

# Configure 10,000ft for Single Sign-On

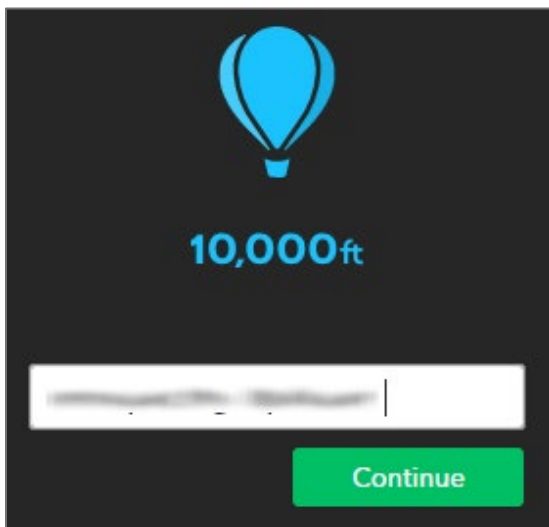
Configuring 10,000ft for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to 10,000ft by using the enterprise credentials.

## Prerequisite

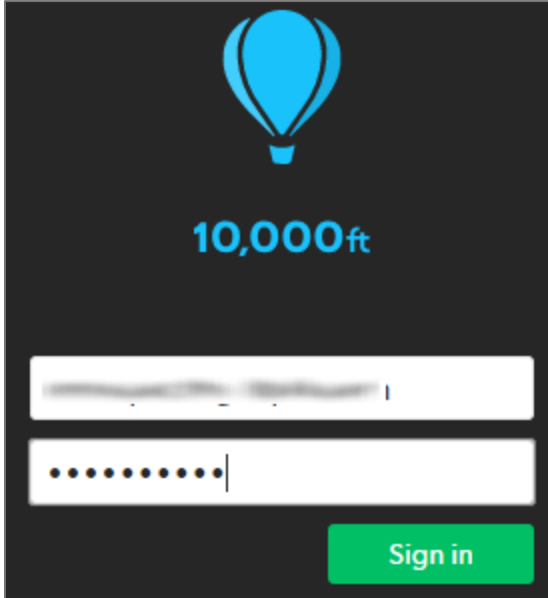
Browser Requirements: Internet Explorer 11 and above

## To configure 10,000ft for SSO by using SAML:

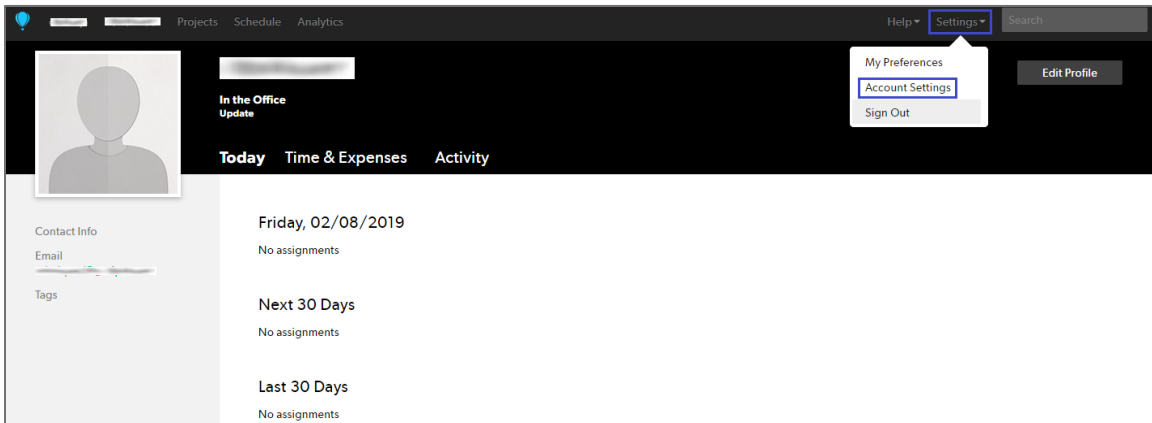
1. In a browser, type <https://app.10000ft.com/si> and press **Enter**.
2. Type your 10,000ft email address and click **Continue**.



3. Type your 10,000ft password and click **Sign in**.



4. In the dashboard page, click **Settings** in the top-right corner and select **Account Settings**.



5. Click **SSO** in the left pane and enter the values for the following:

Required Information	Description
Sign in (SSO) target URL	IdP logon URL
Sign out (SLO) target URL	IdP logout URL
Certificate	Upload the IdP certificate. <b>Note:</b> 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](https://gateway.cloud.com/idp/saml/<citrixcloudcust id>/<app id>/idp_metadata.xml)

## SSO

My Preferences

Account Settings

Billing

Roles

Disciplines

Bill Rates

People

Placeholders

Project Import

Phase Names

Work Status

Expense Categories

Time & Fee Categories

Official Holidays

Clients

Locations

Leave Types

People Tags

Project Tags

Developer API (Pro)

Project Custom Fields (Pro)

People Custom Fields (Pro)

**SSO (Pro)**

Sign in (SSO) target URL

Sign out (SLO) target URL

Certificate must be PEM encoded .pem, .crt or .cer file.

**Replace Certificate File**

Auto-provision authenticated users not in account (account created with email only)

**Cancel** **Save**

6. Finally, click **Save**.