


RSA SECURID[®] ACCESS

Implementation Guide

UseResponse

Gina Salvazo, RSA Partner Engineering
Last Modified: November 17, 2017



Solution Summary

UseResponse is an integrated support suite that combines core functionalities of a help center, communications platform, social CRM, and customer support into a single, unified package.

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

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

Configuration Summary

All of the supported use cases of RSA SecurID Access with UseResponse 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 – UseResponse 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 UseResponse 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 UseResponse 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 UseResponse 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 and choose **IDP-initiated**.

 **Note:** The following IdP-initiated configuration works for SP-initiated UseResponse connections 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

UseResponse

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): 16wti8gc1x39h

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

?

cert.pem

Certificate valid until: Mon
Aug 16 06:45:13 UTC 2021

Include Certificate in Outgoing Assertion

- a. Take note of the Identity Provider URL.
- b. Take note of the Issuer Entity ID.
- 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**.

UseResponse

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

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.userresponse.com/saml/single-login

Audience (Service Provider Entity ID) ?

userresponse.com

6. In the Assertion Consumer Service (ACS) URL field, replace **<DOMAIN>** with your company and **<CompanyID>** with your CompanyID.
7. In the Audience (Service Provider Issuer ID) field, keep it unchanged.
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 the **Show Advance** button.

UseResponse

- Under the Attribute Extension section, enter the attribute **User.email**, **User.FirstName**, **User.LastName** and the mapped Active Directory attribute for these value.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity So ▼	User.email	AD20 ▼	mail ▼	 ⊖
Identity So ▼	User.FirstName	AD20 ▼	cn ▼	 ⊖
Identity So ▼	User.LastName	AD20 ▼	sn ▼	 ⊖
+ ADD				

- 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**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

UseResponse

Before You Begin

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

UseResponse SAML Configuration

Procedure

1. Log into your UseResponse application web account as company administrator.
<https://emc21.userresponse.com/login>
2. To enable SAML, navigate to **Administration -> Login Plus -> Single Sign On.**
3. On Single Sign On page, use the pull down and select method **SAML.**
4. Select **YES** for **Use Only SSO Authentication.**
5. Fill in the **idP Entity ID or Issuer:** field with the Issuer Entity ID from step 4b page 5.
6. Fill in the **External Login URL:** with the Identity Provider URL from step 4a page 5.
7. Fill in the **External Logout URL:** with <https://<portal url>/LogoutServlet> .

idP Entity ID or Issuer *

1ta17e47tj2kg

External Login URL *

https://portal.sso4.pe-lab.com/IdPServlet?idp_id=1ta17e47tj2kg

External Logout URL *

<https://portal.sso4.pe-lab.com/LogoutServlet>

Security

Fingerprint

Certificate

UseResponse

8. **Fingerprint/Certificate:** This should be filled with the public certificate use in step 4d page 5.

Security

Fingerprint Certificate

Certificate *

```
-----BEGIN CERTIFICATE-----
MIICpjCCAY6gAwIBAgIGAVOIgPz2MA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNVBAMT
CWdzbGFilMnVbTAeFw0xNjAzMjMwNjEwNTIaFw0yMDAzMjMwNjEwNTIaMBQxEjAQ
BgNVBAMTCWdzbGFilMnVbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMraYXqMGpvPa+J+rt46Nf5xG1U7Nyle5DCzTNY7uCSAXGgNou7SAN4vAlj9ZGsD
UgVQ2Om8QpMkV5cmCNThNUBAIbhIXpdkSVGcdvHScB14GC25roNYaswGz10Qxus
F/jPypNMzZcJ6pOzCT0yuWgXlyMqbl/CKuFTo/XUFxU26Sz51Yilhhqqp8MMxpt0
bkShIFwZGH/XFi8LSt5T7rZwQGwafuYZa8olevxbISy7Qvfi0tNCIu87eGgG/gp
```

9. For the rest of the fields, leave them as default.

10. Click **Submit**.

11. You can view SP metadata on the same page.

Integration Details

Your application settings to use with IdP

Metadata URL:	https://emc21.userresponse.com/saml/metadata
Assertion Consumer Service URL:	https://emc21.userresponse.com/saml/single-login
Single Logout Service URL:	https://emc21.userresponse.com/saml/single-logout