Configuring Sentry

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

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure Sentry for SSO by using SAML:

- 1. In a browser, type <u>https://sentry.io</u> and press **Enter**.
- 2. Type your Sentry account credentials (Account and Password) and click Continue.

n)	Sign in to continue	
	Login Single Sign-On	
	Account [REQUIRED]	
	and the local sector	O Sign in with GitHub
	Password [REQUIRED]	
	•••••	
	Continue Lost your password?	

3. In the top-left corner, click the user account and select **Organization settings** from the drop-down menu.



4. In the left panel, click **Auth** under **General Settings**.

🔬 Settings > 💿 💷	General		Q Search
ORGANIZATION	Organization Settings		
General Settings			
Projects	GENERAL		
Teams			
Members	Name •	(Ballinger)	
Auth	A unique ID used to identify this organization		
Audit Log	Legacy Name *		
Repositories	DEPRECATED In the future, only Name will be used to identify	(Britant)	
Integrations	your organization		
USAGE & BILLING	Early Adopter		
Overview	Opt-in to new features before they're released to the public		
Usage History			
Update Billing Details	MEMBERSHIP		
Payment Receipts			
Redeem Promotional Code	Default Role	Member	~
Legal & Compliance	The default role new members WIII receive		

5. In the **SAML2 Authentication** page, enter the values for the following fields under **Identity Provider Metadata**.

Field Name	Description
Entity ID	IdP entity ID (Citrix)
Single Sign On URL	IdP logon URL
Single Log Out URL	IdP logout URL
x509 public certificate	Copy and paste the IdP certificate. Note: The IdP Certificate is provided by Citrix and can be accessed from the link below: <u>https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/i</u> <u>dp_metadata.xml</u>

Identity Provider Metadata	Service Provider Metadata
Entity ID [REQUIRED]	
Single Log Out URL	
x509 public certificate [REQUIRED]	*

6. In the **SAML2 Authentication** page, enter the values for the following fields under **Attribute Mappings** and **General Settings**.

Field Name	Description
IdP UserID	UserID
User Email	Email
First Name	Optional
Last Name	Optional
Require SSO	Select this check box to help users access the organization through SSO.
Default Role	Select the respective role from the drop-down list.

IdP User ID [REQUIRED]	
UserID	
The IdPs unique ID attributhe identity provider.	te key for the user. This is what Sentry will used to identify the users identity from
User Email [REQUIRED]	
Email	
The IdPs email address at	ribute key for the user. Upon initial linking this will be used to identify the user in
First Nam e	
First Name	
First Nam e Last Nam e	
First Name Last Name	
First Name Last Name General Settings	
First Name Last Name General Settings Require SSO	
First Name Last Name General Settings Require SSO Require members use a	a valid linked SSO account to access this organization
First Name Last Name General Settings Require SSO Require members use a Default Role [REQUIREE]	a valid linked SSO account to access this organization
First Name Last Name General Settings Require SSO Require members use a Default Role [REQUIRE] Member	a valid linked SSO account to access this organization