

Configuring Sentry

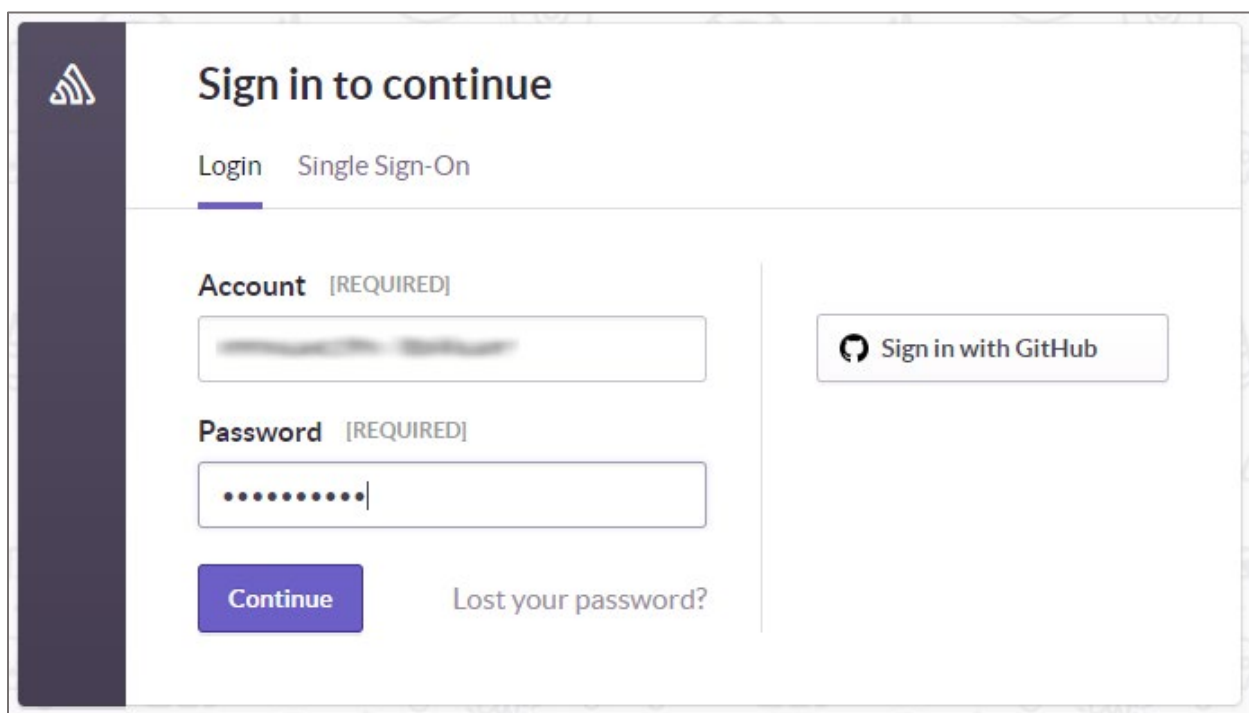
Configuring Sentry for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Sentry by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

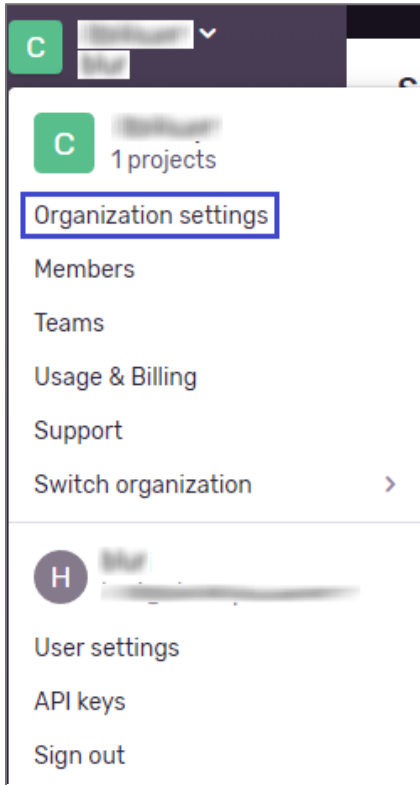
To configure Sentry for SSO by using SAML:

1. In a browser, type <https://sentry.io> and press **Enter**.
2. Type your Sentry account credentials (**Account** and **Password**) and click **Continue**.

