Adding a new SSH key to your GitHub account

In this article

To configure your account on GitHub.com to use your new (or existing) SSH key, you'll also need to add the key to your account.

Mac Windows Linux

GitHub CLI Web browser

About addition of SSH keys to your account

You can access and write data in repositories on GitHub.com 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."

You can also use SSH to sign commits and tags. For more information about commit signing, see "About commit signature verification."

After you generate an SSH key pair, you must add the public key to GitHub.com to enable SSH access for your account.

Prerequisites

Before adding a new SSH key to your account on GitHub.com, complete the following steps.

1. Check for existing SSH keys. For more information, see "Checking for existing SSH keys."

2. Generate a new SSH key and add it to your machine's SSH agent. For more information, see "Generating a new SSH key and adding it to the ssh-agent."

Adding a new SSH key to your account

You can add an SSH key and use it for authentication, or commit signing, or both. If you want to use the same SSH key for both authentication and signing, you need to upload it twice.

After adding a new SSH authentication key to your account on GitHub.com, you can reconfigure any local repositories to use SSH. For more information, see "Managing remote repositories."

> **Note:** GitHub improved security by dropping older, insecure key types on March 15, 2022.
>
> As of that date, DSA keys (`ssh-dss`) are no longer supported. You cannot add new DSA keys to your personal account on GitHub.com.
>
> RSA keys (`ssh-rsa`) with a `valid_after` before November 2, 2021 may continue to use any signature algorithm. RSA keys generated after that date must use a SHA-2 signature algorithm. Some older clients may need to be upgraded in order to use SHA-2 signatures.

1. Copy the SSH public key to your clipboard.

   If your SSH public key file has a different name than the example code, modify the filename to match your current setup. When copying your key, don't add any newlines or whitespace.

   ```
   $ pbcopy < ~/.ssh/id_ed25519.pub
   # Copies the contents of the id_ed25519.pub file to your clipboard
   ```

   > **Tip:** If `pbcopy` isn't working, you can locate the hidden `.ssh` folder, open the file in your favorite text editor, and copy it to your clipboard.

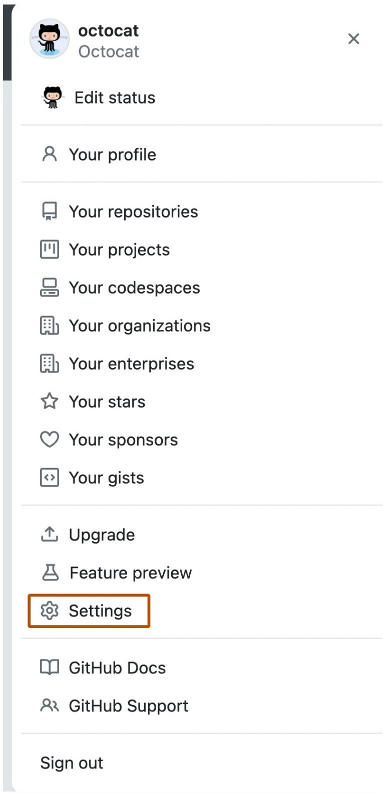
   ```
   $ clip < ~/.ssh/id_ed25519.pub
   # Copies the contents of the id_ed25519.pub file to your clipboard
   ```

   > **Notes:**
   >
   > - With Windows Subsystem for Linux (WSL), you can use `clip.exe`. Otherwise if `clip` isn't working, you can locate the hidden `.ssh` folder, open the file in your favorite text editor, and copy it to your clipboard.
   > - On newer versions of Windows that use the Windows Terminal, or anywhere else that uses the PowerShell command line, you may receive a `ParseError` stating that `The '&lt;' operator is reserved for future use.` In this case, the following alternative `clip` command should be used:
   >
   > ```
   > $ cat ~/.ssh/id_ed25519.pub | clip
   > # Copies the contents of the id_ed25519.pub file to your clipboard
   > ```

   ```
   $ cat ~/.ssh/id_ed25519.pub
   # Then select and copy the contents of the id_ed25519.pub file
   # displayed in the terminal to your clipboard
   ```

   > **Tip:** Alternatively, you can locate the hidden `.ssh` folder, open the file in your favorite text editor, and copy it to your clipboard.

2. In the upper-right corner of any page, click your profile photo, then click **Settings**.



3. In the "Access" section of the sidebar, click **SSH and GPG keys**.

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

5. In the "Title" field, add a descriptive label for the new key. For example, if you're using a personal laptop, you might call this key "Personal laptop".

6. Select the type of key, either authentication or signing. For more information about commit signing, see "About commit signature verification."

7. In the "Key" field, paste your public key.

8. Click **Add SSH key**.

9. If prompted, confirm access to your account on GitHub Enterprise Cloud. For more information, see "Sudo mode."

> To learn more about GitHub CLI, see "About GitHub CLI."

Before you can use the GitHub CLI to add an SSH key to your account, you must authenticate to the GitHub CLI. For more information, see `gh auth login` in the GitHub CLI documentation.

At present, you can only use GitHub CLI to add SSH authentication keys, you cannot add SSH signing keys.

To add an SSH authentication key to your GitHub account, use the `ssh-key add` subcommand, specifying your public key. If you're prompted to request additional scopes, follow the instructions in the command line.

```
gh ssh-key add KEY-FILE
```

To include a title for the new key, use the `-t` or `--title` flag.

```
gh ssh-key add KEY-FILE --title "personal laptop"
```

If you generated your SSH key by following the instructions in "Generating a new SSH key and adding it to the ssh-agent", you can add the key to your account with this command.

```
gh ssh-key add ~/.ssh/id_ed25519.pub
```

Further reading

- "Authorizing an SSH key for use with SAML single sign-on"