RSA SECURID® ACCESS
Implementation Guide

ADP

Gina Salvalzo, RSA Partner Engineering
Last Modified: May 30, 2018

RSA READY

Solution Summary

ADP Portal offers benefit administration, human resource and retirement services for businesses of any size.

The ADP SAML Direct Application in RSA SecurID Access is used to integrate with any/all ADP SAML SP applications. The ADP SAML Direct application has all of the configuration for ADP SAML SP applications pre-configured except for the Connection / Relay State URL. The Connection / Relay State URL is specific to each ADP SAML SP application.

If you are integrating with more than one ADP application using SAML, then an instance of the ADP SAML Direct application should be deployed for each application. All deployed ADP SAML Direct applications should use the same certificate and Issuer Entity ID. Each ADP SAML Direct application will have Connection URLs which are specific to the corresponding ADP application.

Refer to the table below for a list of supported ADP services and their Relay State URLs.

ADP Service Name	Relay State / Connection URL
ADP Workforce Now®	https://fed.adp.com/saml/fedlanding.html?WFN
ADP Workforce Now® Enhanced Time	https://fed.adp.com/saml/fedlanding.html?EETDC2
ADP Vantage HCM®	https://fed.adp.com/saml/fedlanding.html?ADPVANTAGE
ADP Enterprise HR® (ADP Portal)	https://fed.adp.com/saml/fedlanding.html?PORTAL
MyADP®	https://fed.adp.com/saml/fedlanding.html?REDBOX

RSA SecurID Access Features	
ADP	
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 ADP 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 – ADP 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
ADP SAML Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

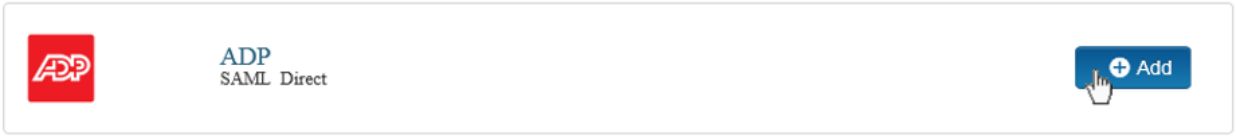
SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for ADP 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.

