SSH Key Generation, Adding to SSH Agent, and Uploading to the Cluster

Markus G. S. Weiss

2024/10/28

Contents

1 Introduction

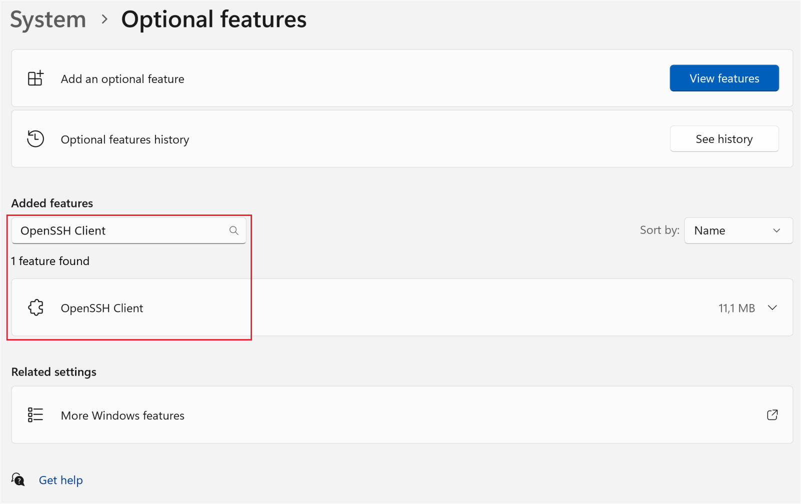
This guide will walk you through generating SSH keys, adding your private key to an SSH agent, and uploading your public key to the cluster for secure authentication. Instructions are provided for both Windows and macOS/Linux users.

2 Generating SSH Keys

SSH keys are used for secure authentication between your local machine and the server. Follow the steps below based on your operating system.

2.1 Installing OpenSSH Client (Windows Only)

1. If you are using **Windows** (11), ensure that the OpenSSH Client is enabled on your machine.
   (a) Open **Settings** and search for **Optional features** or navigate to **System** → **Optional features** for Windows 11 or **Apps** → **Apps and Features** → **Manage Optional Features** for other versions.
   (b) Search for **OpenSSH Client**. If not found, proceed with the next steps.
   (c) Click on **Add a feature**.
   (d) Search for **OpenSSH Client** and install it.



OpenSSH Client

Sort by: Name

1 feature found

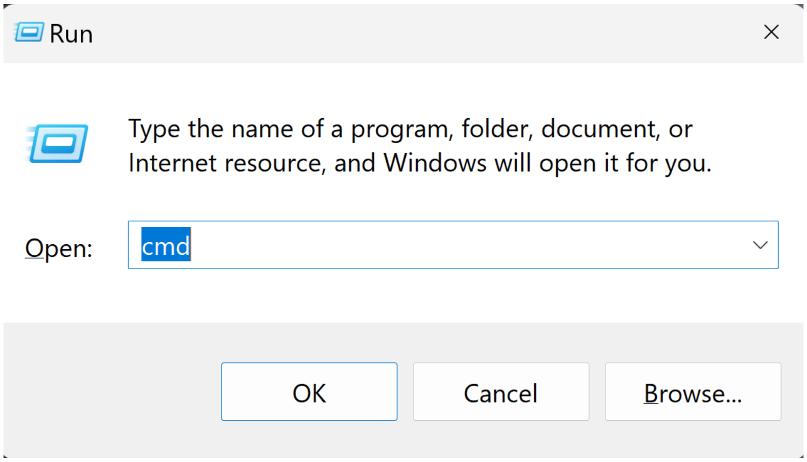
OpenSSH Client 11,1 MB

Figure 1: Enabling the OpenSSH Client in Windows Settings.

2.2 Opening the Terminal

1. Open the appropriate terminal for your operating system:

   - **Windows Users**: Open **Command Prompt** (Press **Windows key** + **R**, type `cmd`, and click **OK**).
   - **macOS/Linux Users**: Open **Terminal** (macOS: Press **Command** + **Space**, type `Terminal`, and press **Enter**; Linux: Press **Ctrl** + **Alt** + **T** or search for `Terminal`).



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

Figure 2: Opening Command Prompt.

2.3 Checking for Existing SSH Keys

Before generating a new SSH key, check if you already have one.

2. List the contents of the `~/.ssh` directory:

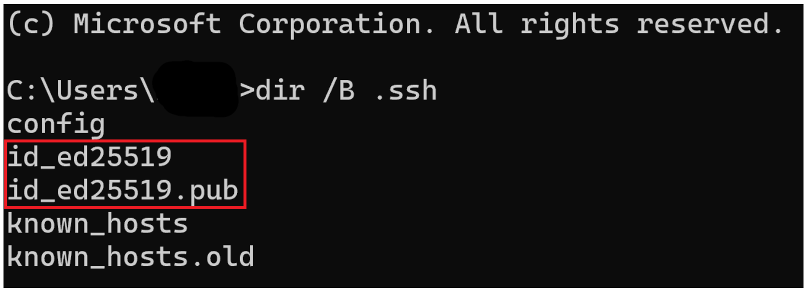
   - **Windows**:

```
dir %USERPROFILE%\.ssh
```

   - **macOS/Linux**:

```
ls ~/.ssh
```

3. If you see files like `id_ed25519` and `id_ed25519.pub`, you already have an SSH key pair. You can use these existing keys or generate a new pair if necessary.



```
(c) Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>dir /B .ssh
config
id_ed25519
id_ed25519.pub
known_hosts
known_hosts.old
```

Figure 3: Existing SSH Keys in `~/.ssh` Directory.

