

Configure Miro for Single Sign-On

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

Prerequisite

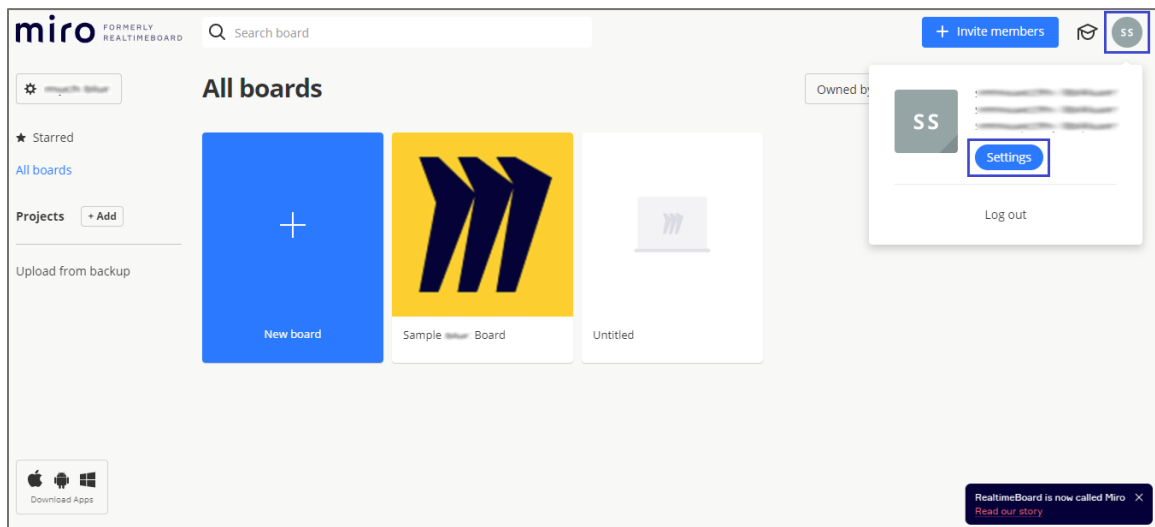
Browser Requirements: Internet Explorer 11 and above

To configure Miro for SSO by using SAML:

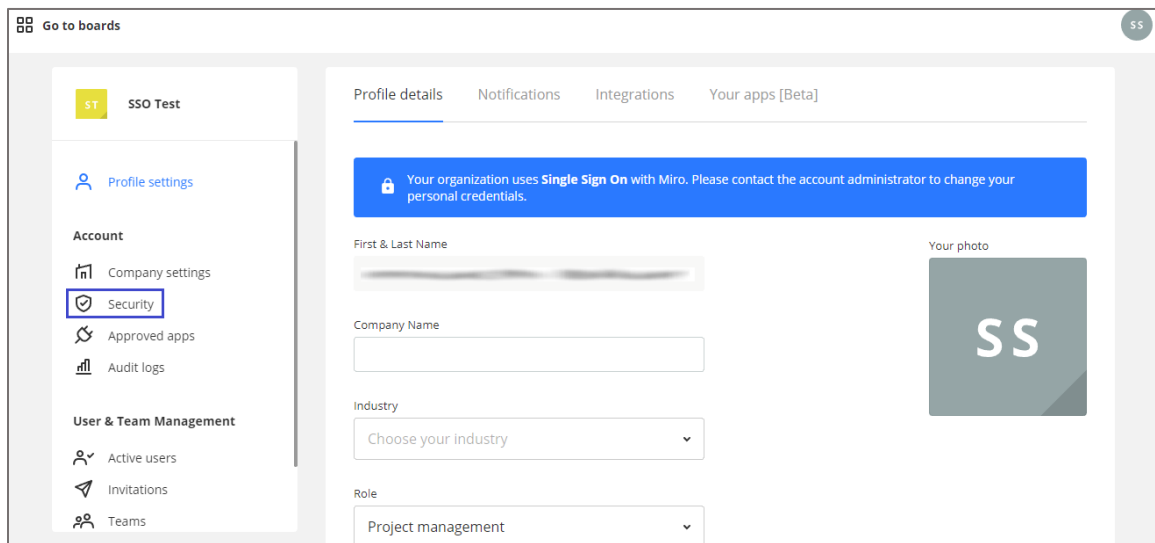
1. In a browser, type <https://miro.com/login/> and press **Enter**.
2. Type your Miro admin account credentials (**Work email** and **Password**) and click **Sign in**.

A screenshot of the Miro 'Sign in' page. The page has a white background with a light blue header area. The title 'Sign in' is in a large, dark blue font. Below the title, there are two input fields. The first field is for an email address, indicated by an envelope icon on the left, and contains a blurred email address. The second field is for a password, indicated by a lock icon on the left, and contains a series of dots. Below the password field, there is a link that says 'Forgot password?'. At the bottom of the form, there is a large blue button with the text 'Sign in' in white.

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



4. Click **Security** from the left pane.



5. Turn on the **Enable SSO/SAML** toggle button and enter the values for the following fields:

Required Information	Description
SAML Sign-in URL	IdP logon URL
Key x509 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. <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
Domains	Organization domain

Security

☒ **Enable SSO/SAML**

All users on the Company plan will authenticate using SSO (personal login credentials will no longer work).

SAML Sign-in URL

Key x509 Certificate

Domains

☐ Automatically add all newly registered users from the listed domains to your Company Account

Choose a default team for newly registered users

Choose

Save

Cancel

6. Finally, click **Save**.