# Configuring SAML single sign-on and SCIM using Okta

**In this article**



You can use Security Assertion Markup Language (SAML) single sign-on (SSO) and System for Cross-domain Identity Management (SCIM) with Okta to automatically manage access to your organization on GitHub.com.

> **Who can use this feature**
> Organization owners can configure SAML SSO and SCIM using Okta for an organization.

## About SAML and SCIM with Okta

You can control access to your organization on GitHub.com and other web applications from one central interface by configuring the organization to use SAML SSO and SCIM with Okta, an Identity Provider (IdP).

**Note:** To use SAML single sign-on, your organization must use GitHub Enterprise Cloud. For more information about how you can try GitHub Enterprise Cloud for free, see "Setting up a trial of GitHub Enterprise Cloud."

SAML SSO controls and secures access to organization resources like repositories, issues, and pull requests. SCIM automatically adds, manages, and removes members' access to your organization on GitHub.com when you make changes in Okta. For more information, see "About identity and access management with SAML single sign-on" and "About SCIM for organizations."

After you enable SCIM, the following provisioning features are available for any users that you assign your GitHub Enterprise Cloud application to in Okta.

| Feature | Description |
| --- | --- |
| Push New Users | When you create a new user in Okta, the user will receive an email to join your organization on GitHub.com. |
| Push User Deactivation | When you deactivate a user in Okta, Okta will remove the user from your organization on GitHub.com. |
| Push Profile Updates | When you update a user's profile in Okta, Okta will update the metadata for the user's |

| | |
|---|---|
| | membership in your organization on GitHub.com. |
| Reactivate Users | When you reactivate a user in Okta, Okta will send an email invitation for the user to rejoin your organization on GitHub.com. |

Alternatively, you can configure SAML SSO for an enterprise using Okta. SCIM for enterprise accounts is only available with Enterprise Managed Users. For more information, see "Configuring SAML single sign-on for your enterprise using Okta" and "Configuring SCIM provisioning for Enterprise Managed Users with Okta."

## Configuring SAML in Okta

1. In the Okta Dashboard, expand the **Applications** menu, then click **Applications**.
2. Click **Browse App Catalog**.
3. Search for the application named "GitHub Enterprise Cloud - Organization."
4. Click **Add Integration**.
5. Fill out the form, providing the name of your organization on GitHub and a unique name in the "Application Label" field.
6. Assign the application to your user in Okta. For more information, see Assign applications to users in the Okta documentation.
7. Under the name of the application, click **Sign on**.
8. Under "SIGN ON METHODS", click **View Setup Instructions**.
9. Enable and test SAML SSO on GitHub using the sign on URL, issuer URL, and public certificates from the "How to Configure SAML 2.0" guide. For more information, see "Enabling and testing SAML single sign-on for your organization."

## Configuring access provisioning with SCIM in Okta

To use SCIM with your organization, you must use a third-party-owned OAuth app. The OAuth app must be authorized by, and subsequently acts on behalf of, a specific GitHub user. If the user who last authorized this OAuth app leaves or is removed from the organization, SCIM will stop working. To avoid this issue, we recommend creating a dedicated user account to configure SCIM. This user account must be an organization owner and will consume a license.

1. Sign into GitHub.com using an account that is an organization owner and is ideally used only for SCIM configuration.
2. To create an active SAML session for your organization, navigate to `https://github.com/orgs/ORGANIZATION-NAME/sso`. For more information, see "About authentication with SAML single sign-on."
3. Navigate to Okta.
4. In the left sidebar, use the **Applications** dropdown and click **Applications**.
5. In the list of applications, click the label for the application you created for the organization that uses GitHub Enterprise Cloud.

6. Under the name of the application, click **Provisioning**.
7. Click **Configure API Integration**.
8. Select **Enable API integration**.
9. Click **Authenticate with GitHub Enterprise Cloud - Organization**.
10. To the right of your organization's name, click **Grant**.
11. Click **Authorize OktaOAN**.
12. Click **Save**.
13. To avoid syncing errors and confirm that your users have SAML enabled and SCIM linked identities, we recommend you audit your organization's users. For more information, see "Troubleshooting identity and access management for your organization."
14. To the right of "Provisioning to App", click **Edit**.
15. To the right of "Create Users," select **Enable**.
16. To the right of "Update User Attributes," select **Enable**.
17. To the right of "Deactivate Users," select **Enable**.
18. Click **Save**.

## Further reading

- "Configuring SAML single sign-on for your enterprise using Okta"
- Understanding SAML in the Okta documentation
- Understanding SCIM in the Okta documentation