GitHub Docs

Enterprise administrators / Manage accounts and repositories / Manage users / View & manage SAML access

Viewing and managing a user's SAML access to your enterprise

In this article

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

> **Who can use this feature**
> Enterprise owners can view and manage a member's SAML access to an organization.

About SAML access to your enterprise account

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

If your enterprise is uses Enterprise Managed Users, your members will use accounts provisioned through your IdP. Managed user accounts will not use their existing user account on GitHub Enterprise Cloud. For more information, see "About Enterprise Managed Users."

Viewing and revoking a linked identity

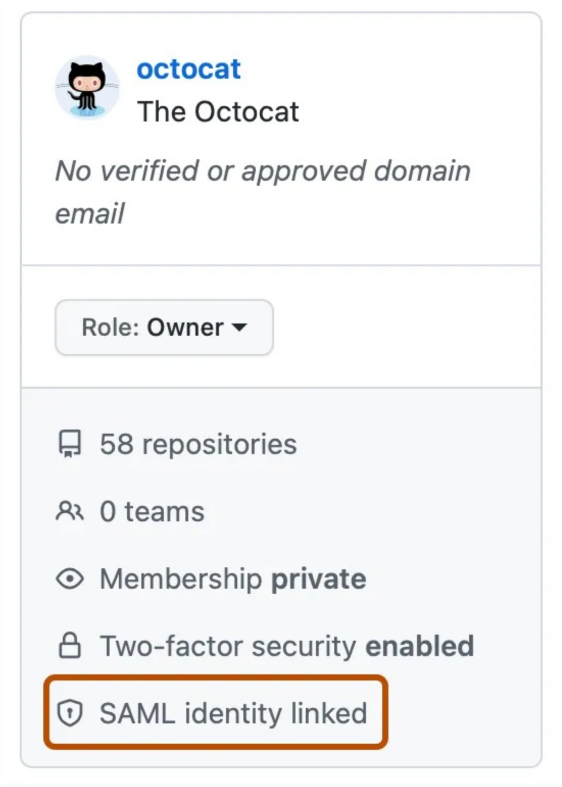
You can view the single sign-on identity that a member has linked to their account on GitHub.com.

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.

If your enterprise uses Enterprise Managed Users, you will not be able to deprovision or remove user accounts from the enterprise on GitHub Enterprise Cloud. Any changes you need to make to your enterprise's managed user accounts should be made through your IdP.

> **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 enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, 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**.



octocat
The Octocat

No verified or approved domain email

Role: Owner

58 repositories

0 teams

Membership **private**

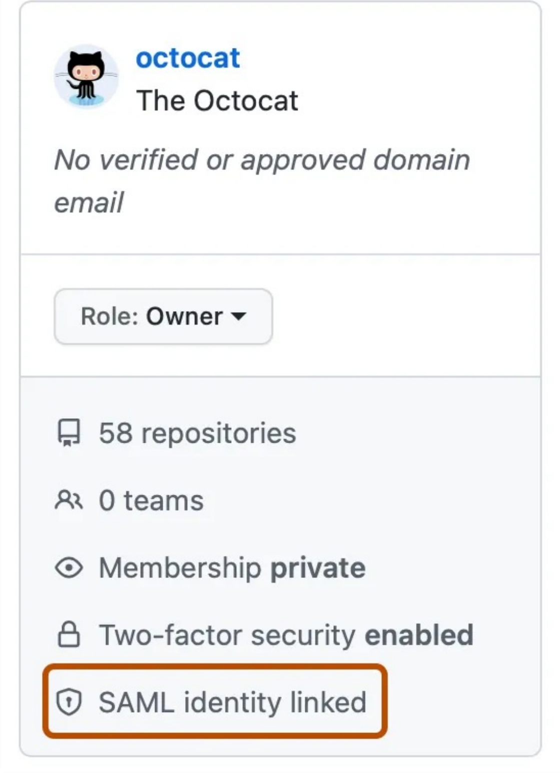
Two-factor security **enabled**

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 enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, 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**.



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 "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.

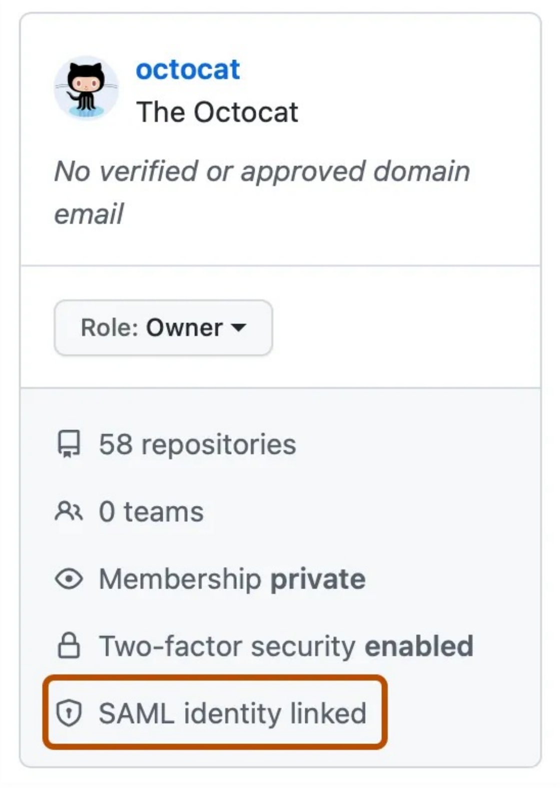
1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.

2. In the list of enterprises, click the enterprise you want to view.

3. In the enterprise account sidebar, 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

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

Legal

Terms Privacy Status Pricing Expert services Blog