RSA SECURID® ACCESS
Implementation Guide

Logit.io

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

RSA READY

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.

RSA SecurID Access Features	
Logit.io	
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 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)

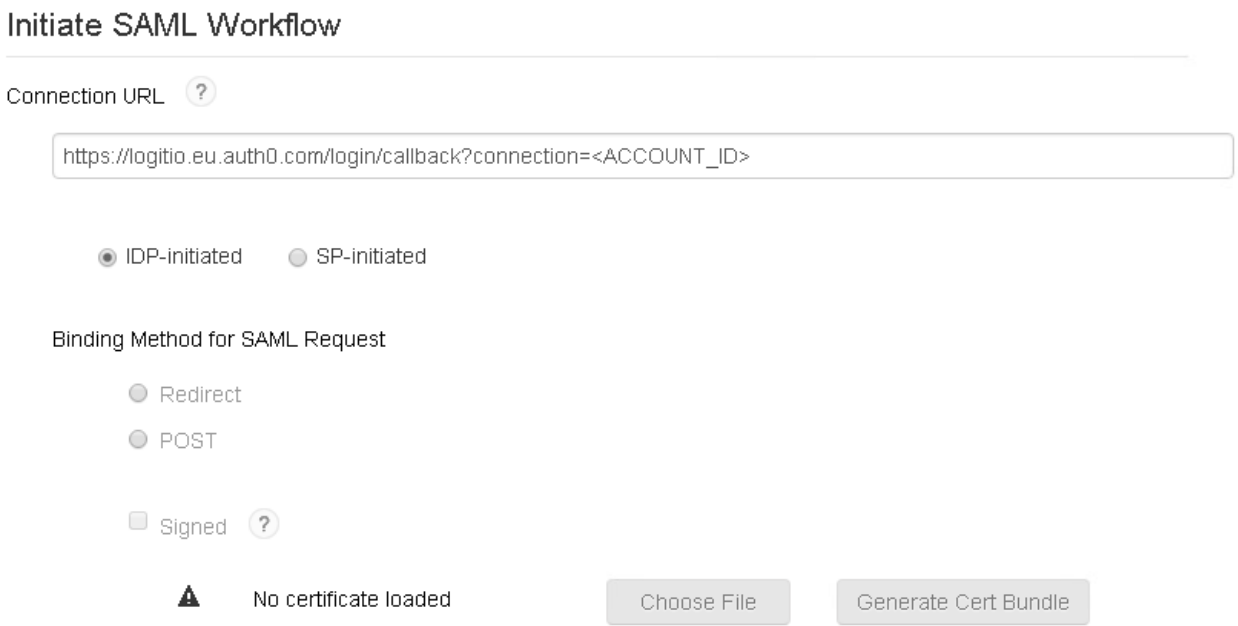
To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Logit.io in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