2.4 Generating the SSH Key

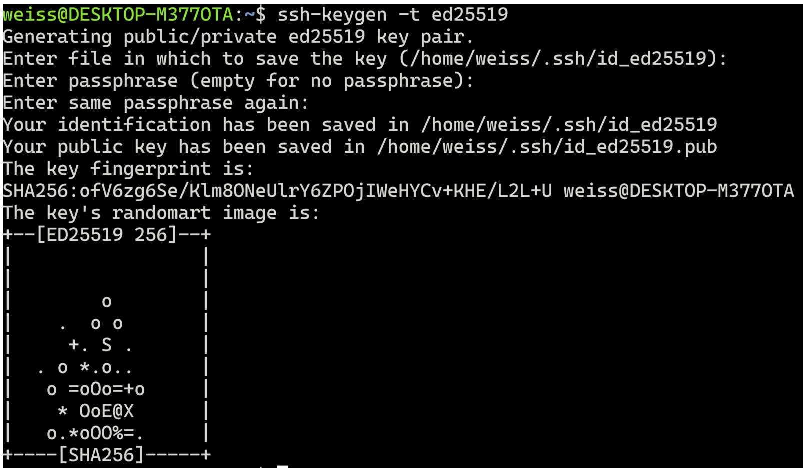
4. Generate an ED25519 SSH key by typing the following command:

```
ssh-keygen -t ed25519
```

5. When prompted for a file in which to save the key, press **Enter** to accept the default location or specify a custom path.

6. If prompted to overwrite an existing key, choose to proceed or specify a different filename.

7. When prompted for a passphrase, you can press **Enter** to leave it empty or enter a secure passphrase (recommended if using an SSH agent).



```
weiss@DESKTOP-M377OTA:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/weiss/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/weiss/.ssh/id_ed25519
Your public key has been saved in /home/weiss/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:ofV6zg6Se/Klm8ONeUlrY6ZPOjIWeHYCv+KHE/L2L+U weiss@DESKTOP-M377OTA
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|                 |
|        o        |
|    .  o o       |
|     +. S .      |
|  . o *.o..      |
|   o =oOo=+o     |
|    * OoE@X      |
|   o.*oOO%=.     |
+----[SHA256]-----+
```

Figure 4: Generating SSH Key.

3 Adding the SSH Key to the SSH Agent

An SSH agent holds your private keys in memory, allowing you to use them without re-entering your passphrase every time. Follow the instructions for your operating system.

3.1 macOS and Linux

1. Start the SSH agent:

```
ssh-agent
```

2. Add your private key to the SSH agent:

```
ssh-add ~/.ssh/id_ed25519
```

3. If prompted, enter your passphrase.

4. Verify that your key has been added:

```
ssh-add -l
```

5. You should see a list of your added SSH keys.

3.2 Windows (Using OpenSSH Agent)

1. Ensure the SSH agent service is running and set to start automatically. Run the following command in **PowerShell** as Administrator:

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

2. Add your private key to the SSH agent:

   ```
   ssh-add %USERPROFILE%\.ssh\id_ed25519
   ```

3. If prompted, enter your passphrase.

4. Verify that your key has been added:

   ```
   ssh-add -l
   ```

5. You should see a list of your added SSH keys.

Note: If you're using PuTTY's Pageant as your SSH agent:

1. Open Pageant.

2. Click on **Add Key**.

3. Navigate to your private key file. If your key is in OpenSSH format, you may need to convert it using PuTTYgen.

4. Enter your passphrase if prompted.

5. The key is now loaded into Pageant.

4 Copying the Public Key to the Server

Depending on your operating system, follow the appropriate method to copy the public key to the server:

4.1 For macOS/Linux Users: Using ssh-copy-id

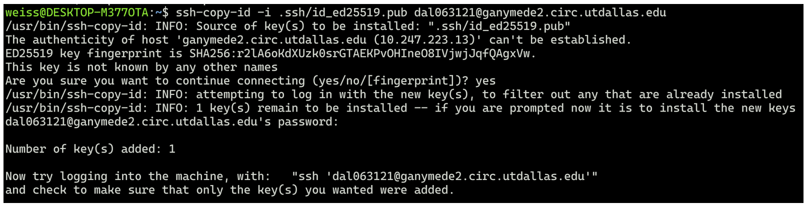
1. Use the `ssh-copy-id` command to copy your public key to the server. Replace `your_netid` with your actual NetID:

