RSA SECURID® ACCESS
Implementation Guide

Robin

Gina Salvalzo, RSA Partner Engineering
Last Modified: August 30, 2017

RSA READY

Solution Summary

Robin is a meeting room booking system that simplifies your day. Robin makes scheduling meetings a snap with easy calendar integration, usage analytics and room displays. Robin delivers a single sign on experience to the user through SAML. This integration supports both IdP and SP initiated authentication flows.

RSA SecurID Access Features	Robin
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

Configuration Summary

All of the supported use cases of RSA SecurID Access with Robin require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Robin can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

Cloud Authentication Service – Identity Router IdP Configuration
Robin SAML Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

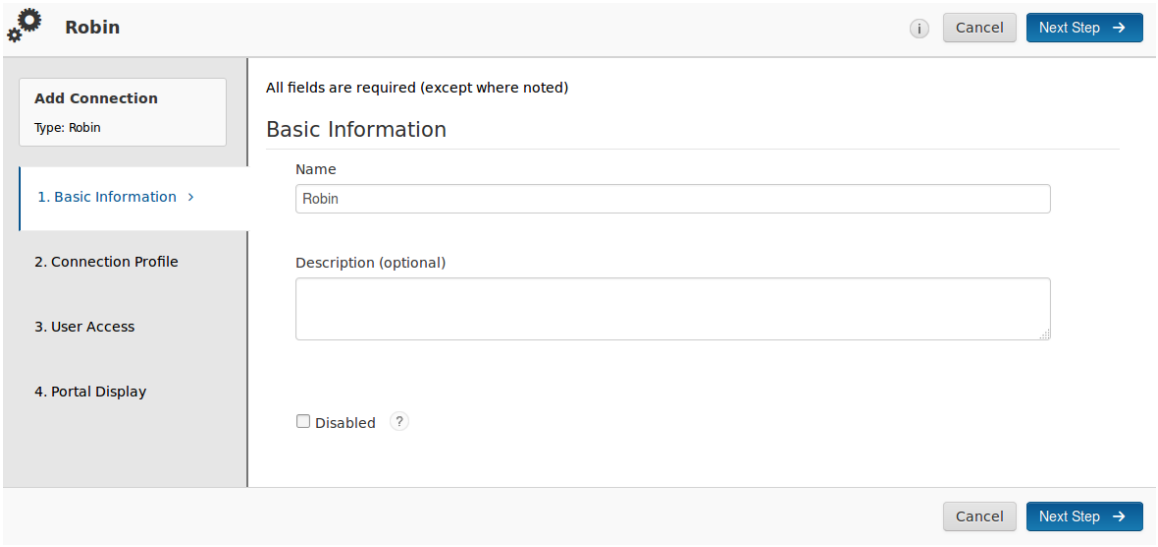
To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Robin in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

Configure RSA Identity Router SAML IdP

Procedure

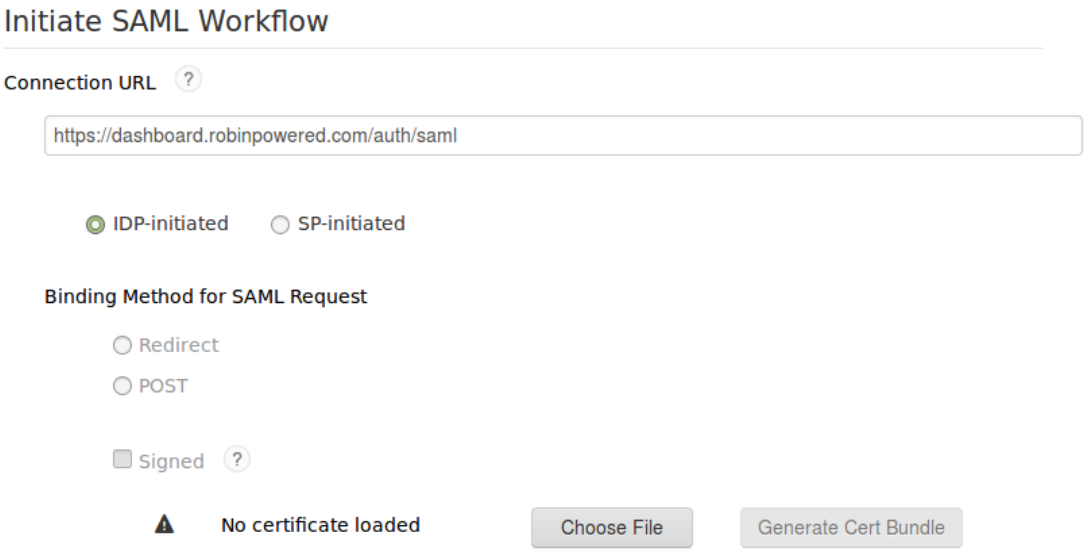
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Robin.

