RSA SECURID® ACCESS
Implementation Guide

KnowledgeOwl

Gina Salvalzo, RSA Partner Engineering
Last Modified: May 15, 2018

RSA READY

Solution Summary

KnowledgeOwl is a cloud-based knowledge management solution that is suitable for businesses of all sizes. KnowledgeOwl enables you to create a website to share information with customers, clients, employees, and others. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. KnowledgeOwl supports user auto-provisioning.

RSA SecurID Access Features	
KnowledgeOwl	
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 KnowledgeOwl 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 – KnowledgeOwl 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**
- **KnowledgeOwl 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 KnowledgeOwl 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.

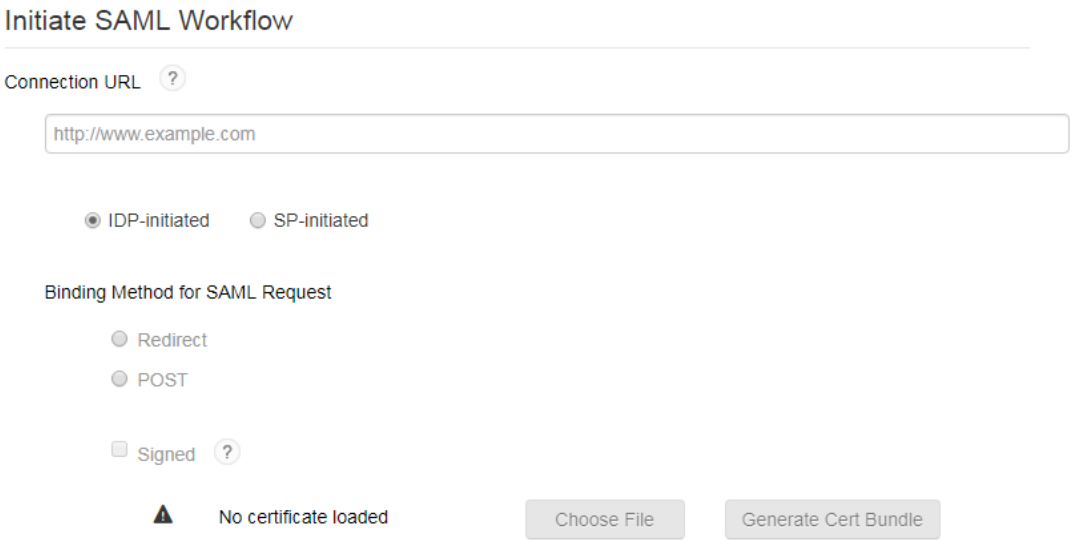
Configure RSA Identity Router SAML IdP

Procedure

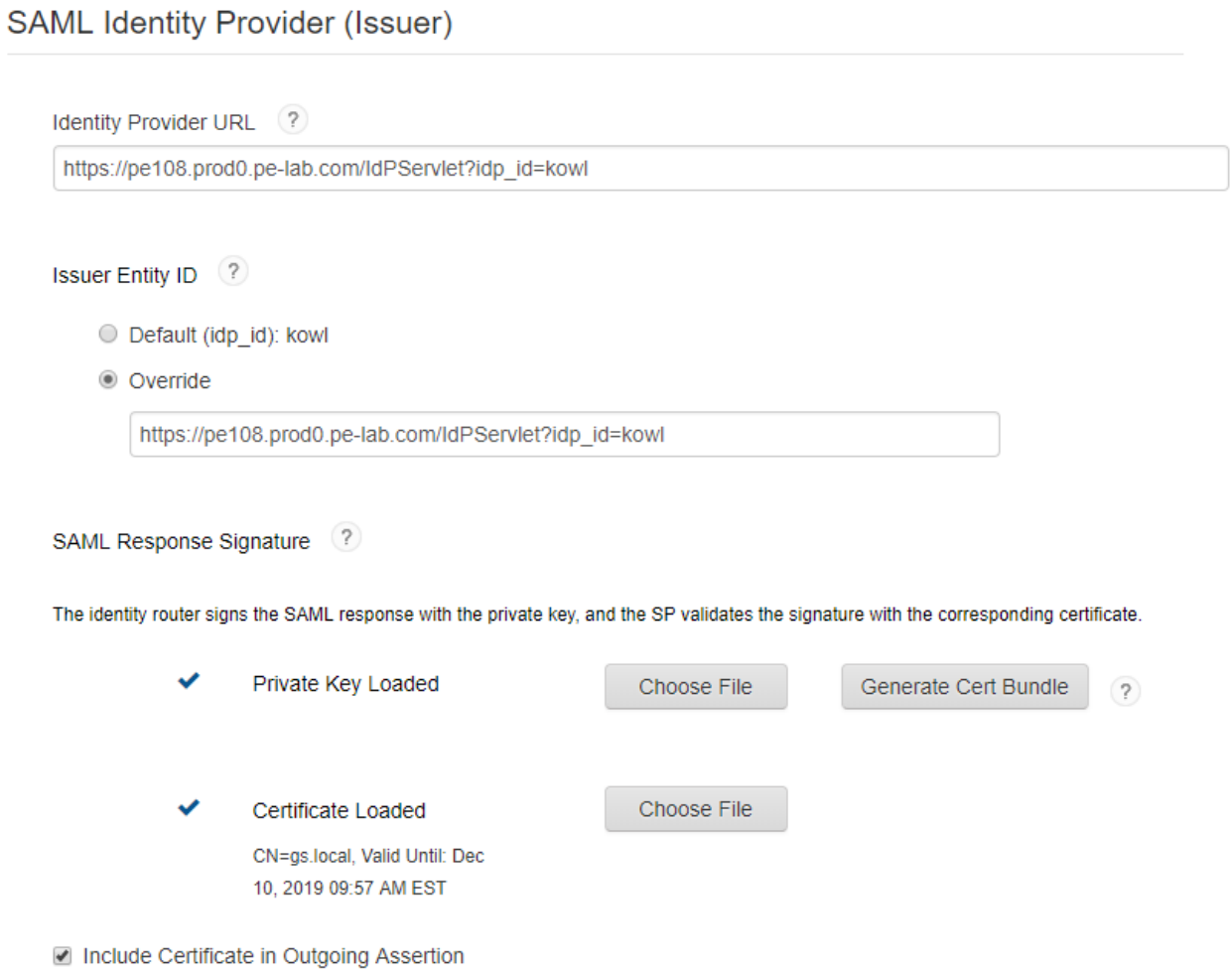
1. Logon to the RSA SecurID Access console and browse to Applications > Application Catalog, search for KnowledgeOwl and click +Add to add the connector.

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.
   b. Choose **IdP-initiated.**

