RSA SecurID Access SAML Configuration for Envoy

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

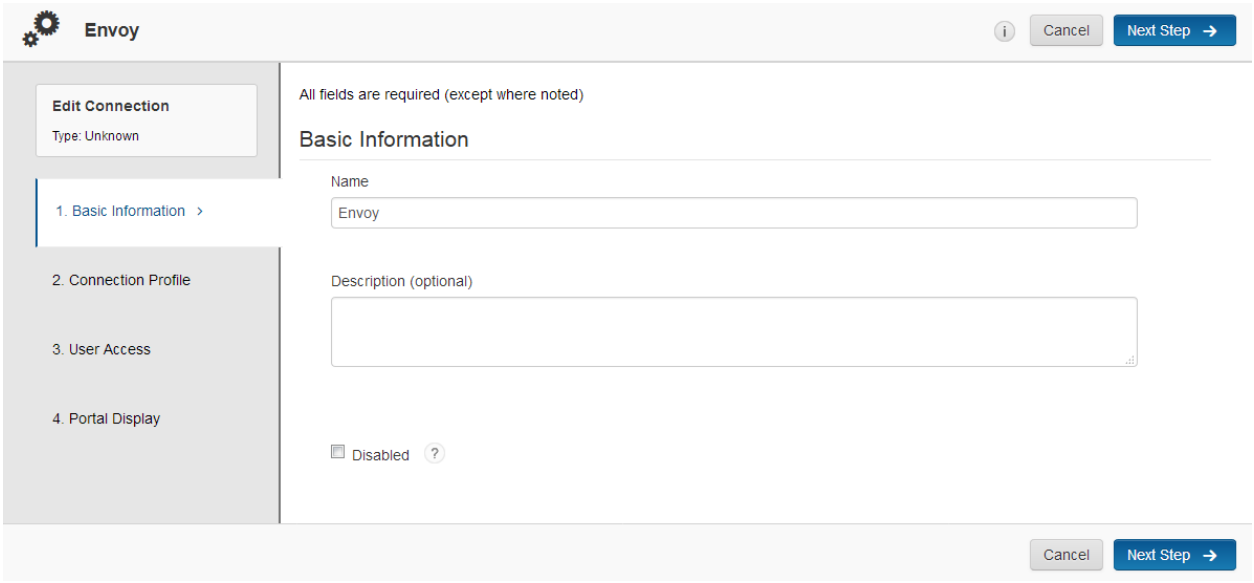
1. Add the Application in RSA SecurID Access
2. Configure Envoy to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

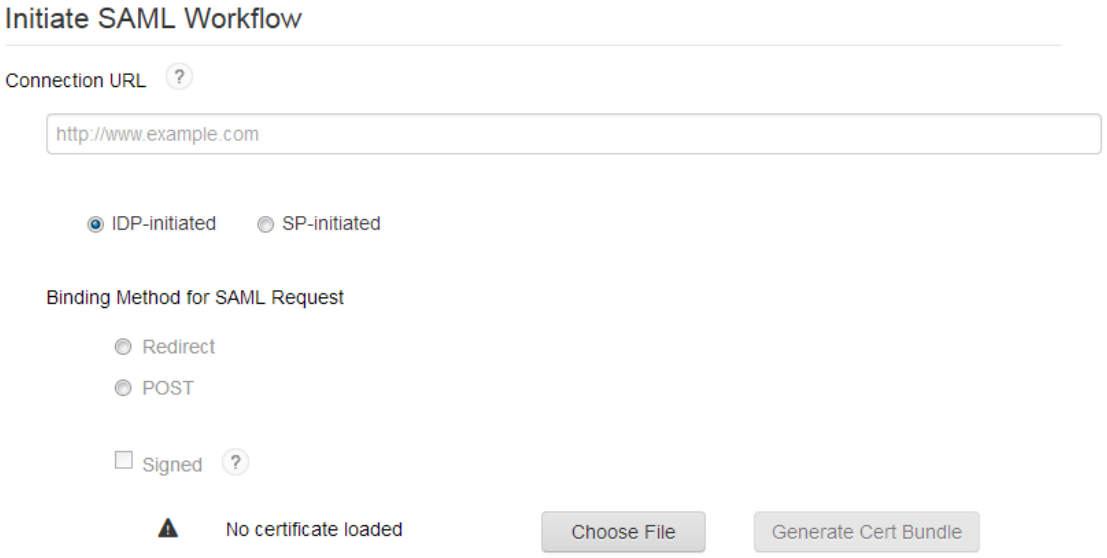
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Envoy.

