Managing your organization's SSH certificate authorities

In this article

Adding an SSH certificate authority

Deleting an SSH certificate authority

You can add or delete SSH certificate authorities from your organization.

> **Who can use this feature**
> Organization owners can manage an organization's SSH certificate authorities (CA).

You can allow members to access your organization's repositories using SSH certificates you provide by adding an SSH CA to your organization. You can require that members use SSH certificates to access organization resources, unless SSH is disabled in your repository. For more information, see "About SSH certificate authorities."

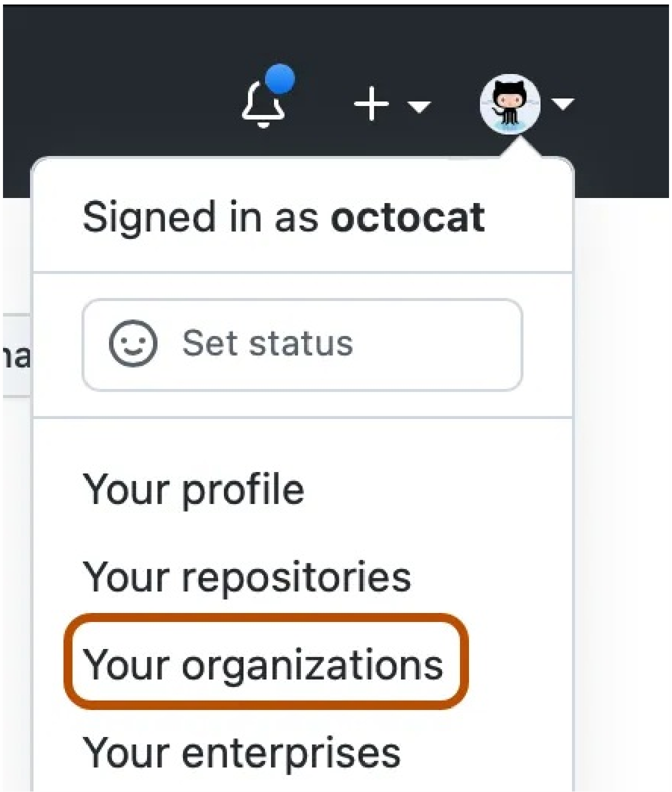
When you issue each client certificate, you must include an extension that specifies which GitHub Enterprise Server user the certificate is for. For more information, see "About SSH certificate authorities."

Adding an SSH certificate authority

If you require SSH certificates for your enterprise, enterprise members should use a special URL for Git operations over SSH. For more information, see "About SSH certificate authorities."

Each certificate authority can only be uploaded to one account on GitHub.com. If an SSH certificate authority has been added to an organization or enterprise account, you cannot add the same certificate authority to another organization or enterprise account on GitHub.com.

1. In the top right corner of GitHub Enterprise Server, click your profile photo, then click **Your organizations**.



2. Next to the organization, click **Settings**.

3. In the "Security" section of the sidebar, click **Authentication security**.

4. To the right of "SSH Certificate Authorities", click **New CA**.

5. Under "Key," paste your public SSH key.

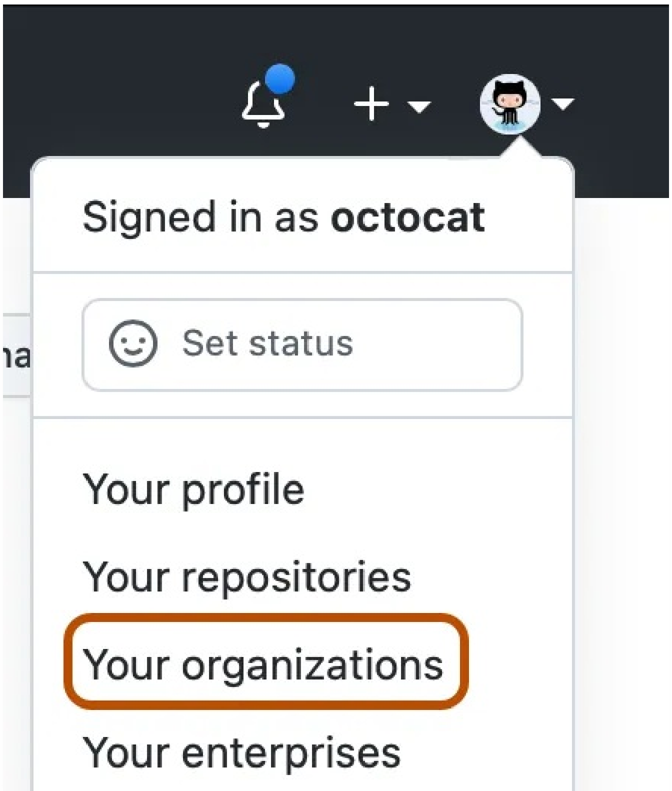
6. Click **Add CA**.

7. Optionally, to require members to use SSH certificates, select **Require SSH Certificates**, then click **Save**.

   Note: When you require SSH certificates, the requirement does not apply to authorized OAuth apps and GitHub Apps (including user-to-server tokens) or to GitHub features such as GitHub Actions, which are trusted environments within the GitHub ecosystem.

Deleting an SSH certificate authority

1. In the top right corner of GitHub Enterprise Server, click your profile photo, then click **Your organizations**.



2. Next to the organization, click **Settings**.
3. In the "Security" section of the sidebar, click 🛡 **Authentication security**.
4. Under "SSH Certificate Authorities", to the right of the CA you want to delete, click **Delete**.
5. Read the warning, then click **I understand, please delete this CA**.