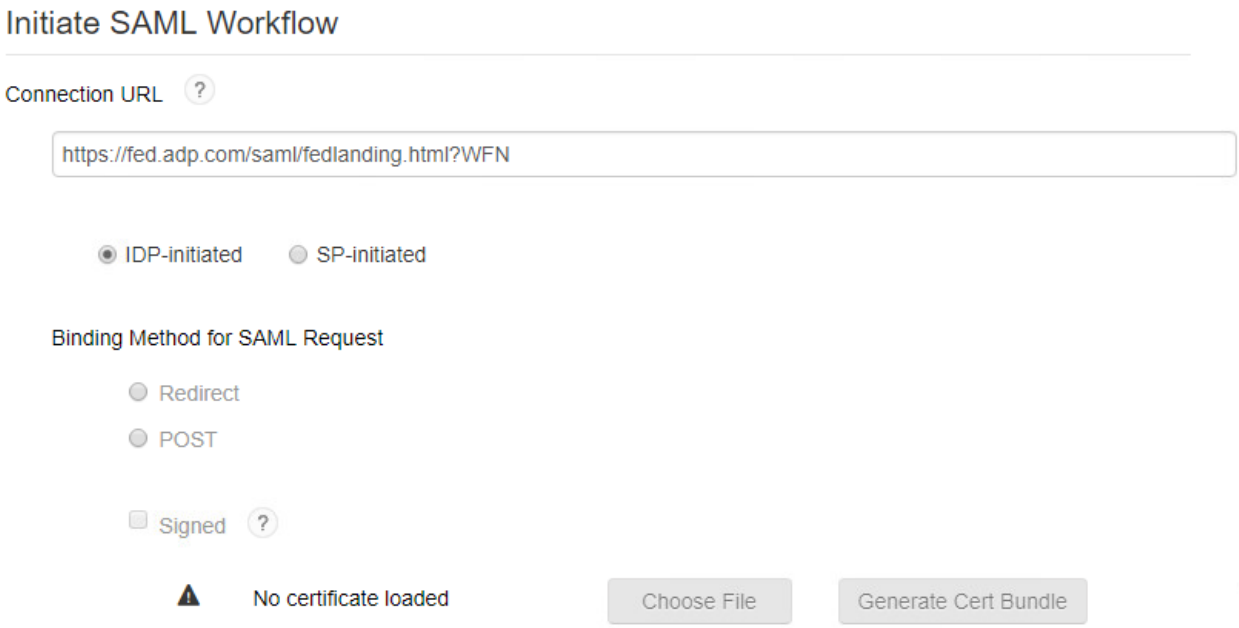
Configure RSA Identity Router SAML IdP

Procedure

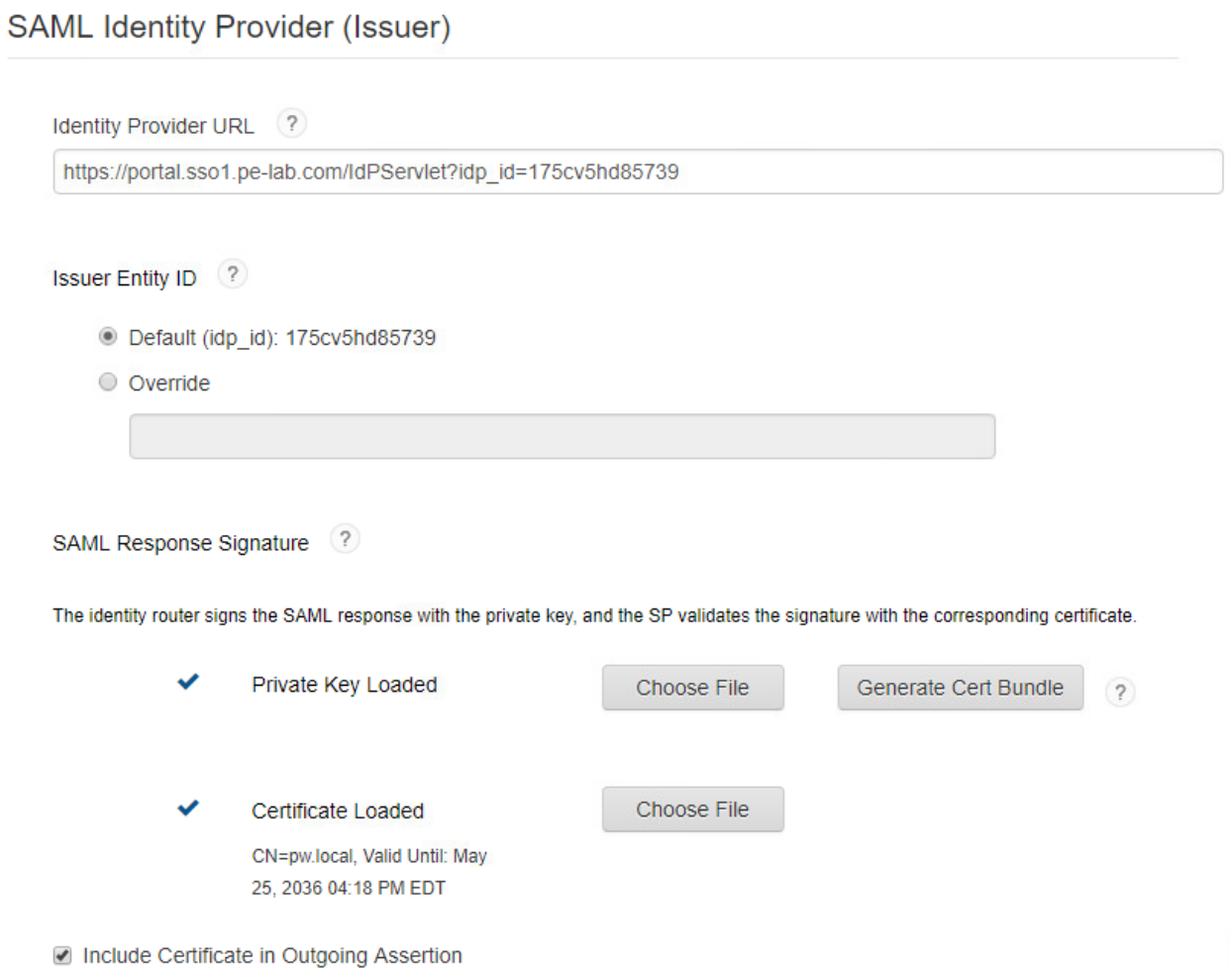
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for ADP and click **+Add** to add the connector.



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, add the relayState URL to that of your ADP application.
    b. Choose **IDP-initiated.**