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

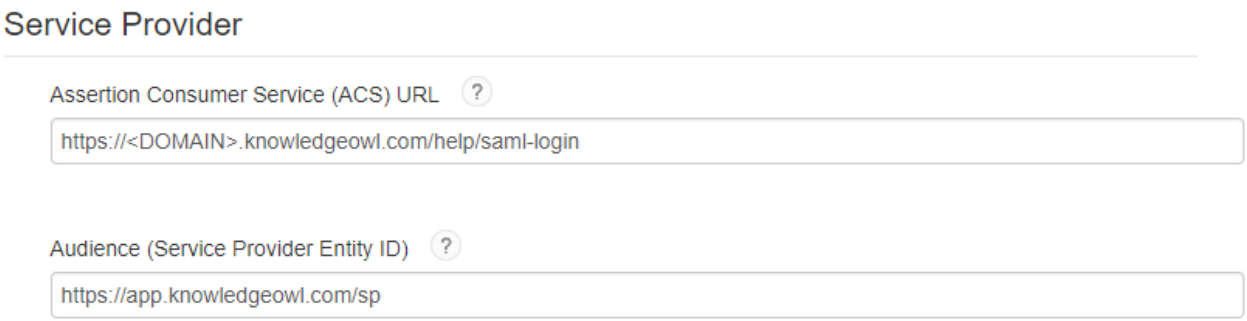


4. Scroll down to SAML Identity Provider (Issuer) section.

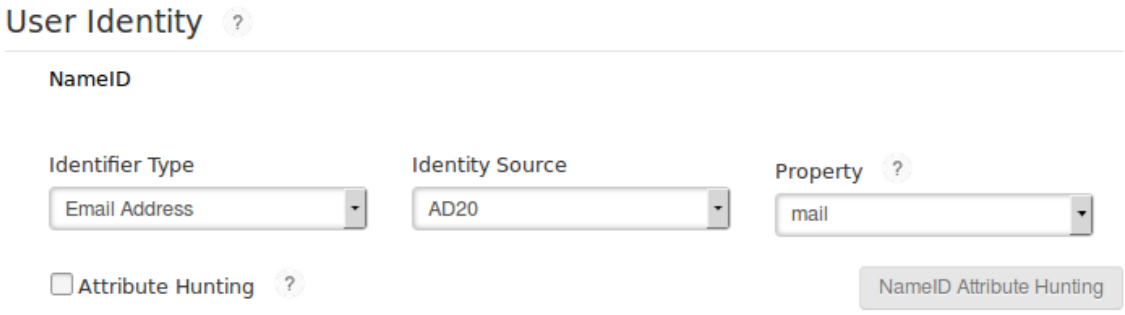


a. Make a note of Identity Provider URL field value, as it will be needed later to configure the Service Provider configuration.
b. Select Issuer Entity ID **Override** and paste the Identity Provider URL in that field.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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

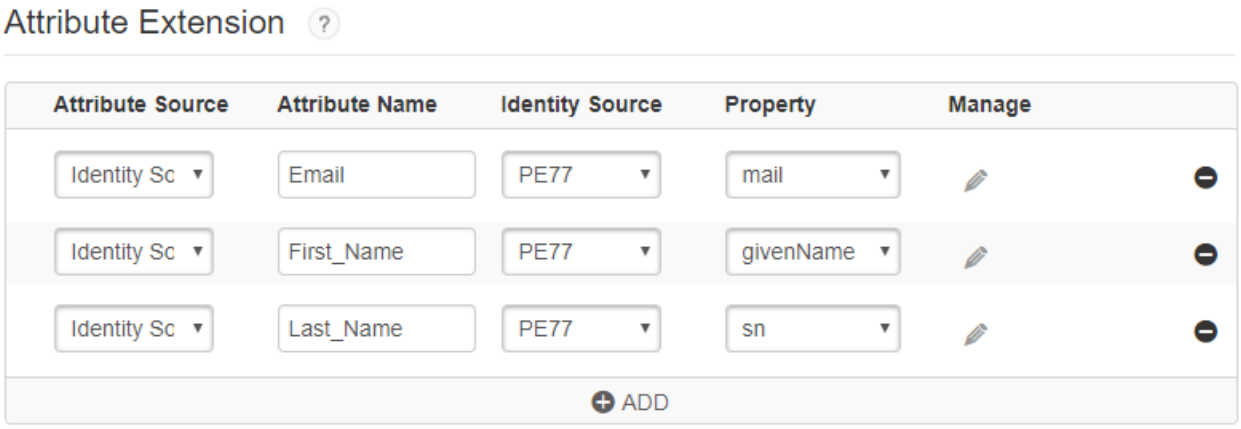


6. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your KnowledgeOwl organization domain.
7. Verify the **Audience (Service Provider Issuer ID)** field is **https://app.knowledgeowl.com/sp**.
8. Scroll down to the **User Identity** section.
   Verify the settings are correct 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.

