

RSA SECURID[®] ACCESS

Implementation Guide

Skeddly

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

Solution Summary

Skeddly automates your Amazon Web Services resources. Schedule AWS EC2 backups and simplify your snapshots. Skeddly delivers a single sign on experience to the user through SAML. This integration supports IdP initiated authentication flow.

RSA SecurID Access Features	
Skeddly	
On Premise Methods	
RSA SecurID	<input checked="" type="checkbox"/>
On Demand Authentication	<input checked="" type="checkbox"/>
Risk-Based Authentication (AM)	<input type="checkbox"/>
Cloud Authentication Service Methods	
Authenticate App	<input checked="" type="checkbox"/>
FIDO Token	<input checked="" type="checkbox"/>
SSO	
SAML SSO	<input checked="" type="checkbox"/>
HFED SSO	<input type="checkbox"/>

Identity Assurance	
Collect Device Assurance and User Behavior	<input checked="" type="checkbox"/>

Configuration Summary

All of the supported use cases of RSA SecurID Access with Skeddly 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 – Skeddly 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 Skeddly 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 Skeddly 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** Skeddly.



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

Skeddly

All fields are required (except where noted)

Basic Information


Name
Skeddly

Description (optional)

Disabled ?

Cancel Next Step →

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

 **Note:** Skeddly application supports IDP-initiated SSO only.

Initiate SAML Workflow

Connection URL ?

http://www.example.com


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?

 No certificate loaded

Choose File

Generate Cert Bundle

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?
 Default (idp_id): 1b5uk0iyql6p7
 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.

Private Key Loaded ?

Certificate Loaded
CN=gslab.com, Valid Until:
05/03/2021

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**.
- c. Select **Choose File** and upload the private key.
- d. Select **Choose File** and 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 ?

Audience (Service Provider Entity ID) ?

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: unspecified

Identity Source: AD20

Property: mail

Attribute Hunting ? NameID Attribute Hunting

8. Select **Show Advanced Configuration**.
9. In the Attribute Extension section, select **Identity Source** as the Attribute Source. Enter <https://skeddly.com/SAML/Attributes/Roles> in the Attribute Name field. Select the **Property** attribute which must contain the Skeddly Provider SRN appended by a comma-separated list of policies roles:
 - a. The Skeddly Provider SRN can be copied from your identity provider's "view" page in your Skeddly account. Refer to page 10 step 4.
 - b. Append a comma and one or more SRNs of Managed Policies to be applied to the user when they are signed-in. These SRNs can be found on the *Users & Identity > Managed Policies* pages in your Skeddly account.

For example, the value for this Property attribute could be:
srn:skeddly:idp::6817f979:IDR, srn:skeddly:policy:::standard

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity So	https://skeddly.co	AD20	employeeTy	
+ ADD				

10. Click **Next Step**.

11. On the **User Access** page, select **Allow All Authenticated Users**.

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

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.

Publish Changes Status:  Changes Pending


16. Navigate to **Applications > My Applications**.
17. Locate Skeddly in the list and from the **Edit** option, select **Export Metadata**.



