

# Configure Monday.com for Single Sign-On

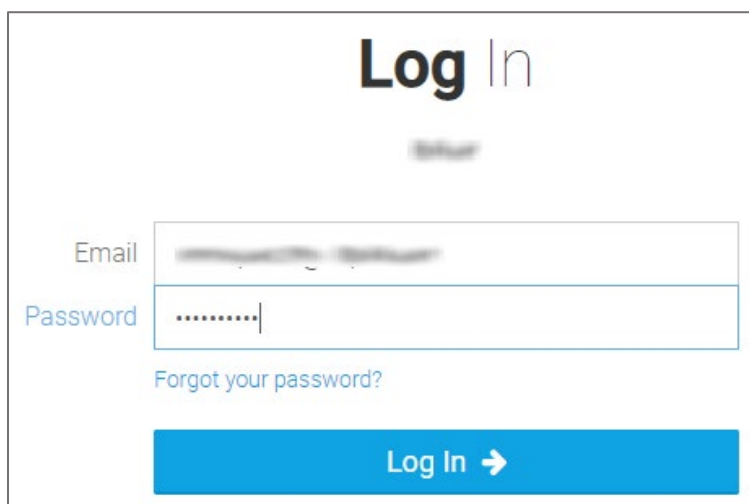
Configuring Monday.com for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Monday.com by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

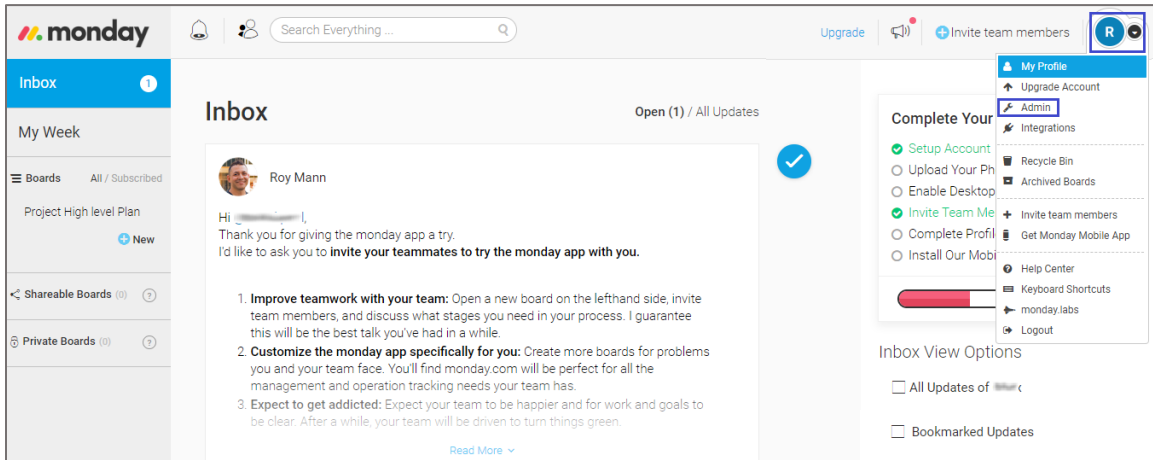
## To configure Monday.com for SSO by using SAML:

1. In a browser, type <https://<customer domain>.monday.com/> and press **Enter**.
2. Type your Monday.com admin account credentials (**Email** and **Password**) and click **Log In**.

