RSA SECURID® ACCESS
Implementation Guide

WhosOnLocation

Gina Salvalzo, RSA Partner Engineering
Last Modified: November 7, 2017

Solution Summary

WhosOnLocation is an easy way to manage visitors, contractors, and employees signing in/out of your sites. Know who is authorized to be on-site, due on-site soon, on-site right now and who was on-site.

RSA SecurID Access Features	
WhosOnLocation	
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 WhosOnLocation 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 – WhosOnLocation 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
WhosOnLocation 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 WhosOnLocation 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.

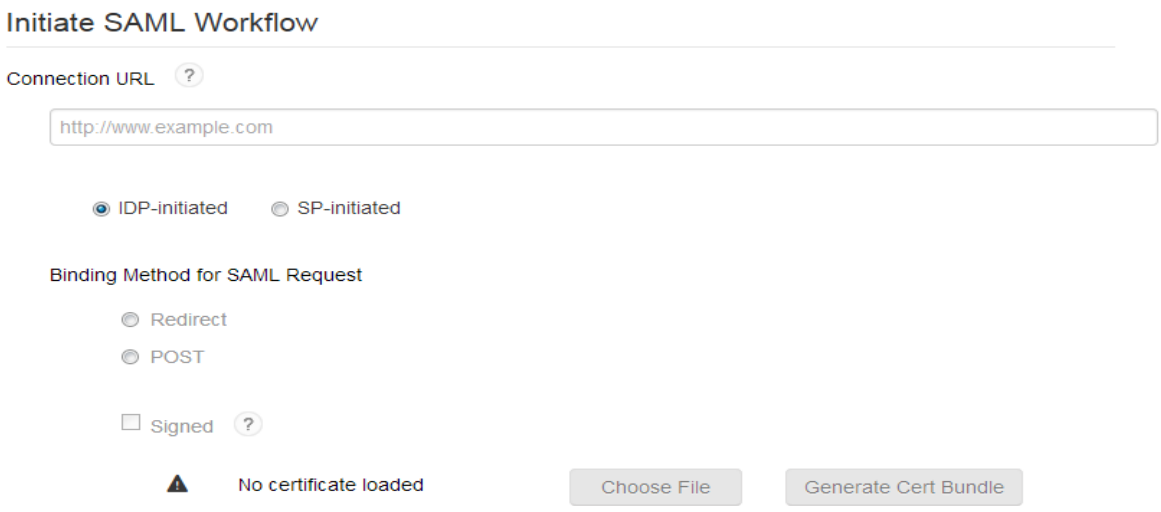
Configure RSA Identity Router SAML IdP

Procedure

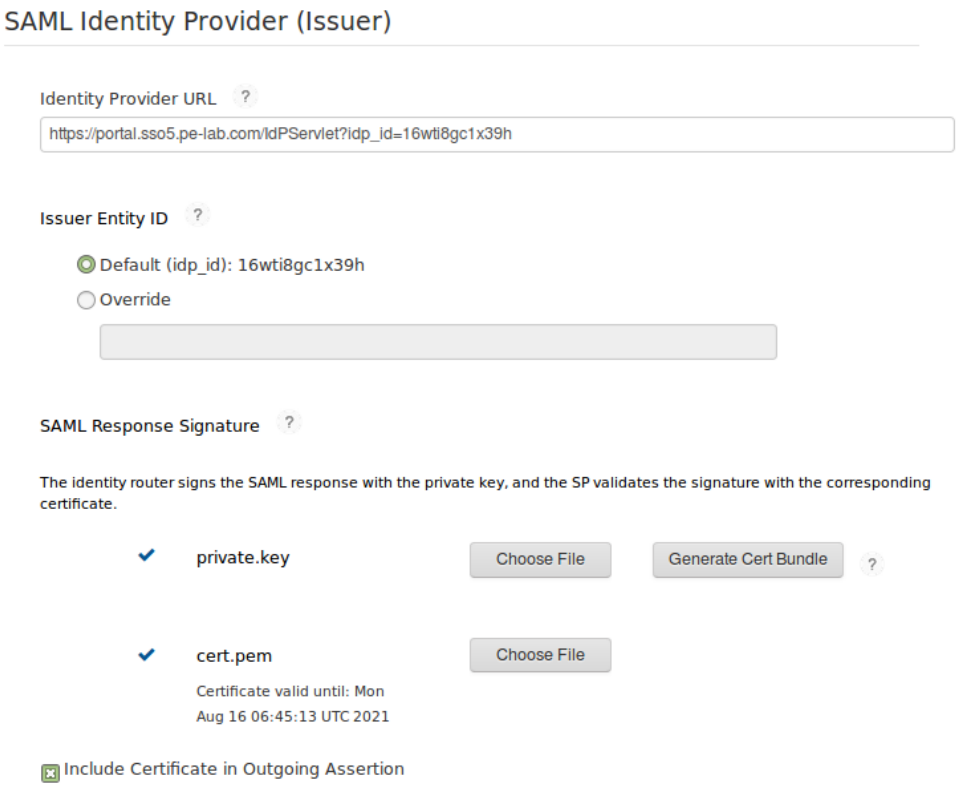
1. Logon to the RSA SecurID Access console and browse to Applications > Application Catalog, search for WhosOnLocation and click **+Add** to add the connector.

