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

If you don't already have an SSH key, you must generate a new SSH key. If you're unsure whether you already have an SSH key, check for existing keys.

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.

```
$ 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 rsa key pair.
```

3. 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_rsa): [Press enter
```

4. 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
```

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, replacing `~/.ssh/id_rsa` if you are not using the default location and name for your `id_rsa` key.

```
Host *
  AddKeysToAgent yes
  UseKeychain yes
  IdentityFile ~/.ssh/id_rsa
```

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_rsa* in the command with the name of your private key file.

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

> **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 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."

4. Add the 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"