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

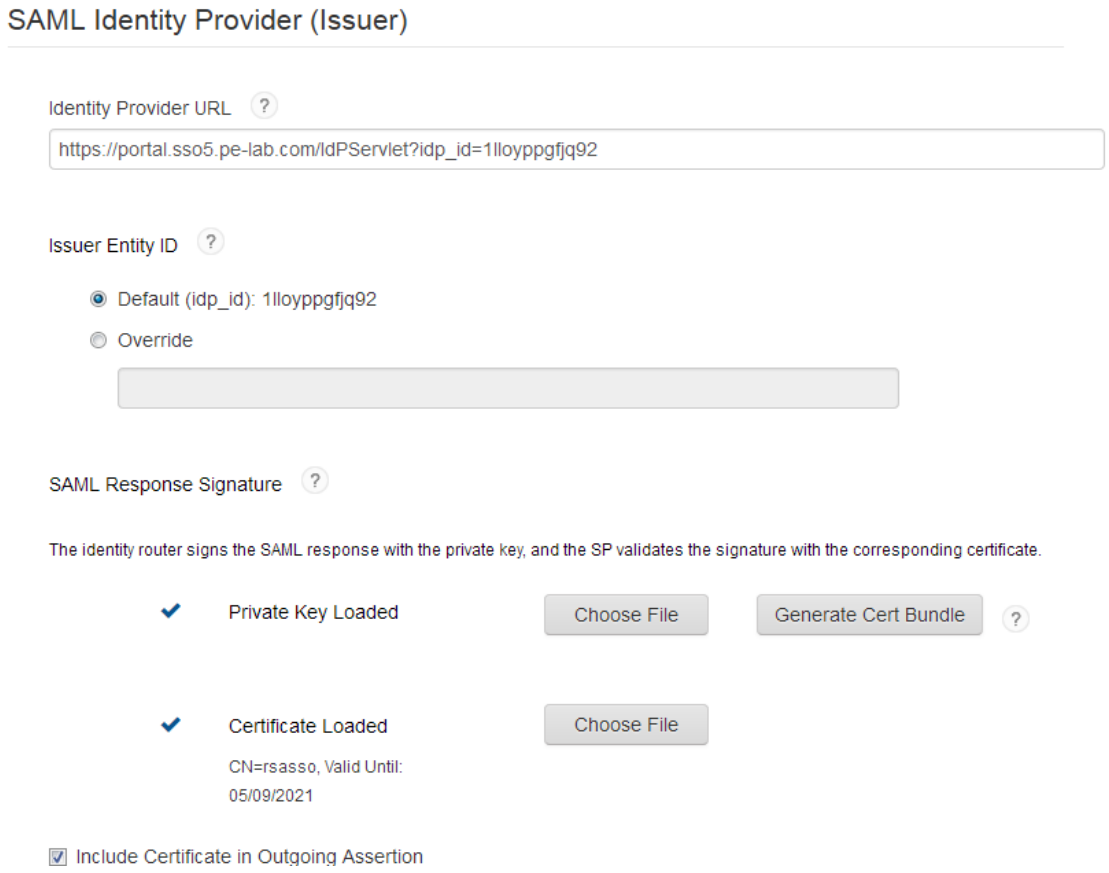


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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



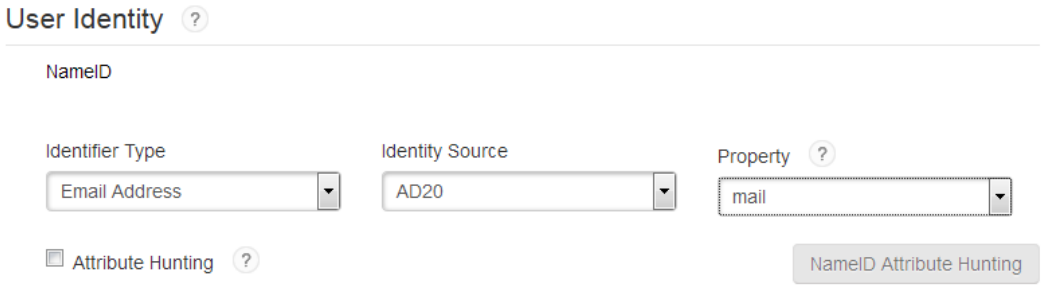
5. Scroll down to **SAML Identity Provider (Issuer)** section.



