RSA SECURID® ACCESS
Implementation Guide

Rollbar

Gina Salvalzo, RSA Partner Engineering
Last Modified: February 07, 2018

RSA READY

Solution Summary

Rollbar provides real-time error alerting & debugging tools for developers. Ruby, Python, PHP, Node.js, JavaScript, Android, iOS etc. languages supported. Rollbar application does not support auto-provisioning of the user.

RSA SecurID Access Features	
Rollbar	
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 Rollbar 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 – Rollbar 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
Rollbar 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 Rollbar 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

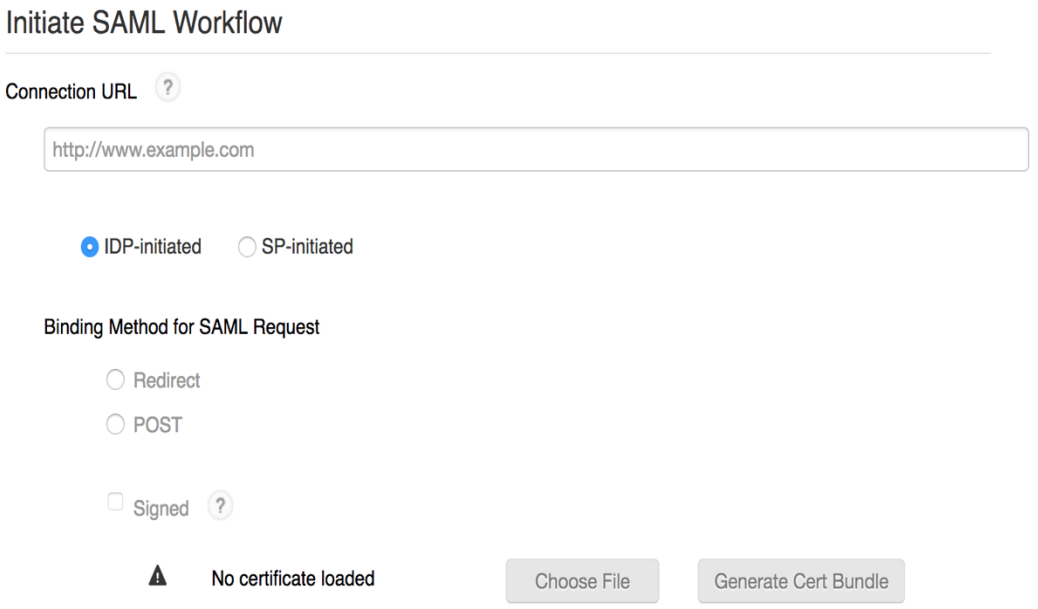
Procedure

1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for Rollbar and click **+Add** to add the connector.

