

Last Modified: June 14, 2017

Envoy is the solution to sign in visitors. It collects guest's information, capture their photos and have them sign legal documents. Envoy helps boost front desk efficiency. It makes sign-in a breeze, whether you have one or hundreds of visitors per day.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Envoy.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	https://dashboard.envoy.com/login
ACS URL	https://web.envoy.com/saml/consume
Service Provider Issuer ID	https://web.envoy.com/saml/consume

Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Envoy to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Envoy.



Envoy
SAML Direct




3. On the Basic Information page, specify the application name and click **Next Step**.

The screenshot shows the 'Edit Connection' interface for an application named 'Envoy'. The page has a sidebar with navigation steps: 1. Basic Information (selected), 2. Connection Profile, 3. User Access, and 4. Portal Display. The main content area is titled 'Basic Information' and contains the following fields and options:

- Name:** A text input field containing the value 'Envoy'.
- Description (optional):** A larger text area for providing additional details.
- Disabled:** A checkbox that is currently unchecked, with a help icon (?) next to it.

At the top right and bottom right of the main content area, there are 'Cancel' and 'Next Step' buttons. A note at the top of the main area states: 'All fields are required (except where noted)'.

4. Navigate to **Initiate SAML Workflow** section.
 - a. In the **Connection URL** field, keep the field blank as the value is not required.
 - b. Choose **IDP-initiated**.

 **Note:** The following IdP-initiated configuration works for SP-initiated Envoy connections as well.

Initiate SAML Workflow

The 'Initiate SAML Workflow' configuration page includes the following elements:

- Connection URL:** A text input field containing 'http://www.example.com'.
- Initiation Type:** Two radio buttons: 'IDP-initiated' (selected) and 'SP-initiated'.
- Binding Method for SAML Request:** Three radio buttons: 'Redirect' (selected), 'POST', and 'Signed' (with a help icon ?).
- Certificate Status:** A warning icon (triangle) and the text 'No certificate loaded'.
- Buttons:** 'Choose File' and 'Generate Cert Bundle' buttons.

5. Scroll down to **SAML Identity Provider (Issuer)** section.

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?
 Default (idp_id): 1lloyppgfjq92
 Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

<input checked="" type="checkbox"/> Private Key Loaded	<input type="button" value="Choose File"/>	<input type="button" value="Generate Cert Bundle"/> ?
<input checked="" type="checkbox"/> Certificate Loaded CN=rsasso, Valid Until: 05/09/2021	<input type="button" value="Choose File"/>	

Include Certificate in Outgoing Assertion

- a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
- b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
- c. Select **Choose File** and upload the private key.
- d. Select **Choose File** to import the public signing certificate.
- e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

6. Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://web.envoy.com/saml/consume

Audience (Service Provider Entity ID) ?

https://web.envoy.com/saml/consume

7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

8. Click **Next Step**.
9. On the **User Access** page, select **Allow All Authenticated Users** user policy from the available options.

Access Policy

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy ?

No Access Allowed

10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.