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

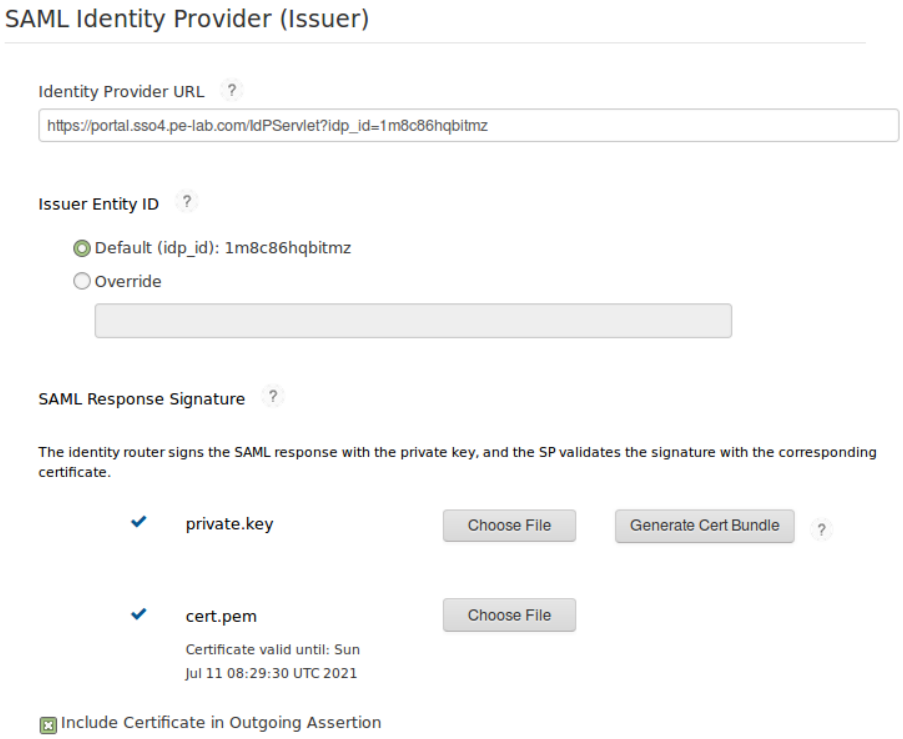


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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