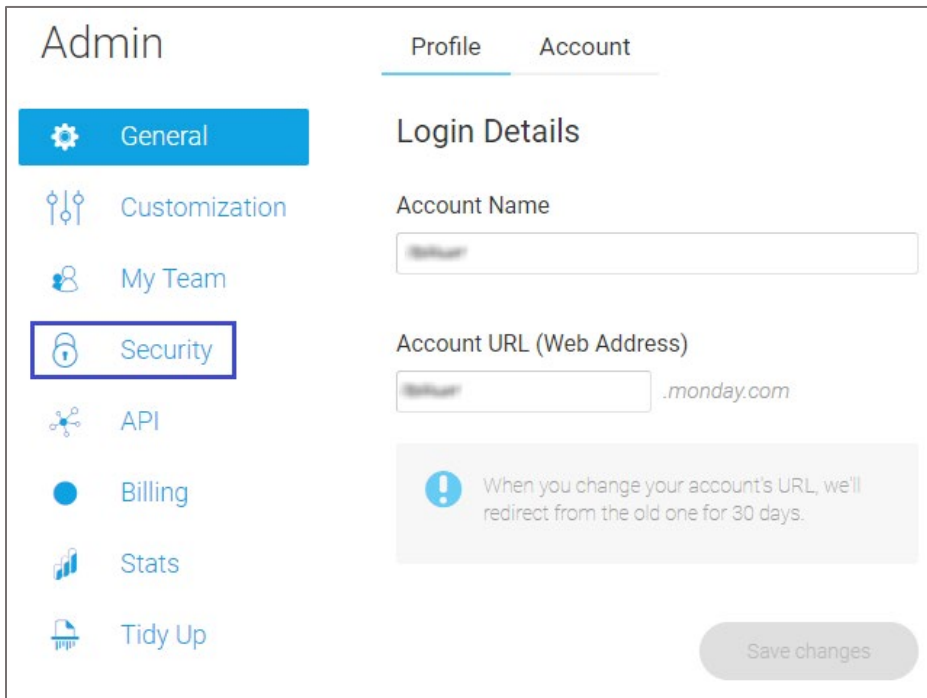


The image shows a screenshot of the Monday.com login page. At the top, the text "Log In" is displayed in a large, bold, black font. Below this, there are two input fields: "Email" and "Password". The "Email" field contains a blurred email address, and the "Password" field contains a series of dots. Below the "Password" field, there is a link that says "Forgot your password?". At the bottom of the form, there is a blue button with the text "Log In" and a right-pointing arrow.

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



4. In the **Admin** page, click **Security** from the left pane.



- Click **Edit** in the **SAML** tile.

The screenshot shows the 'Security & Authentication Settings' page. At the top, there are tabs for 'Login', 'Sessions', 'Audit', and 'Advanced'. Below the tabs, the page title is 'Security & Authentication Settings' with a subtitle: 'Use these settings to manage how people sign up and login to your monday.com account.' There are three main settings sections: 'Email & Password' with an 'Open' button, 'Google apps Authentication' with an 'Open' button, and 'SAML' which is currently 'Active' and has an 'Edit' button.

- Enter the values for the following fields:

Required Information	Description
SAML provider	Select <b>Custom SAML 2.0</b> .
SAML SSO Url	IdP logon URL
Identity provider issuer	Issuer URL
Public certificate	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with            -----Begin Certificate----- and -----End Certificate-----</p> <p><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.  <a href="https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust id&gt;/&lt;app id&gt;/idp_metadata.xml">https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust id&gt;/&lt;app id&gt;/idp_metadata.xml</a></p>

Login Sessions Audit Advanced

## Security & Authentication Settings

Use these settings to manage how people sign up and login to your monday.com account.

📧 Email & Password Open

📱 Google apps Authentication Open

🔒 SAML Active Close

1 SAML provider

- OKTA
- OneLogin
- Oracle
- Custom SAML 2.0

Provider Information

SAML SSO Url  ?

Identity provider issuer  ?

Public certificate  ?

Provisioning Information

Provisioning Token  ?

Provisioning URL  ?

Generate

2 Login Restrictions Policy

- All users must use SAML authentication
- All users except guests must use SAML authentication (Recommended)
- Using SAML authentication is optional

Any of your users will be able to Log In either via SAML Apps or with their email & password Password Policy is active

3 Password Policy

- Secure Password Policy ?
- Very Strict Password Policy ?

Save Changes Disable SAML authentication ?

7. Finally, click **Save Changes**.