RSA SECURID® ACCESS
Implementation Guide

Skuid

Gina Salvalzo, RSA Partner Engineering
Last Modified: October 16, 2017

RSA READY

Solution Summary

Skuid is a CRM platform for company. An organization can drive rapid sales innovation and engagement with Skuid's no-code design-and-deploy platform. Skuid 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	Skuid
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 Skuid 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 – Skuid 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
Skuid 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 Skuid 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.

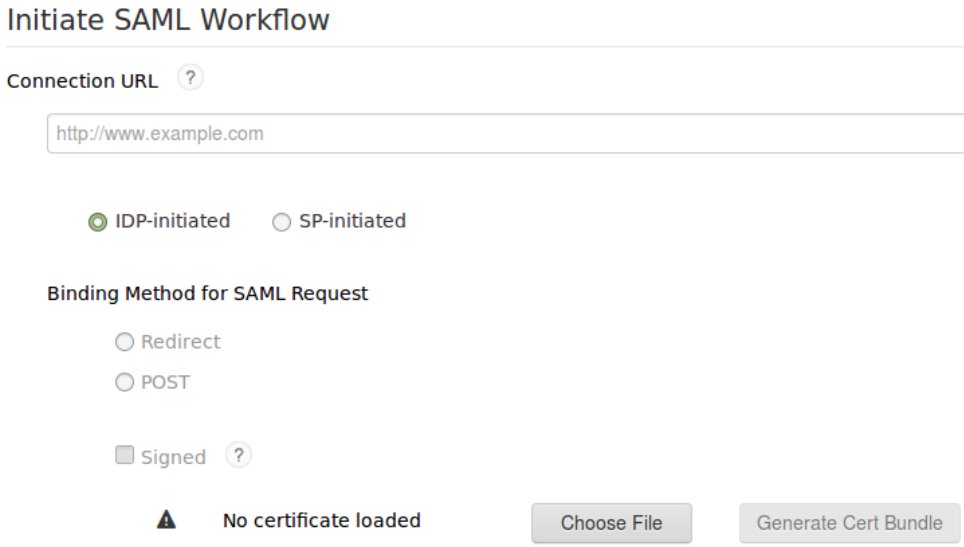
Configure RSA Identity Router SAML IdP

Procedure

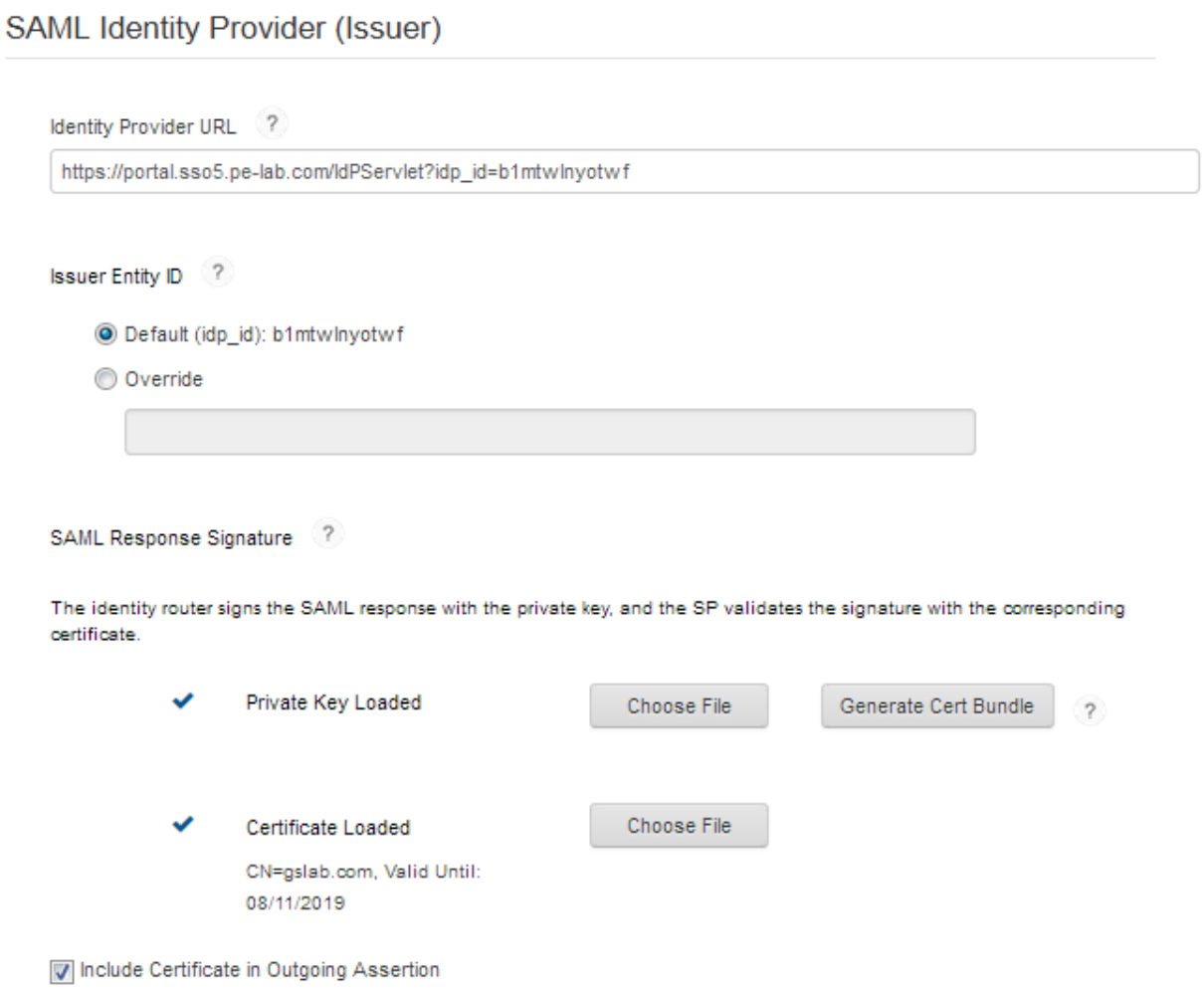
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for Skuid and click **+Add** to add the connector.

