RSA SECURID® ACCESS
Implementation Guide

UseResponse

Gina Salvalzo, 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	✓
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 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.

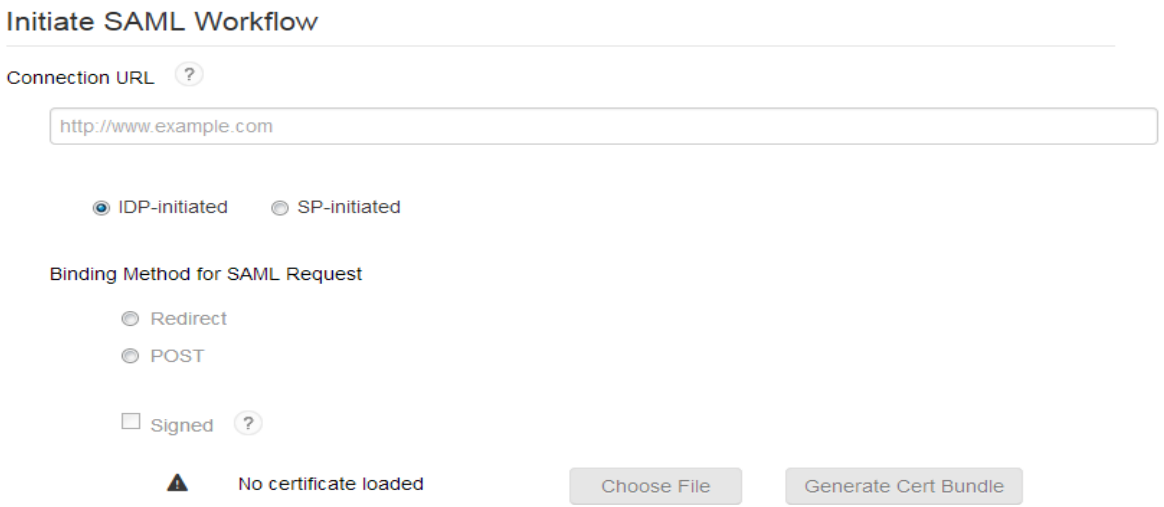
Configure RSA Identity Router SAML IdP

Procedure

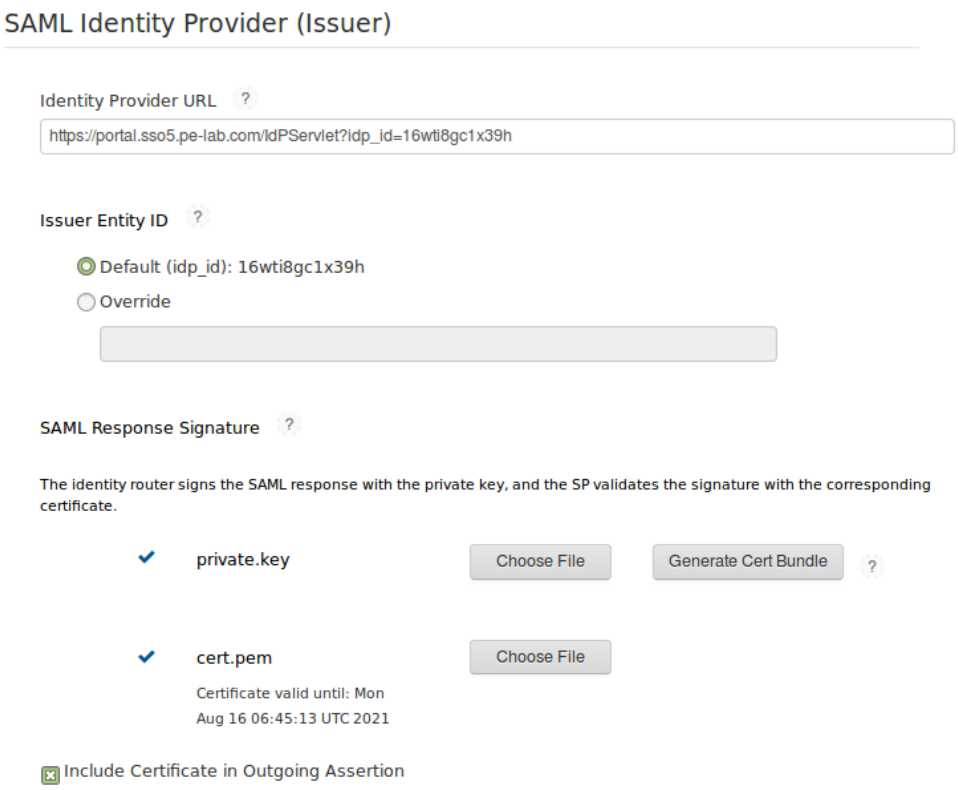
1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for UseResponse and click **+Add** to add the connector.

