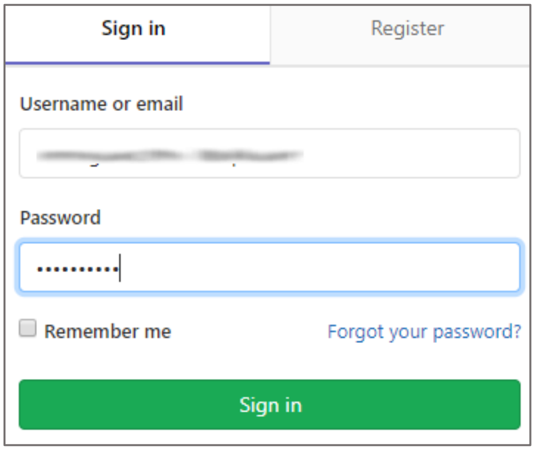
Configure GitLab for Single Sign-On

Configuring GitLab for single sign-on (SSO) enables administrators to manage users of Citrix Gateway service. Users can securely log on to GitLab by using the enterprise credentials.

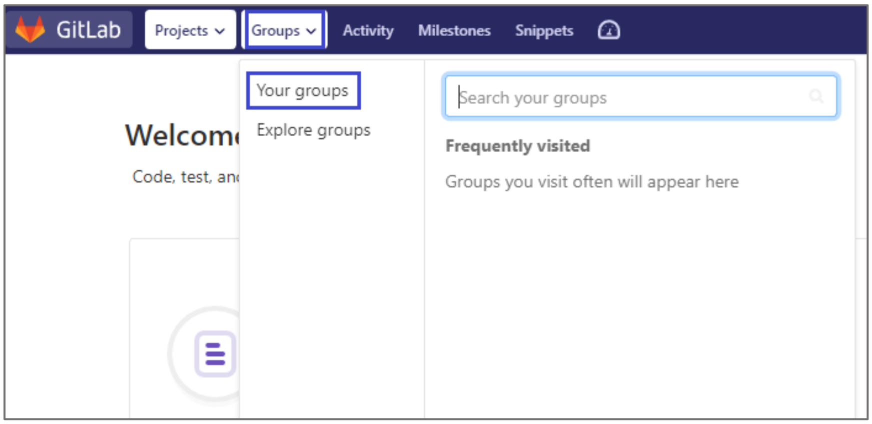
To configure GitLab for SSO by using SAML:

1. In a browser, type https://gitlab.com/users/sign_in and press **Enter**.

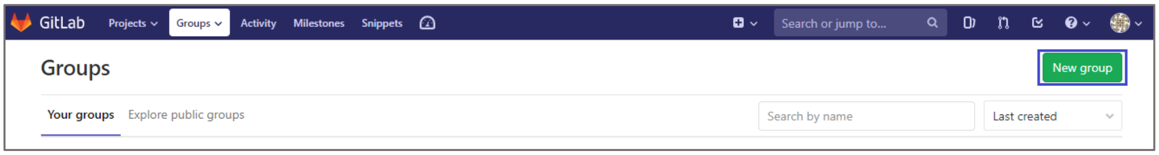
2. Enter your GitLab admin account credentials (**Username or Email** and **Password**) and click **Sign in**.



