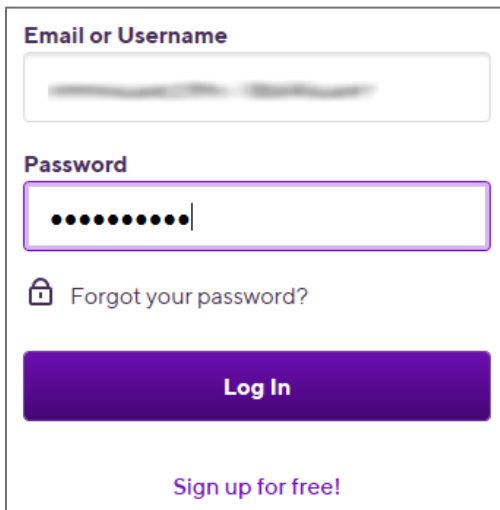# Configure Bitrise for Single Sign-On

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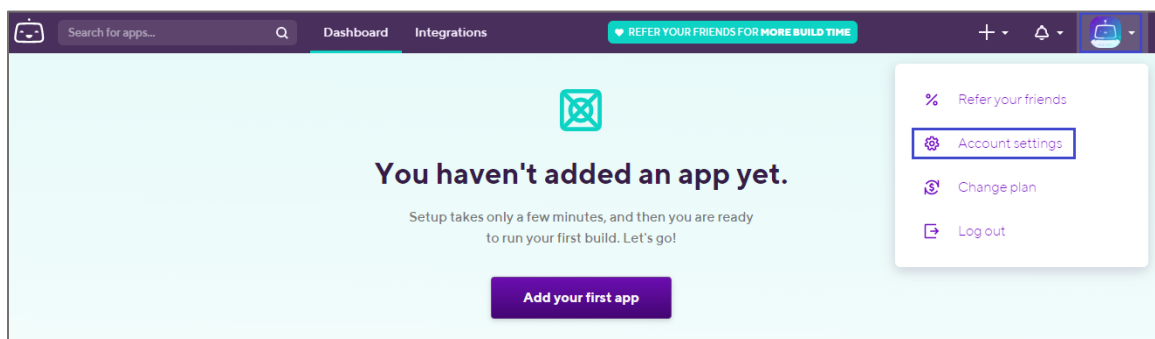
Prerequisite

Browser Requirements: Internet Explorer 11 and above

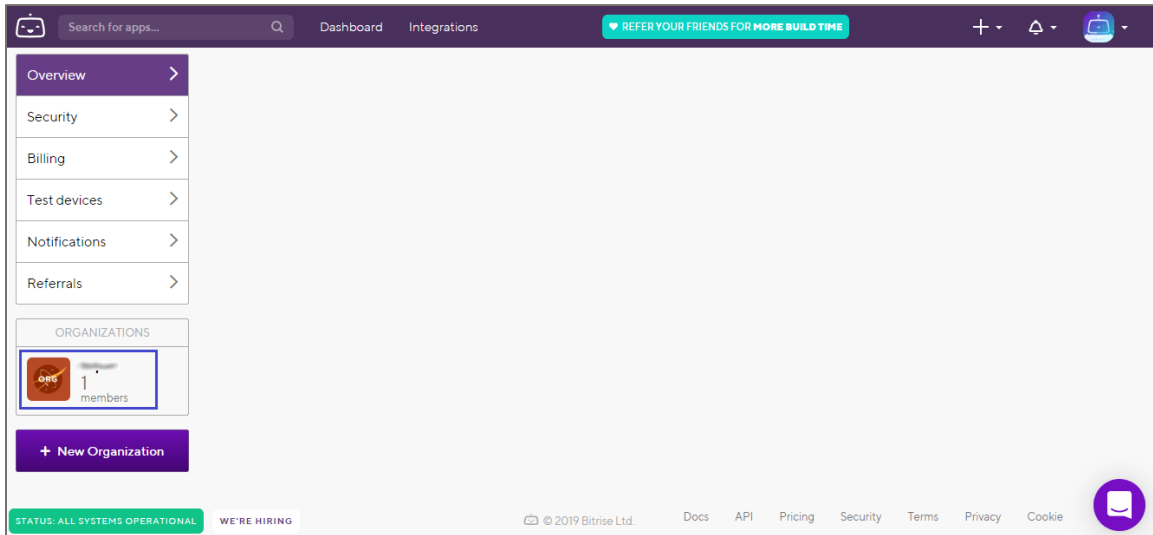**To configure Bitrise for SSO by using SAML:**

