

RSA SECURID[®] ACCESS

Implementation Guide

LoopUp

Gina Salvazo, RSA Partner Engineering
Last Modified: July 18, 2018



Solution Summary

LoopUp is a premium remote meeting solution that makes it easier to collaborate in real time. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. LoopUp supports user auto-provisioning.

RSA SecurID Access Features	
LoopUp	
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

The following supported use case of RSA SecurID Access with LoopUp 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 – LoopUp 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 LoopUp 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 LoopUp 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 LoopUp 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. Leave the **Connection URL** 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): LoopUp_IdP

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. Select **Override** and paste the Identity Provider URL into the field.
- 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 ?

Audience (Service Provider Entity ID) ?

6. Verify the **Assertion Consumer Service (ACS) URL** field.
7. Verify the **Audience (Service Provider Issuer ID)** field.
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

Identity Source

Property ?

Attribute Hunting ?

NameID Attribute Hunting

9. Click **Show Advanced Configuration**.



- Under Attribute Extension, enter attributes **email**, **firstName**, **lastName**, **fullName**, **phoneNumber**, **mobileNumber**, and **alias** with the correlating value from your Identity source. Alias represents the user’s secondary email address.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc ▾	email	PE77 ▾	mail ▾	
Identity Sc ▾	firstName	PE77 ▾	givenName ▾	
Identity Sc ▾	lastName	PE77 ▾	sn ▾	
Identity Sc ▾	fullName	PE77 ▾	displayNam ▾	
Identity Sc ▾	phoneNumber	PE77 ▾	telephoneNt ▾	
Identity Sc ▾	mobileNumber	PE77 ▾	mobile ▾	
Identity Sc ▾	alias	PE77 ▾	userPrincipæ ▾	

+ ADD

- Under Uncommon Formatting SAML Response Options, verify the **Signature Algorithm** and **Digest Algorithm** are correct for your environment.

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response
 Assertion within response

Signature Algorithm rsa-sha256 ▾

Digest Algorithm sha256 ▾

Encrypt Assertion ?

No certificate loaded

Choose File

Encryption Algorithm Triple DES ▾

Encryption Key Transport RSA15 ▾

Relay State URL Encoding

Send encoded URL in outgoing assertion ?

Include Issuer NameID Format

NameID Format Unspecified ▾

- Click **Next Step**.



13. 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

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

Publish Changes Status: Changes Pending

18. Navigate to **Applications > My Applications**.
19. Locate **LoopUp** in the list and from the **Edit** option, select **Export Metadata**.



LoopUp
Created From: LoopUp
SAML Direct

Edit

- Edit
- Export Metadata
- Delete



Partner Product Configuration

Before You Begin

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

LoopUp SAML Configuration

Procedure

Contact LoopUp support with the following:
SSO domain name, whether auto-provision is allowed, include the RSA metadata file and the SSO Logout URL.