2. Enter a name for the application 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, keep the field blank as the value is not required.
    b. Choose **IDP-initiated.**

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

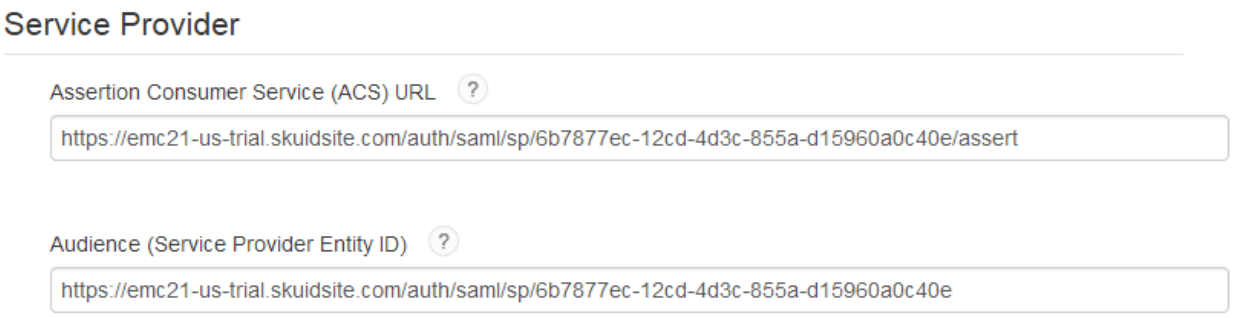


4. Scroll down to SAML Identity Provider (Issuer) section.

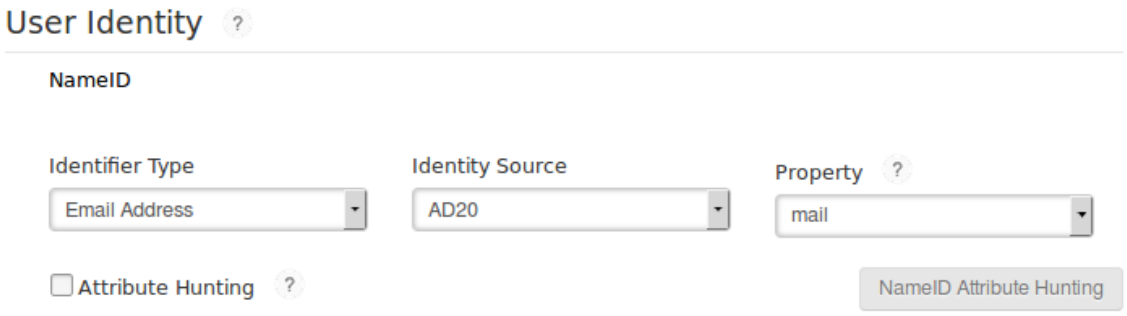


a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File**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