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.

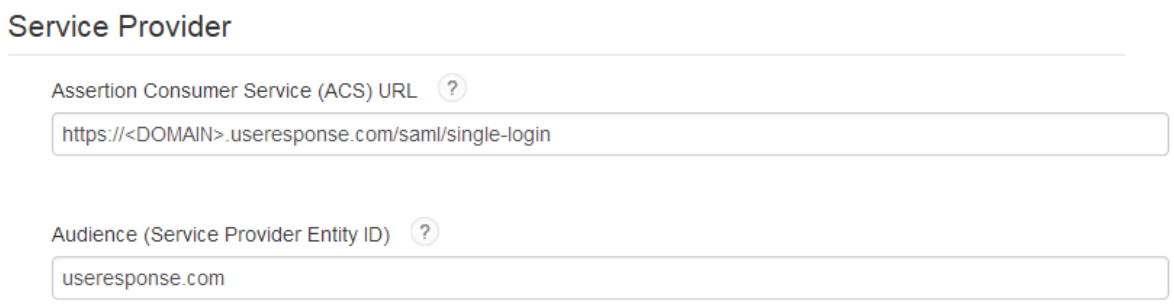


4. Scroll down to SAML Identity Provider (Issuer) section.

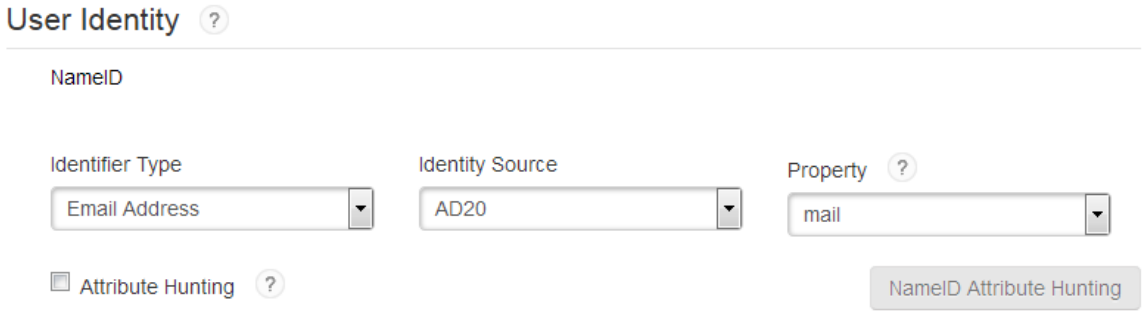


a. Take note of the Identity Provider URL.
b. Take note of the Issuer Entity ID.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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

