

Configure Float for Single Sign-On

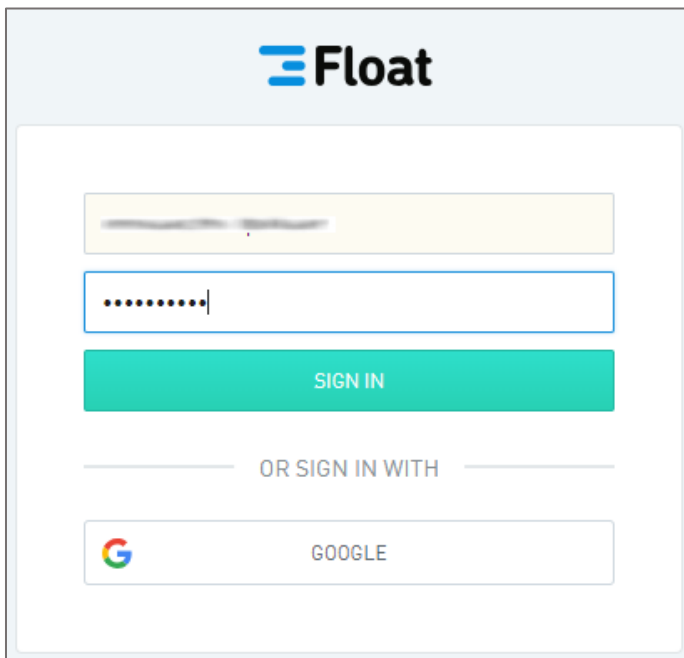
Configuring Float for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Float by using the enterprise credentials.

Prerequisite

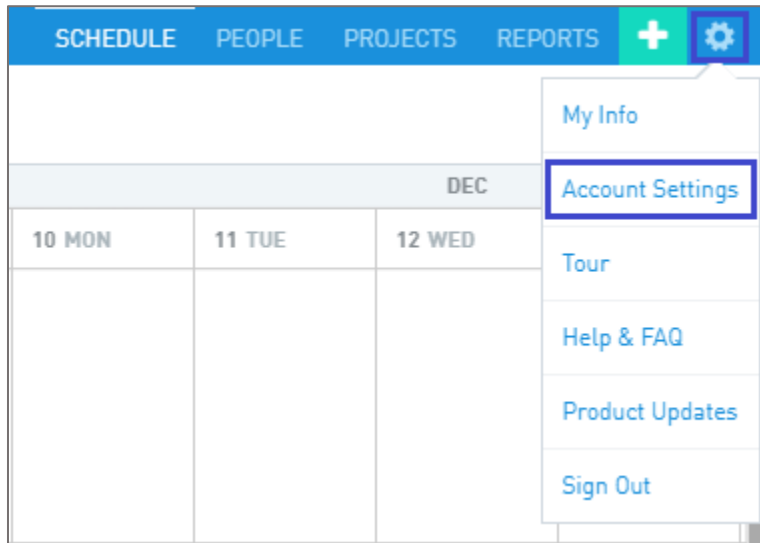
Browser Requirements: Internet Explorer 11 and above

To configure Float for SSO by using SAML:

1. In a browser, type <https://login.float.com/login> and press **Enter**.
2. Type your Float admin account credentials (**Email** and **Password**) and click **SIGN IN**.

A screenshot of the Float login interface. At the top, the 'Float' logo is displayed in a light blue header. Below the logo, there is a login form with a yellow background. The form contains two input fields: the first for an email address (partially obscured by a blurred image) and the second for a password (represented by dots). Below these fields is a prominent teal 'SIGN IN' button. Underneath the button, the text 'OR SIGN IN WITH' is centered, followed by a button featuring the Google logo and the word 'GOOGLE'.

3. In the dashboard page, click the Settings icon from the top-right corner and select **Account Settings**.



4. In the **General Settings** page, scroll down and click **CONFIGURE** under **Authentication**.

Account Owner

The Account Owner is the only person who can view this page, access the API key, billing details, upgrade and downgrade plans. You can transfer ownership.

Account Owner

[TRANSFER](#)

Authentication

Float supports SAML-based single-sign on (SSO) using [OneLogin](#) and [Okta](#). Get started by selecting Float from your identity provider's application directory or [learn more about setting up SSO](#).

[CONFIGURE](#)

Delete Team

Deleting a Float team cannot be undone. All data will be deleted and irretrievable. [Delete team](#)

5. In the **Configure SAML Authentication** pop-up window, enter the values for the following fields:

Required Information	Description
SAML 2.0 Endpoint URL (HTTP)	IdP logon URL
Identity Provider Issuer	Issuer URL
X.509 Certificate	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate-----</p> <p>Note: The IdP metadata URL 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>

Configure SAML Authentication

SAML 2.0 Endpoint URL (HTTP)

Identity Provider Issuer

X.509 Certificate

As soon as you're authenticated, your team will be able to sign in from your identity provider and a SAML button added to your Float login page. They will continue to maintain the option to sign in using email and password.

SAVE

CANCEL

6. Finally, click **SAVE**.