RSA SECURID® ACCESS
Implementation Guide

People HR

Gina Salvalzo, RSA Partner Engineering
Last Modified: May 8, 2018

RSA READY

Solution Summary

People HR is an easy-to-use, modern HR software system. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. People HR does not support user auto-provisioning.

RSA SecurID Access Features	
People HR	
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 People HR 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 – People HR 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
People HR 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 People HR 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.

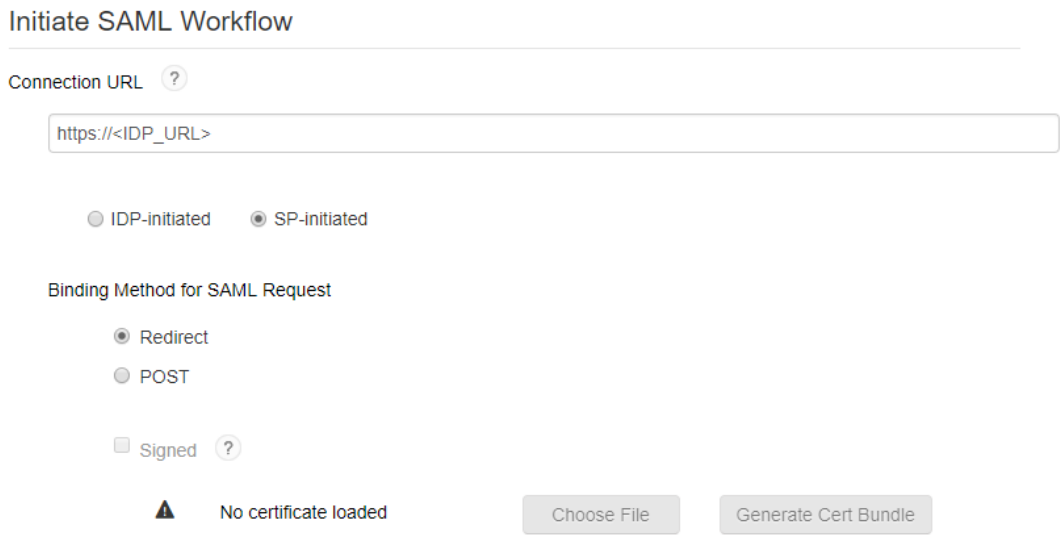
Configure RSA Identity Router SAML IdP

Procedure

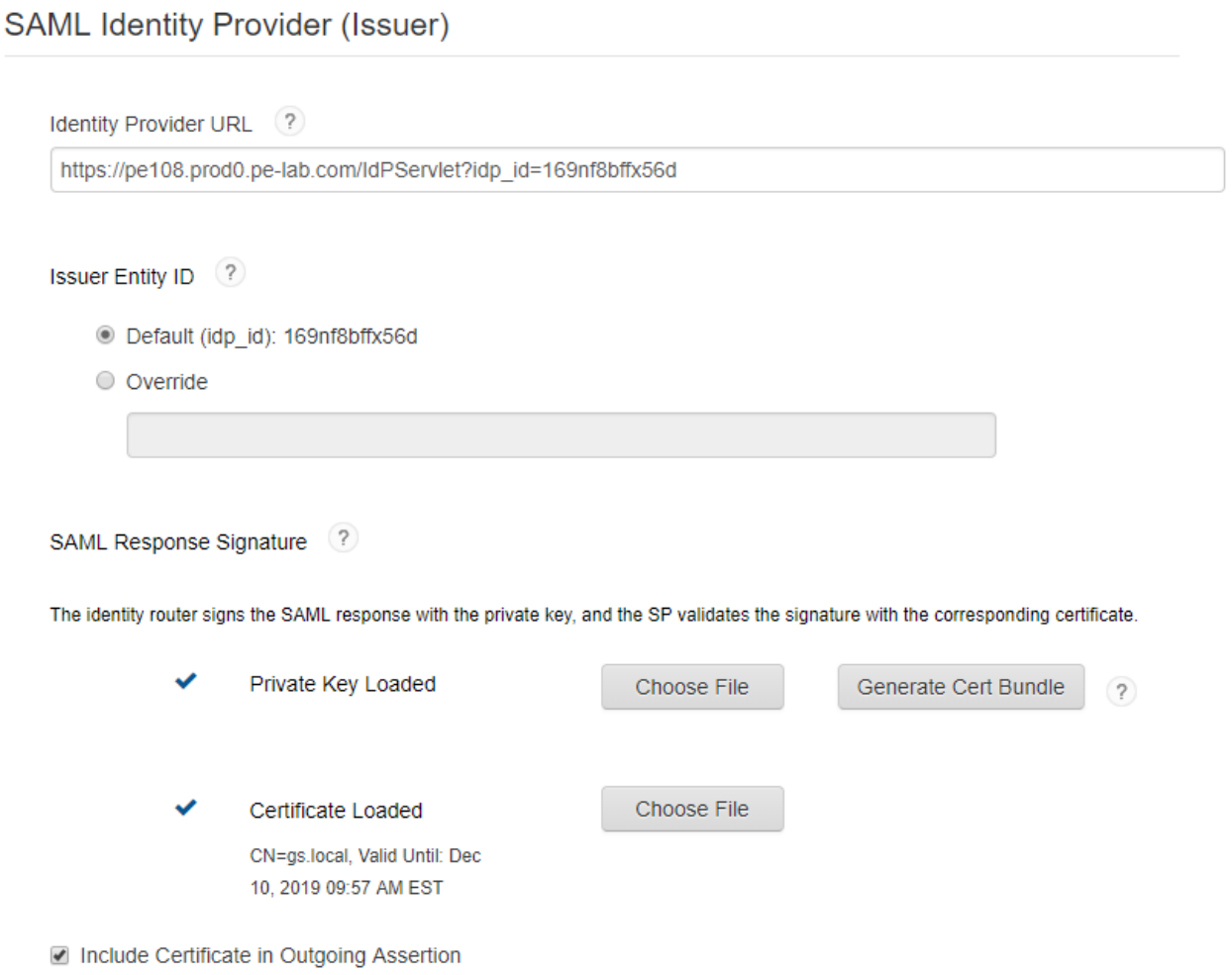
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for People HR and click **+Add** to add the connector.

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, enter the Identity Provider URL from step 4.
    b. Choose **SP-initiated.**
    c. Select binding method **Redirect**.

Note: The following IdP-initiated configuration works for SP-initiated as well.



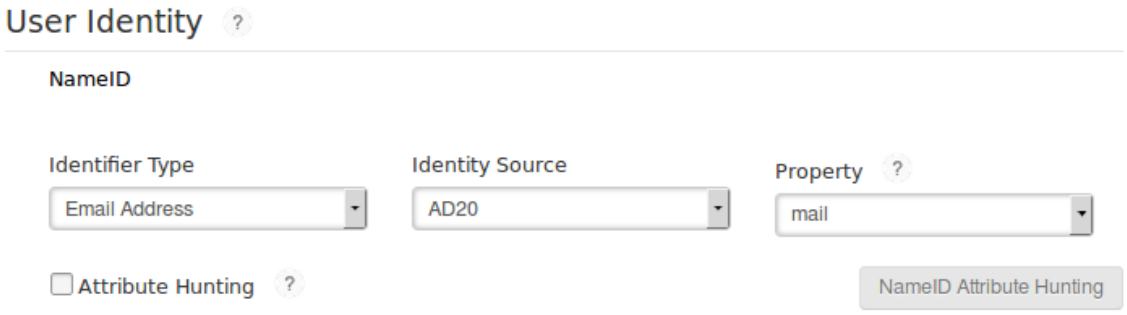
4. Scroll down to SAML Identity Provider (Issuer) section.



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**.

