RSA SECURID® ACCESS
Implementation Guide

Skeddly

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

RSA READY

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	✓
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 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

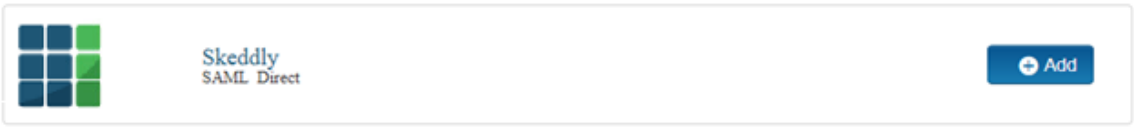
SAML via RSA Identity Router (IdP)

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.

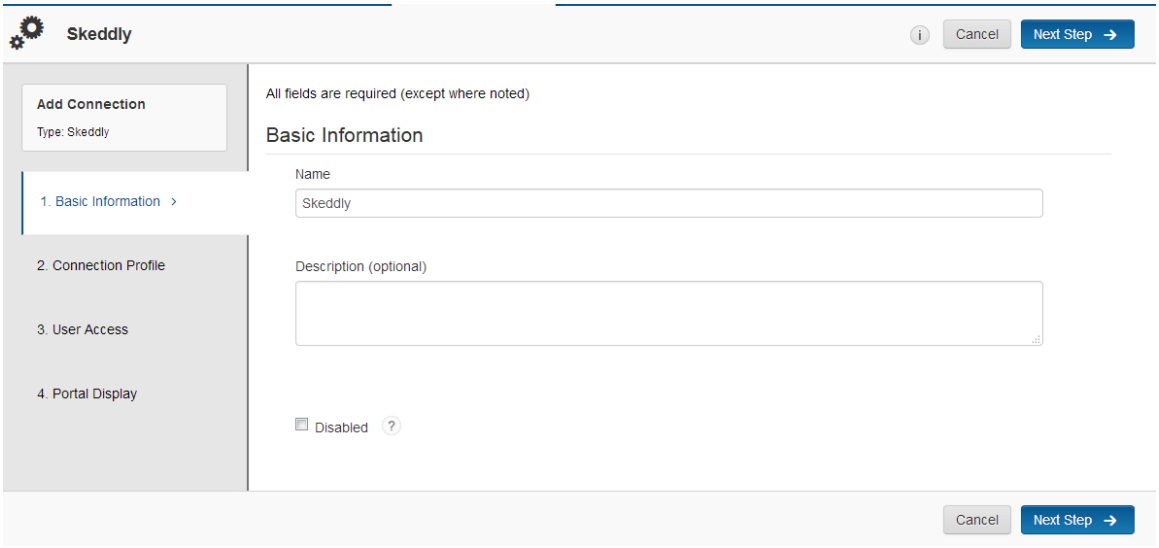
Configure RSA Identity Router SAML IdP

Procedure

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

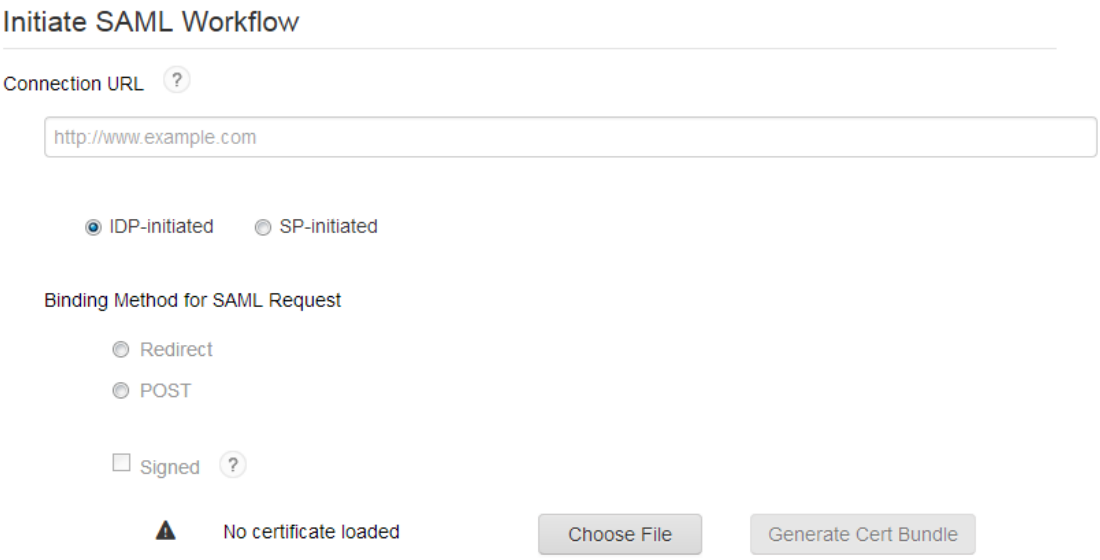


