

Configure Built.io for Single Sign-On

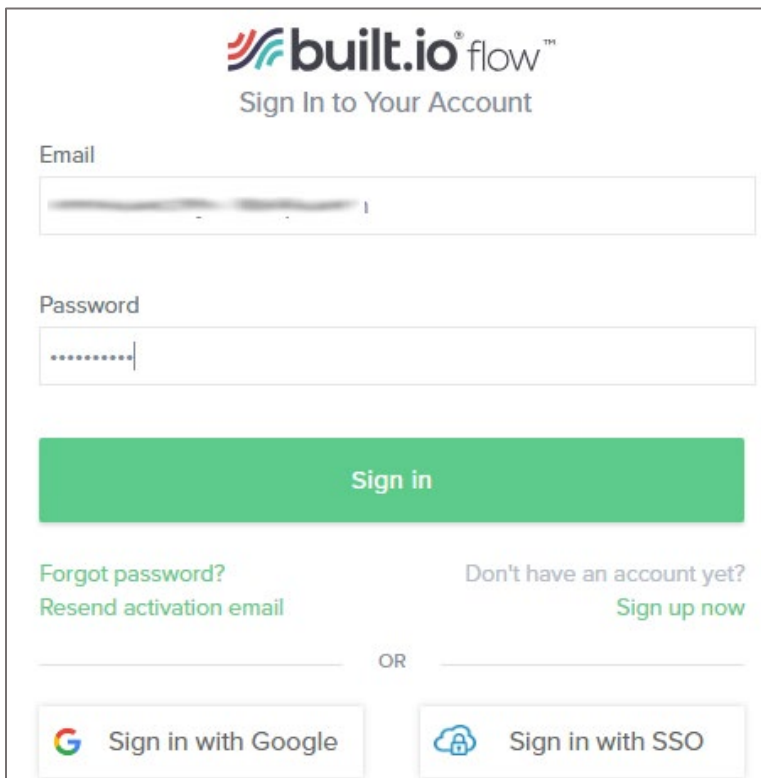
Configuring Built.io for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Built.io by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

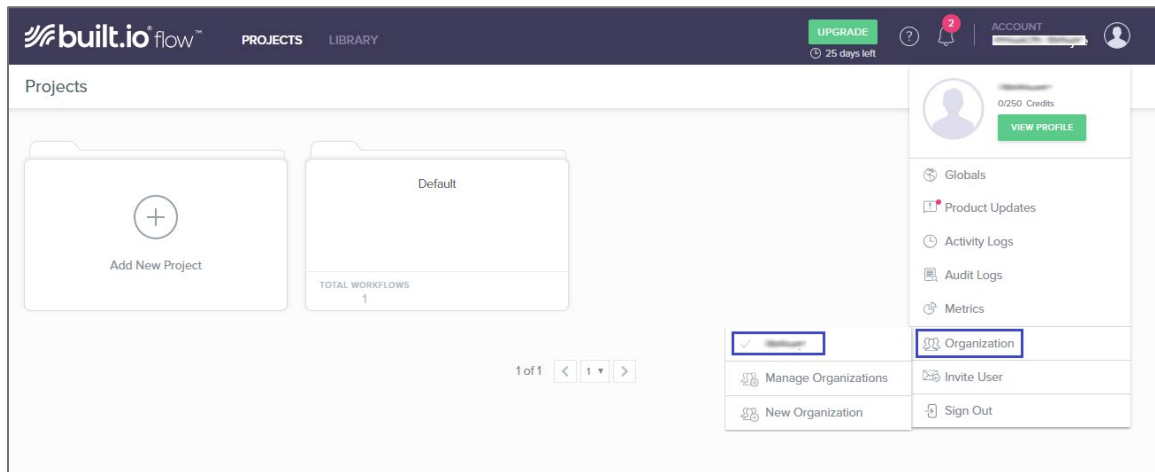
To configure Built.io for SSO by using SAML:

1. In a browser, type <https://www.built.io/> and press **Enter**.
2. Type your Built.io admin account credentials (**Email** and **Password**) and click **Sign in**.

