

Configure Pendo for Single Sign-On

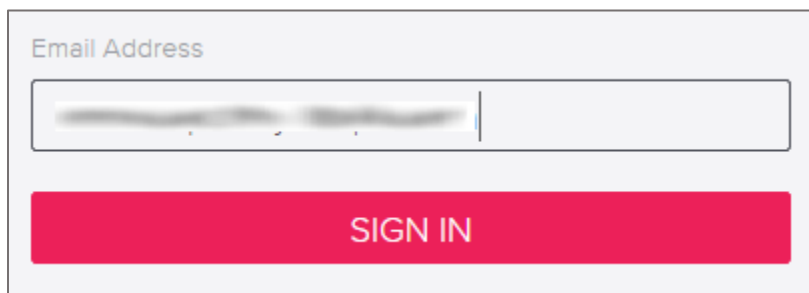
Configuring Pendo for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Pendo by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

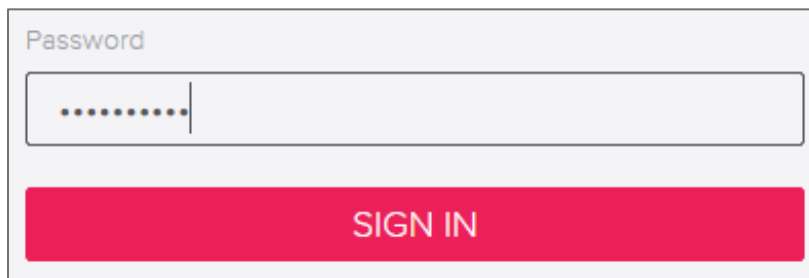
To configure Pendo for SSO by using SAML:

1. In a browser, type <https://app.pendo.io/login> and press **Enter**.
2. Type your Pendo admin email address and click **SIGN IN**.



The screenshot shows a login form with a light gray background. At the top, the text "Email Address" is displayed in a small, light gray font. Below it is a white input field with a thin gray border. A redacted email address is visible inside the field. Below the input field is a large, solid red button with the text "SIGN IN" in white, uppercase letters.

3. Type your Pendo admin password and click **SIGN IN**.



The screenshot shows a login form with a light gray background. At the top, the text "Password" is displayed in a small, light gray font. Below it is a white input field with a thin gray border. The password is redacted with a series of dots. Below the input field is a large, solid red button with the text "SIGN IN" in white, uppercase letters.

4. To enable and configure SSO, the user must contact Pendo support team and provide them with the IdP metadata.

Required Information	Description
Certificate	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

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