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

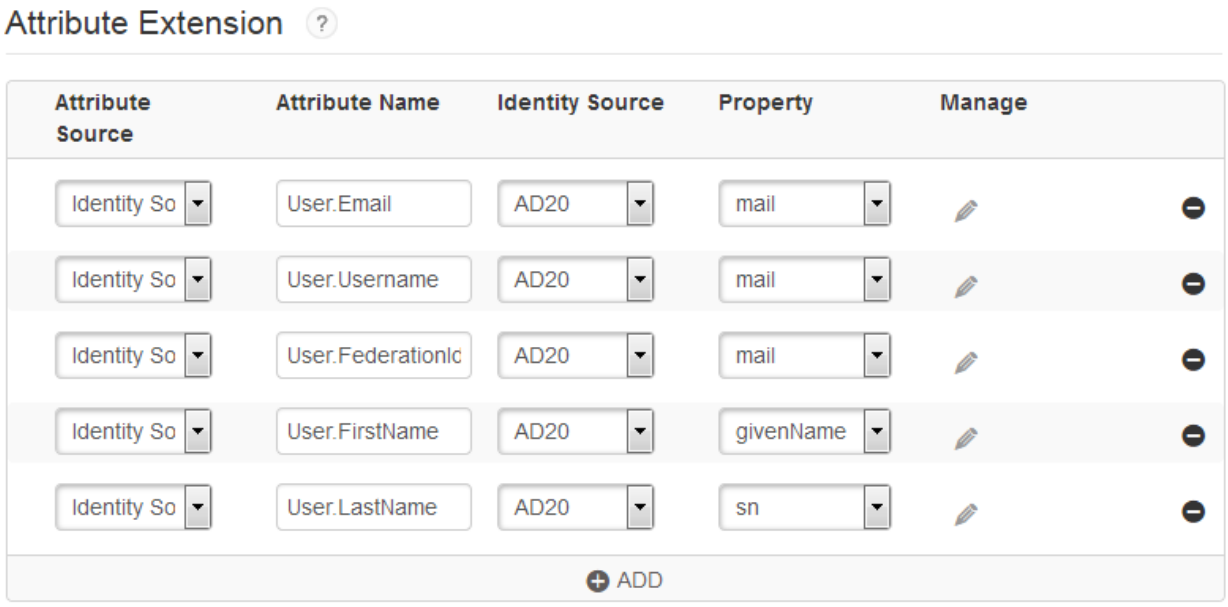


6. In the **Assertion Consumer Service (ACS) URL** field, insert the value from step 11 page 13.
7. In the **Audience (Service Provider Issuer ID)** field, insert the value from step 11 page 13.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

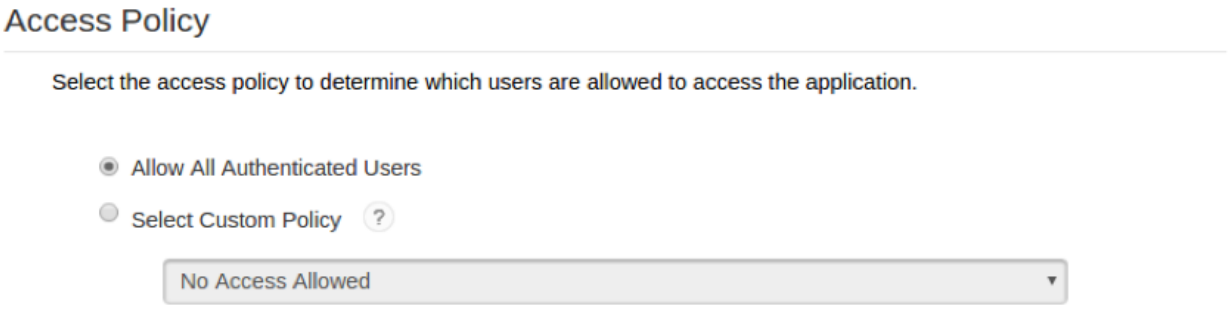


9. Scroll down below to *Advanced Configuration* section. Verify the settings are correct for your environment. **User.Email** is a required attribute.
   In this example, *User.FirstName* will be validated against *givenName* from the user store selected.