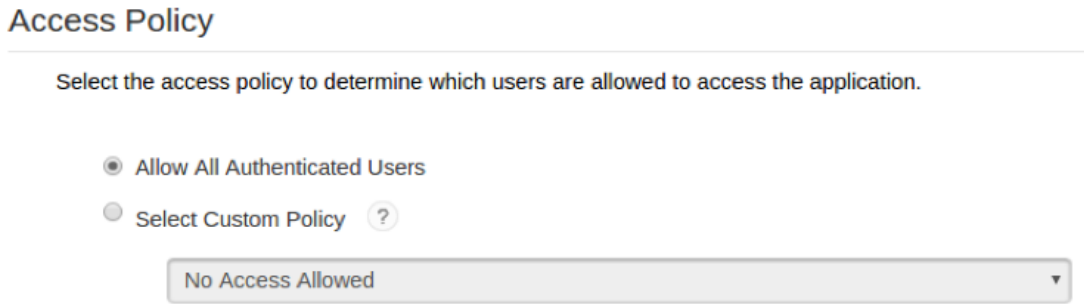
5. Scroll down to the **Service Provider** section.

6. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your People HR organization domain.
7. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> with your People HR organization domain.
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.

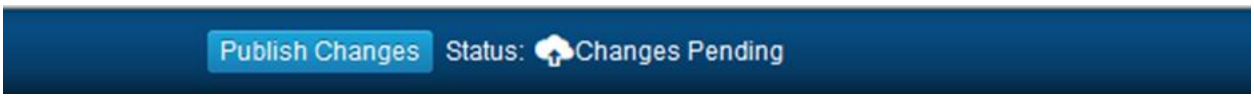


10. Click **Next Step**.

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.



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

Partner Product Configuration

Before You Begin

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

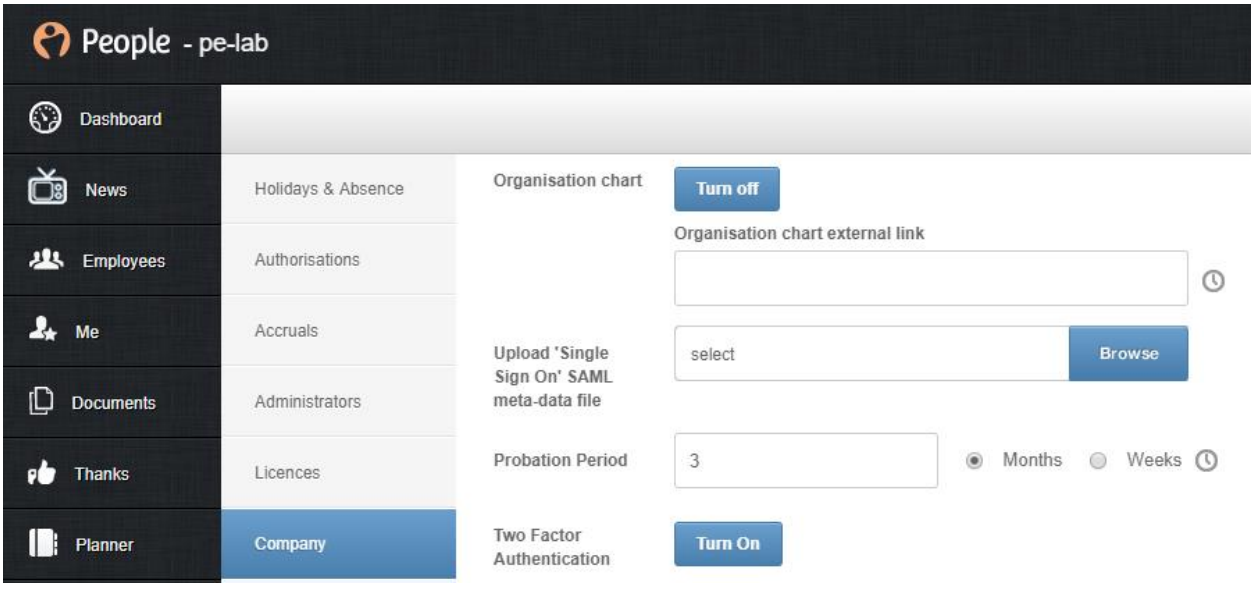
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

People HR SAML Configuration

Procedure

1. Login to People HR as an administrator. **https://<yourdomain>.peoplehr.net**
2. Navigate to **Settings > Company**.



3. Select **Browse** next to the Upload 'Single Sign On' SAML meta-data file field.
4. Select the metadata file you download in step 18 on page 7.
5. Navigate to **Employees** and add your users.