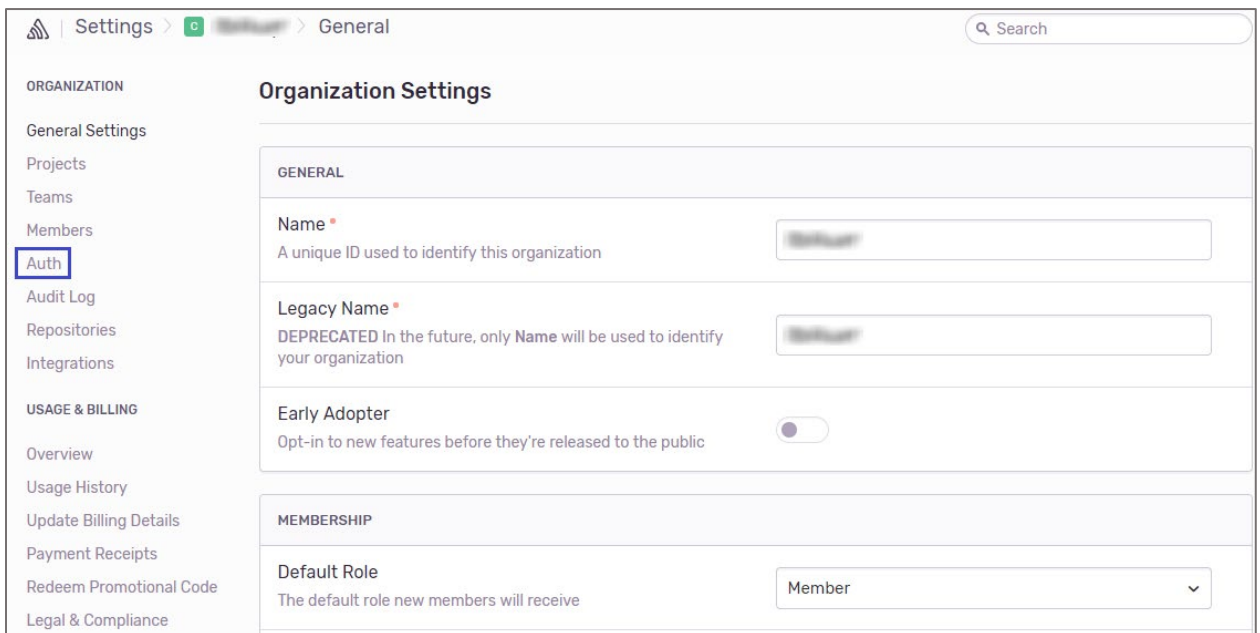


The screenshot shows the Sentry login interface. At the top left is the Sentry logo. The main heading is "Sign in to continue". Below this, there are two tabs: "Login" and "Single Sign-On", with "Single Sign-On" being the active tab. The form contains two input fields: "Account [REQUIRED]" and "Password [REQUIRED]". The "Account" field has a blurred value, and the "Password" field has a masked value of ".....". To the right of these fields is a button labeled "Sign in with GitHub". At the bottom left of the form is a blue "Continue" button, and to its right is a link that says "Lost your password?".

3. In the top-left corner, click the user account and select **Organization settings** from the drop-down menu.



4. In the left panel, click **Auth** under **General Settings**.



- In the **SAML2 Authentication** page, enter the values for the following fields under **Attribute Mappings** and **General Settings**.

Field Name	Description
IdP UserID	UserID
User Email	Email
First Name	Optional
Last Name	Optional
Require SSO	Select this check box to help users access the organization through SSO.
Default Role	Select the respective role from the drop-down list.

Attribute Mappings

IdP User ID [REQUIRED]

The IdPs unique ID attribute key for the user. This is what Sentry will used to identify the users identity from the identity provider.

User Email [REQUIRED]

The IdPs email address attribute key for the user. Upon initial linking this will be used to identify the user in

First Name

Last Name

General Settings

Require SSO

Require members use a valid linked SSO account to access this organization

Default Role [REQUIRED]

The default role new members will receive when logging in for the first time.

Save Settings