Creating an SSH Key Pair for Service Account SFTP Access (Windows)

1. Why SSH Key Authentication Is Required for Service Accounts

Secure File Transfer Protocol (SFTP) uses **SSH (Secure Shell)** to securely authenticate users and encrypt data in transit.

Instead of usernames and passwords, **Press Ganey requires SSH key based authentication**, which:

- Is **more secure** than passwords
- Prevents brute-force and credential-theft attacks
- Allows automated and unattended file transfers
- Meets standard security and compliance best practices

With SSH authentication:

- **You keep the private key** (never shared)
- **Share only the public key** with Press Ganey
- Access is granted only if the keys match

2. Overview of What You Will Do

On a Windows system, you will:

1. Install an SSH key generation tool
2. Generate an SSH key pair (public + private key)
3. Store the private key securely
4. Share the public key with Press Ganey
5. Use the private key when connecting to our SFTP host

3. Required Software (Windows)

OpenSSH (Built into Modern Windows)

- Windows 10 and later include OpenSSH by default.
- You may already have it installed. This option is suitable for advanced or command-line users.

4. Creating an SSH Key Pair (OpenSSH – Command Line)

If using OpenSSH:

1. Open **Command Prompt** or **PowerShell**
2. Run: ssh-keygen -t rsa -b 4096 (minimum 2048 bit, 4096 recommended)
3. When prompted:
    - Accept the default file location
    - Enter a passphrase (recommended)

This creates the keys in your home directory C:\Users\<USERNAME>\.ssh\

- **Private key**: id_rsa
- **Public key**: id_rsa.pub

The public key is already in **OpenSSH format**.

Notes and Common Variations

- <USERNAME> is the Windows login user who ran ssh-keygen
- The .ssh directory is **hidden by default**
- If the directory does not exist, OpenSSH creates it automatically

If run as a different account

- **Administrator / service account**: C:\Users\Administrator\.ssh\
- **Automated service or scheduled task**: The keys are created under **that account's profile**, not the interactive user

5. Only share the public key

You may provide it as:

- The .pub file
- Or the full public key text (preferred)

❌ **Do NOT share**

- Private key files (.ppk, id_rsa)
- Passphrases
- Screenshots of private keys

6. How Press Ganey Uses Your Public Key

Once we receive your public key:

1. We install it on our SFTP host

2. It is mapped to your SFTP account
3. You authenticate using your private key
4. Password authentication is disabled (for security)

7. Using the Key to Connect (High Level)

When connecting via an SFTP client:

- Configure the connection to:
    - Use **SFTP**
    - Specify your **private key**
    - Enter your key passphrase (if set)

Popular SFTP clients:

- PuTTY / PSFTP
- WinSCP
- FileZilla (with SFTP support)

8. Key Security Best Practices

- Store private keys in a secure location
- Restrict file permissions where possible
- Do not email private keys
- Rotate keys every 12 months
- Use one key per system or application