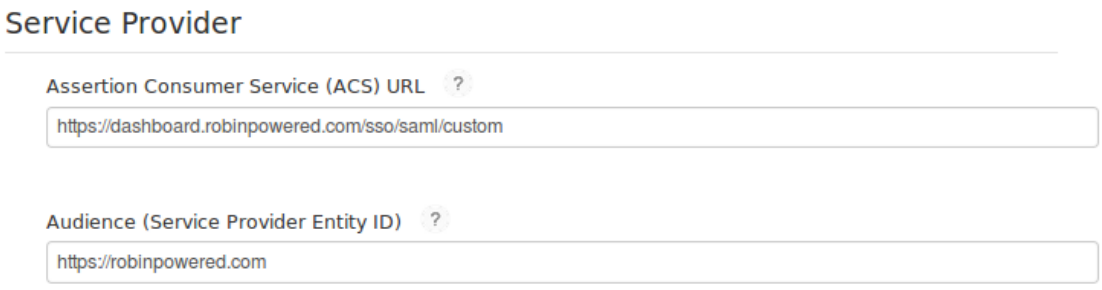


5. Scroll down to **SAML Identity Provider (Issuer)** section.



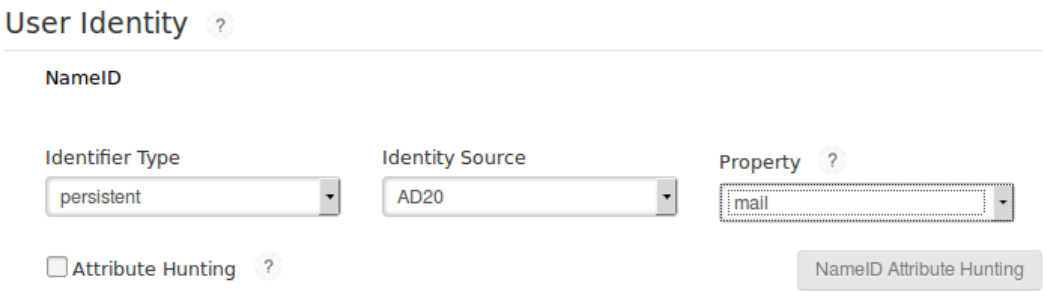
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File**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

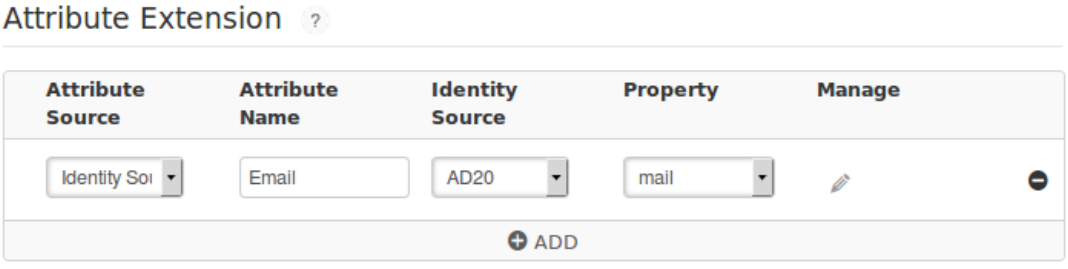


   a) In the Assertion Consumer Service (ACS) URL field, provide the value as per received with service provider metadata.
   b) In the Audience (Service Provider Issuer ID) field, provide the value as per received with service provider metadata.