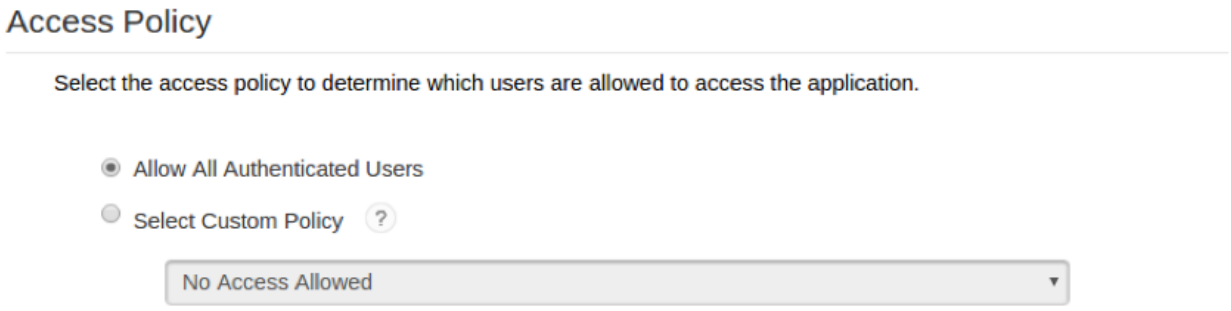


9. Click **Show Advanced Configuration**.

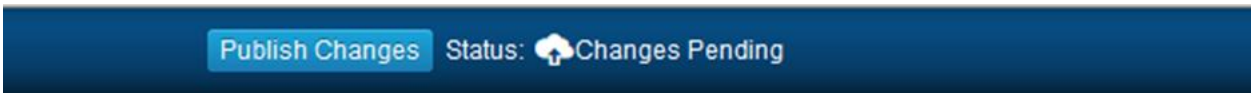
10. In the Attribute Extension section, choose the correct property variables for Email, First_Name and Last_Name.



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



13. Click **Next Step**.
14. On the **Portal Display** page, select **Display in Portal**.
15. Click **Save and Finish**.
16. Click **Publish Changes**.



Partner Product Configuration

Before You Begin

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

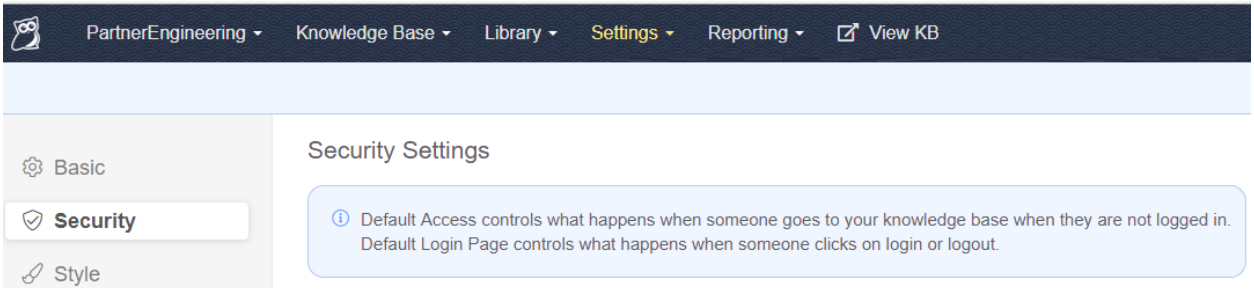
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