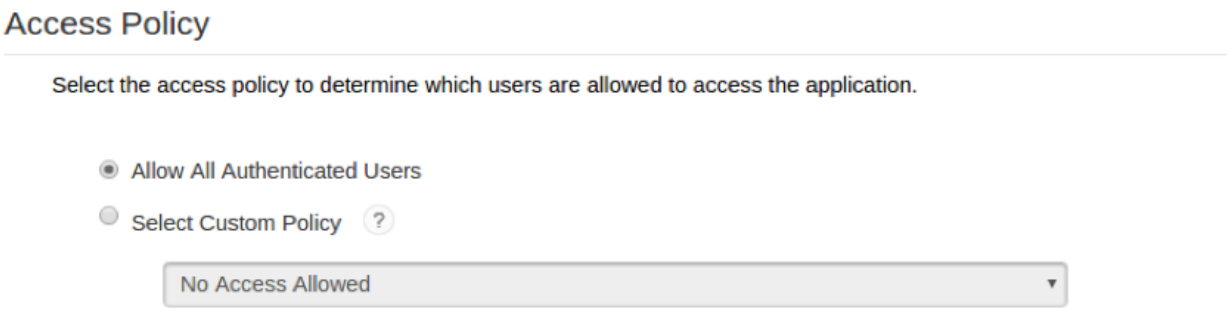
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** 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.

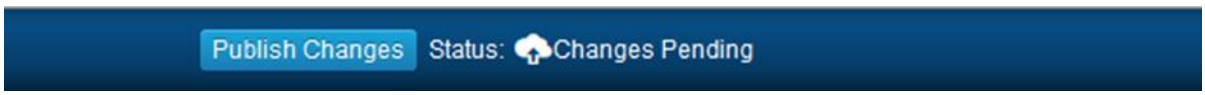
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



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



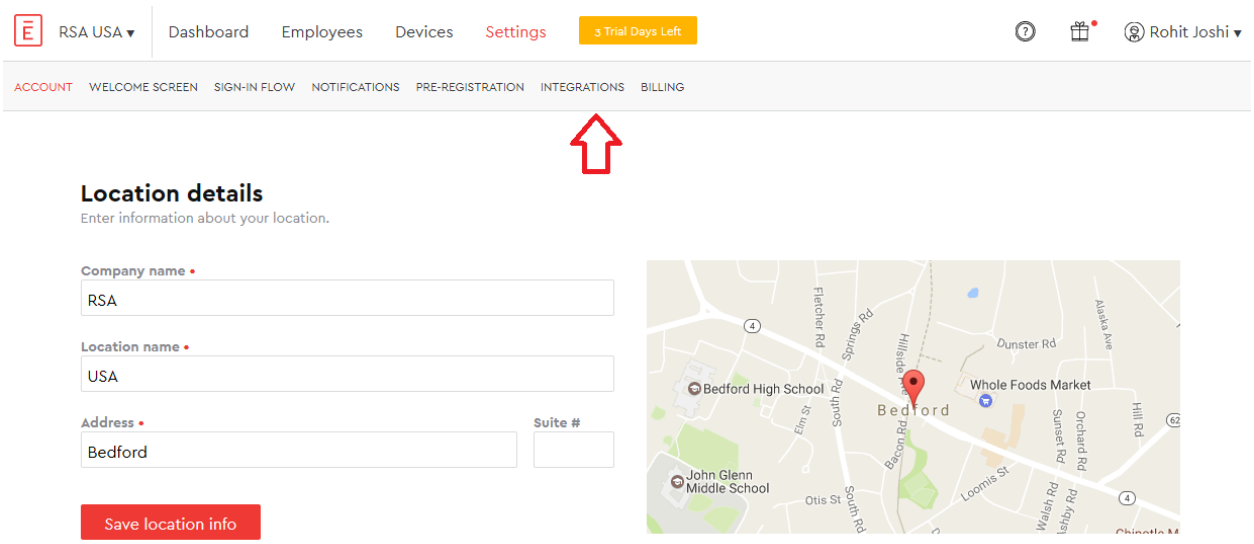
10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



