

# RSA SECURID<sup>®</sup> ACCESS

## Implementation Guide

Logit.io

Gina Salvazo, RSA Partner Engineering  
Last Modified: February 9, 2018

## Solution Summary

---

Logit.io provide enterprise cloud and on-premise ELK services. This integration supports both IdP initiated and SP-initiated authentication flow. Logit.io application supports auto-provisioning of the user.

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

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

## Configuration Summary

---

All of the supported use cases of RSA SecurID Access with Logit.io 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** – Logit.io 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 Logit.io 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 Logit.io 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 Logit.io 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, replace <ACCOUNT\_ID> with the value provide to from Logit.io support.
  - b. Choose **IdP-initiated**.

#### 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): 1uxy2m1mihn2

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, Valid Until:  
08/16/2021

Include Certificate in Outgoing Assertion

- a. Select **Choose File** and upload the private key.
- b. Select **Choose File** to import the public signing certificate.
- c. 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://logitio.eu.auth0.com/login/callback?connection=<ACCOUNT\_ID>

Audience (Service Provider Entity ID) ?

urn:auth0:logitio:<ACCOUNT\_ID>

- a. In the **Assertion Consumer Service (ACS) URL** field, put the value received after creating account.
  - b. In the **Audience (Service Provider Issuer ID)** field, put your organization unique domain value received after creating account.
6. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in unspecified 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

7. Click **Next Step**.

- 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

- Click **Next Step**.
- On the Portal Display page, select **Display in Portal**.
- Click **Save and Finish**.
- Click **Publish Changes**.

Publish Changes

Status:  Changes Pending

- Navigate to **Applications > My Applications**.
- Locate **Logit.io** in the list and from the **Edit** option, select **Export Metadata**.



Logit.io

Created From: Logitlo  
SAML Direct

Edit

 Edit

 Export Metadata

 Delete

## Partner Product Configuration

---

### Logit.io SAML Configuration

#### Procedure

To enable SAML SSO, send IDP metadata from page 7 step 14 to Logit.io at **support@logit.io**.