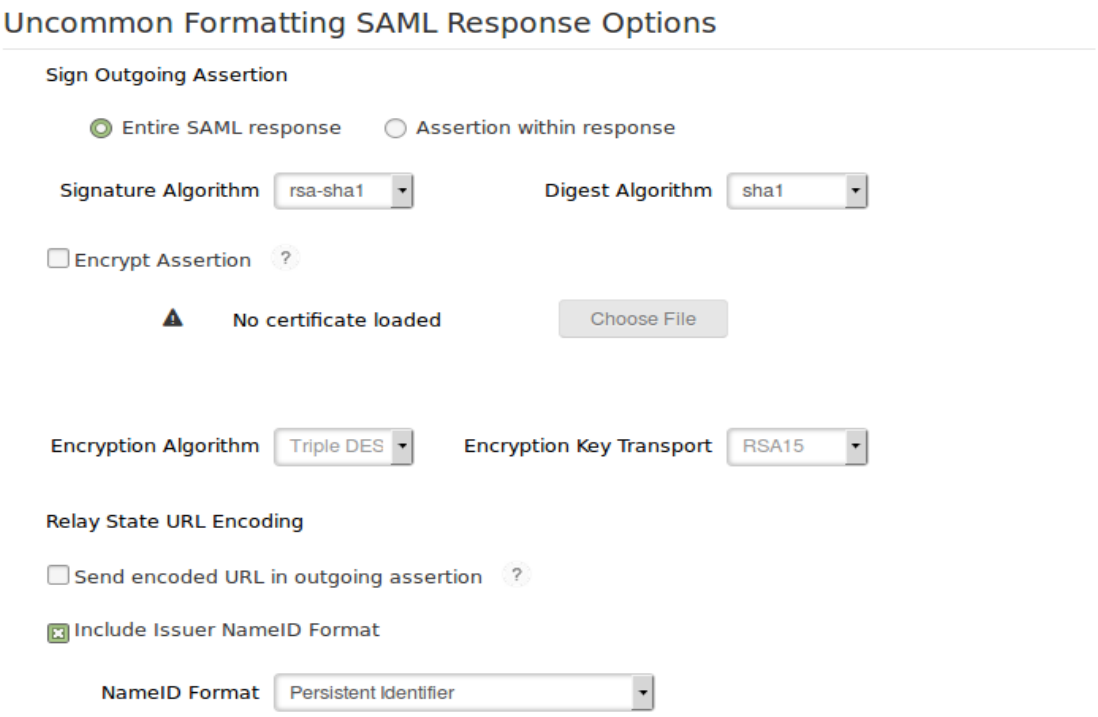
7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



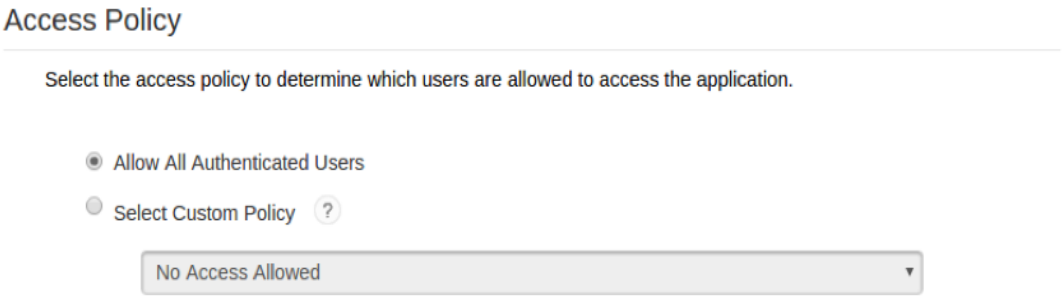
8. Select **Show Advanced Configuration**. In the **Attribute Extension** section, add **Email**. These are mandatory provisioning attributes needs to be forwarded at the time of SSO.



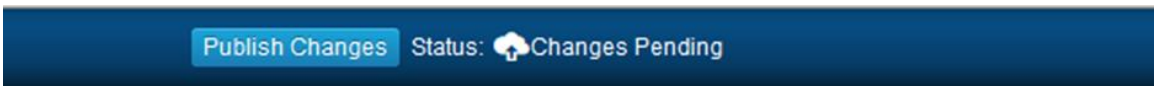
9. Under Uncommon Formatting SAML Response Options, in the Relay State URL Encoding section, check **Include Issuer NameID Format** and from the NameID Format dropdown select **Persistent Identifier**.



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



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



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Robin with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

