Generating a new SSH key and adding it to the ssh-agent

In this article

After you've checked for existing SSH keys, you can generate a new SSH key to use for authentication, then add it to the ssh-agent.

Mac Windows Linux

About SSH key passphrases

You can access and write data in repositories on your GitHub Enterprise Server instance using SSH (Secure Shell Protocol). When you connect via SSH, you authenticate using a private key file on your local machine. For more information, see "About SSH."

When you generate an SSH key, you can add a passphrase to further secure the key. Whenever you use the key, you must enter the passphrase. If your key has a passphrase and you don't want to enter the passphrase every time you use the key, you can add your key to the SSH agent. The SSH agent manages your SSH keys and remembers your passphrase.

If you don't already have an SSH key, you must generate a new SSH key to use for authentication. If you're unsure whether you already have an SSH key, you can check for existing keys. For more information, see "Checking for existing SSH keys."

If you want to use a hardware security key to authenticate to GitHub Enterprise Server, you must generate a new SSH key for your hardware security key. You must connect your hardware security key to your computer when you authenticate with the key pair. For more information, see the OpenSSH 8.2 release notes.

Generating a new SSH key

You can generate a new SSH key on your local machine. After you generate the key, you can add the public key to your account on your GitHub Enterprise Server instance to enable authentication for Git operations over SSH.

If you are a site administrator for your GitHub Enterprise Server instance, you can use the same key to grant yourself administrative SSH access to the instance. For more information, see "Accessing the administrative shell (SSH)."

1. Open TerminalTerminalGit Bash.

2. Paste the text below, replacing the email used in the example with your GitHub Enterprise Server email address.

```
ssh-keygen -t ed25519 -C "your_email@example.com"
```

> **Note:** If you are using a legacy system that doesn't support the Ed25519 algorithm, use:
>
> ```
> ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
> ```

This creates a new SSH key, using the provided email as a label.

```
> Generating public/private ALGORITHM key pair.
```

When you're prompted to "Enter a file in which to save the key", you can press **Enter** to accept the default file location. Please note that if you created SSH keys previously, ssh-keygen may ask you to rewrite another key, in which case we recommend creating a custom-named SSH key. To do so, type the default file location and replace id_ssh_keyname with your custom key name.

```
> Enter a file in which to save the key (/Users/YOU/.ssh/id_ALGORITHM):
[Press enter]
```

```
> Enter a file in which to save the key (/c/Users/YOU/.ssh/id_ALGORITHM):
[Press enter]
```

```
> Enter a file in which to save the key (/home/YOU/.ssh/ALGORITHM):[Press
enter]
```

3. At the prompt, type a secure passphrase. For more information, see "Working with SSH key passphrases."

```
> Enter passphrase (empty for no passphrase): [Type a passphrase]
> Enter same passphrase again: [Type passphrase again]
```

Adding your SSH key to the ssh-agent

Before adding a new SSH key to the ssh-agent to manage your keys, you should have checked for existing SSH keys and generated a new SSH key. When adding your SSH key to the agent, use the default macOS `ssh-add` command, and not an application installed by macports, homebrew, or some other external source.

1. Start the ssh-agent in the background.

```
$ eval "$(ssh-agent -s)"
> Agent pid 59566
```

Depending on your environment, you may need to use a different command. For example, you may need to use root access by running `sudo -s -H` before starting the ssh-agent, or you may need to use `exec ssh-agent bash` or `exec ssh-agent zsh` to run the ssh-agent.

2. If you're using macOS Sierra 10.12.2 or later, you will need to modify your

`~/.ssh/config` file to automatically load keys into the ssh-agent and store passphrases in your keychain.

- First, check to see if your `~/.ssh/config` file exists in the default location.

  ```
  $ open ~/.ssh/config
  > The file /Users/YOU/.ssh/config does not exist.
  ```

- If the file doesn't exist, create the file.

  ```
  touch ~/.ssh/config
  ```

- Open your `~/.ssh/config` file, then modify the file to contain the following lines. If your SSH key file has a different name or path than the example code, modify the filename or path to match your current setup.

  ```
  Host HOSTNAME
    AddKeysToAgent yes
    UseKeychain yes
    IdentityFile ~/.ssh/id_ed25519
  ```

  Notes:

  - If you chose not to add a passphrase to your key, you should omit the `UseKeychain` line.
  - If you see a `Bad configuration option: usekeychain` error, add an additional line to the configuration's' `Host *.HOSTNAME` section.

