh** directory:
    - Private key: **/home/<user>/.ssh/id_rsa.pub**
    - Public key: **/home/<user>/.ssh/id_rsa**

Tip If necessary, you may convert an OpenSSH-style private key to a PPK-style private key or vice versa easily.

Install your public key

If you have access to an administrative account in SameGoal, follow the steps below to install the public key to the district's SFTP account **authorized_keys** file using the SameGoal web interface.

If not, please email your public key to tier2help@samegoal.com or your SameGoal representative for installation.

Steps *To install the public key:*

1. Login with an administrative account.
2. Visit **Settings > Technical Settings**.
3. Depending on your operating system:
    - **Mac or Linux**: Copy/paste the contents of **id_rsa.pub** into the SFTP Account **authorized_keys files** box.
    - **Windows**: Copy/paste the contents of **Public key for pasting into OpenSSH authorized_keys file** displayed at the top of the WinSCP PuTTYgen window after keys are generated. If you have already closed this window, you may copy/paste the contents of your public key file after removing all line breaks from the key and adding "ssh-rsa " to the front.
4. Scroll to the bottom of the page and click the **Save** button.

Tip It can take up to 60 minutes to propagate new key information to the server after updating the authorized_keys file.

Verify you can connect

Tip If you recently added or changed key information, wait 60 minutes before trying to connect.

Use an SFTP tool to connect.

- Windows: WinSCP
- Mac: Cyberduck
- Linux: OpenSSH

Connection information:

- Host: **sftp.samegoal.com**
- Username: your district domain
- Authentication: Public key only

Tip Only use SFTP to test the connection. Do not use SSH or SCP. You do not have shell access and these programs will appear to hang when you appear to connect.

Tip If you are having trouble connecting, make sure you are using keys compatible with the SFTP tool you are using. For example:

- WinSCP uses a PPK-style private key. Use your **id_rsa.ppk** file to connect.
- SG-Agent, Cyberduck, OpenSSH and SG-SFTP require OpenSSH-style public/private keys. Use your **id_rsa.pub** and **id_rsa** files to connect.