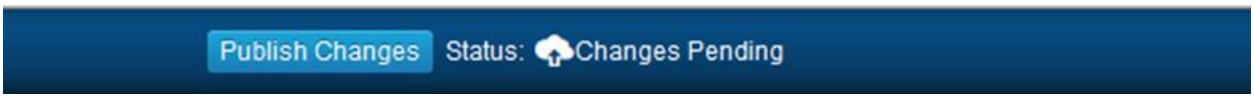
> **Note: If you have selected** User Provisioning **in Skuid settings then all attributes are required.**



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 Skuid with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

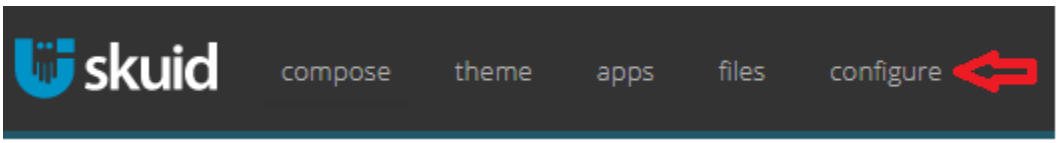
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

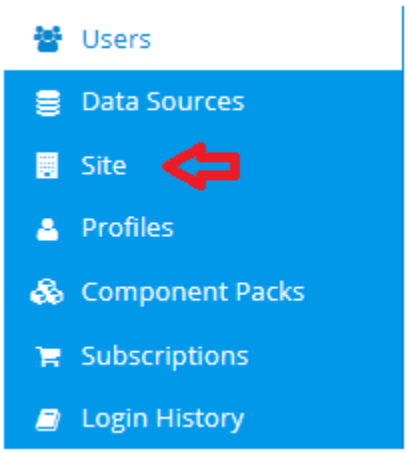
Skuid SAML Configuration

Procedure

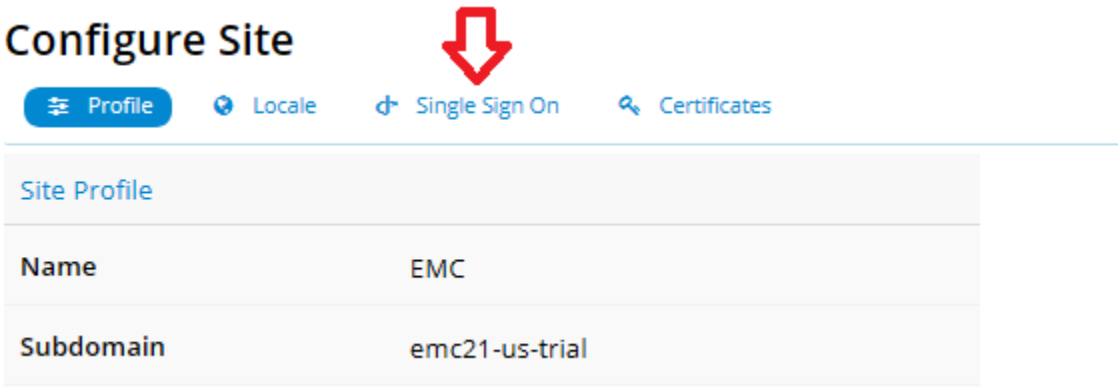
1. Login to your Skuid application web account.
   https://<COMPANY_NAME>.skuidsite.com/ui/login
2. On the displayed page, go to *configure.*



