SFTP - Using a Private Key for Authentication

Last Modified on 03/16/2020 3:32 pm EDT

The SFTP connector supports authentication via RSA private key and RSA private key + passphrase.

To generate an RSA private key (on Mac OSX), complete these steps:

1. Open your terminal.
2. Enter the following command:

   ```
   ssh-keygen -t rsa -C "your_email@example.com"
   ```

   - Follow the prompts, making note of your passphrase if you choose to use one (this is strongly recommended for security purposes).
3. Once complete, check that your RSA key is in a format compatible with the SFTP connector

   ```
   head -1 ~/[path and name of your key]
   ```

   - You should see the following in your terminal:

     ```
     -----BEGIN RSA PRIVATE KEY-----
     ```

   - If you see this instead, please see instructions below for converting to the correct RSA format:

     ```
     -----BEGIN OPENSSH PRIVATE KEY-----
     ```

4. Base64 encode your key:

   ```
   base64 -i  -o
   ```

   - Do not use openssl base64 as it will create a newline delimited string that is not compatible.
   - If you use a copy/paste base64 encoder (outside of the terminal), all of the contents of the key file must be encoded, including the header and footer.
5. In the call to POST /instances:

  - Pass the base64 encoded RSA key in the 'Private Key' field
  - If you used a passphrase when generating the key, enter the passphrase in the 'Private Key Password' field (note: the passphrase should not be base64 encoded).

Converting an OPENSSH key to the Correct RSA Format

1. Open your terminal.
2. Enter the following command:
   ```
   ssh-keygen -p -m PEM -f ~/.ssh/[key file name]
   ```
3. If you'd like to generate a new key instead:
   ```
   ssh-keygen -m PEM -t rsa -C "your_email@example.com"
   ```