Configure RSA Identity Router SAML IdP

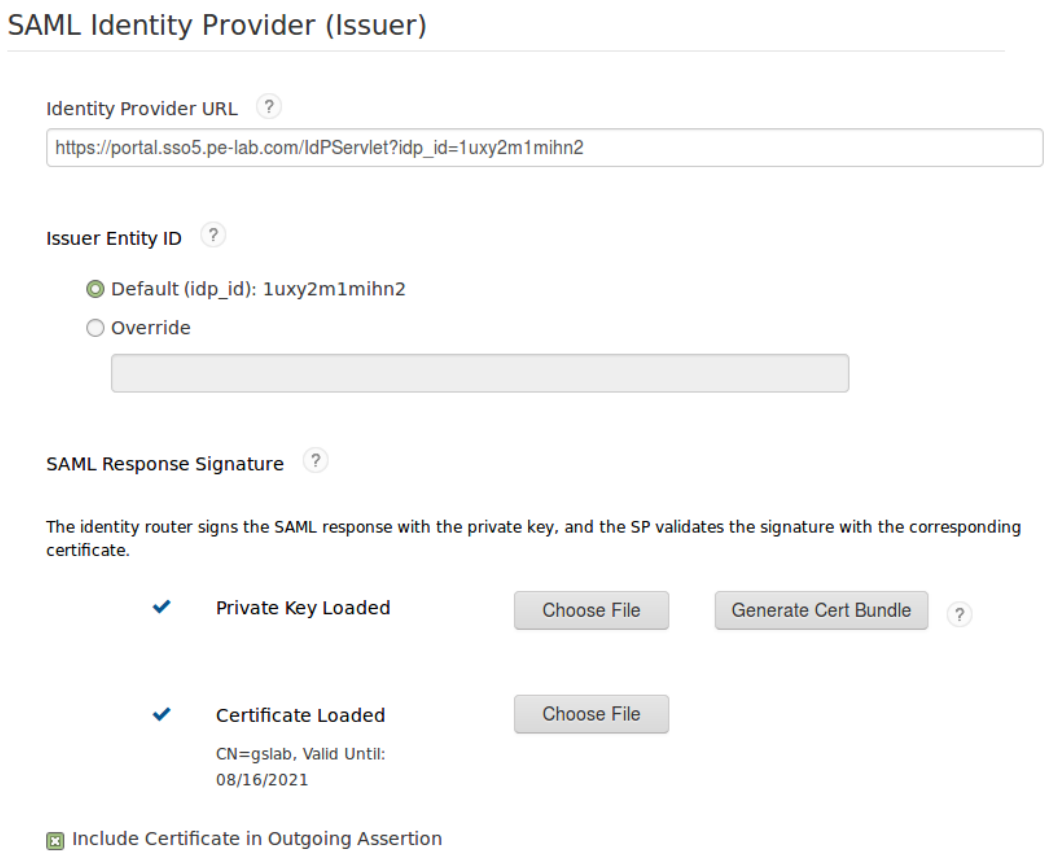
Procedure

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.**

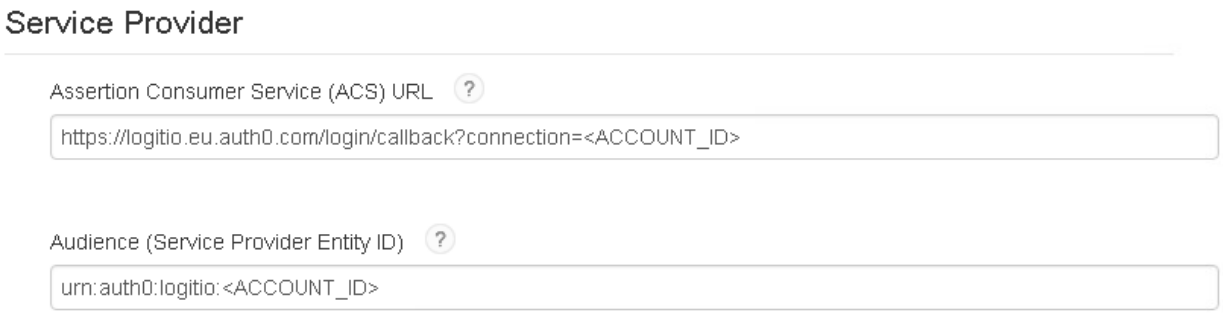


4. Scroll down to SAML Identity Provider (Issuer) section.



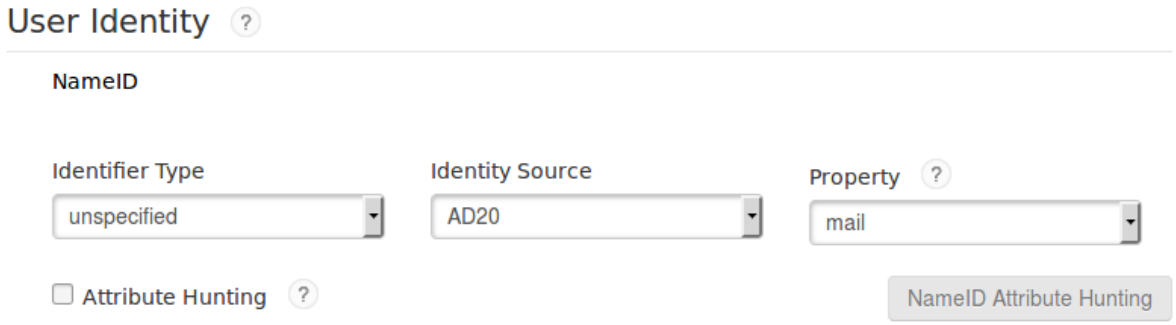
   a. Select **Choose File** and upload the private key.
   b. Select **Choose File** to import the public signing certificate.
   c. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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



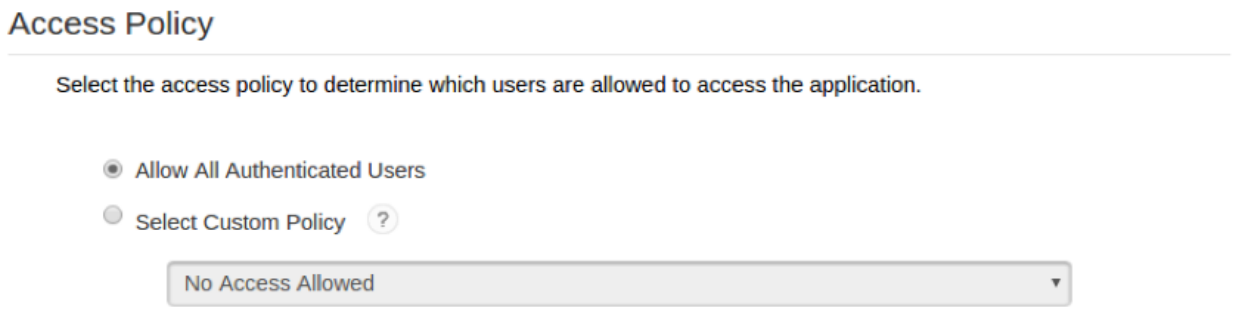
   a. In the **Assertion Consumer Service (ACS) URL** field, put the value received after creating account.
   b. In the **Audience (Service Provider Issuer ID)** field, put your organization unique domain value received after creating account.

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.

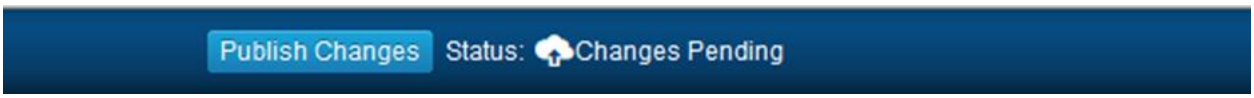


7. Click **Next Step**.

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



9. Click **Next Step**.
10. On the Portal Display page, select **Display in Portal**.
11. Click **Save and Finish**.
12. Click **Publish Changes**.



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

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**.