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

MAC | WINDOWS | LINUX

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.

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 Git Bash.
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.
```

Article versions

GitHub.com
GitHub Enterprise 2.15
GitHub Enterprise 2.14
GitHub Enterprise 2.13
GitHub Enterprise 2.12

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 (/c/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.

If you have GitHub Desktop installed, you can use it to clone repositories and not deal with SSH keys. It also comes with the Git Bash tool, which is the preferred way of running `git` commands on Windows.

1. Ensure the ssh-agent is running:

   - If you are using the Git Shell that's installed with GitHub Desktop, the ssh-agent should be running.
   - If you are using another terminal prompt, such as Git for Windows, 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
     $ eval $(ssh-agent -s)
     Agent pid 59566
     ```

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

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

3. Add the SSH key to your GitHub account.

Further reading

- "About SSH"
- "Working with SSH key passphrases"
- "Authorizing an SSH key for use with a SAML single sign-on organization"

Contact a human