

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

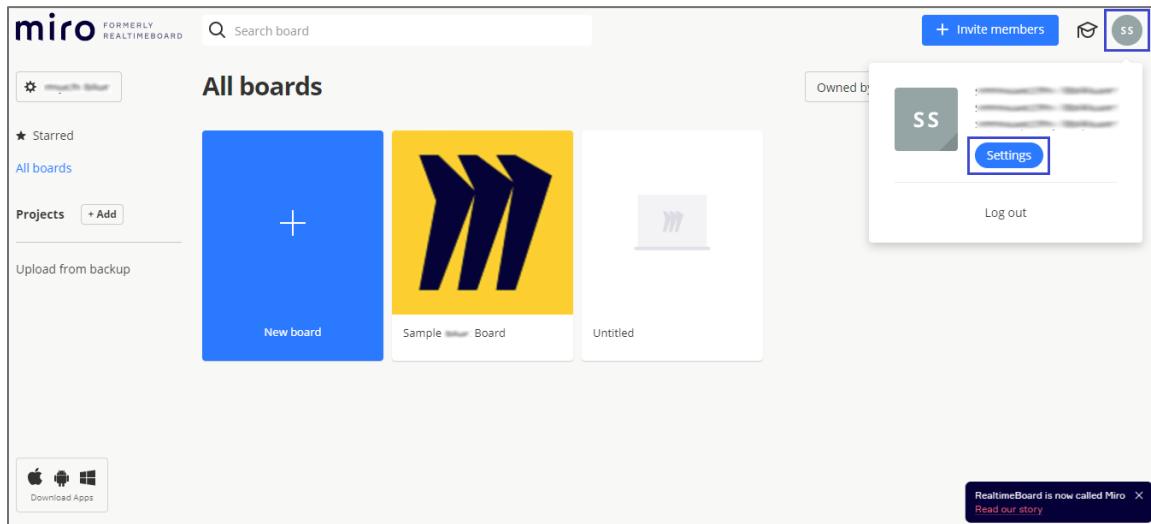
To configure Miro for SSO by using SAML:

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**.

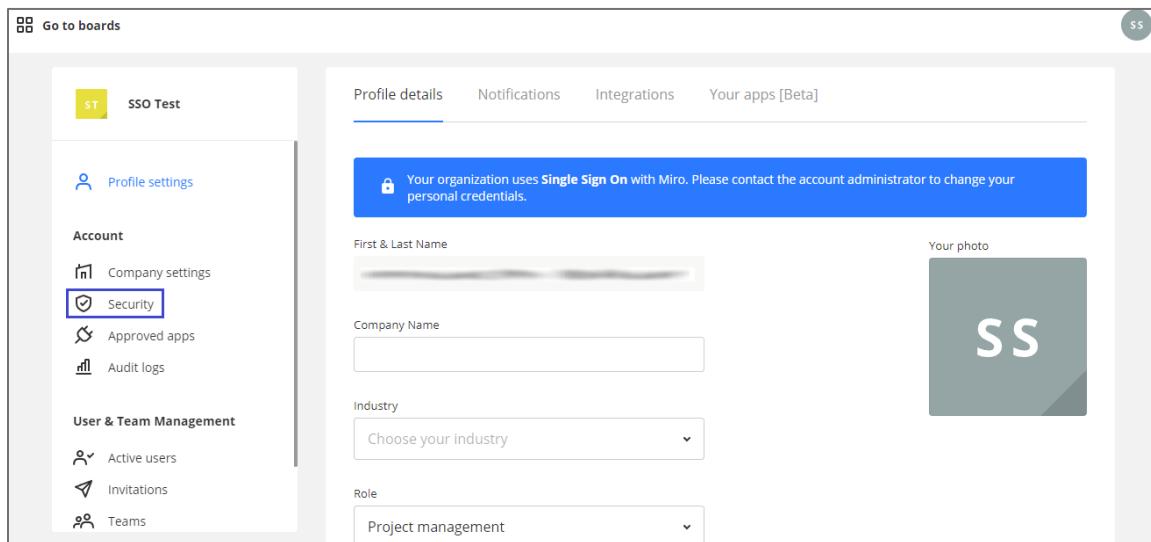


The image shows the Miro Sign in page. It features a large 'Sign in' header at the top. Below it are two input fields: the top one for 'Work email' (with a placeholder 'Email' and a blurred input field) and the bottom one for 'Password' (with a placeholder 'Password' and a blurred input field). Below the password field is a 'Forgot password?' link. At the bottom is a large blue 'Sign in' button.

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	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with</p> <p>-----Begin Certificate----- and -----End Certificate-----</p> <p>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.</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>
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

Specify email domains to be allowed to authenticate via your SAML server. We need a list of all the email domains that your users will be using to access Miro. Public domains (e.g., gmail.com, outlook.com, etc.) are not permitted.

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

Choose a default team for newly registered users

Save **Cancel**

6. Finally, click **Save**.