

Configure CloudRanger for Single Sign-On

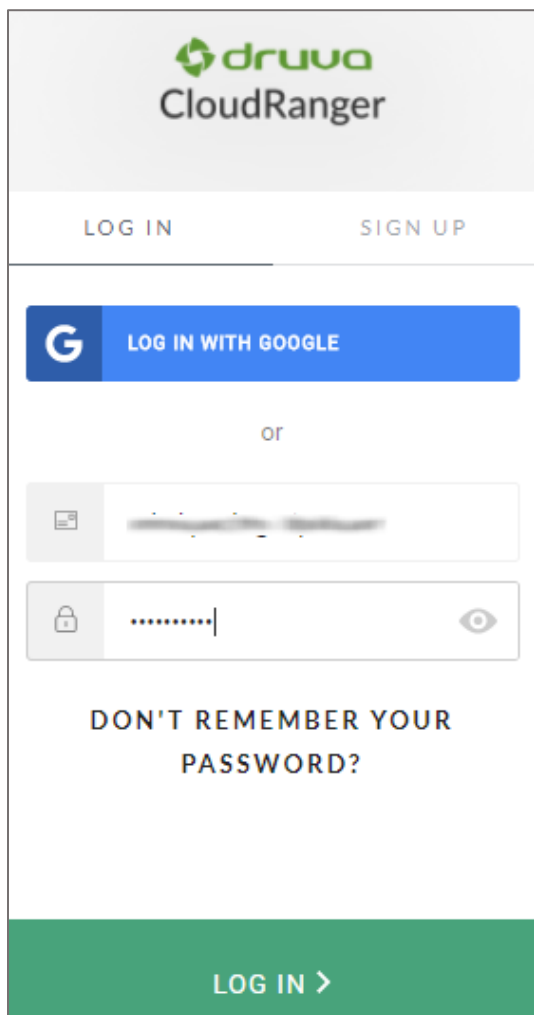
Configuring CloudRanger for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to CloudRanger by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure CloudRanger for SSO by using SAML:

1. In a browser, type <https://console.cloudranger.com/#/login> and press **Enter**.
2. Type your CloudRanger admin account credentials (**email** and **password**) and click **LOG IN**.



The screenshot shows the login interface for Druva CloudRanger. At the top, the logo consists of a green circular icon with a white arrow and the text 'druva CloudRanger'. Below the logo are two buttons: 'LOG IN' and 'SIGN UP'. A large blue button with a white 'G' icon and the text 'LOG IN WITH GOOGLE' is positioned below these. Underneath is the word 'or'. There are two input fields: the first is for an email address, and the second is for a password, which has a lock icon on the left and an eye icon on the right to toggle visibility. Below the password field is the text 'DON'T REMEMBER YOUR PASSWORD?'. At the bottom of the form is a large green button with the text 'LOG IN >'.

- To enable and configure SSO, the user must contact CloudRanger support team and provide them with the following:

Required Information	Description
Protocol	SAML
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
Sign in URL	IdP logon URL
Sign out URL	IdP logout URL

Note: The support team will configure the SP from the backend.