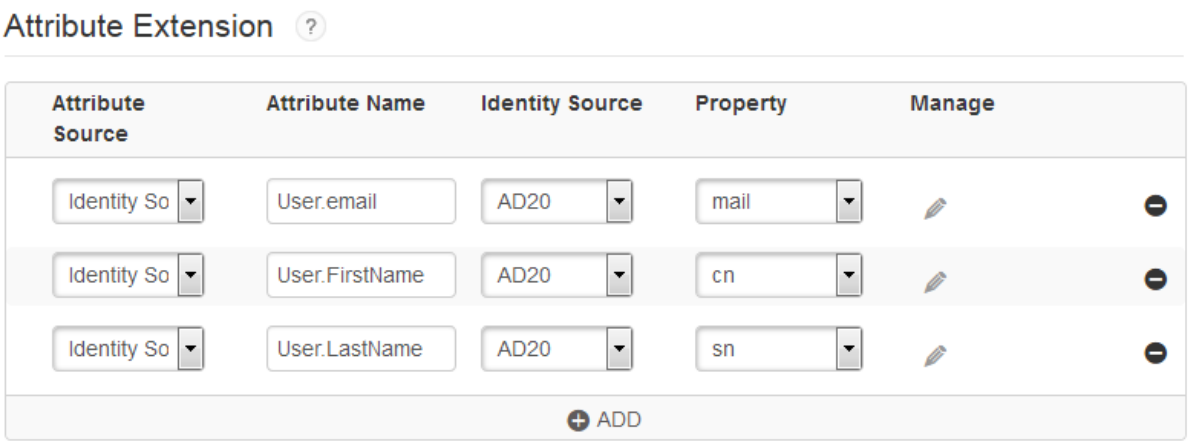


6. In the Assertion Consumer Service (ACS) URL field, replace **<DOMAIN>** with your company and **<CompanyID>** with your CompanyID.
7. In the Audience (Service Provider Issuer ID) field, keep it unchanged.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

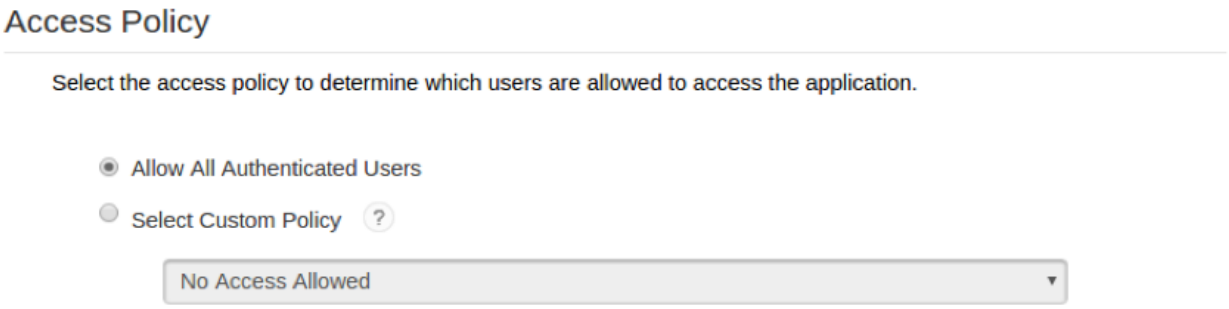


9. Click the **Show Advance** button.

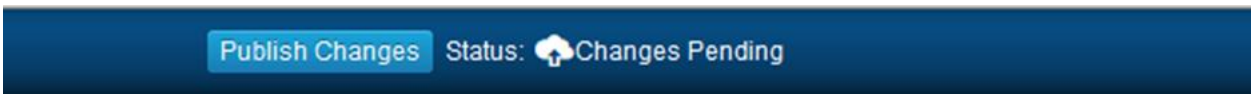
10. Under the Attribute Extension section, enter the attribute **User.email, User.FirstName, User.LastName** and the mapped Active Directory attribute for these value.



11. Click **Next Step**.
12. On the User Access page, select **Allow All Authenticated Users** user policy from the available options.



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



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.

