Setting up an SSH token for a Github Account

The following guide is a concatenation of three different tutorials published by github. The original tutorials are linked at the bottom of the document for reference.

1. Open a terminal window
2. Paste the following into terminal and replace the email with the email connected to your github account

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

   You should see an output that looks something like this:

   ```
   > Generating public/private ed25519 key pair.
   ```

3. You will be prompted to enter a file location for saving the ssh key. Press `ENTER` which tells to computer to save the key in the default file location

   ```
   > Enter a file in which to save the key
   (/Users/you/.ssh/id_ed25519): [Press enter]
   ```

4. You will be prompted to enter a passphrase for the ssh key. Press `ENTER` which instructs the computer not to require a password when using the ssh key

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

   ```
   > Enter same passphrase again: [Type passphrase again]
   ```

5. Run the following command:

   ```
   eval "$(ssh-agent -s)"
   ```

6. Run the following command:

```
open ~/.ssh/config
```

If you receive a message stating that the file does not exist, run the following command:

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

Then run the command to open the file:

```
open ~/.ssh/config
```

7. If the file is empty paste the following into the file and save the changes. If the file already contains content, make sure the settings align the text below:

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

8. Save the file with **command-s** (for macs), and run the following in terminal:

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

9. Run the following in terminal

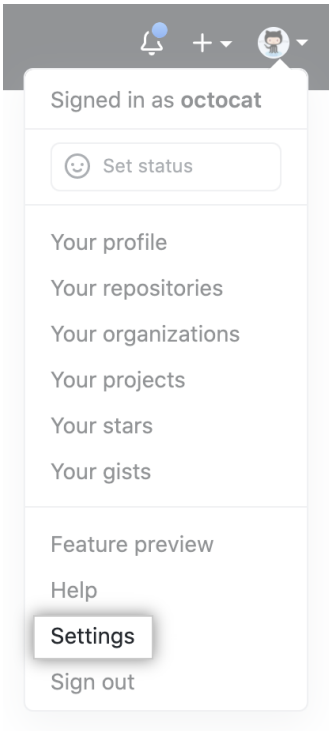
Mac computers:

```
pbcopy < ~/.ssh/id_ed25519.pub
```

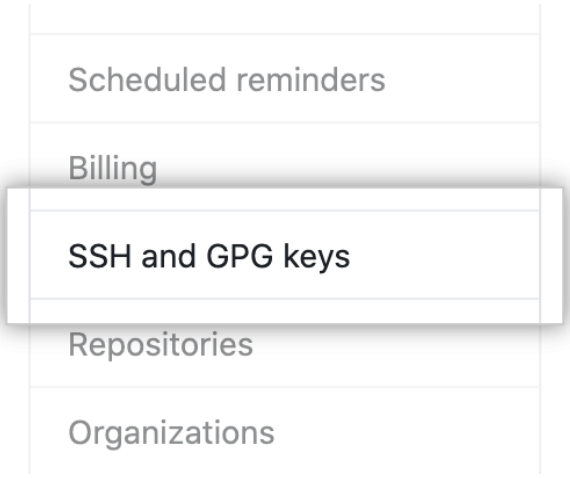
Windows computers:

```
clip < ~/.ssh/id_ed25519.pub
```

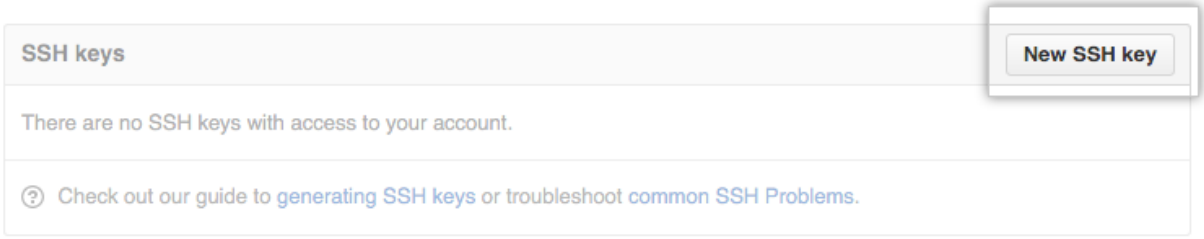
10. Navigate to the settings page on github.