3. On the Basic Information page, specify the application name and click **Next Step**.

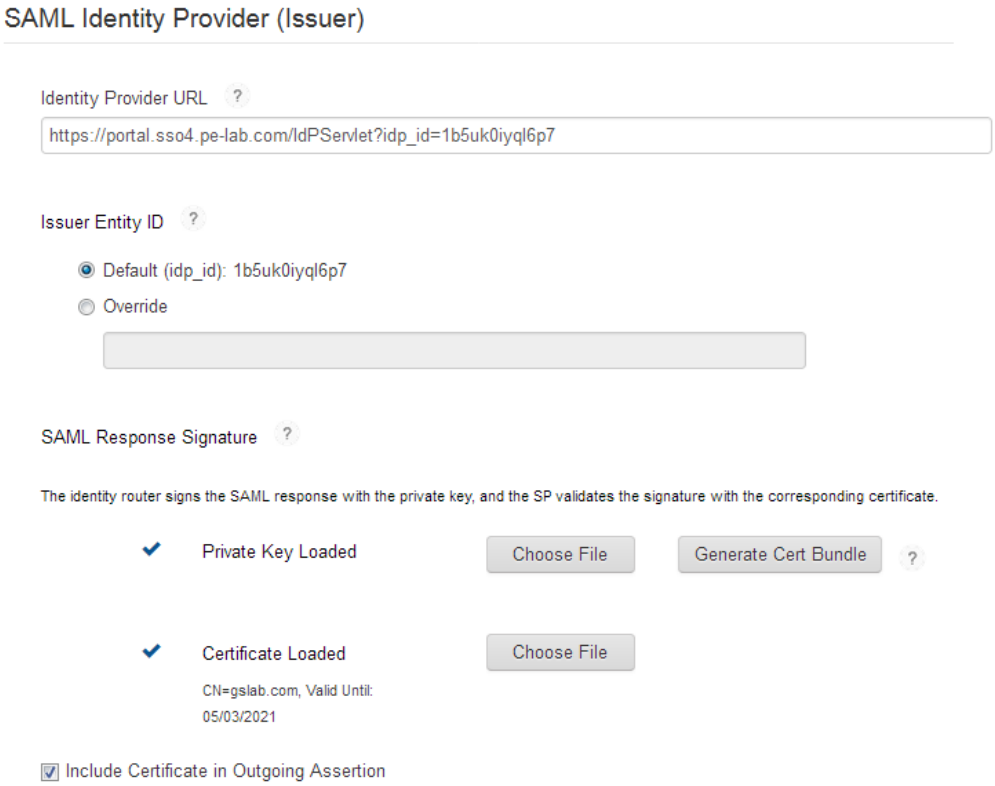


4. Navigate to **Initiate SAML Workflow** section.
   a. Keep the **Connection URL** field blank as the value is not required.
   b. Choose **IDP-initiated.**

Note: Skeddly application supports IDP-initiated SSO only.



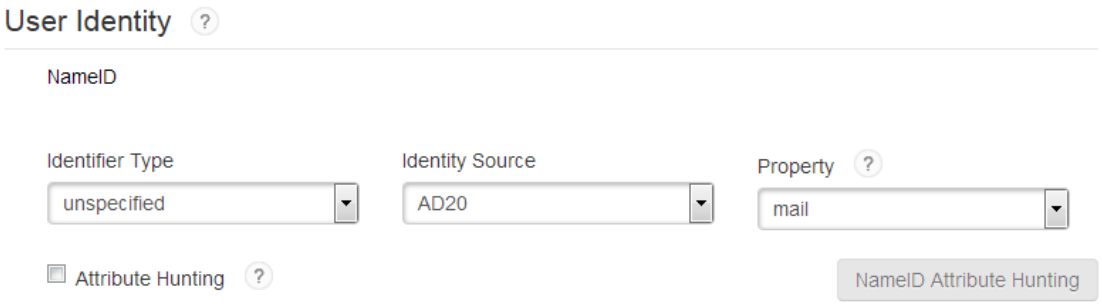
5. Scroll down to **SAML Identity Provider (Issuer)** section.



   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**.
   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**.

