

Configure Chartio for Single Sign-On

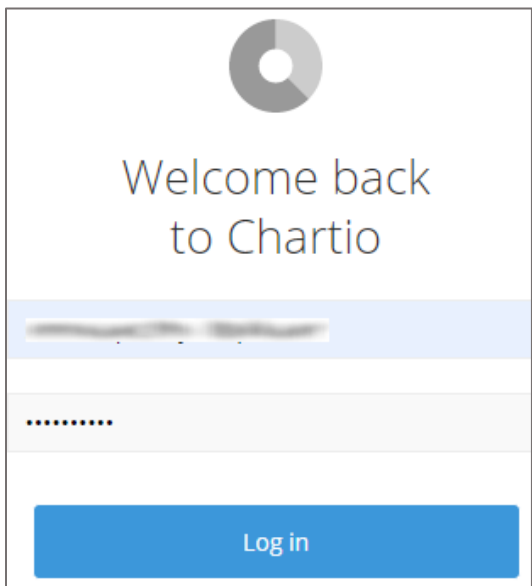
Configuring Chartio for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Chartio by using the enterprise credentials.

Prerequisite

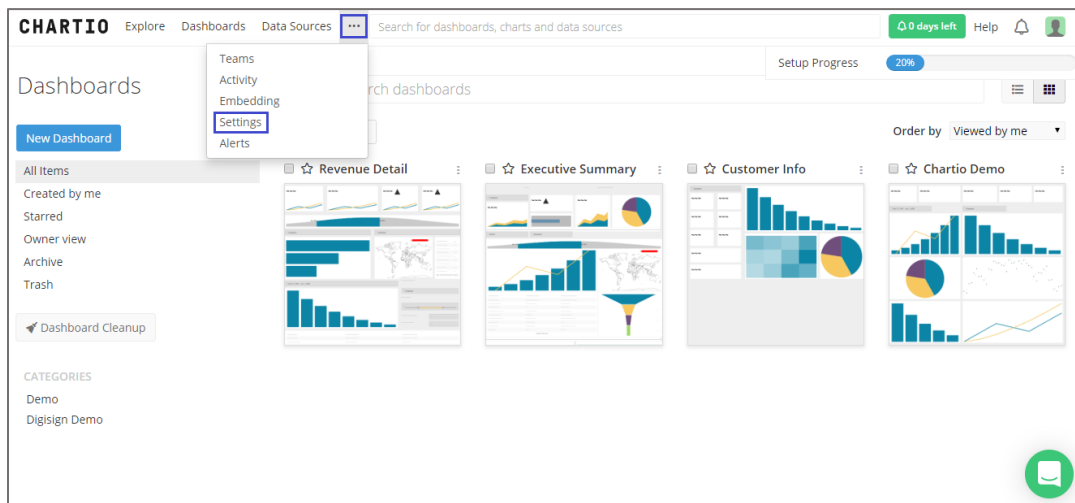
Browser Requirements: Internet Explorer 11 and above

To configure Chartio for SSO by using SAML:

1. In a browser, type <https://chartio.com/login/> and press **Enter**.
2. Type your Chartio admin account credentials (**email** and **password**) and click **Log in**.

The image shows the Chartio login page. At the top center is a circular logo with a white center and a grey outer ring. Below the logo, the text "Welcome back to Chartio" is displayed in a sans-serif font. Underneath this text are two input fields. The first field is for the email address, with a light blue background and a grey border. The second field is for the password, with a light grey background and a grey border, and it contains a series of dots to mask the text. At the bottom of the form is a blue rectangular button with the text "Log in" in white.

3. In the dashboard page, click the menu icon and select **Settings**.



4. In the **Settings** page, scroll down and enter the values for the following fields under **Authentication**:

Required Information	Description
Login Methods	Select the SAML check box.
SAML entity ID	Entity ID
SAML SSO URL	IdP logon URL
X.509 Certificate	Copy and paste the IdP 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

Authentication

Choose the allowed authentication methods for users in your organization.

Login Methods

☐ Chartio
☐ Google
☒ SAML

Warning: disabling login methods will immediately affect logged in users, including you! Make sure you have recently logged in with one of the selected login methods before updating this for your organization

SAML entity ID

SAML SSO URL

X.509 certificate

Update

5. Finally, click **Update**.