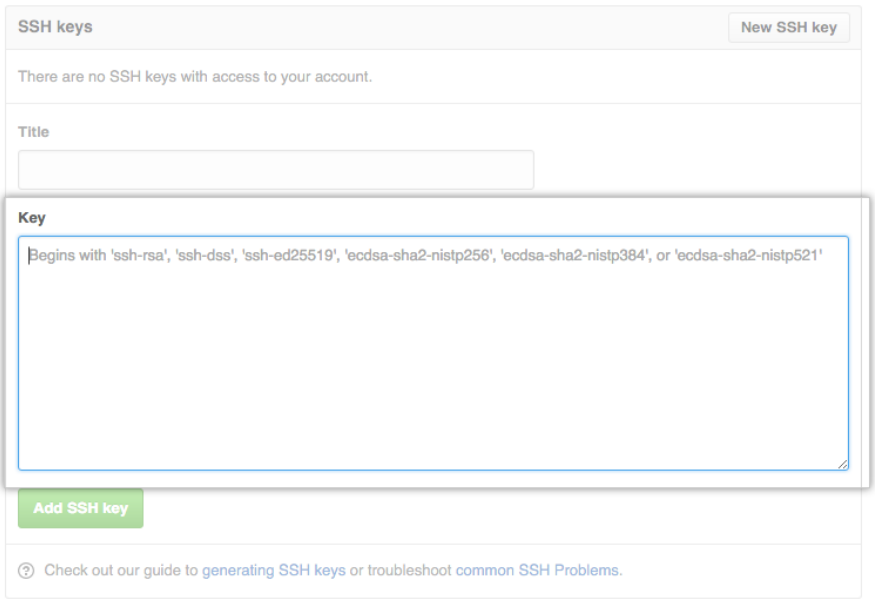
11. Select `SSH and GPG keys` from the left side bar.



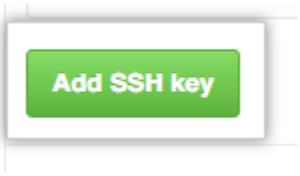
12. Click **New SSH key** or **Add SSH key**.



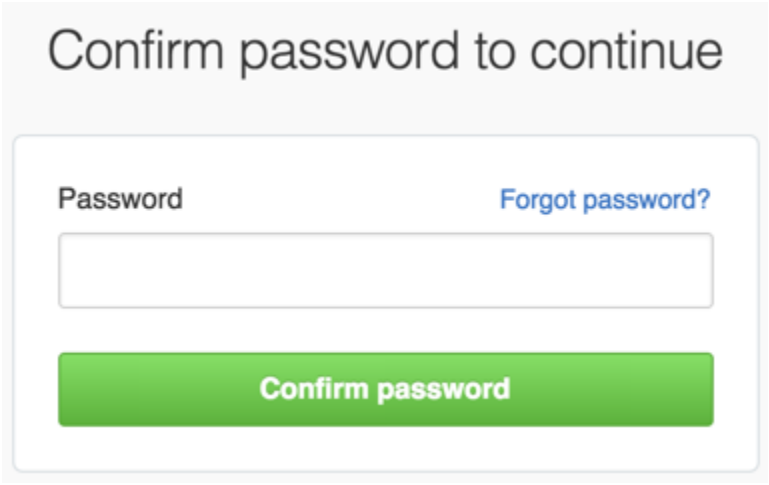
13. In the "Title" field, add a descriptive label for the new key. For example, if you're using a personal Mac, you might call this key "Personal MacBook Air".
14. Step 9 stored the ssh key on your clipboard. Click into the **Key** text box and paste the key into the text box.



15. Click **Add SSH key**.



16. If prompted, confirm your GitHub password.



17. Enter the following in a terminal window

```
ssh -T git@github.com
```

a. If you see the following message:

```
> The authenticity of host 'github.com (IP ADDRESS)' can't be
established.

> RSA key fingerprint is
SHA256:nThbg6kXUpJWGl7E1IGOCspRomTxdCARLviKw6E5SY8.

> Are you sure you want to continue connecting (yes/no)?
```

Enter **yes**

18. If you see the following message, you have successfully connect to github using an ssh key

```
> Hi username! You've successfully authenticated, but GitHub does
not

> provide shell access.
```

19. Last step is to set ssh as the global authentication protocol by running the following line:

```
git config --global url.ssh://git@github.com/.insteadOf
https://github.com/
```

Github tutorials:

1. Generating a new SSH key and adding it to the ssh-agent
2. Adding a new SSH key to your GitHub account
3. Testing your SSH connection