Install Private Key (SSH)

Here are step-by-step instructions on how to **store an SSH private key securely** once generated on both **Windows** and **Mac** systems:

Windows

1. **Default Location**
   - By default, SSH private keys are saved in your user profile directory under:

     ```
     C:\Users\<your_username>\.ssh\
     ```

   - The private key file is usually named `id_rsa` or similar.
2. **Set File Permissions**
   - Ensure only your user account has access to the private key file:
     - Right-click the private key file > Properties > Security tab.
     - Remove access for any other users or groups except yourself.
3. **Use SSH-Agent for Secure Key Storage**
   - Open **PowerShell as Administrator**.
   - Enable and start the ssh-agent service:

     ```
     Get-Service ssh-agent | Set-Service -StartupType Automatic
     Start-Service ssh-agent
     ```

   - Add your private key to ssh-agent to avoid typing your passphrase every time:

     ```
     ssh-add $env:USERPROFILE\.ssh\id_rsa
     ```

   - The ssh-agent stores your private keys encrypted, protected by your Windows user credentials.
4. **Backup Private Key Securely**
   - Copy the private key file to an **encrypted external drive** or secure **password manager**.
   - Avoid storing private keys in shared or non-encrypted folders.
   - Do NOT share the private key.

Mac (macOS)

1. **Default Location**
   - Private keys are stored in the hidden `.ssh` folder in your home directory:

```
~/.ssh/id_rsa
```

- Use `ls -la ~/.ssh` in Terminal to view.

2. **Set Proper File Permissions**
   - Ensure your private key file is readable only by you:

```
chmod 600 ~/.ssh/id_rsa
```

3. **Add SSH Key to ssh-agent**
   - Start the ssh-agent:

```
eval "$(ssh-agent -s)"
```

   - Add your private key with:

```
ssh-add -K ~/.ssh/id_rsa
```

   - This stores your key securely in the macOS keychain.
4. **Backup Private Key Safely**
   - Store a copy on an **encrypted USB drive** or a **password manager** like 1Password.
   - Never upload your private key unencrypted to cloud storage.
   - Keep backups separate from your main machine to avoid loss.

Security best practices:

- Always protect your private key with a **strong passphrase** when generating it.
- Keep private key files with strict permissions so only your user account can read them.
- Use **ssh-agent** to manage keys in memory instead of repeatedly entering passwords or exposing keys.
- Backup private keys securely and do not share your private keys with anyone.

Revision #1
Created 24 July 2025 17:02:49 by avelica.ws@gmail.com
Updated 25 July 2025 08:37:46 by avelica.ws@gmail.com