

# Configuring Bugsnag

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

## Prerequisite

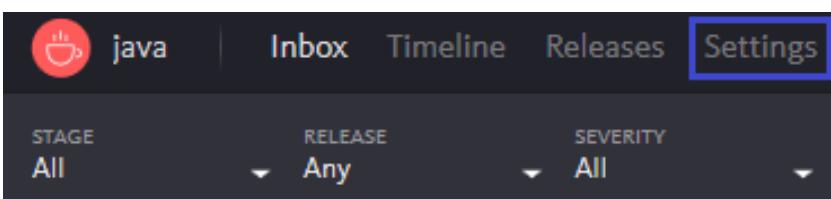
Browser Requirements: Internet Explorer 11 and above

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

1. In a browser, type <https://www.bugsnag.com/> and press Enter.
2. Type your Bugsnag admin account credentials (**Email** and **Password**) and click **Sign in**.

The screenshot shows the 'Sign in to Bugsnag' page. It features a large title at the top. Below it is a light gray horizontal bar. The main form area has two input fields: 'Email' with a blurred placeholder and 'Password' with a redacted placeholder. A large blue 'Sign in' button is centered below the fields. At the bottom left, there is a 'Forgot Password?' link.

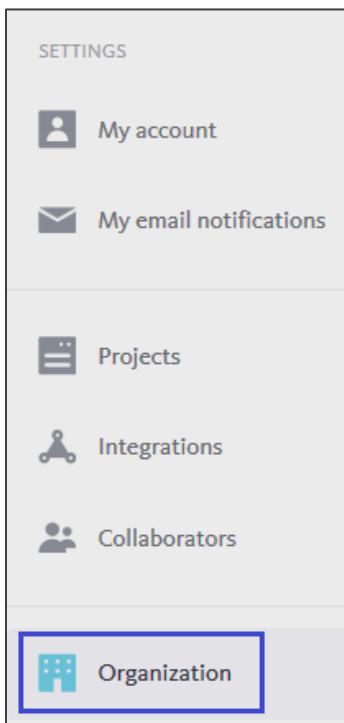
3. Click **Settings** present in the navigation bar of the dashboard.



Citrix Gateway



4. In the left panel, select **Organization**.



5. In the **Authentication** section, click **Single sign-on** to change the setting to **Enabled**. This will update the SSO provider settings.

A screenshot of a configuration page. At the top, there is a "Delete organization" button with a tooltip: "Delete your organization and remove all data &amp; billing details from Bugsnag". Below this is a "Single sign-on" section. The "Enabled" button in this section is highlighted with a blue rectangular border. To the right of the "Enabled" button is a right-pointing arrow.

**Note:** Contact the support team if **Single sign-on** tab is not available.

6. In the **Update SSO Settings** section, enter the values for the following fields.

Field Name	Description
SAML/IdP metadata URL from your SSO provider	Paste the IdP metadata URL. <b>Note:</b> The SP metadata is provided by Citrix and can be accessed from the link below: <a href="https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatestest/idp_metadata.xml">https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatestest/idp_metadata.xml</a>
SAML endpoint URL to add to your SSO provider's configuration	SAML endpoint URL

**Update SSO settings**

Enable your team to log in via Okta, OneLogin, or other SAML SSO providers. [Learn more >](#)

SAML/IdP metadata URL from your SSO provider [?](#)

SAML endpoint URL to add to your SSO provider's configuration [?](#)

Auto-provision users on first login [?](#)

Force your team to log in via your SSO provider [?](#)

This option is disabled until you successfully authenticate via your SSO provider.

[Disable SSO...](#)

[CANCEL](#) [SAVE](#)

7. Finally, click **Save**.