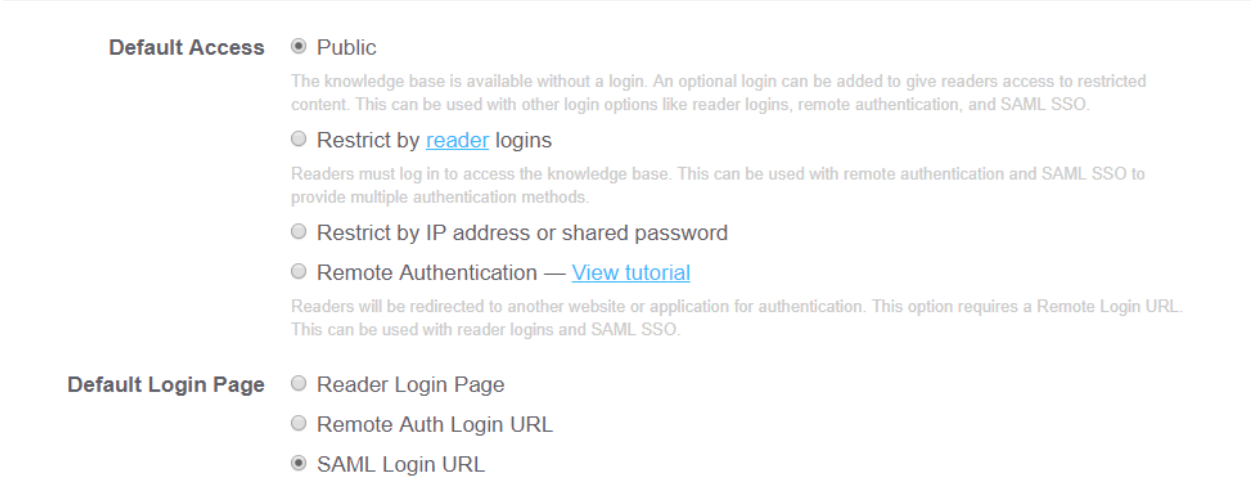
KnowledgeOwl SAML Configuration

Procedure

1. Login to KnowledgeOwl as an administrator. **https://app.knowledgeowl.com**
2. Navigate to **Settings > Security**.



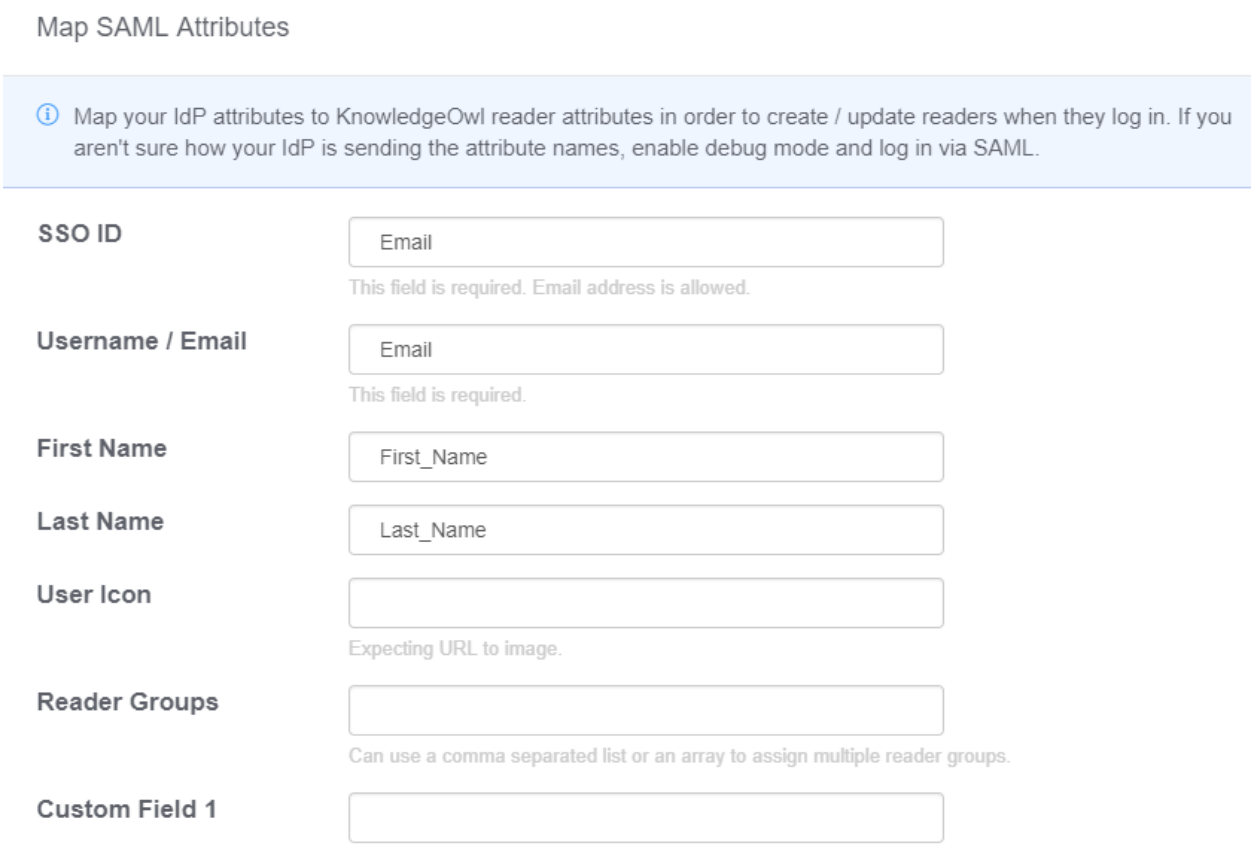
3. Change the Default Login Page for what is desired for your environment.



4. Scroll down to the SAML SSO Integration section.

a. Select the **Enable SAML SSO** checkbox.
b. Enter the Override URL from page 5 into the **IdP entityID** field.
c. Enter the Identity Provider URL from page 5 into the **IdP Login URL.**
d. Enter the **IdP Logout URL.**
e. Click the **Upload IdP Certificate** link and select the public certificate used in step 4d page 5.

f. Click the **Map SAML Attributes** link and enter values for **SSO ID, Username, First Name** and **Last Name**. Other fields are options.
g. Paste the public certificate from page 5 step 4d into the IDENTITY PROVIDER VERTIFICATE window.



5. Click **SAVE**.