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 WhosOnLocation connections as well.



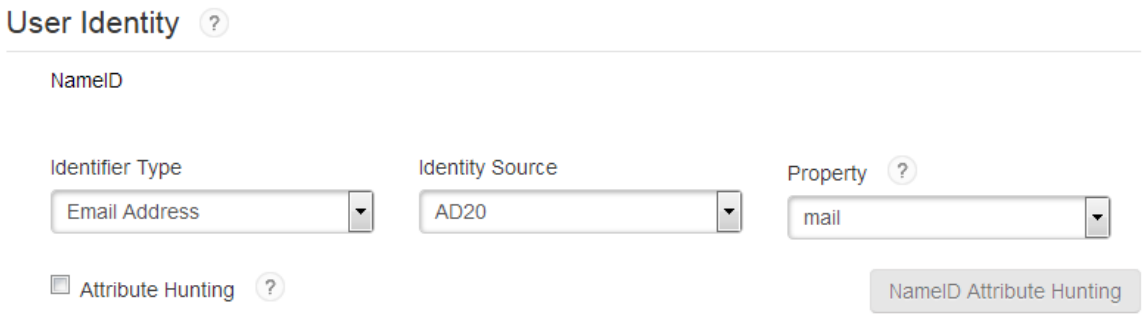
4. Scroll down to SAML Identity Provider (Issuer) section.



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**.

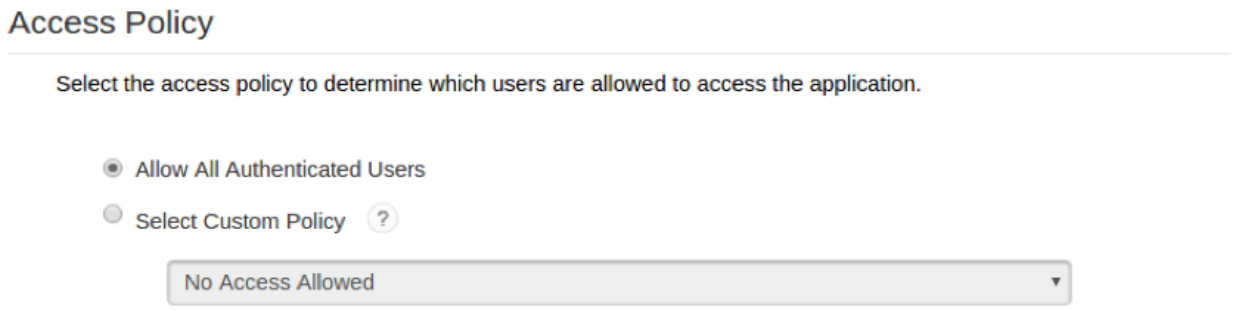
5. Scroll down to the **Service Provider** section.

6. In the Assertion Consumer Service (ACS) URL field, replace **<ConfigID>** with your company ID.
7. In the Audience (Service Provider Issuer ID) field, replace **<ConfigID>** with your company ID.
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.

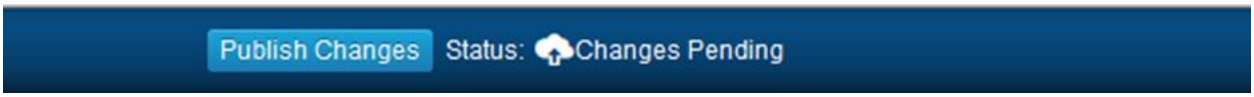


9. Click **Next Step**.

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



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



15. Navigate to **Applications** > **My Applications**.
16. Locate **WhosOnLocation** in the list and from the **Edit** option, select **Export Metadata**.

Before You Begin

This section provides instructions for configuring WhosOnLocation with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

