

Viewing and managing a member's SAML access to your organization

In this article

About SAML access to your organization

Viewing and revoking a linked identity

Viewing and revoking an active SAML session

Viewing and revoking authorized credentials

Further reading

You can view and revoke an organization member's linked identity, active sessions, and authorized credentials.

Who can use this feature

Organization owners can view and manage a member's SAML access to an organization.

About SAML access to your organization [↗](#)

When you enable SAML single sign-on for your organization, each organization member can link their external identity on your identity provider (IdP) to their existing account on GitHub.com. To access your organization's resources on GitHub Enterprise Cloud, the member must have an active SAML session in their browser. To access your organization's resources using the API or Git, the member must use a personal access token or SSH key that the member has authorized for use with your organization.

You can view and revoke each member's linked identity, active sessions, and authorized credentials on the same page.

Viewing and revoking a linked identity [↗](#)

You can view the single sign-on identity that a member has linked to their account on GitHub.com.


If a member links the wrong identity to their account on GitHub.com, you can revoke the linked identity to allow the member to try again.

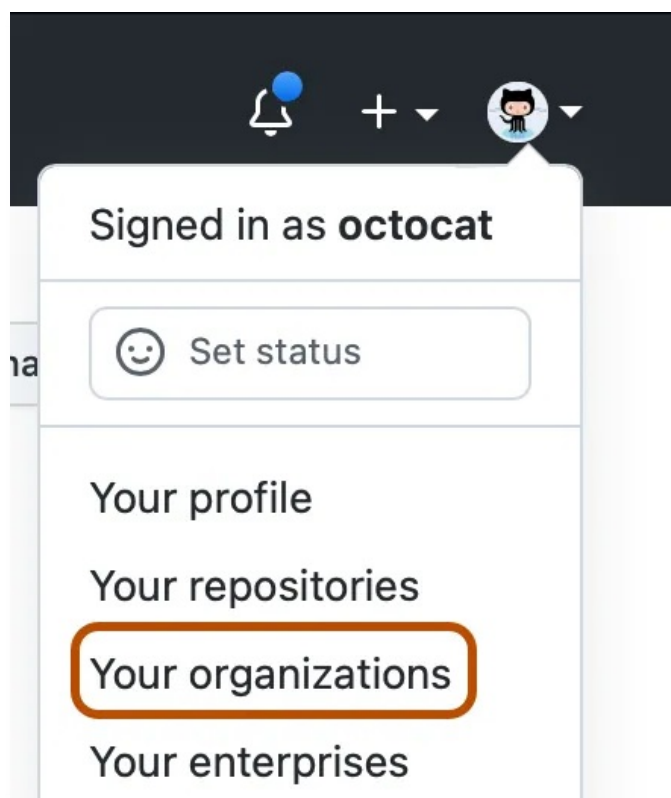
When available, the entry will include SCIM data. For more information, see "[About SCIM for organizations](#)."


Warning: For organizations using SCIM:

- Revoking a linked user identity on GitHub Enterprise Cloud will also remove the SAML and SCIM metadata. As a result, the identity provider will not be able to synchronize or deprovision the linked user identity.
- An admin must revoke a linked identity through the identity provider.
- To revoke a linked identity and link a different account through the identity provider, an admin can remove and re-assign the user to the GitHub Enterprise Cloud application. For more information, see your identity provider's documentation.

Warning: If your organization uses team synchronization, revoking a person's SSO identity will remove that person from any teams mapped to IdP groups. For more information, see ["Synchronizing a team with an identity provider group."](#)

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



- 2 Click the name of your organization.
- 3 Under your organization name, click  **People**.



- 4 Click on the name of the member whose linked identity you'd like to view or revoke.
- 5 In the left sidebar, click **SAML identity linked**.

The screenshot shows the GitHub profile for the organization 'octocat', also known as 'The Octocat'. It indicates that no verified or approved domain email is present. The user's role is 'Owner'. The profile lists 58 repositories, 0 teams, and private membership. Two-factor security is enabled, and SAML identity is linked, with the latter highlighted by an orange box.

octocat
The Octocat

No verified or approved domain email

Role: Owner ▾

58 repositories

0 teams

Membership **private**

Two-factor security **enabled**

SAML identity linked

- 6 Under "Linked SSO identity", view the linked SSO identity for the member.
- 7 To revoke the linked identity, to the right of the identity, click **Revoke**.
- 8 Read the information, then click **Revoke external identity**.

Viewing and revoking an active SAML session [🔗](#)

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

The screenshot shows the GitHub user interface with the profile dropdown menu open. The menu shows the user is signed in as 'octocat'. Options include 'Set status', 'Your profile', 'Your repositories', 'Your organizations' (highlighted with an orange box), and 'Your enterprises'.