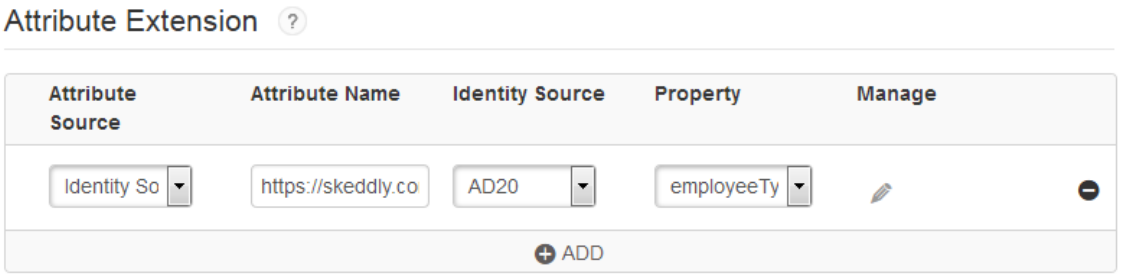
6. Scroll down to the **Service Provider** section.

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.



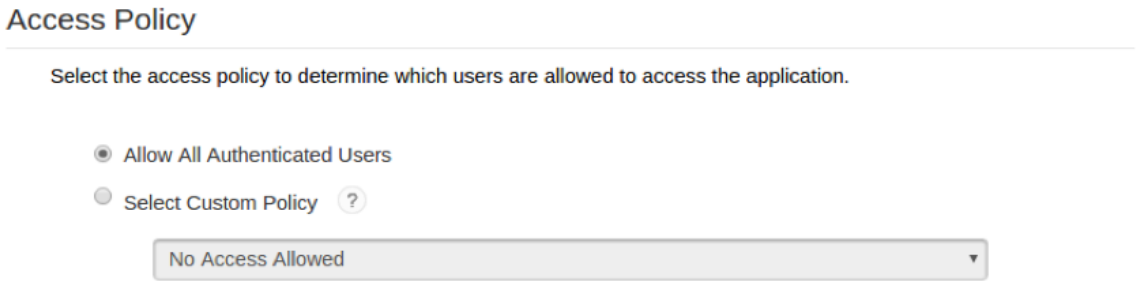
8. Select **Show Advanced Configuration**.
9. In the Attribute Extension section, select **Identity Source** as the Attribute Source. Enter **https://skeddly.com/SAML/Attributes/Roles** in the Attribute Name field. Select the **Property** attribute which must contain the Skeddly Provider SRN appended by a comma-separate 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



10. Click **Next Step**.

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



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.

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

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.

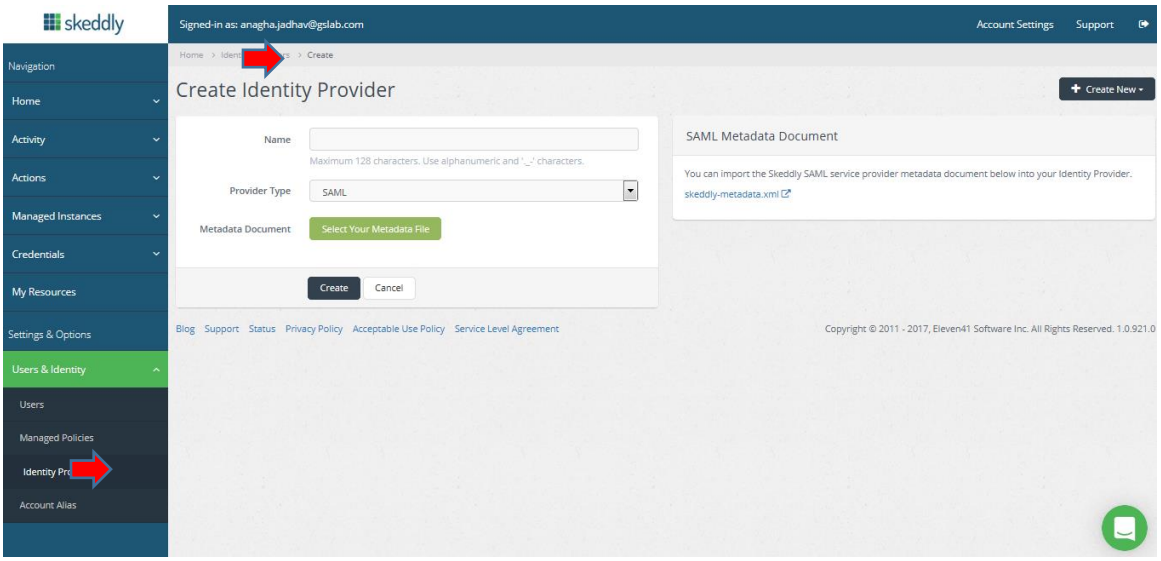
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.