

# **RSA SECURID<sup>®</sup> ACCESS**

## **Implementation Guide**

**KnowledgeOwl**

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



## 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	
<b>On Premise Methods</b>	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
<b>Cloud Authentication Service Methods</b>	
Authenticate App	✓
FIDO Token	✓
<b>SSO</b>	
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.**

#### Initiate SAML Workflow

Connection URL ?

IDP-initiated     SP-initiated

Binding Method for SAML Request

Redirect  
 POST  
 Signed ?

▲ No certificate loaded



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

### SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

- Default (idp\_id): kowl
- 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=gs.local, Valid Until: Dec  
10, 2019 09:57 AM EST

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 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.

## Service Provider

Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.knowledgeowl.com/help/saml-login

Audience (Service Provider Entity ID) ?

https://app.knowledgeowl.com/sp

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.

## User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

9. Click **Show Advanced Configuration**.



10. In the Attribute Extension section, choose the correct property variables for Email, First\_Name and Last\_Name.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc ▾	Email	PE77 ▾	mail ▾	
Identity Sc ▾	First_Name	PE77 ▾	givenName ▾	
Identity Sc ▾	Last_Name	PE77 ▾	sn ▾	
ADD				

11. Click **Next Step**.

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

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 ▾

13. Click **Next Step**.

14. On the **Portal Display** page, select **Display in Portal**.

15. Click **Save and Finish**.

16. Click **Publish Changes**.

Publish Changes
Status: Changes Pending



# 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.

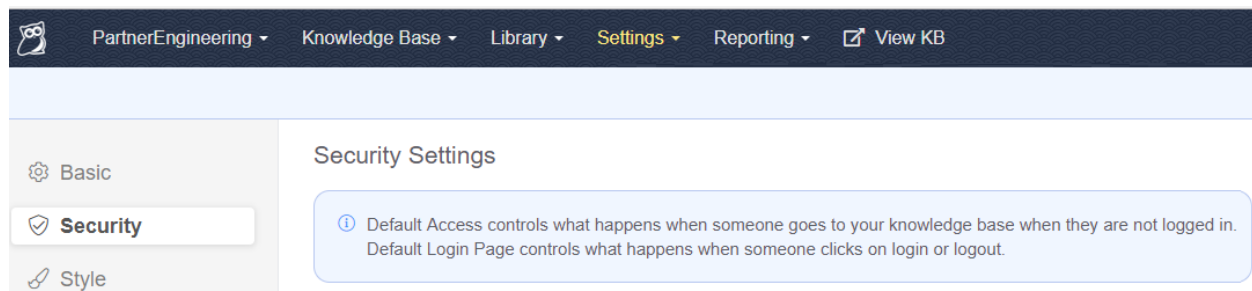
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.

**Default Access**

- Public  
The knowledge base is available without a login. An optional login can be added to give readers access to restricted content. This can be used with other login options like reader logins, remote authentication, and SAML SSO.
- Restrict by [reader logins](#)  
Readers must log in to access the knowledge base. This can be used with remote authentication and SAML SSO to provide multiple authentication methods.
- Restrict by IP address or shared password
- Remote Authentication — [View tutorial](#)  
Readers will be redirected to another website or application for authentication. This option requires a Remote Login URL. This can be used with reader logins and SAML SSO.

**Default Login Page**

- Reader Login Page
- Remote Auth Login URL
- SAML Login URL







4. Scroll down to the SAML SSO Integration section.

**Enable SAML**  Enable SAML SSO — [View tutorial](#)

Restrict Access to SSO

Enable Debug Mode

**SP Entity ID**

**SP Login URL**

**SP Logout URL**

**IdP entityID**

**IdP Login URL**

**IdP Logout URL**

[KnowledgeOwl SP Metadata](#)   [Map SAML Attributes](#)   [Upload IdP Certificate](#)

**Advanced Options**

Use a unique SP entity ID for this knowledge base  
Entity ID and metadata will be updated upon saving.

Issue a remote logout request using the logout URL below when a reader logs out

On IdP initiated SSO, send readers to the RelayState specified landing page  
Default behavior is to send readers to the home page.

Sign all messages coming from this SP

Sign metadata coming from this SP

Sign all logout requests coming from this SP

Require all IdP assertions to be signed

Require all IdP messages to be signed


Require all IdP assertions to be encrypted  
Encryption uses rsa-sha256 algorithm. The SP public key can be found in the KnowledgeOwl XML Metadata.

- 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.

## Map SAML Attributes

 Map your IdP attributes to KnowledgeOwl reader attributes in order to create / update readers when they log in. If you aren't sure how your IdP is sending the attribute names, enable debug mode and log in via SAML.

<b>SSO ID</b>	<input type="text" value="Email"/>
	<small>This field is required. Email address is allowed.</small>
<b>Username / Email</b>	<input type="text" value="Email"/>
	<small>This field is required.</small>
<b>First Name</b>	<input type="text" value="First_Name"/>
<b>Last Name</b>	<input type="text" value="Last_Name"/>
<b>User Icon</b>	<input type="text"/>
	<small>Expecting URL to image.</small>
<b>Reader Groups</b>	<input type="text"/>
	<small>Can use a comma separated list or an array to assign multiple reader groups.</small>
<b>Custom Field 1</b>	<input type="text"/>

5. Click **SAVE**.