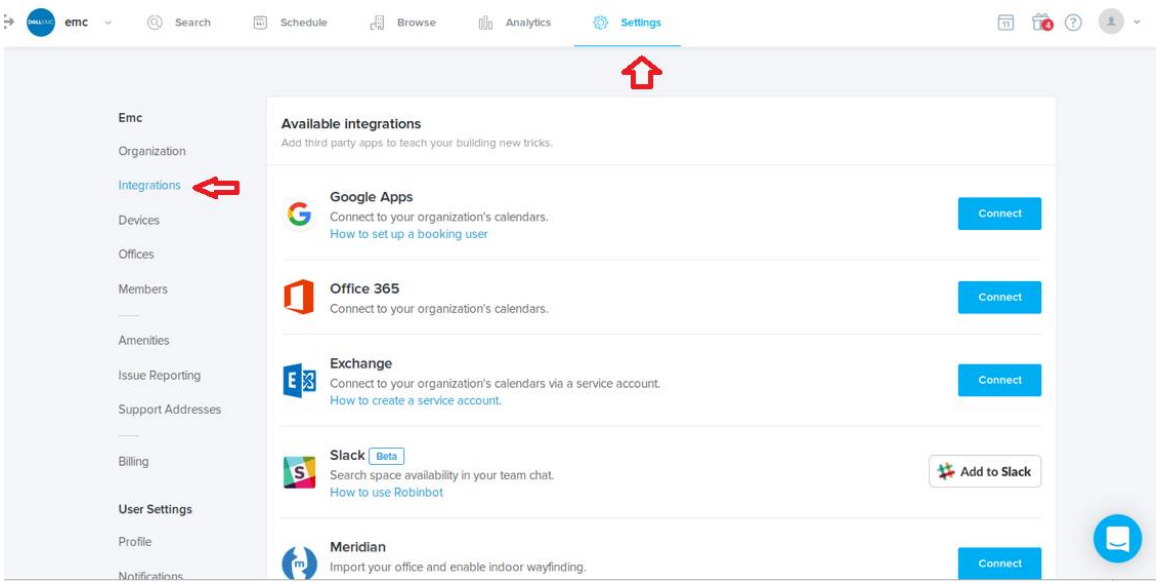
All Robin components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Robin SAML Configuration

