

# Configure ClicData for Single Sign-On

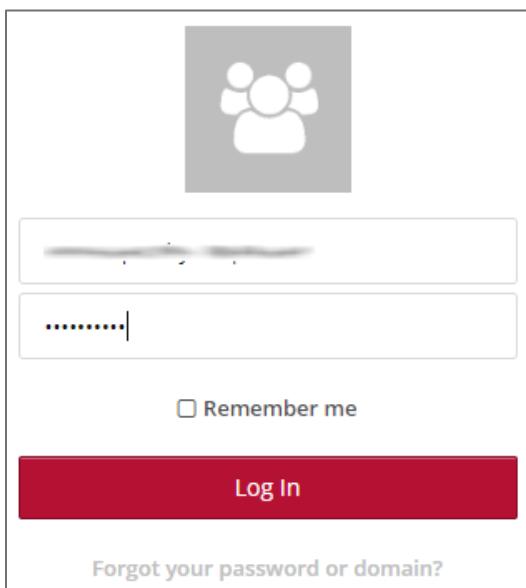
Configuring ClicData for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to ClicData by using the enterprise credentials.

## Prerequisite

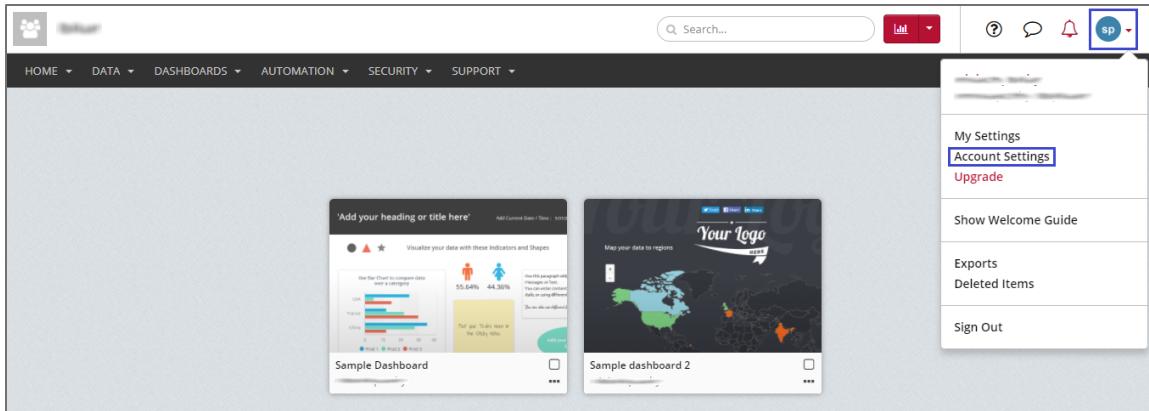
Browser Requirements: Internet Explorer 11 and above

### To configure ClicData for SSO by using SAML:

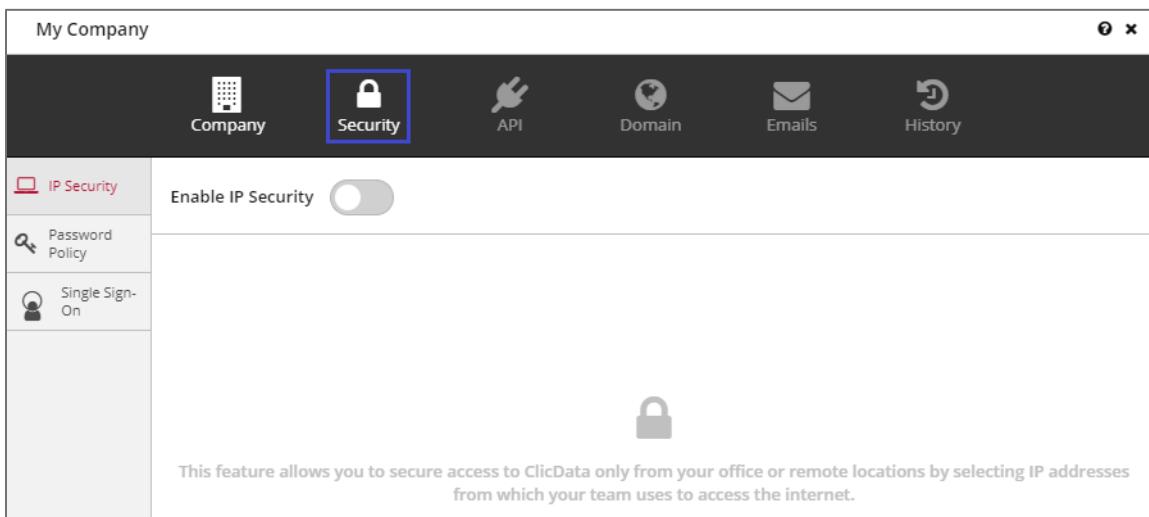
1. In a browser, type <https://<customer domain>.clicdata.com/login> and press **Enter**.
2. Type your ClicData admin account credentials (**Email** and **Password**) and click **Log In**.



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



4. In the pop-up window, click the **Security** tab.



5. Click **Single Sign-On** from the left pane and turn on the **Enable Single Sign-On** toggle button.

Enable Single Sign-On

**SAML Configuration** If you have the SAML metadata XML file from your Identity Provider, you can upload it below and we will take care of setting things up for you. Otherwise you can always fill the fields below yourself.

**Entity Identifier** Example: <https://idp.com/saml/metadata>

**SignOn URL** Example: <https://idp.com/saml/sso>

**Logout URL** Example: <https://idp.com/saml/slo>

**Certificate** Paste the Identity Provider certificate base64 string (the contents of the .cer file)

**Sign Authn Request**

**Want Assertion Signed**

**Cancel** **Save**

6. Scroll down and click **Import Identity Provider Metadata** in **SAML Configuration** to upload the metadata file in XML format.

7. You can also enter the values for the following fields:

Required Information	Description
Entity Identifier	Entity ID
SignOn URL	IdP logon URL
Logout URL	IdP logout URL
Certificate*	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with</p> <p style="text-align: center;">-----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.</p> <p style="text-align: center;"><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>

8. Scroll down and enter the user attributes.

Required Information	Description
E-mail	mail
First name	firstName
Last name	ln
Can sign in?	yes

The screenshot shows the Citrix Cloud interface for managing Single Sign-On (SSO) settings. The top navigation bar includes links for Company, Security, API, Domain, Emails, and History. On the left, a sidebar lists IP Security, Password Policy, and Single Sign-On (which is currently selected). The main content area is titled 'Enable Single Sign-On' and contains a toggle switch that is turned on. Below this, the 'User Attributes' section is configured with the following mappings:

- E-mail: Example: mail (Note: Must match the e-mail of current users.)
- First name: Example: givenName
- Last name: Example: sn
- Can sign in?: Example: canSignInClicData (Note: User value must be yes or no.)

The 'Verification' section provides instructions for validating user accounts when SSO is active. The 'Status' section at the bottom indicates that validation is required, with a link to 'click here to validate'.

9. Click the link in **Status** to validate.

10. Finally, click **Save**.