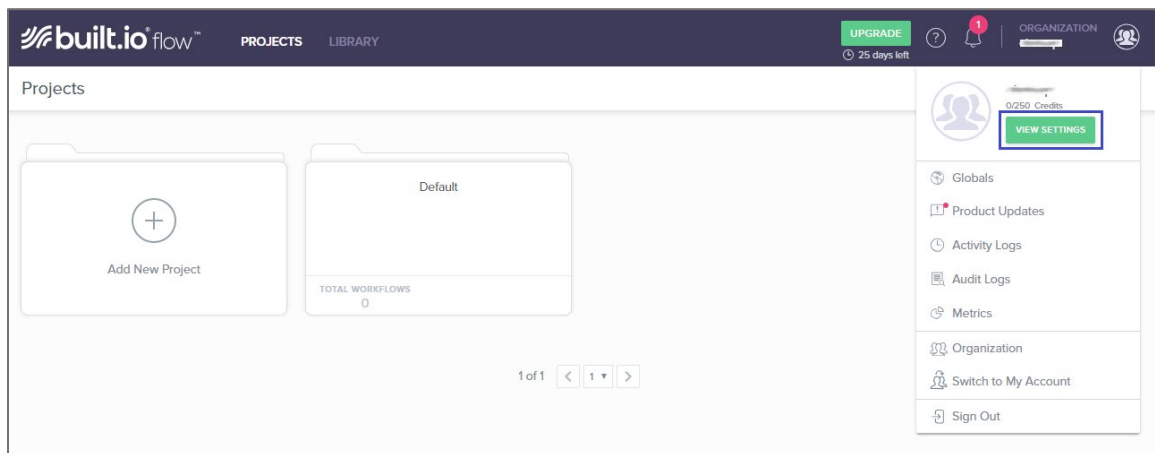


The image shows the Built.io flow sign-in page. At the top is the Built.io flow logo with the text "Sign In to Your Account". Below this are two input fields: "Email" and "Password". The "Email" field contains a blurred email address, and the "Password" field contains a series of dots. Below the input fields is a large green "Sign in" button. Underneath the button are two links: "Forgot password? Resend activation email" on the left and "Don't have an account yet? Sign up now" on the right. Below these links is a horizontal line with the word "OR" in the center. At the bottom are two buttons: "Sign in with Google" (with the Google logo) and "Sign in with SSO" (with a cloud and lock icon).

3. In the dashboard page, click the username in the top-right corner.
4. Hover the cursor over **Organization** and select the organization name.



5. In the organization page, click the organization name in the top-right corner and select **VIEW SETTINGS**.



6. In the **Organization Settings** page, click **SINGLE SIGN-ON** from the left panel.

Organization Settings

Organization Trial Plan

PLANS

ROLES

USERS

SINGLE SIGN-ON

TRIAL PLAN	BUSINESS \$599/month <i>Billed Annually</i>	PRO \$1,499/month <i>Billed Annually</i>	ENTERPRISE
2 ✓ Triggers ⓘ	10 ✓ Triggers ⓘ	25 ✓ Triggers ⓘ	Looking for more? Enterprise plans are tailored according to the needs ✓ Unlimited Workflows, Triggers, Credits
250 ✓ Credits ⓘ	25,000/month ✓ Credits ⓘ	100,000/month ✓ Credits ⓘ	
2 ✓ Active Workflows ⓘ	10 ✓ Active Workflows ⓘ	25 ✓ Active Workflows ⓘ	

7. Enter the values for the following fields:

Field Name	Description
Single Sign-On URL	IdP logon URL
Entity ID	Issuer URL
Signature Algorithm	Select SHA-26 from the drop-down list.
Public Key Certificate	<p>Upload the IdP certificate.</p> <p>Note: The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app.</p> <p><a href="https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml">https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml</p>

SINGLE SIGN-ON

Single Sign-On (SSO) is a mechanism that allows users to authenticate only once using their SAML identity provider login credentials, and automatically log in to multiple applications.

If Single Sign-On is enabled for this organization, the users of this organization will be required to sign into Built.io Flow using their organization name and SAML identity provider login details. Owners, however, are allowed to sign in using Built.io Flow credentials (without single sign-on).

Assertion Consumer Service (ACS) URL

Identifier Format

Single Sign-On URL (required)

Entity ID (required)

Signature Algorithm

Public Key Certificate (required)

saml_cert.cer

Private Key Certificate

Session Duration in Hours

Notes

SAML Version
Version 2.0

Attribute
first_name, last_name, email

Name Id Format
Email

TEST

DISABLE SSO

Note: Note down the **Assertion Consumer Service (ACS) URL**, **Attribute**, and **Name Id Format** for IdP configuration.

8. Click **TEST**.
9. Finally, click **ENABLE SSO**.