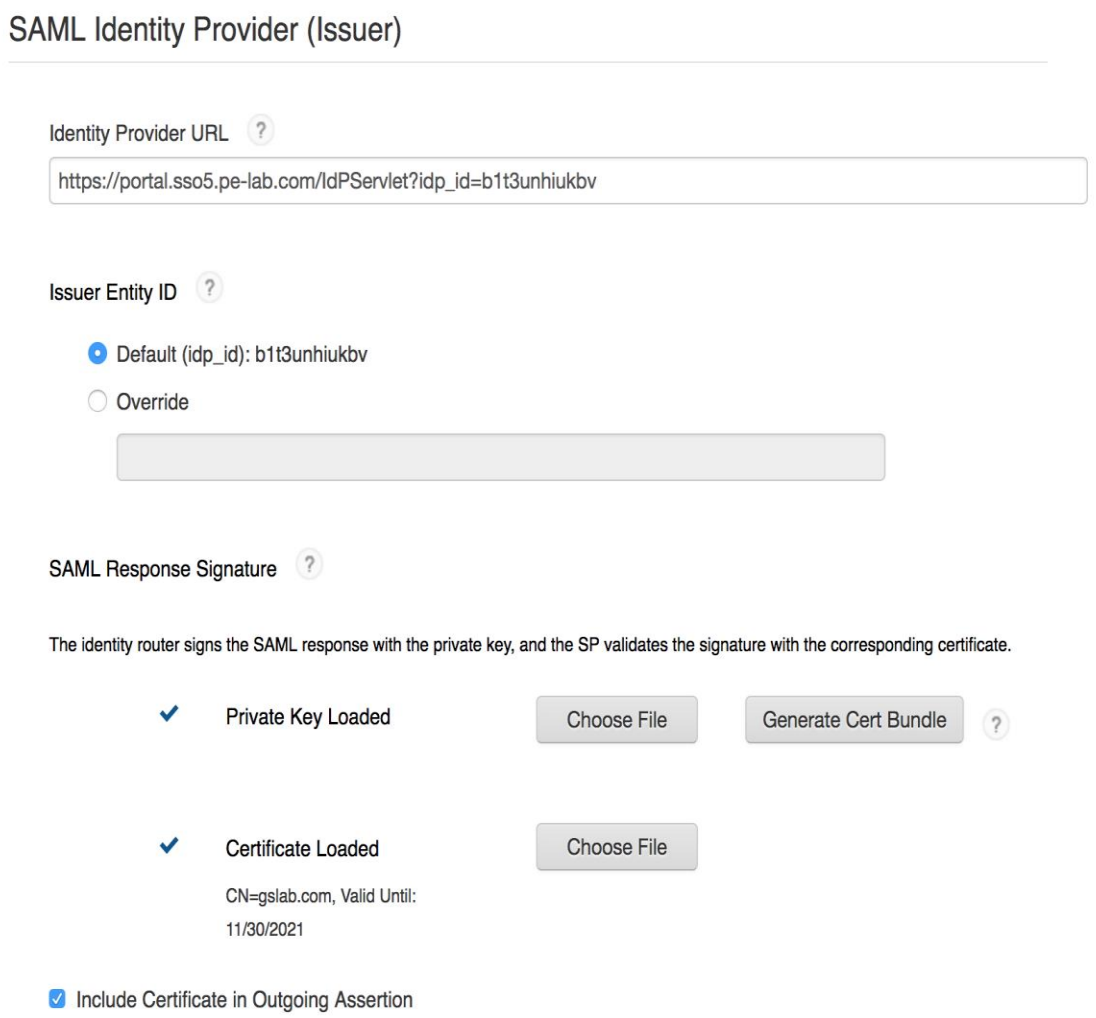
2. Enter a name for the application i.e. *Rollbar* in the **Name** field on the Basic Information page and click the **Next Step** button.

3. Navigate to Initiate SAML Workflow section.
    a. In the **Connection URL** field, leave the field blank as no value is required.
    b. Choose **IDP-initiated**.