1. In a browser, type https://app.bitrise.io/users/sign_in and press **Enter**.

2. Type your Bitrise admin account credentials (**Email or Username** and **Password**) and click **Log In**.
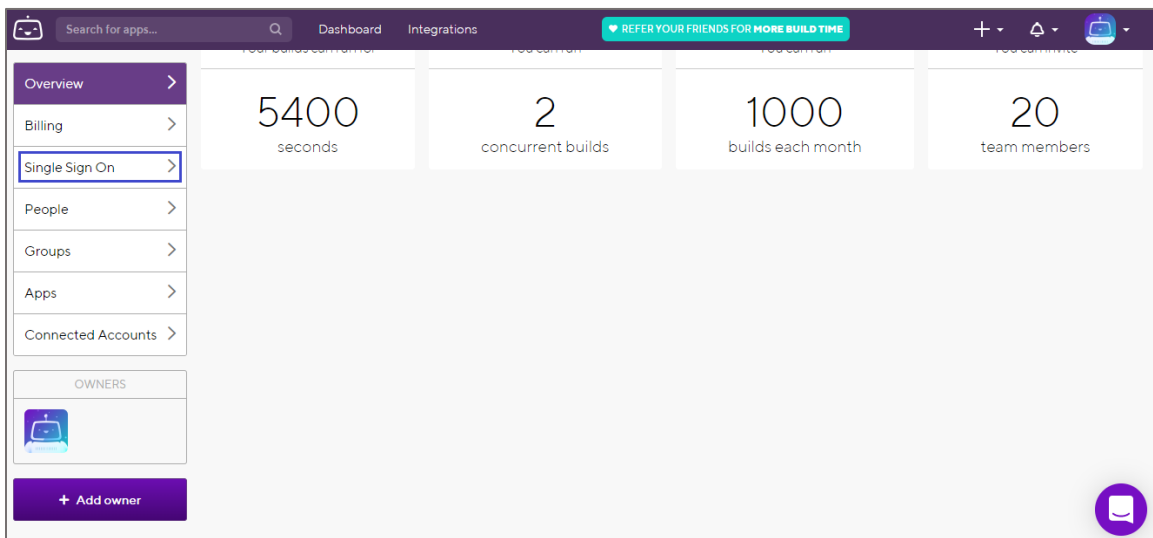

3. In the dashboard page, click the user account in the top-right corner and select **Account settings**.

4. In the left pane, click the organization name.

5. In the left pane, click **Single Sign On**.

6. Enter the values for the following fields:

Required Information	Description
Single Sign-On URL	IdP logon URL
Identity provider sign-on URL	IdP logon URL
Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with - - - - -Begin Certificate- - - - - and - - - - -End Certificate- - - - - **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. https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml

Enable Single Sign-On

1 To connect Bitrise to your SSO provider, log in to your identity provider and add Bitrise as an application.
For getting the required credentials, you'll need the URL below.

Single Sign-On URL

https://app.bitrise.io/users/auth/saml/callback?organizat...   **Copy Link**

2 Add your Single Sign-On credentials here. You've received a URL and a Certificate from your provider, paste those below.

Identity provider sign-on URL:

Certificate:

After pressing Configure SSO, all the members of this Org will be signed out and be prompted to sign in again via the added SSO service.

Configure SSO

7. Finally, click **Configure SSO**.