Skeddly
Created From: Skeddly
SAML Direct

Edit

 Edit

 Export Metadata

 Delete

Partner Product Configuration

Before You Begin

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

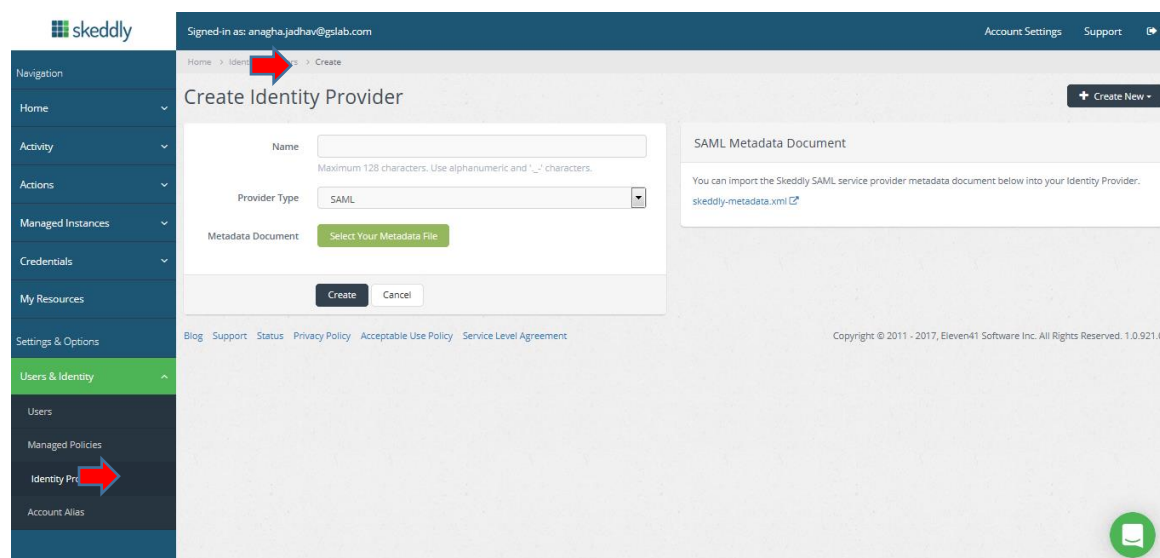
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Skeddly SAML Configuration

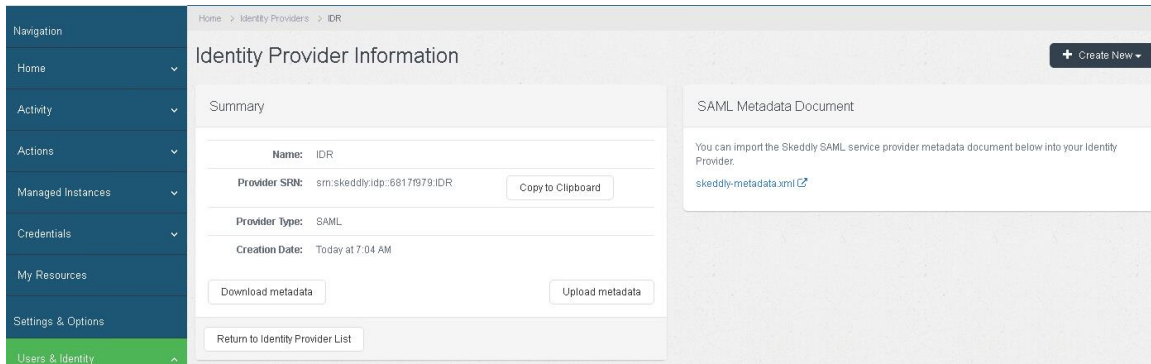
Procedure

1. Login to your Skeddly application web account.
(<https://app.skeddly.com/Account/LogOn>)
2. Navigate to *Users & Identity > Identity Providers*.
3. Click **Create Identity Provider**. Following UI will be displayed.



- a. Provide *Name* as name for identity provider.
- b. Select *Provider Type* as SAML.
- c. For *Metadata Document* field upload IDR metadata file. Refer to page 8 step 17.
- d. Click *Create* button.

4. Your Skeddly account is now enabled for SAML SSO authentication.



The screenshot shows the 'Identity Provider Information' page in the Skeddly interface. The page is divided into two main sections: 'Summary' and 'SAML Metadata Document'.

Summary:

- Name:** IDR
- Provider SRN:** sm:skeddly.idp:6817f979:IDR (with a 'Copy to Clipboard' button)
- Provider Type:** SAML
- Creation Date:** Today at 7:04 AM

Buttons at the bottom of the summary section include 'Download metadata', 'Upload metadata', and 'Return to Identity Provider List'.

SAML Metadata Document:

You can import the Skeddly SAML service provider metadata document below into your Identity Provider.

[skeddly-metadata.xml](#)