   ```
   ssh-copy-id your_netid@ganymede2.circ.utdallas.edu
   ```

2. When prompted, type `yes` to continue connecting and press **Enter**.

3. Enter your **NetID password** when prompted.

4. This command appends your public key to the `authorized_keys` file on the server automatically.



```
weiss@DESKTOP-M377OTA:~$ ssh-copy-id -i .ssh/id_ed25519.pub dal063121@ganymede2.circ.utdallas.edu
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ".ssh/id_ed25519.pub"
The authenticity of host 'ganymede2.circ.utdallas.edu (10.247.223.13)' can't be established.
ED25519 key fingerprint is SHA256:r2lA6oKdXUzk0srGTAEKPvOHIneO8IVjwjJqfQAgxVw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
dal063121@ganymede2.circ.utdallas.edu's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'dal063121@ganymede2.circ.utdallas.edu'"
and check to make sure that only the key(s) you wanted were added.
```

Figure 5: Using ssh-copy-id to Copy Public Key.

4.2 For Windows Users: Command-Line Method

1. Open **Command Prompt**.

2. Use the following command to copy your public key to the server. Replace `your_netid` with your actual NetID:

   ```
   type %USERPROFILE%\.ssh\id_ed25519.pub | ssh
     your_netid@ganymede2.circ.utdallas.edu "cat >> /home/
     your_netid/.ssh/authorized_keys"
   ```

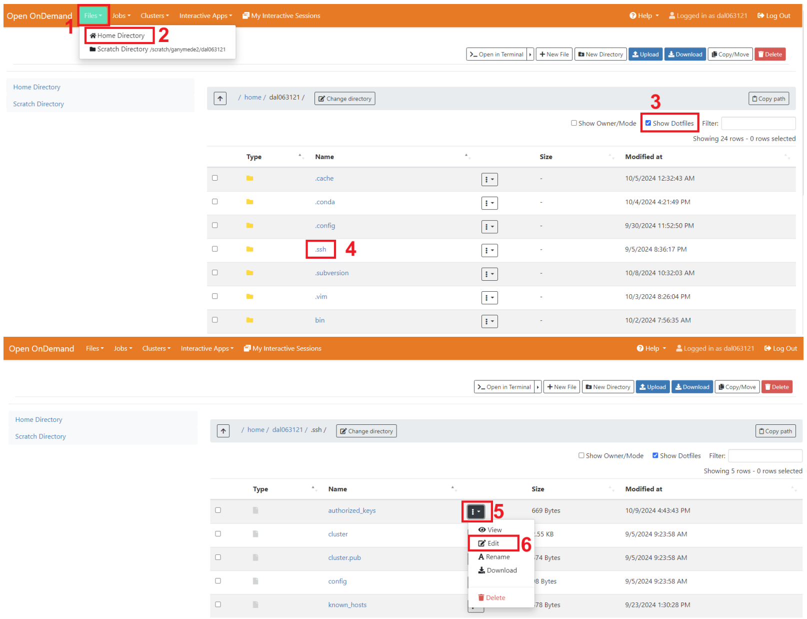
3. When prompted, enter your **NetID password**.

4. This command appends your public key to the `authorized_keys` file on the server automatically.

4.3 Alternative Method for Windows and Other Systems: Manual Copy via Browser

If the command-line method doesn't work, you can manually copy your public key to the server:

1. Locate your public key file, typically found at `~/.ssh/id_ed25519.pub`.
2. Open the file (`id_ed25519.pub`) and copy the entire contents. **Never share your private key!**
3. Open a web browser and navigate to `https://g2-ood.circ.utdallas.edu`.
4. Log in with your credentials.
5. Click on **Files** and **Home Directory**, then check the **Show dot files** box.
6. Navigate to your `~/.ssh` directory. (If it doesn't exist, create it.)
7. Open the `authorized_keys` file (or create it if it doesn't exist).
8. Paste your **public key** on a **new line** in the file and **save** it.



□ Show Owner/Mode ☑ Show Dotfiles Filter:

Showing 24 rows - 0 rows selected

	Type	Name		Size	Modified at
□		.cache		-	10/5/2024 12:32:43 AM
□		.conda		-	10/4/2024 4:21:49 PM
□		.config		-	9/30/2024 11:52:50 PM
□		.ssh		-	9/5/2024 8:36:17 PM
□		.subversion		-	10/8/2024 10:32:03 AM
□		.vim		-	10/3/2024 8:26:04 PM
□		bin		-	10/2/2024 7:56:35 AM

□ Show Owner/Mode ☑ Show Dotfiles Filter:

Showing 5 rows - 0 rows selected

	Type	Name		Size	Modified at
□		authorized_keys		669 Bytes	10/9/2024 4:43:43 PM
□		cluster		.55 KB	9/5/2024 9:23:58 AM
□		cluster.pub		74 Bytes	9/5/2024 9:23:58 AM
□		config		8 Bytes	9/5/2024 9:23:58 AM
□		known_hosts		78 Bytes	9/23/2024 1:30:28 PM

Figure 6: Pasting Public Key into `authorized_keys`.

5 Conclusion

You have successfully generated an SSH key pair, added your private key to the SSH agent, and uploaded your public key to the cluster. This will enable secure, password-less authentication when connecting to the server.