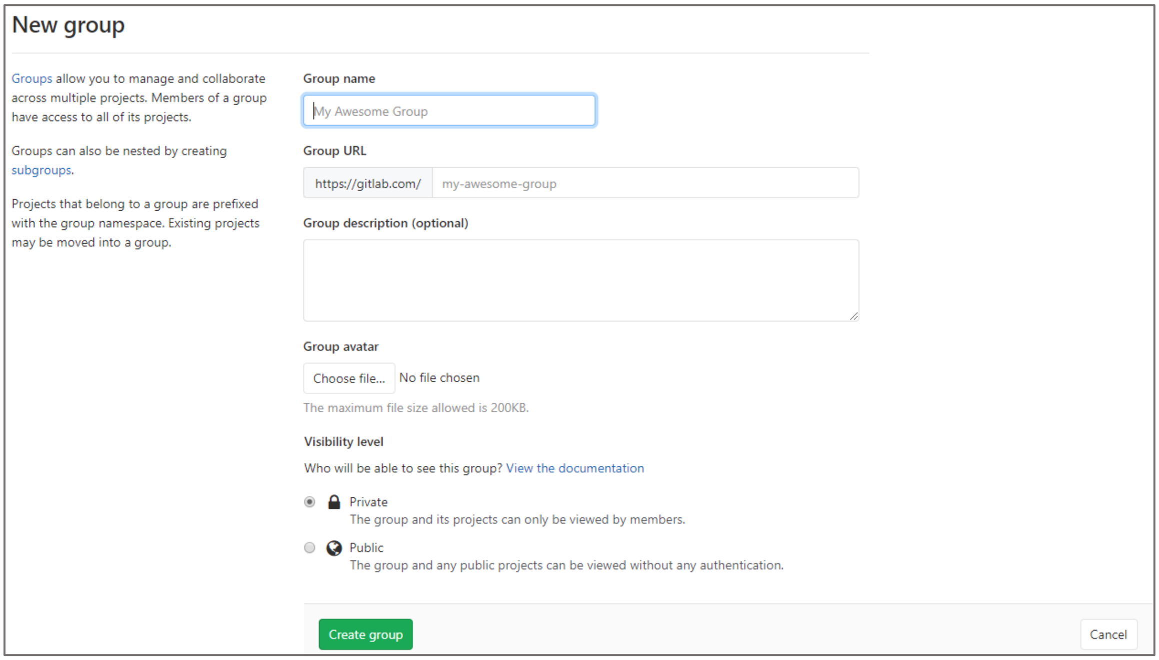
3. In the dashboard page, click **Groups** > **Your groups**.



4. In the **Groups** page, click **New group**.



5. In the **New group** page, enter the group details and click **Create group**.



New group

Groups allow you to manage and collaborate across multiple projects. Members of a group have access to all of its projects.

Groups can also be nested by creating subgroups.

Projects that belong to a group are prefixed with the group namespace. Existing projects may be moved into a group.

Group name: My Awesome Group

Group URL: https://gitlab.com/ my-awesome-group

Group description (optional)

Group avatar

The maximum file size allowed is 200KB.