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

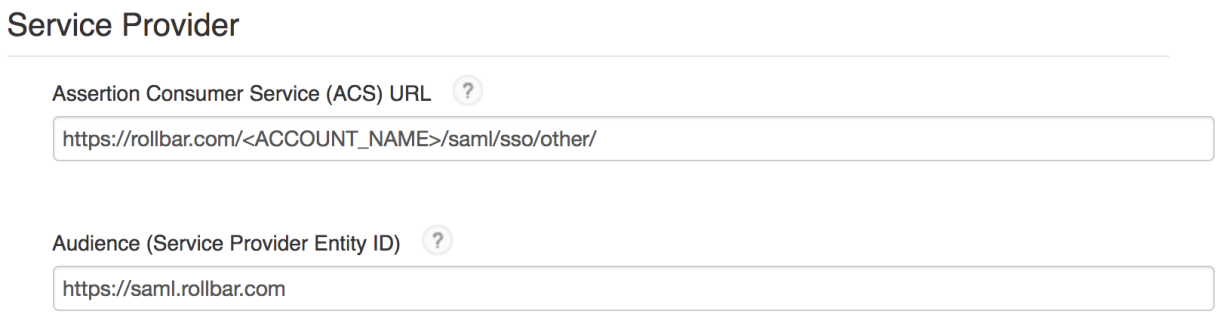


4. Scroll down to SAML Identity Provider (Issuer) section.



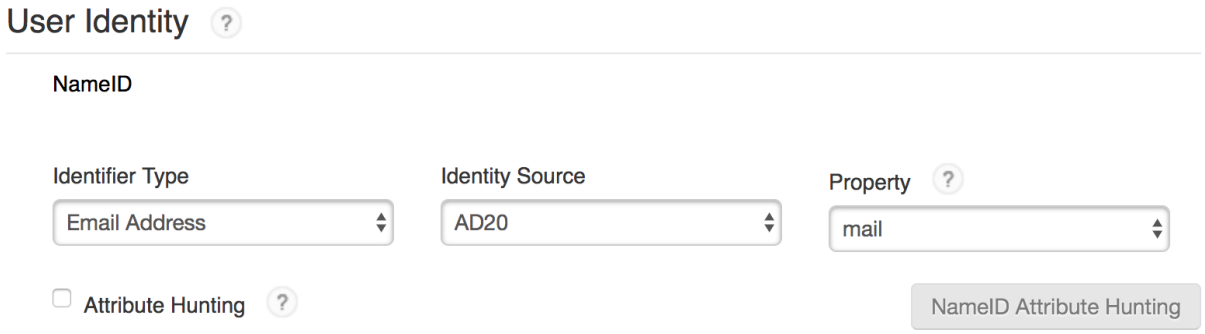
a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File**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

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



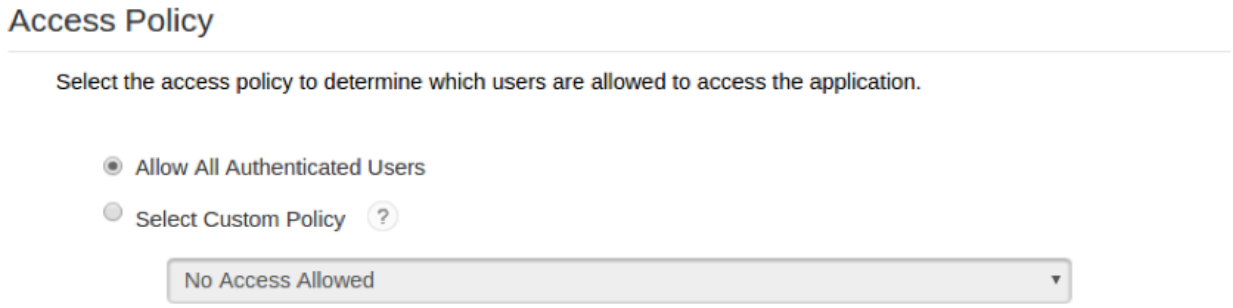
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <ACCOUNT_NAME> value as per your username for the account.
   b. In the **Audience (Service Provider Issuer ID)** field, the value as been defined for you but can be modified if required.

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

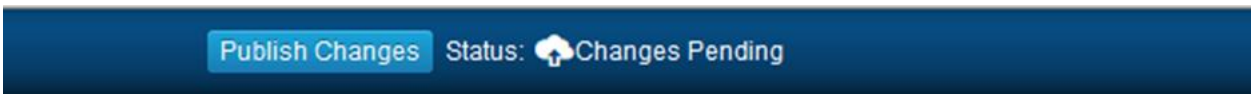


7. Click **Next Step**.

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



9. Click **Next Step**.
10. On the **Portal Display** page, select **Display in Portal**.
11. Click **Save and Finish**.
12. Click **Publish Changes**.



13. Navigate to **Applications** > **My Applications**.
14. Locate Rollbar in the list and from the **Edit** option, select **Export Metadata**.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Rollbar 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.

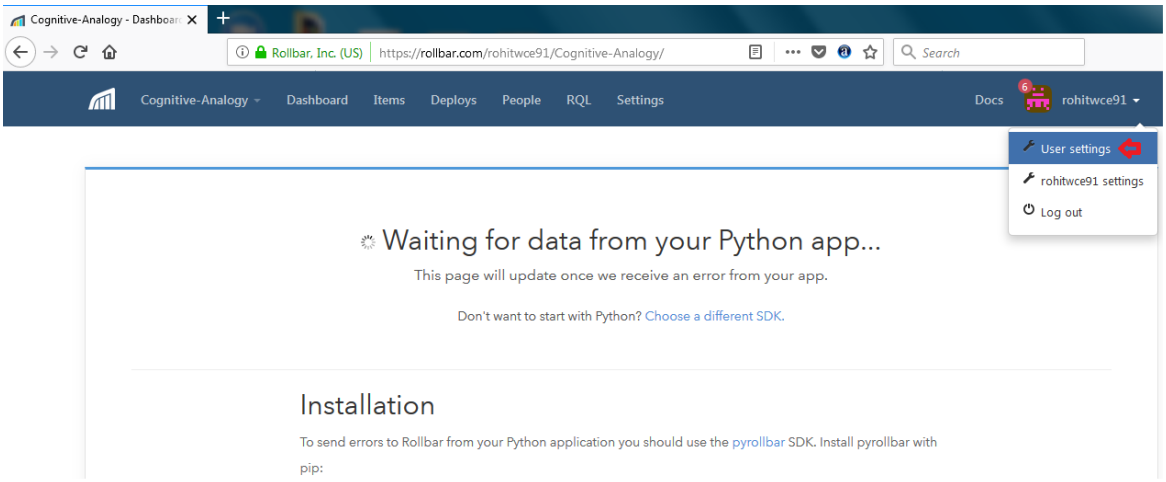
All Rollbar components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Rollbar SAML Configuration