Signed in as **octocat**


Set status

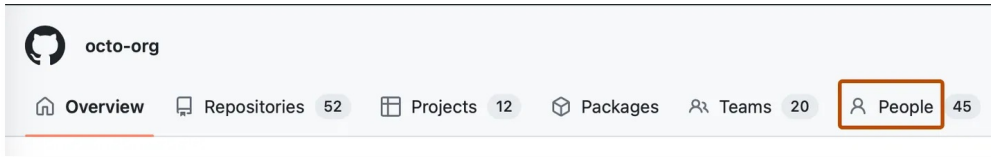
Your profile

Your repositories

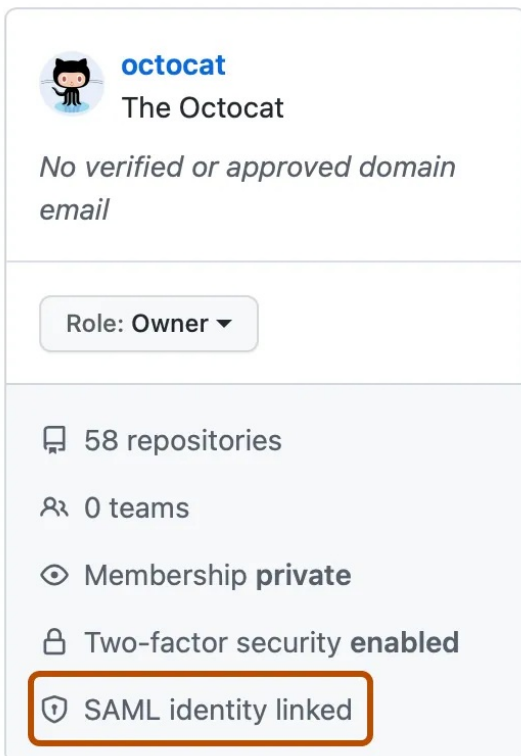
Your organizations

Your enterprises

- 2 Click the name of your organization.
- 3 Under your organization name, click  **People**.




- 4 Click on the name of the member whose SAML session you'd like to view or revoke.
- 5 In the left sidebar, click **SAML identity linked**.

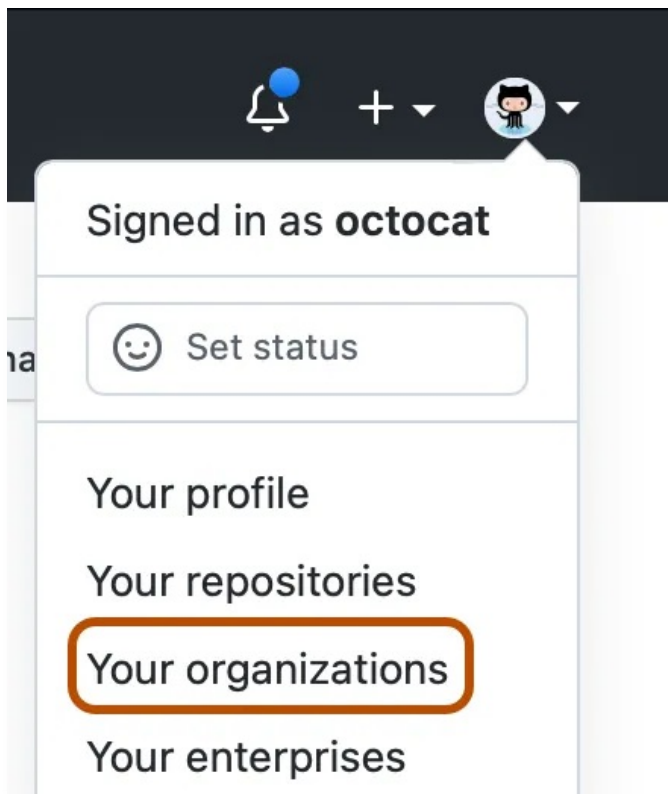



- 6 Under "Active SAML sessions", view the active SAML sessions for the member.
- 7 To revoke a session, to the right of the session you'd like to revoke, click **Revoke**.

Viewing and revoking authorized credentials

You can see each personal access token and SSH key that a member has authorized for API and Git access. Only the last several characters of each token or key are visible. If necessary, work with the member to determine which credentials you should revoke.


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



- 2 Click the name of your organization.
- 3 Under your organization name, click  **People**.





- 4 Click on the name of the member whose authorized credentials you'd like to view or revoke.
- 5 In the left sidebar, click **SAML identity linked**.


**octocat**
The Octocat


No verified or approved domain email


Role: Owner ▼

 58 repositories

 0 teams

 Membership **private**

 Two-factor security **enabled**

 **SAML identity linked**

- 6 Under "Authorized credentials", view the authorized credentials for the member.
- 7 To revoke credentials, to the right of the credentials you'd like to revoke, click **Revoke**.
- 8 Read the information, then click **I understand, revoke access for this token**.

Further reading

- "[About identity and access management with SAML single sign-on](#)"
- "[Viewing and managing a user's SAML access to your enterprise](#)"

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)