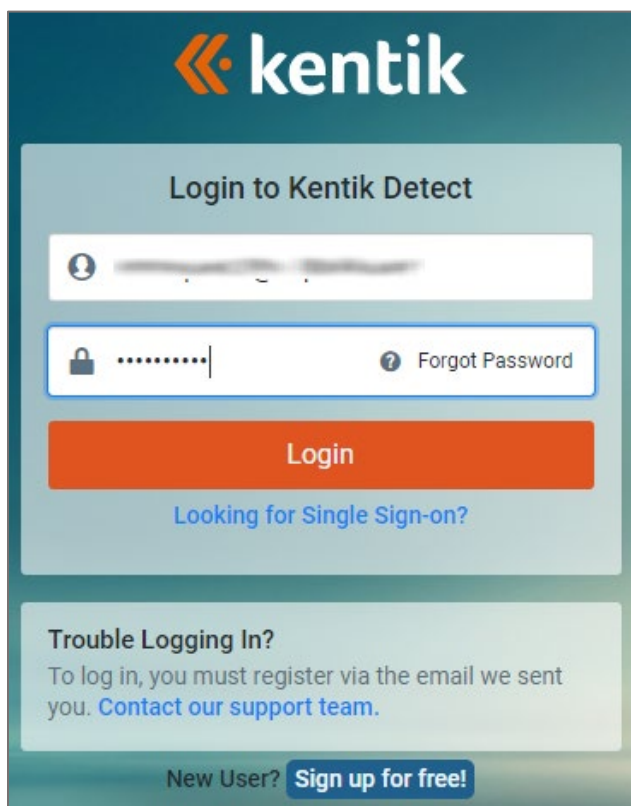# Configuring Kentik

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

Prerequisite
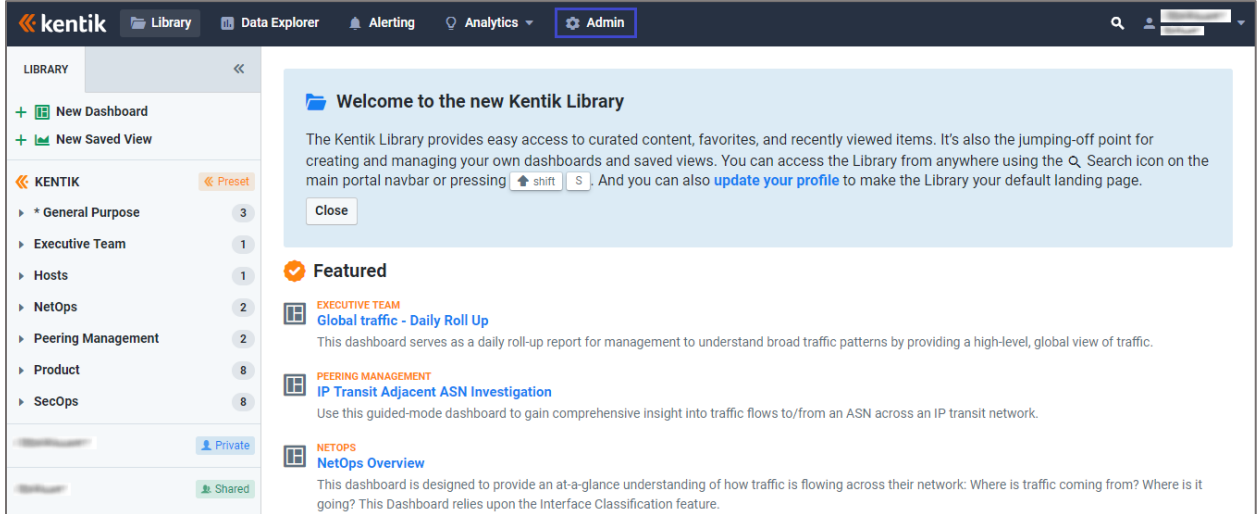
Browser Requirements: Internet Explorer 11 and above

To configure Kentik for SSO by using SAML:

1. In a browser, type https://www.kentik.com/ and press **Enter**.

2. Type your Kentik admin account credentials (**Email Address** and **Password**) and click **Login**.

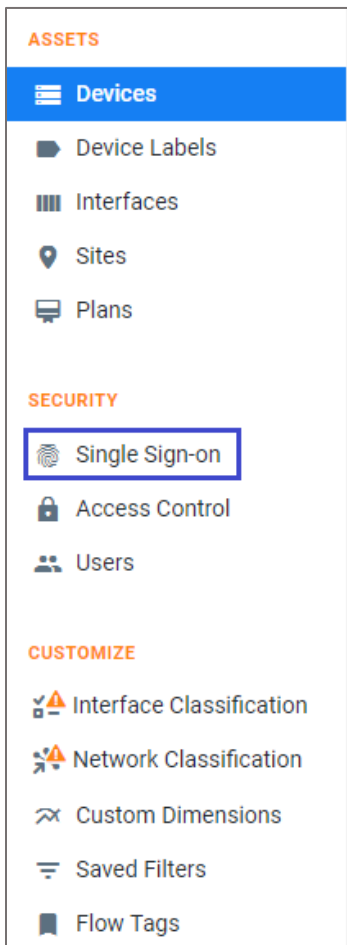3. In the home page, click **ADMIN** in the ribbon present at the top of the page.

4. In the left panel, click **Single Sign-on** under **SECURITY**.

5. Scroll down and enter the values for the following fields:

Field Name	Description
SSO Enabled	Enable Single Sign-on.
SP Entity Id*	SP Entity ID
SP ACS Url*	SP ACS URL
IDP SSO Url*	IdP SSO entry point URL
Email Attrib. Key*	Profile attribute for user email
IDP Signing Cert	This is an optional field. Copy and paste the IdP certificate content here.

Admin > **Single Sign-on**

SSO Enabled

🔵 On
Enable Single Sign-on

SSO Required

⚪ Off
Require Single Sign-on

Disable 2FA

⚪ Off
Disable 2FA when user has authenticated via Single Sign-on

Auto-Provisioning

⚪ Off
Allow auto-provisioning of new users

SP Entity Id*

Service Provider (SP) entity id

SP ACS Url*

Service Provider (SP) Assertion Consumer Service (ACS) url

IDP SSO Url*

Identity Provider (IDP) SSO entry point url

Email Attrib. Key*

Profile attribute for user email

User Level Attrib. Key

Profile attribute for user level (Values: 0 = Member, 1 = Admin)

Encrypt Assertions

⚪ Off
Enable if IDP requires encrypted assertions

IDP Signing Cert

IDP public signing key, leave empty if IDP sending unsigned response

⊕ **Download Kentik SP Metadata**

Cancel Save

6. Finally, click **Save.**