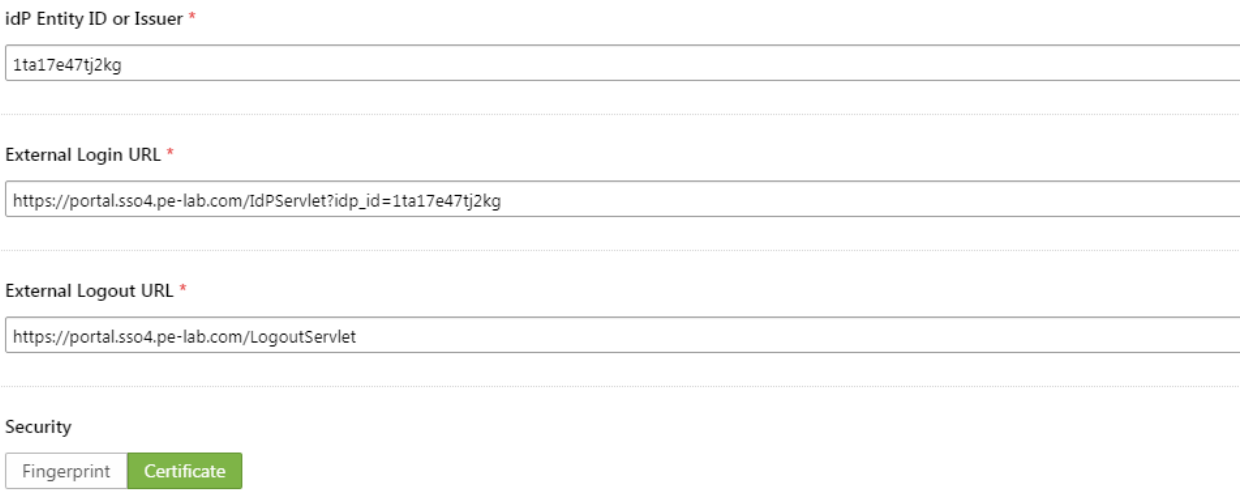
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All UseResponse components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

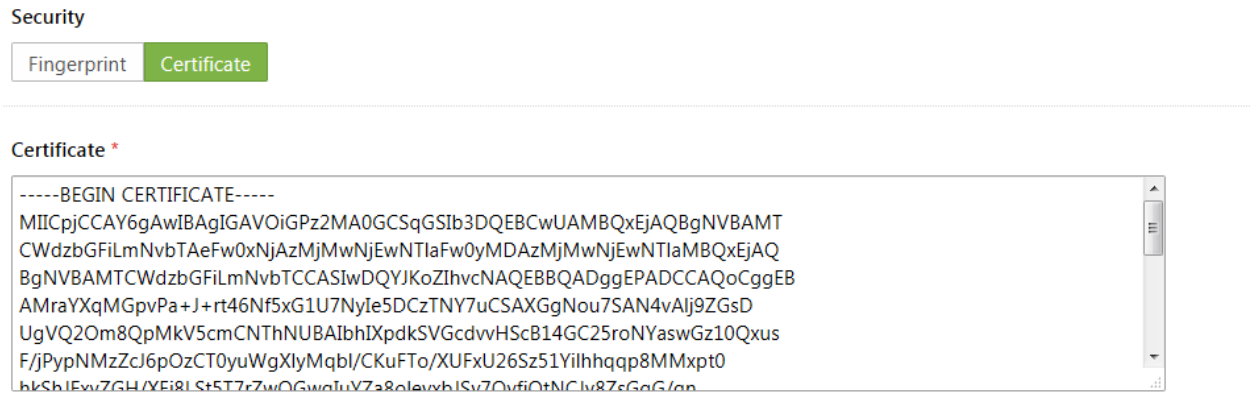
UseResponse SAML Configuration

Procedure

1. Log into your UseResponse application web account as company administrator. **https://emc21.useresponse.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** .



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



9. For the rest of the fields, leave them as default.
10. Click **Submit.**
11. You can view SP metadata on the same page.