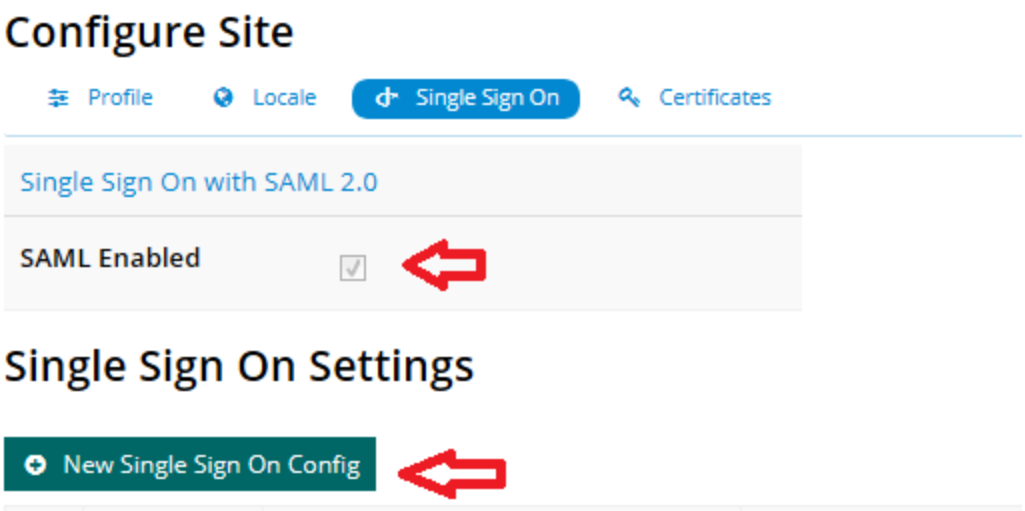
3. Following UI will be displayed. Go to *Site* tab.



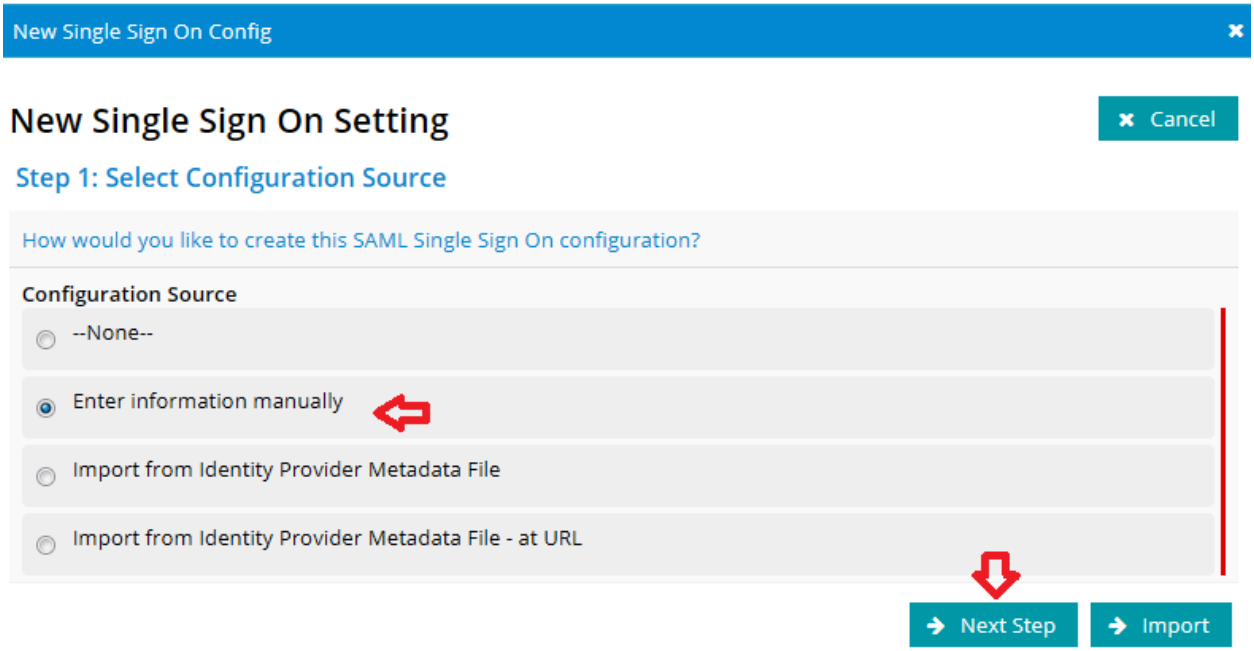
4. On the displayed page, Click on *Single Sign On* option.