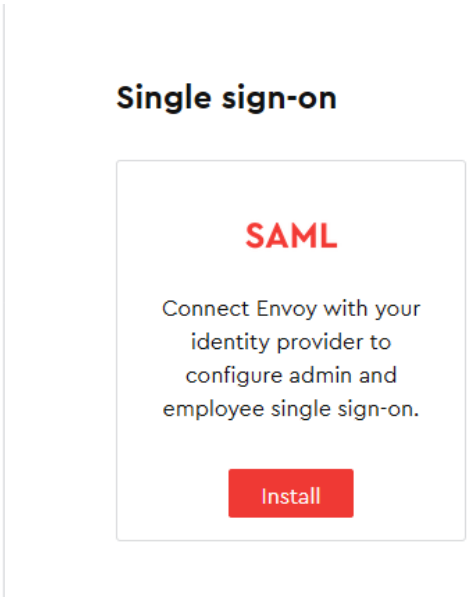
Configure Envoy to Use RSA SecurID Access as an Identity Provider

Procedure

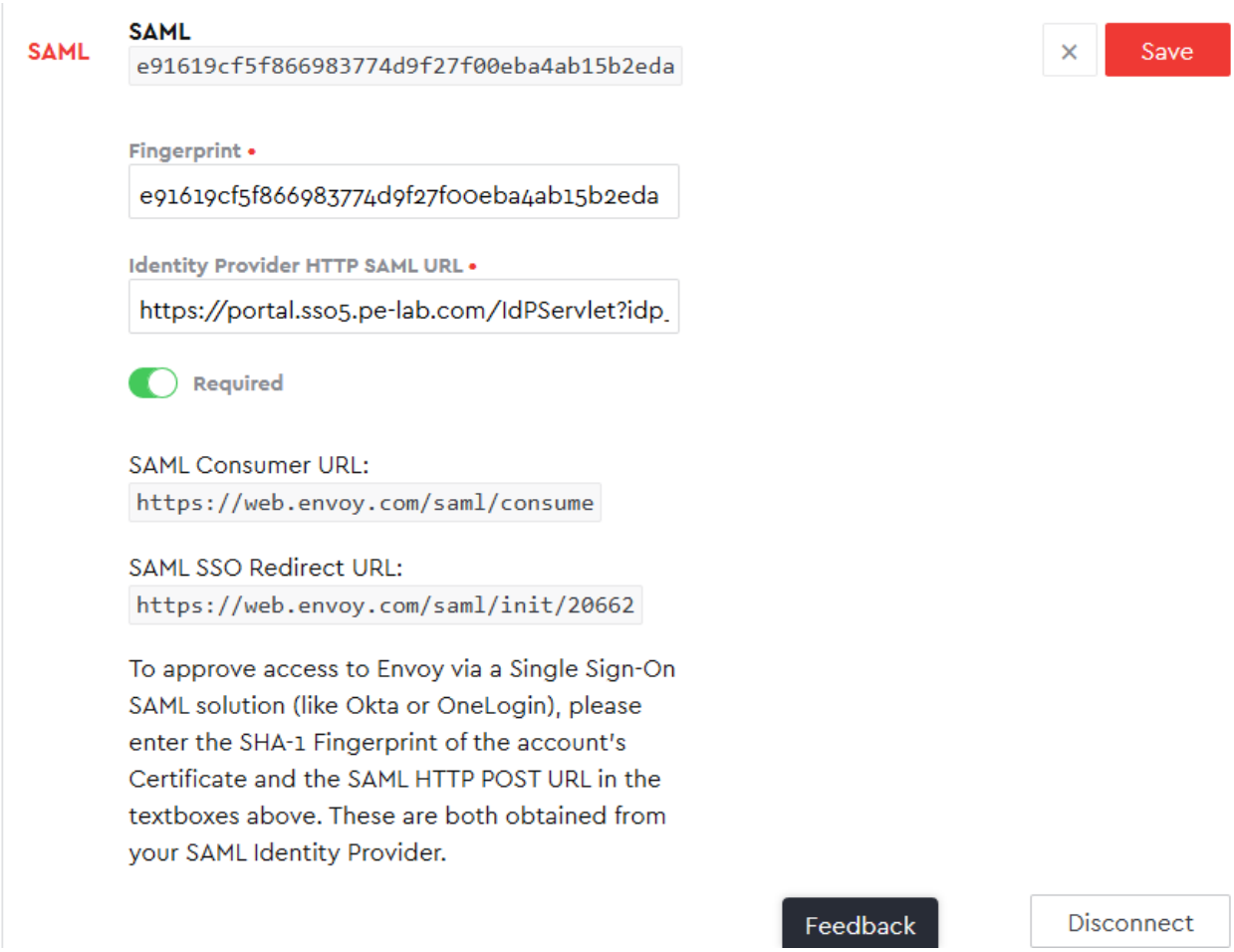
1. Login to your Envoy domain click on *Settings* – *Integrations* (https://dashboard.envoy.com/login)



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



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



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

AA