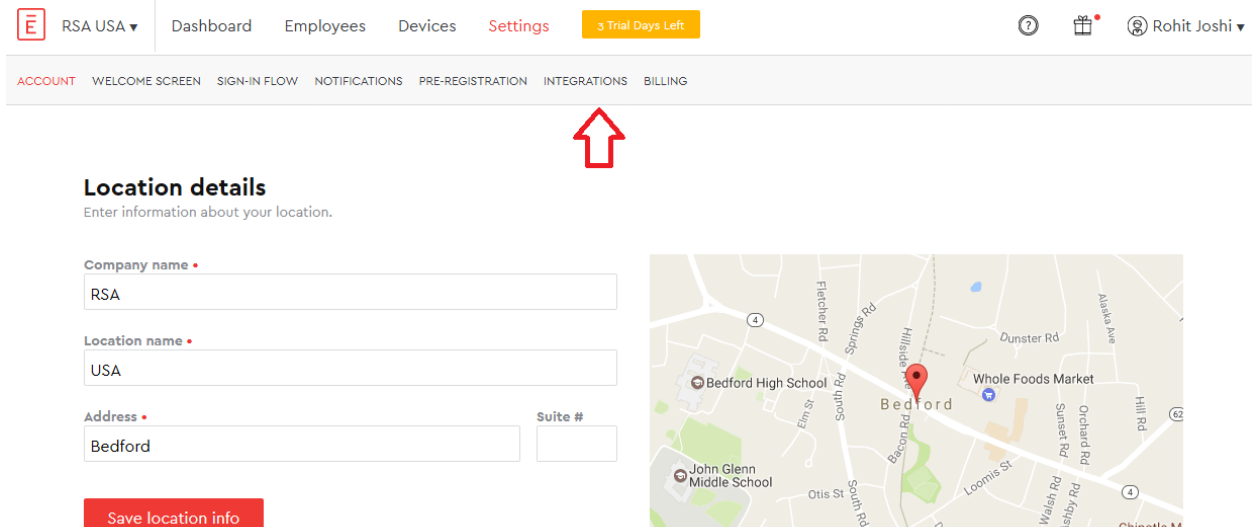
Publish Changes

Status:  Changes Pending

Configure Envoy to Use RSA SecurID Access as an Identity Provider

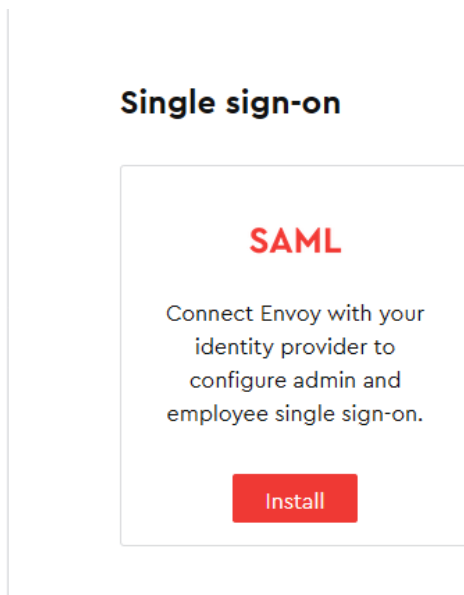
Procedure

1. Login to your Envoy domain click on *Settings – Integrations* (<https://dashboard.envoy.com/login>)



The screenshot shows the Envoy dashboard interface. At the top, there is a navigation bar with the RSA USA logo, a dropdown menu, and several menu items: Dashboard, Employees, Devices, Settings, and a yellow button for '5 Trial Days Left'. On the right side of the navigation bar, there are icons for help, a gift, and a user profile for 'Rohit Joshi'. Below the navigation bar is a secondary menu with links for ACCOUNT, WELCOME SCREEN, SIGN-IN FLOW, NOTIFICATIONS, PRE-REGISTRATION, INTEGRATIONS, and BILLING. The 'INTEGRATIONS' link is highlighted with a red arrow pointing upwards. The main content area is titled 'Location details' and includes the instruction 'Enter information about your location.' Below this are three input fields: 'Company name' (containing 'RSA'), 'Location name' (containing 'USA'), and 'Address' (containing 'Bedford'). There is also a 'Suite #' field which is currently empty. A red 'Save location info' button is located below the address field. To the right of the form is a map of Bedford, MA, showing streets like Fletcher Rd, South Rd, and Loomis St, and landmarks like Bedford High School and Whole Foods Market.

2. Search for *Single Sign-On* box and click on *Install*



The screenshot shows the 'Single sign-on' section of the Envoy dashboard. The title 'Single sign-on' is displayed in bold black text. Below the title is a large white box with a red border. Inside this box, the word 'SAML' is written in large, bold, red letters. Below 'SAML', there is a paragraph of text: 'Connect Envoy with your identity provider to configure admin and employee single sign-on.' At the bottom of this box is a red button with the word 'Install' written in white text.

3. Enter your *Fingerprint* certificate created from your RSA public certificate and *Identity Provider URL* found on page 3 step 5.

SAML

Fingerprint •

Identity Provider HTTP SAML URL •

Required

SAML Consumer URL:

SAML SSO Redirect URL:

To approve access to Envoy via a Single Sign-On SAML solution (like Okta or OneLogin), please enter the SHA-1 Fingerprint of the account's Certificate and the SAML HTTP POST URL in the textboxes above. These are both obtained from your SAML Identity Provider.

4. Click on *Save* button and Envoy is ready for SSO.