

Configuring Envoy

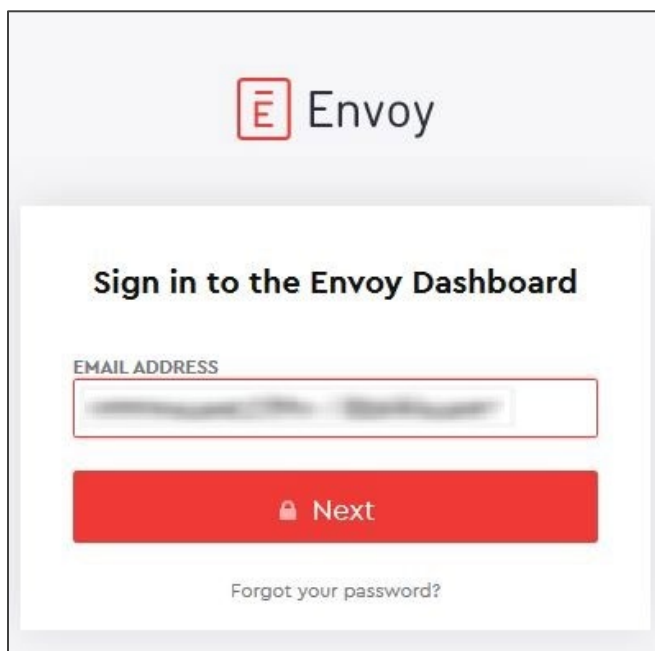
Configuring Envoy for single sign-on (SSO) enables administrators to manage users using Citrix ADC. Users can securely log on to Envoy by using the enterprise credentials.

Prerequisite

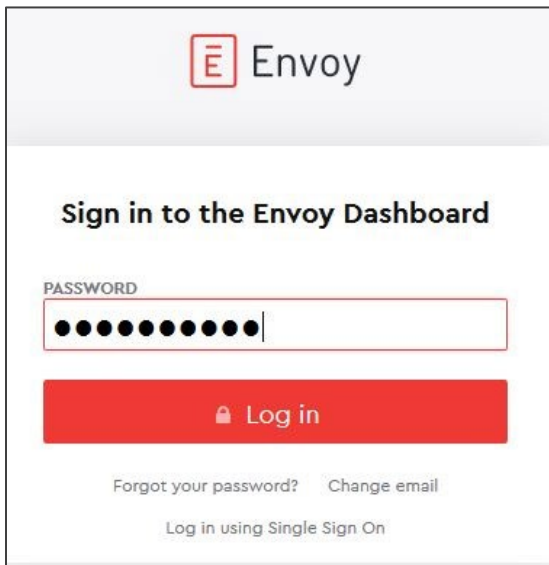
Browser Requirements: Internet Explorer 11 and above

To configure Envoy for SSO by using SAML:

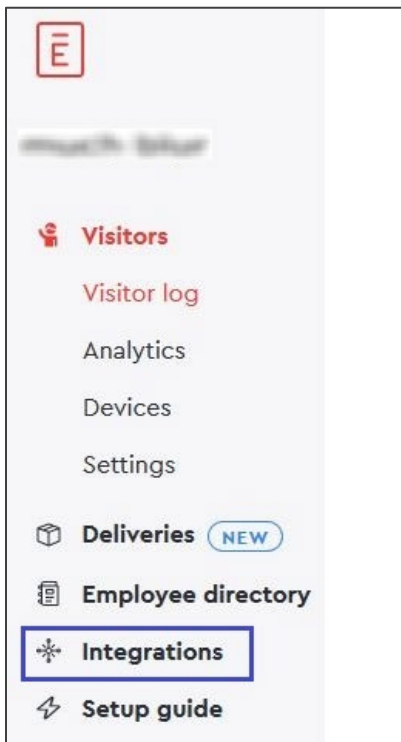
1. In a browser, type <https://www.envoy.com> and press **Enter**.
2. Type your admin email address in **EMAIL ADDRESS** and click **NEXT**.

The image shows a screenshot of the Envoy login interface. At the top, there is the Envoy logo, which consists of a red square containing a white 'E' followed by the word 'Envoy' in a sans-serif font. Below the logo, the text 'Sign in to the Envoy Dashboard' is centered. Underneath this, there is a label 'EMAIL ADDRESS' above a text input field. The input field contains a blurred email address. Below the input field is a prominent red button with the text 'Next' and a small lock icon to its left. At the bottom of the form, there is a link that says 'Forgot your password?'.

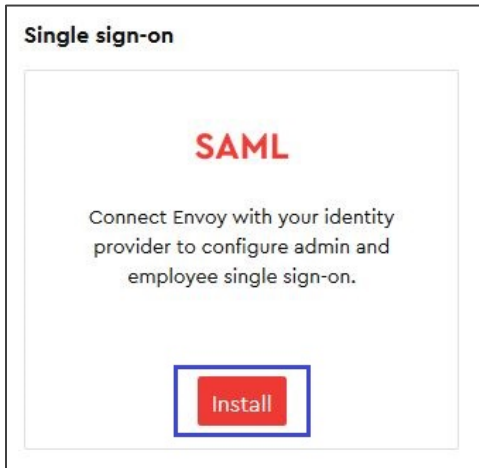
3. Type your admin password in **PASSWORD** and click **Log in**.



3. In the left panel of the dashboard menu, select **Integrations**.



4. Scroll down to **Single sign-on** and click **Install** in the **SAML** tile.



5. In the SAML page, enter the values for the following fields:

Field Name	Description
FINGERPRINT	Copy and paste the IdP certificate fingerprint from the https://www.samltool.com/fingerprint.php link, Select Algorithm and Generate the Fingerprint .
IDENTITY PROVIDER SAML URL	IdP logon URL

Note: Enabling the **REQUIRED** option will create a user account automatically.

Assertion Consumer Service (ACS) URL	<code>https://app.envoy.com/a/saml/consume</code>
Issuer URL	<code>https://app.envoy.com/a/saml/metadata</code>
SAML Identifier	<code>https://app.envoy.com/a/saml/metadata</code>
Sign On URL (SP-initiated only)	<code>https://app.envoy.com/a/saml/auth/37672</code>

Configure Single Sign-On for your company by entering the SHA-1 or SHA-256 fingerprint provided by your SAML Identity Provider (i.e. Google, Okta, etc.). To allow users to initiate SSO from Envoy please also enter your provider's SAML HTTP POST URL in the field above.

[To learn more about SAML, read our help docs →](#)

6. Finally, click **Save**.