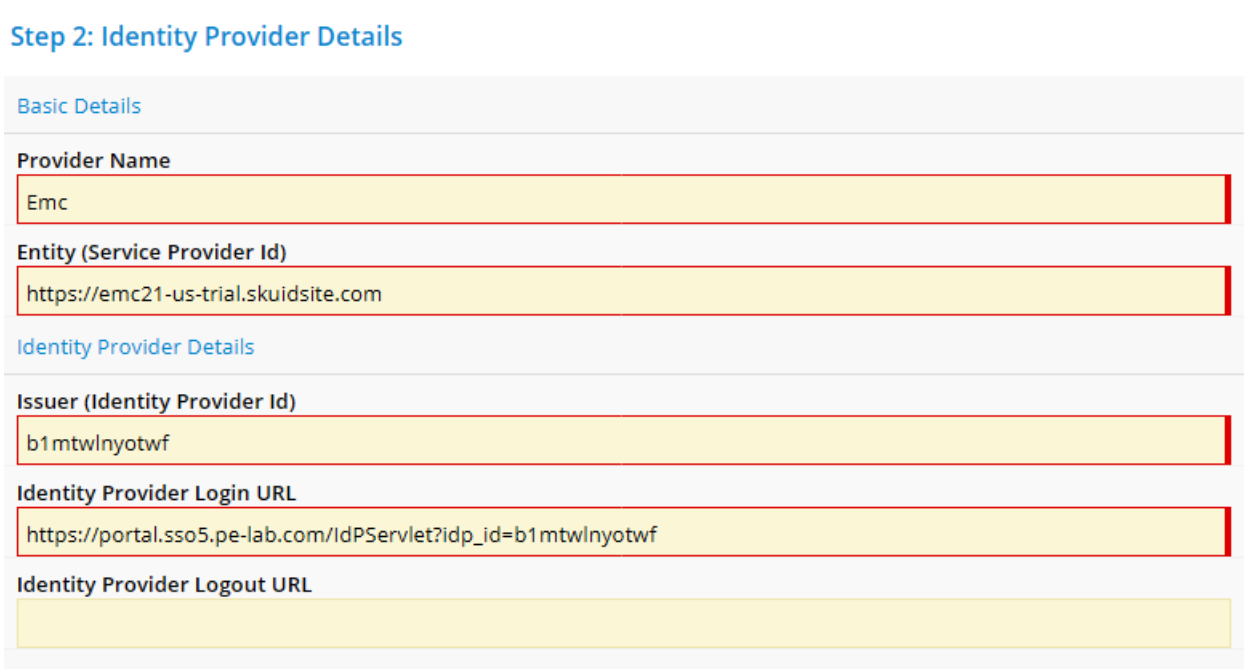
5. On the displayed settings, tick on *SAML Enabled* checkbox as shown in image below. Click on *New Single Sign On Config* to create new SAML configuration.



