

RSA SECURID[®] ACCESS

Implementation Guide

Awardco

Gina Salvazo, RSA Partner Engineering
Last Modified: May 23, 2018



Solution Summary

Awardco’s software technology makes it easy for employees and managers to reward their colleagues for moments that matter. Users can log in and redeem products from Amazon directly. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. Awardco does not support user auto-provisioning.

RSA SecurID Access Features	
Awardco	
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 Awardco 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 – Awardco 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 Awardco 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 Awardco 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 Awardco and click **+Add** to add the connector.




Awardco
SAML Direct

+ Add

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, copy and paste the Identity Provider URL in the field.
 - b. Choose **SP-initiated**.
 - c. Select **Redirect** for Binding Method for SAML Request.

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

Initiate SAML Workflow

Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

Choose File

Generate Cert Bundle



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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): atest

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 **Choose File** and upload the private key.
- c. Select **Choose File** to import the public signing certificate.
- d. 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>.awardco.com/sso/saml

Audience (Service Provider Entity ID) ?

https://<DOMAIN>.awardco.com/sso/saml

6. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your Awardco organization domain.
7. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> with your Awardco organization domain.
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

unspecified

Identity Source

PE77

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

9. Click **Next Step**.



10. 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 ▼

11. Click **Next Step**.
12. On the **Portal Display** page, select **Display in Portal**.
13. Click **Save and Finish**.
14. Click **Publish Changes**. Your application is now enabled for SSO.

[Publish Changes](#)

Status:  Changes Pending



Partner Product Configuration

Before You Begin

This section provides instructions for configuring Awardco 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 Awardco components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Awardco SAML Configuration

Procedure

1. Login to Awardco as an administrator and navigate to **Admin > Settings > Single Sign On**.
2. Enter the Identity Provider URL from page 5 step 4 into the **SSO URL**: field.
3. Enter the Issuer Entity ID from page 5 step 4 into the **Entity Id**: field.
4. Paste the public certificate into the Certificate field.
5. Enter a text label for the **Sign In Button Label**: field.
6. Select **SSO with SAML**: to **On**.

The screenshot shows the 'Settings' page in Awardco, specifically the 'Single Sign On' configuration section. The left sidebar contains a menu with options like General, Branding, Award Network, Catalogs, Upload Items, Groups, Cost Centers, Hashtags, Peer to Peer, Recognition, Approval, Nomination, Service Awards, Programs, Addresses, Managers, Password, and Single Sign On. The main content area is titled 'Single Sign On' and includes the following fields and controls:

- Standard Login:** A toggle switch set to 'On'.
- SSO with SAML:** A toggle switch set to 'On' with a 'Download Metadata' link below it.
- SAML Response Signed:** A toggle switch set to 'Off'.
- SSO URL:** A text input field containing 'https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=atest'.
- Entity Id:** A text input field containing 'atest'.
- Certificate:** A large text area containing a multi-line certificate string starting with '-----BEGIN CERTIFICATE-----' and ending with '-----END CERTIFICATE-----'.
- Sign In Button Label:** A text input field containing 'RSA SAML'.