Configure Honeybadger for Single Sign-On

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

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure Honeybadger for SSO by using SAML:

- 1. In a browser, type <u>https://app.honeybadger.io/users/sign_in</u> and press **Enter**.
- 2. Type your Honeybadger admin account credentials (**Email** and **Password**) and click **Sign** in.

\$	
Sign In	
Email	
Password	
✓ Keep me signed-in for 2 weeks	Sign in

3. In the dashboard page, click the username in the top-right corner and select **User Settings**.

Search Errors in All Projects			User Settings My Projects
Projects		My Teams Product Changes	
Q-	1 Hour	Unresolved Last	Log Out
and the	0	0	•

4. Click **Authentication** from the left panel.

Profile	User Profile
Authentication	
Notifications	Subscription Plan
Digest Emails	
Local Editor	You're subscribed to the Extra Large plan.
Mobile Devices	Your plan allows you to see detailed error data back to June 10, 2018.
Billing	Switch Plans

5. In the **User Authentication** page, scroll down and click **View SAML Configuration** under **SAML SSO**.

Notifications	These settings apply only to your personal account. Project-wide authentication can be set up via each project's settings page.
Digest Emails	settings page.
Local Editor	Your Honeybadger API Token
Mobile Devices	
Billing	This token is used for accessing the read API and RSS feeds for each project.
	A Reset your Authentication Token
	GitHub Connection
	By connecting your account to GitHub, you'll be able to log in via GitHub and manually create issues from errors in Honeybadger.
	O Connect GitHub
	SAML SSO
	When you set up single-sign-on with SAML, people working on your projects will be able to log into Honeybadger via a SSO provider, like Google Apps for Work.
	View SAML Configuration

6. In the **SAML Settings** page, enter the values for the following fields:

Required Information	Description
IDP Metadata	Copy and paste the IdP certificate. Note: The IdP metadata URL is provided by Citrix and can be
	accessed from the link below. The link is displayed while configuring SSO settings for your app.
	https://gateway.cloud.com/idp/saml/ <citrixcloudcust_id>/<app_id> /idp_metadata.xml</app_id></citrixcloudcust_id>

SAML Settings	
SSO URL	https://app.honeybadger.io/saml/-
Entity ID	https://saml.honeybadger.io
Name ID Format	EmailAddress
Application username	Email
IDP Metadata	
Team Access	The selected teams will automatically add users who authenticate via this SAML endpoint without having to have an invitation to the team. Default Team
	Save changes Delete these settings

7. Finally, click **Save changes**.