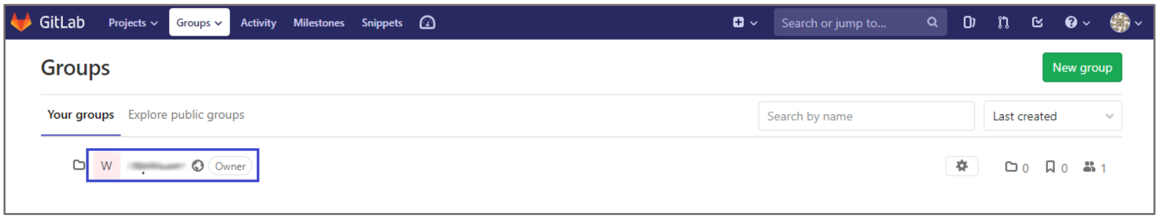
Visibility level

Who will be able to see this group? View the documentation

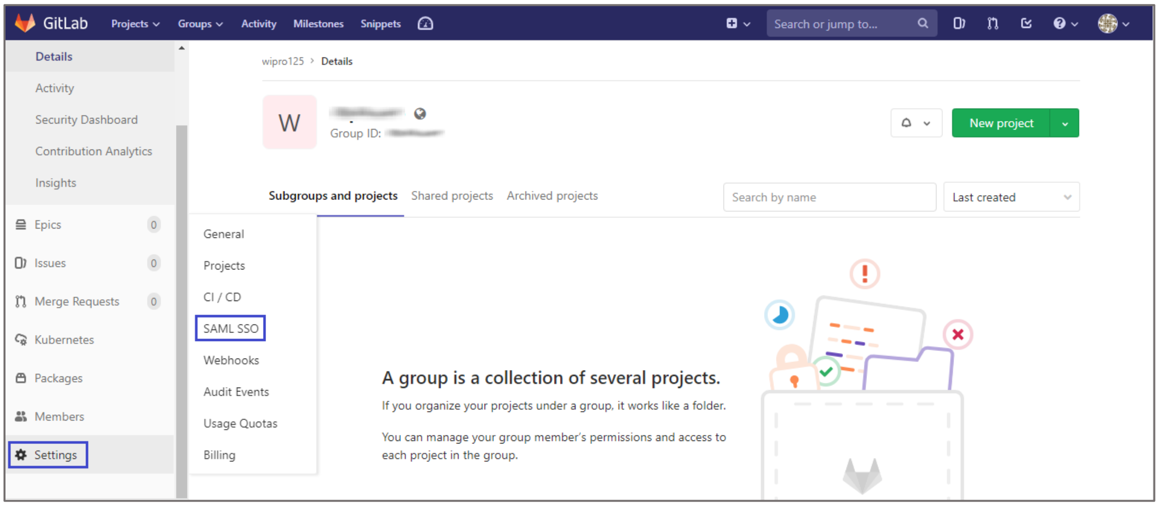
● Private
The group and its projects can only be viewed by members.

○ Public
The group and any public projects can be viewed without any authentication.

6. In the **Groups** page, click your group name.



7. In the left pane, click **Settings** > **SAML SSO**.



[redacted]

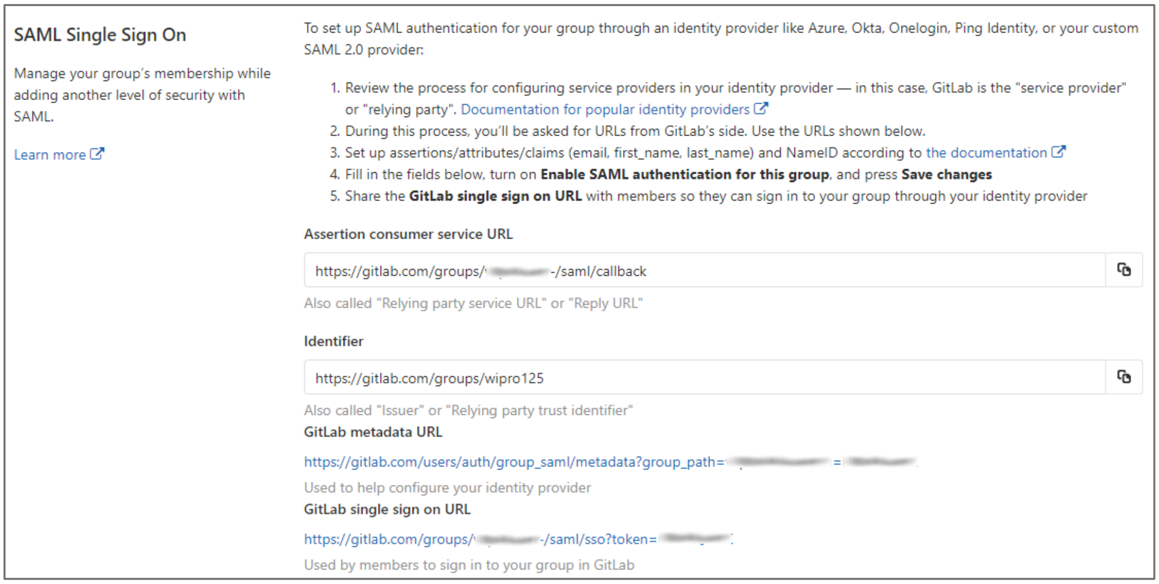
Group ID: [redacted]

A group is a collection of several projects.

If you organize your projects under a group, it works like a folder.

You can manage your group member's permissions and access to each project in the group.

8. In the **SAML Single Sign On** page, copy the **Assertion consumer service URL**, **Identifier**, **GitLab metadata URL**, and **GitLab single sign on URL** for IdP configuration



SAML Single Sign On

Manage your group's membership while adding another level of security with SAML.