    ```
    Host HOSTNAME
      IgnoreUnknown UseKeychain
    ```

3. Add your SSH private key to the ssh-agent and store your passphrase in the keychain. If you created your key with a different name, or if you are adding an existing key that has a different name, replace *id_ed25519* in the command with the name of your private key file.

   ```
   ssh-add --apple-use-keychain ~/.ssh/id_ed25519
   ```

   Note: The `--apple-use-keychain` option stores the passphrase in your keychain for you when you add an SSH key to the ssh-agent. If you chose not to add a passphrase to your key, run the command without the `--apple-use-keychain` option.

   The `--apple-use-keychain` option is in Apple's standard version of `ssh-add`. In MacOS versions prior to Monterey (12.0), the `--apple-use-keychain` and `--apple-load-keychain` flags used the syntax `-K` and `-A`, respectively.

   If you don't have Apple's standard version of `ssh-add` installed, you may receive an error. For more information, see "Error: ssh-add: illegal option -- apple-use-keychain."

   If you continue to be prompted for your passphrase, you may need to add the command to your `~/.zshrc` file (or your `~/.bashrc` file for bash).

4. Add the SSH public key to your account on GitHub. For more information, see "Adding a new SSH key to your GitHub account."

If you have GitHub Desktop installed, you can use it to clone repositories and not deal with SSH keys.

1. In a new *admin elevated* terminal window (PowerShell or CMD), ensure the ssh-agent is running. You can use the "Auto-launching the ssh-agent" instructions in "Working with SSH key passphrases", or start it manually:

```
# start the ssh-agent in the background
Get-Service -Name ssh-agent | Set-Service -StartupType Manual
Start-Service ssh-agent
```

2. In a terminal window without elevated permissions, add your SSH private key to the ssh-agent. If you created your key with a different name, or if you are adding an existing key that has a different name, replace *id_ed25519* in the command with the name of your private key file.

```
ssh-add C:\Users\YOU/.ssh/id_ed25519
```

3. Add the SSH public key to your account on GitHub. For more information, see "Adding a new SSH key to your GitHub account."

1. Start the ssh-agent in the background.

```
$ eval "$(ssh-agent -s)"
> Agent pid 59566
```

   Depending on your environment, you may need to use a different command. For example, you may need to use root access by running `sudo -s -H` before starting the ssh-agent, or you may need to use `exec ssh-agent bash` or `exec ssh-agent zsh` to run the ssh-agent.

2. Add your SSH private key to the ssh-agent.

   If you created your key with a different name, or if you are adding an existing key that has a different name, replace *id_ed25519* in the command with the name of your private key file.

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

3. Add the SSH public key to your account on GitHub. For more information, see "Adding a new SSH key to your GitHub account."

Generating a new SSH key for a hardware security key

If you are using macOS or Linux, you may need to update your SSH client or install a new SSH client prior to generating a new SSH key. For more information, see "Error: Unknown key type."

1. Insert your hardware security key into your computer.
2. Open TerminalTerminalGit Bash.
3. Paste the text below, substituting in the email address for your account on GitHub Enterprise Server.

```
ssh-keygen -t ed25519-sk -C "YOUR_EMAIL"
```


```
ssh-keygen -t ed25519-sk -C "YOUR_EMAIL"
```


Note: If the command fails and you receive the error `invalid format` or `feature not supported,` you may be using a hardware security key that does not support the Ed25519 algorithm. Enter the following command instead.

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

4. When you are prompted, touch the button on your hardware security key.
5. When you are prompted to "Enter a file in which to save the key," press Enter to accept the default file location.

```
> Enter a file in which to save the key (/Users/YOU/.ssh/id_ed25519_sk):
[Press enter]
```

```
> Enter a file in which to save the key (/c/Users/YOU/.ssh/id_ed25519_sk):
[Press enter]
```

```
> Enter a file in which to save the key (/home/YOU/.ssh/id_ed25519_sk):
[Press enter]
```

6. When you are prompted to type a passphrase, press **Enter**.

```
> Enter passphrase (empty for no passphrase): [Type a passphrase]
> Enter same passphrase again: [Type passphrase again]
```

7. Add the SSH public key to your account on GitHub. For more information, see "Adding a new SSH key to your GitHub account."