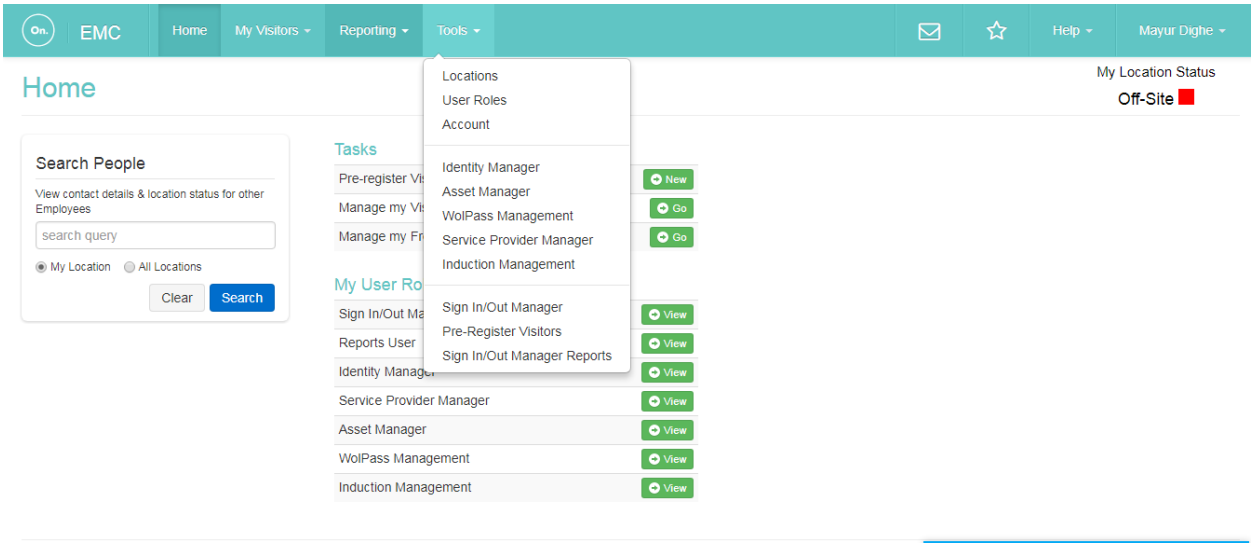
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

WhosOnLocation SAML Configuration

Procedure

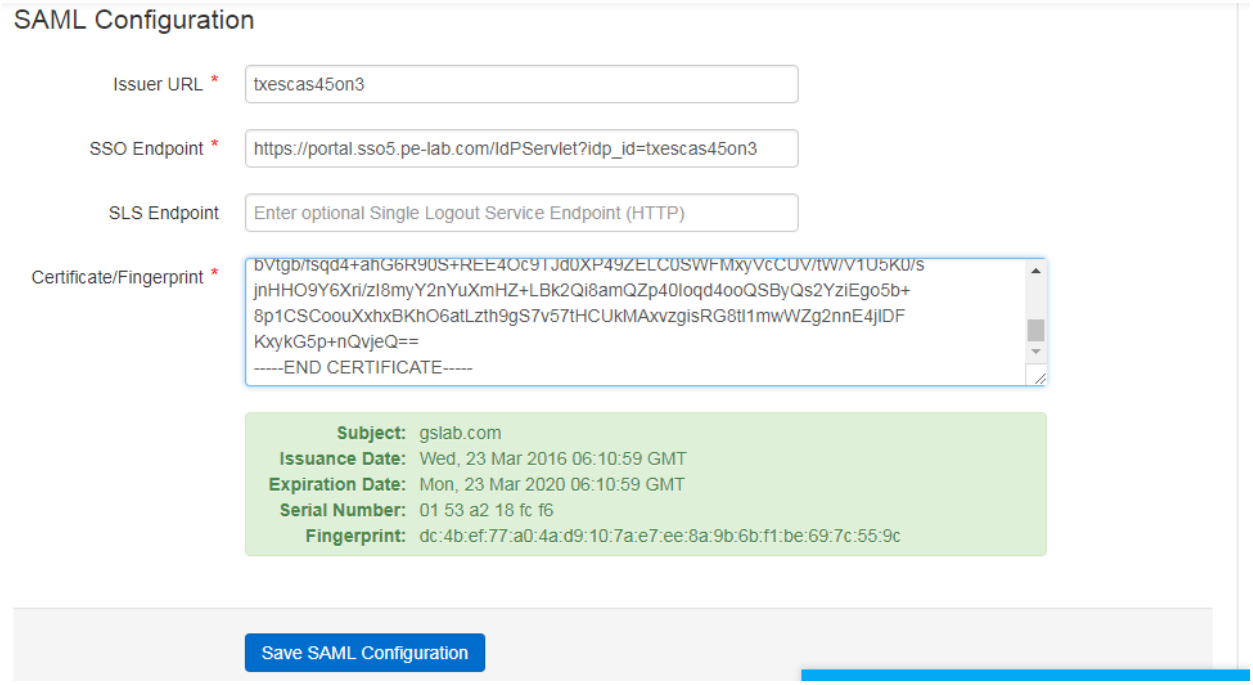
1. Log into your WhosOnLocation application web account as company administrator. **https://login.whosonlocation.com/login**
2. Select **Tools** drop-down menu and then **Account**.



3. Inside Account, select **Employee Access**.
4. Click on **Yes** on the option of **Single Sign On with SAML**.
5. You can now fill in the relevant fields here:

   Issuer URL: This should be set to the **Issuer EntityID** in step 4b page 5.
   SSO Endpoint : This should be set to **Identity Provider URL** in step 4a page 5.
   SLS Endpoint : Keep this field empty.
   Certificate/Fingerprint : Paste the X509 **public certificate** copied from step 4d page 5.

6. Click **Save SAML Configuration**.



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