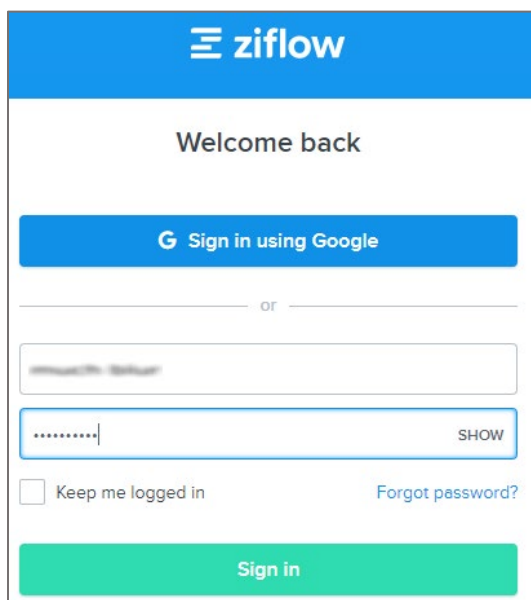# Configure Ziflow for Single Sign-On

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

Prerequisite

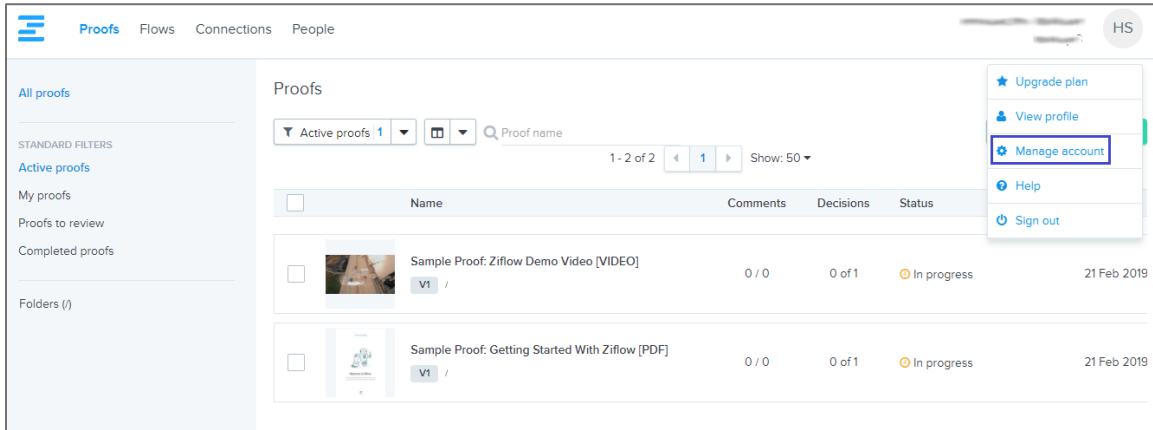Browser Requirements: Internet Explorer 11 and above

To configure Ziflow for SSO by using SAML:

1. In a browser, type https://www.ziflow.io/#/login/ and press **Enter**.

2. Type your Ziflow admin account credentials (**E-mail address** and **Password**) and click **Sign in**.

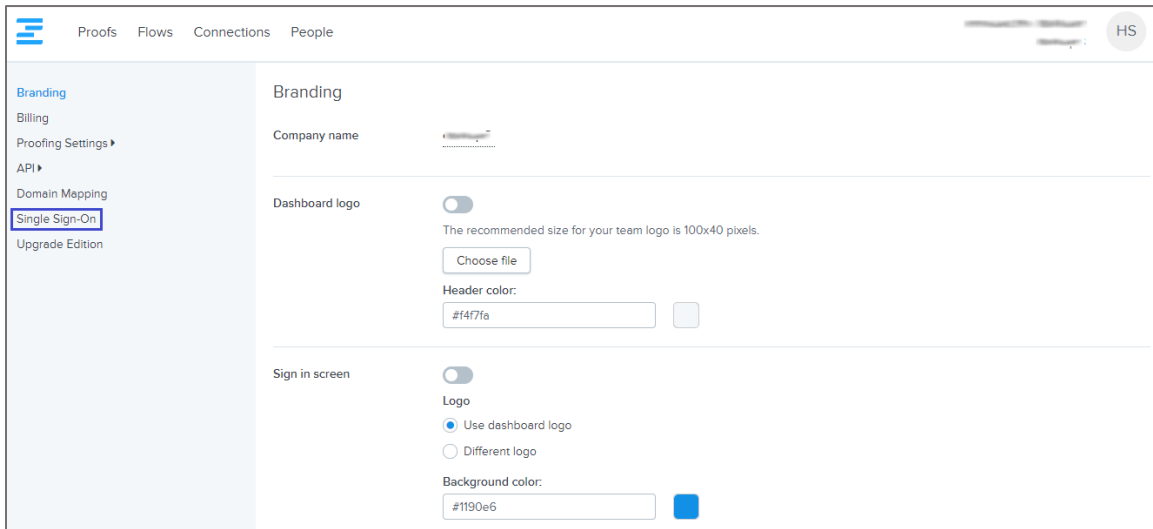3. In the dashboard page, click the user account in the top-right corner and select **Manage account**.

4. Click **Single Sign-On** from the left pane.

5. In the **Single Sign-On** page, enter the values for the following fields:

Required Information	Description
Type	Select **SAML 2.0** from the drop-down list.
Sign In URL	IdP logon URL
X509 Signing 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

Sign Out URL	IdP logon URL
Binding Protocol	Select **HTTP-POST** from the drop-down list.

Note: Note down the **Callback URL** and **Settings** for IdP configuration.

6. Turn on the **Single Sign-On** toggle button.