Learn more

To set up SAML authentication for your group through an identity provider like Azure, Okta, Onelogin, Ping Identity, or your custom SAML 2.0 provider:

1. Review the process for configuring service providers in your identity provider — in this case, GitLab is the "service provider" or "relying party". Documentation for popular identity providers
2. During this process, you'll be asked for URLs from GitLab's side. Use the URLs shown below.
3. Set up assertions/attributes/claims (email, first_name, last_name) and NameID according to the documentation
4. Fill in the fields below, turn on **Enable SAML authentication for this group**, and press **Save changes**
5. Share the **GitLab single sign on URL** with members so they can sign in to your group through your identity provider

Assertion consumer service URL

https://gitlab.com/groups/[redacted]-/saml/callback

Also called "Relying party service URL" or "Reply URL"

Identifier

https://gitlab.com/groups/wipro125

Also called "Issuer" or "Relying party trust identifier"

GitLab metadata URL

https://gitlab.com/users/auth/group_saml/metadata?group_path=[redacted]=[redacted]

Used to help configure your identity provider

GitLab single sign on URL

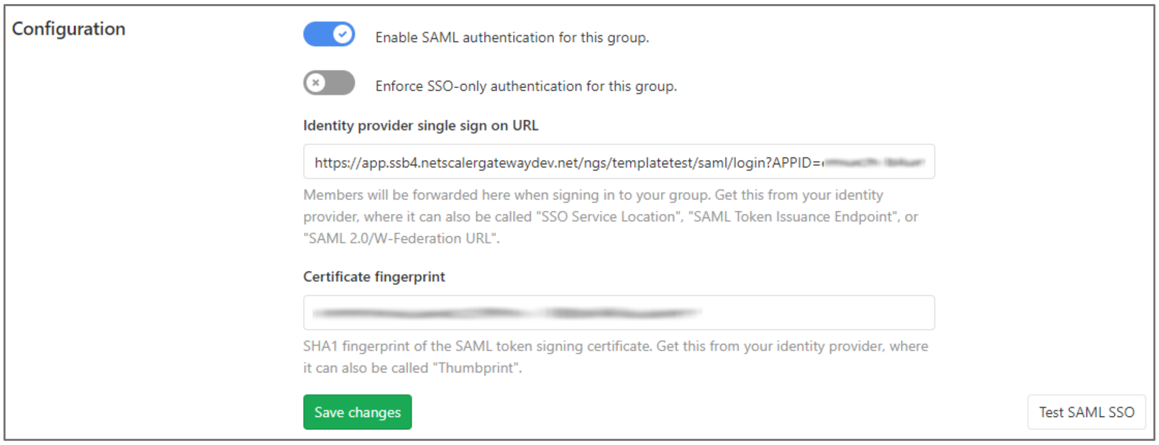
https://gitlab.com/groups/[redacted]-/saml/sso?token=[redacted]

Used by members to sign in to your group in GitLab

9. Scroll down and turn on the **Enable SAML authentication for this group** toggle button.

10. Enter the values for the following fields:

Required Information	Description
Identity provider single sign on URL	IdP logon URL
Certificate fingerprint	Copy and paste the generated certificate fingerprint. **Note:** The IdP metadata is provided by Citrix and can be accessed from the link below: https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/<app_id>/idp_metadata.xml



Configuration

● Enable SAML authentication for this group.

○ Enforce SSO-only authentication for this group.

Identity provider single sign on URL

https://app.ssb4.netscalergatewaydev.net/ngs/templatetest/saml/login?APPID=[redacted]

Members will be forwarded here when signing in to your group. Get this from your identity provider, where it can also be called "SSO Service Location", "SAML Token Issuance Endpoint", or "SAML 2.0/W-Federation URL".

Certificate fingerprint

[redacted]

SHA1 fingerprint of the SAML token signing certificate. Get this from your identity provider, where it can also be called "Thumbprint".

11. Click **Save changes**.