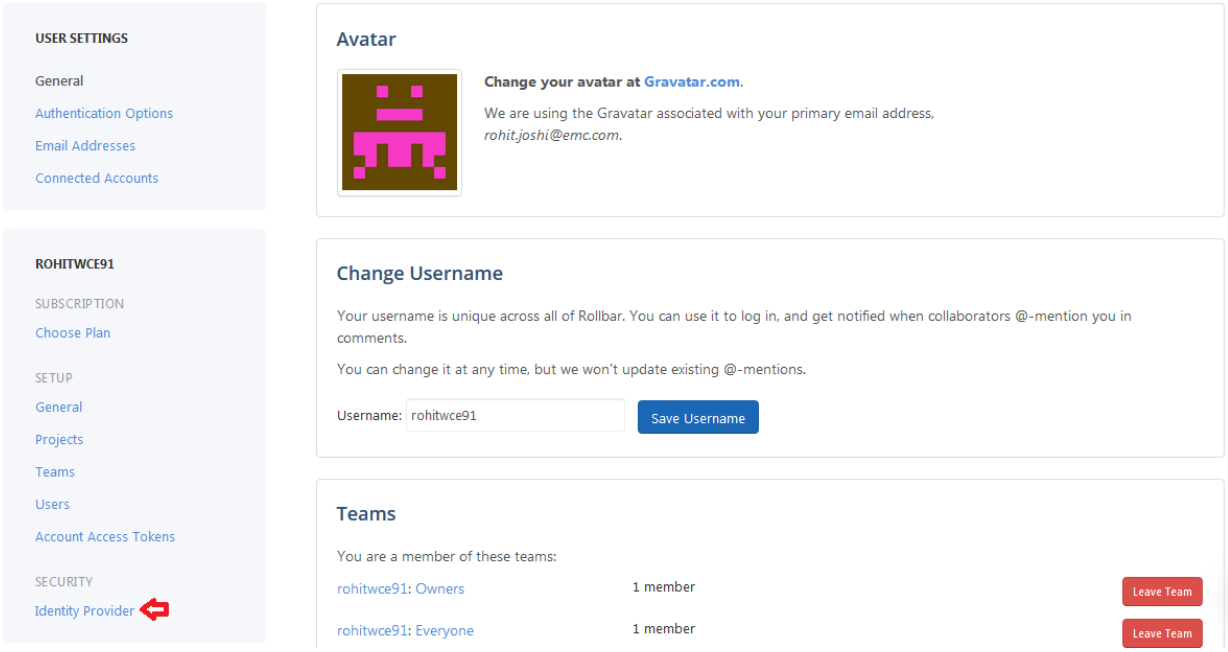
Procedure

1. Sign in to your Rollbar application web account.
   https://rollbar.com/login/

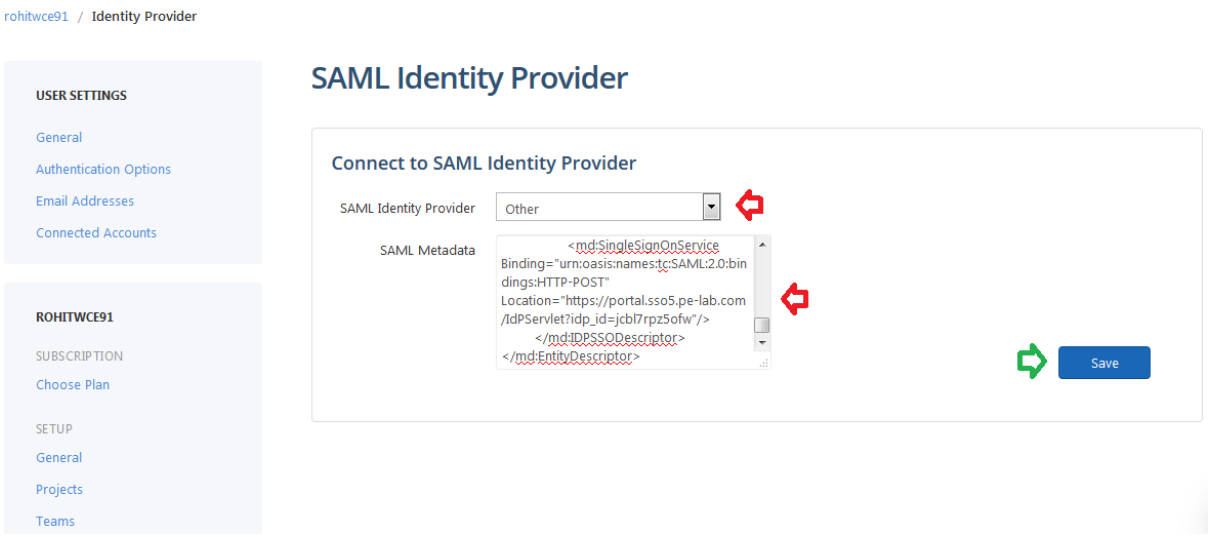
2. Following UI will be displayed. Select your username then *User settings*.



3. Following UI will be displayed. Go to *SECURITY -> Identity Provider.*



4. Following UI will be displayed. Start editing SAML settings under *SAML Identity Provider* section.



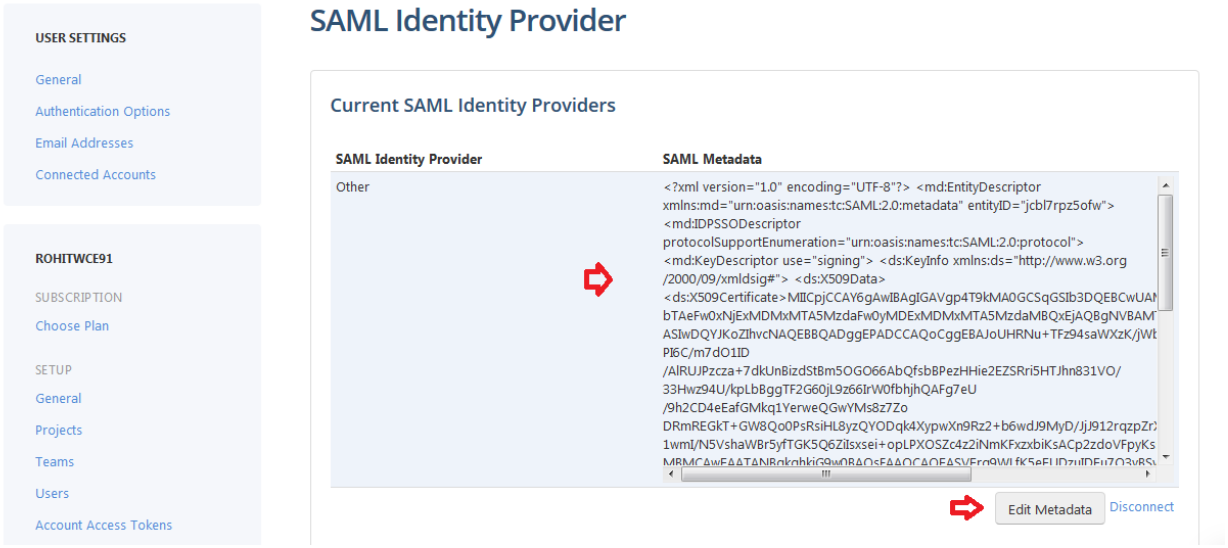
5. In the SAML Identity Provider field, select **Other** from the drop down list.
6. Using a text editor modify the identity provider metadata file that you downloaded from step 14 on page 8 and paste it in the SAML Metadata window. Add the follow 2 lines if missing.

<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>

<md:SingleSignOnService Location="*IDP URL*" Binding="**urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>**

7. Click **Save**.

8. Once SAML configurations completed, following UI will be displayed. You can *Edit Metadata* OR *Disconnect* and configure new identity provider settings as per need here.



9. Your Rollbar account is now enabled for SAML SSO authentication.