6. Click on *Enter information manually* option. Click on *Next Step*.



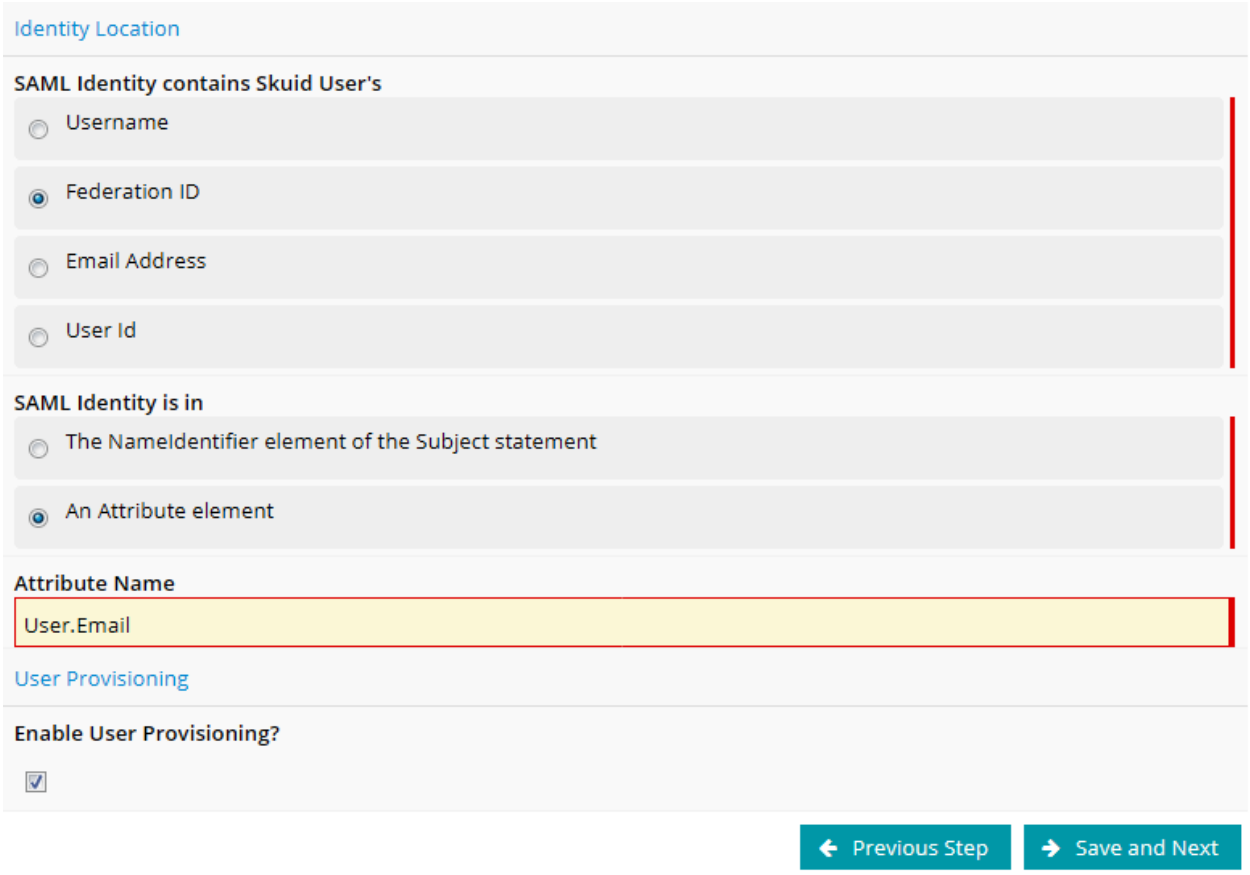
7. Below settings will get displayed.



a) **Provider Name**: Enter provider name of your choice to identify settings.
b) **Entity:** Enter your domain name for Skuid. This will be replaced by Skuid after settings are complete.
c) **Issuer:** Enter **IDP ID** value received from IDP settings.

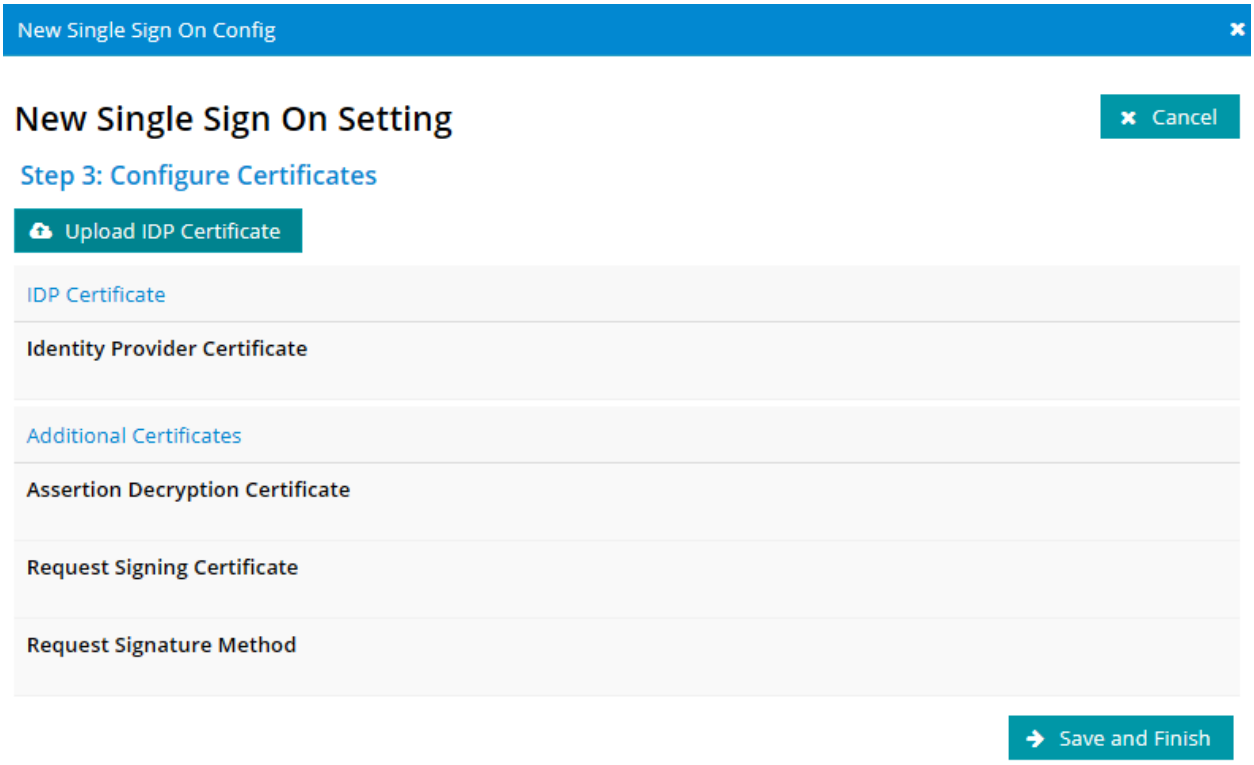
d) **Identity Provider Login URL:** Enter IDP URL value received from idp settings.
e) **Identity Provider Logout URL:** This field is not mandatory and can be left blank.