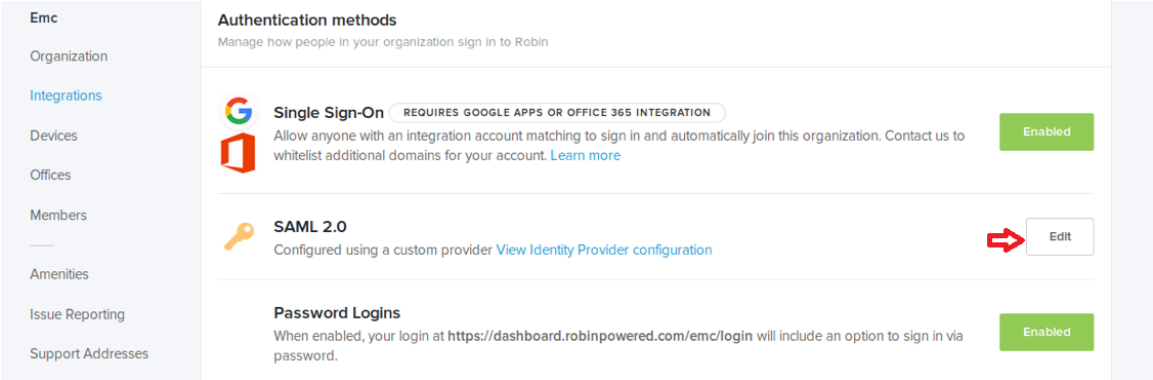
Procedure

1. Login to your Robin application web account.
   https://dashboard.robinpowered.com/<domain>/login

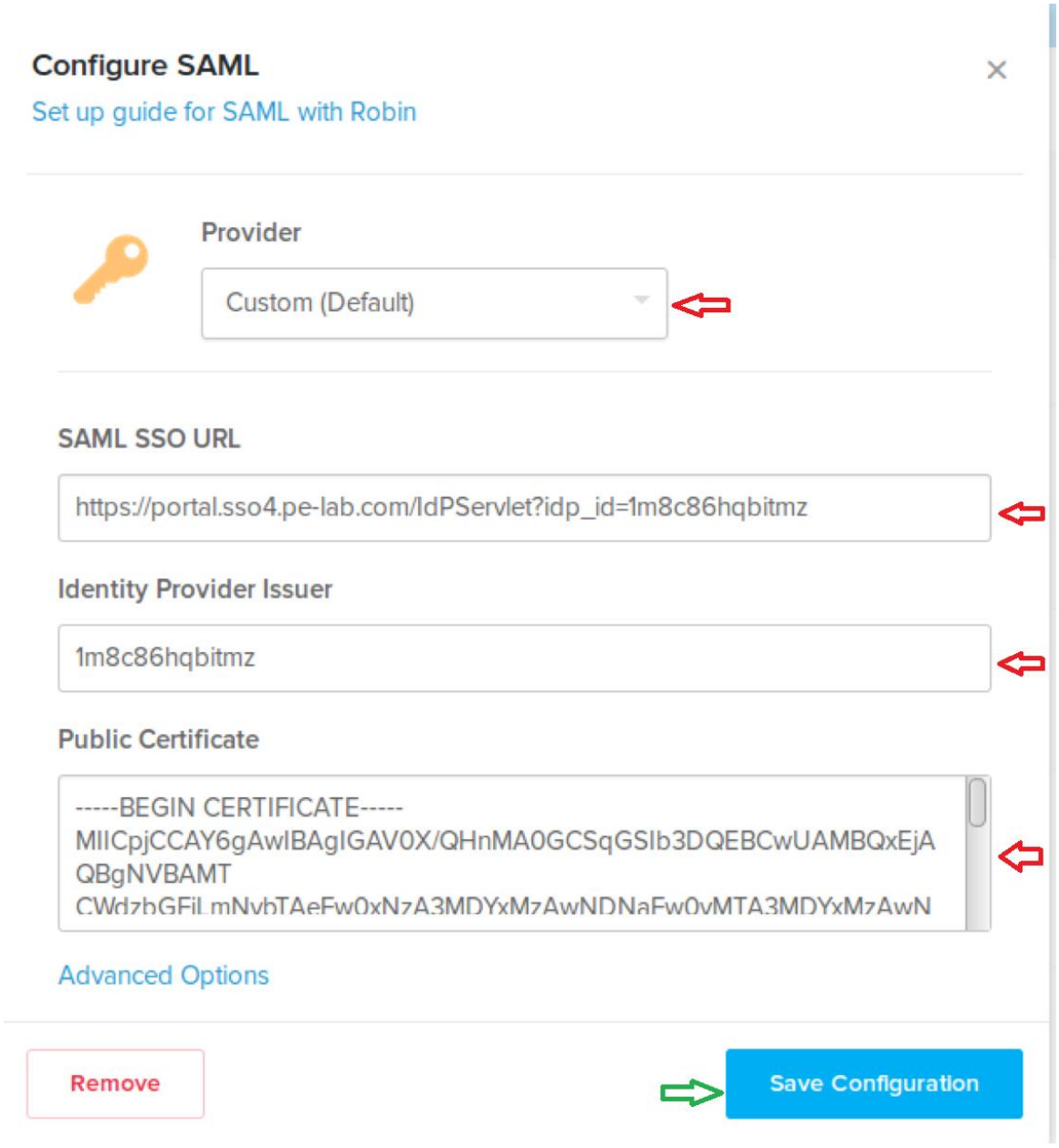
2. Following UI will be displayed. Go to *Settings (geared icon)* → *Integrations*.



3. Scroll down to *Authentication methods* > *SAML 2.0*. Click on the **Edit** button.



4. The following UI will be displayed.



a) Choose **Custom(Default)** from available drop down options for **Provider** field.
b) **SAML SSO URL** : Enter the **Identity Provider URL** which can be found in *step – 5* on *page 6*. It is of following format : **https://<Your_Portal_URL>?idp_id=<Unique_IdP_ID>**
c) **Identity Provider Issuer** : Enter IDP Issuer Entity ID value received from idp settings.
d) **Public Certificate** : Paste the RSA SecurID Access IdP public certificate here.
e) Once sure of all the settings, click on **Save Configuration** button to complete the configurations.