GitHub Docs

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

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

In this article

About SSH key generation
Generating a new SSH key
Adding your SSH key to the ssh-agent
Generating a new SSH key for a hardware security key
Further reading

About SSH key generation

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, 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.

If you don't want to reenter your passphrase every time you use your SSH key, you can add your key to the SSH agent, which manages your SSH keys and remembers your passphrase.

Generating a new SSH key

1. Open Terminal.
2. Paste the text below, substituting in your GitHub email address.

2 Paste the text below, substituting in your GitHub 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.
```

1 When you're prompted to "Enter a file in which to save the key," press Enter. This accepts the default file location.

```
> Enter a file in which to save the key (/Users/you/.ssh/id_algorithm): [Pres
```

2 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 *
       AddKeysToAgent yes
       UseKeychain yes
       IdentityFile ~/.ssh/id_ed25519
     ```

     Note: If you chose not to add a passphrase to your key, you should omit the `UseKeychain` line.

     Note: If you see an error like this

     ```
     /Users/USER/.ssh/config: line 16: Bad configuration option: usekeychain
     ```

     add an additional config line to your `Host *` section:

     ```
     Host *
       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 -K ~/.ssh/id_ed25519
```

> **Note:** The `-K` option is Apple's standard version of `ssh-add`, which 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 `-K` option.
>
> If you don't have Apple's standard version installed, you may receive an error. For more information on resolving this error, see "Error: ssh-add: illegal option -- K."
>
> In MacOS Monterey (12.0), the `-K` and `-A` flags are deprecated and have been replaced by the `--apple-use-keychain` and `--apple-load-keychain` flags, respectively.

4. Add the SSH 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 Terminal.
3. Paste the text below, substituting in the email address for your account on GitHub.

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

> **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): [Pre
```

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

Further reading

- "About SSH"
- "Working with SSH key passphrases"
- "Authorizing an SSH key for use with SAML single sign-on" in the GitHub Enterprise Cloud documentation