8. Scroll down to the below section.

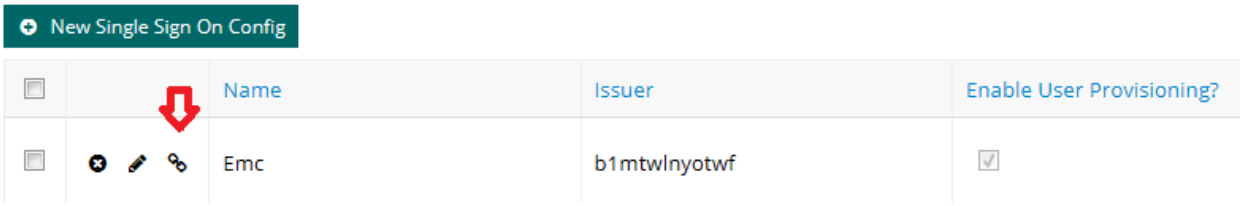


a) Select *SAML Identity contains Skuid User's* **Federation ID**.
b) Select *SAML Identity is in* **An Attribute element**.
c) Enter Attribute Name as **User.Email**. Note that here Federation ID is User.Email which is used to check user's identity.
d) If you want to enable user provisioning, then select checkbox for **Enable User Provisioning**.
e) Click on ***Save and Next***.

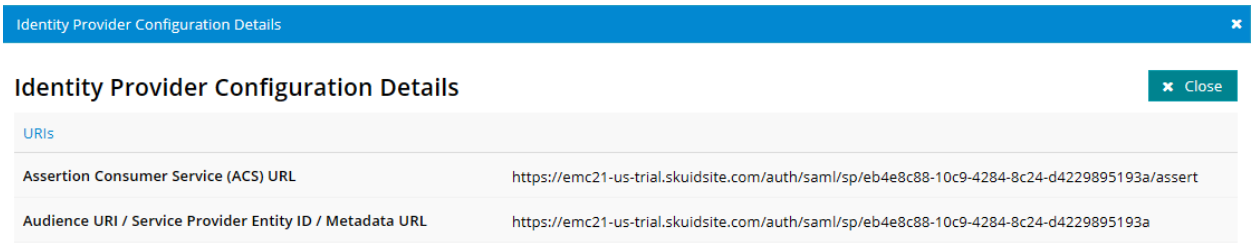
9. Click on *Upload IDP Certificate* in the displayed UI. Select the **IDP public Certificate** you have uploaded in IDP configuration. Click on *Save and Finish*.



10. You will see your SP configurations as shown below. Click on *chain icon* as shown.



11. You will get **ACS URL** needed to configure the IDP in step 6 page 6.



12. Click the pencil icon to get the Entity ID (Service Provider Id) which has been updated and is needed to configure the IDP in step 7 page 6.
13. Click on **Save** in the upper right corner of the page.

Note: Before testing make sure your user profile has Skuid Page Viewer permission.