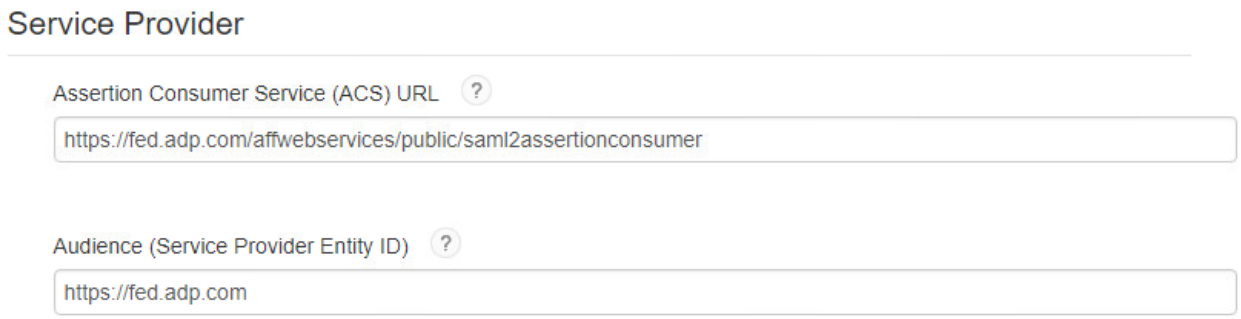


4. Scroll down to SAML Identity Provider (Issuer) section.

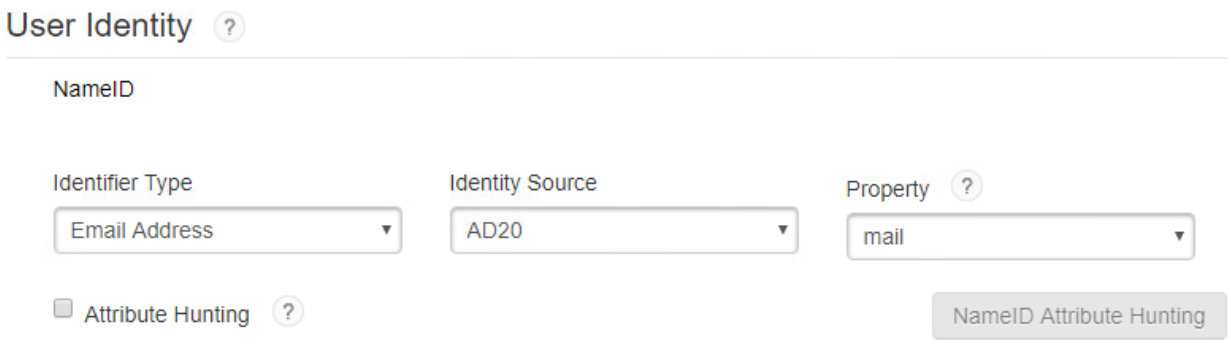


a. In the **Identity Provider URL** field, leave the default value or, optionally, change it. The Identity Provider URL for this ADP SAML Direct application must be unique to the RSA SecurID Access deployment.
b. Set the **Issuer Entity ID** to **Default**. The Issuer Entity ID must be the same as for all other (if any) ADP SAML Direct applications that are deployed on RSA SecurID Access. Use the Override option on any additional application to match.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to locate and import a private key to sign the SAML assertion. The certificate must be the same as all for all other (if any) ADP SAML Direct applications that are deployed on RSA SecurID Access.

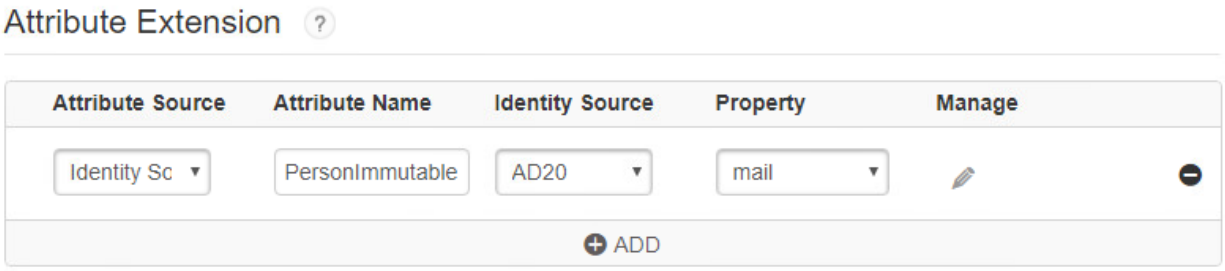
5. Verify the **Assertion Consumer Service URL** and **Audience** settings as shown below and scroll down to the User Identity section.



6. Set the **Identifier type** to **Email Address**, the **Property** to **mail** and scroll down to the Attribute Extension section.



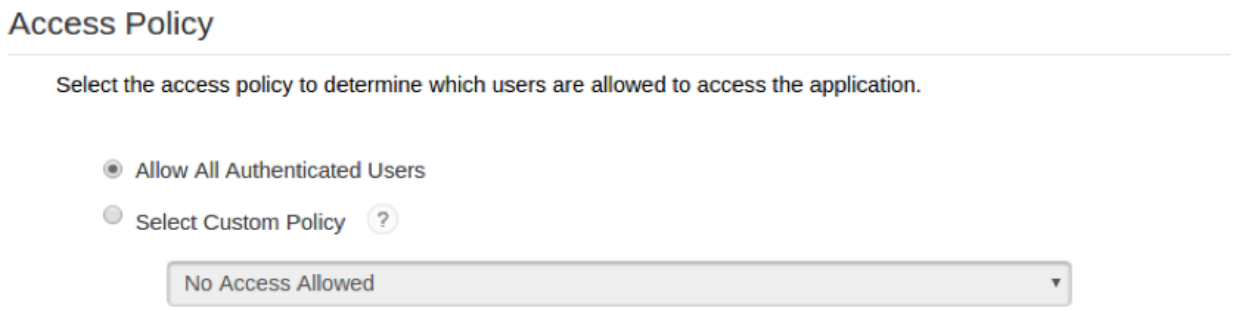
7. Add an attribute extension using the following settings.



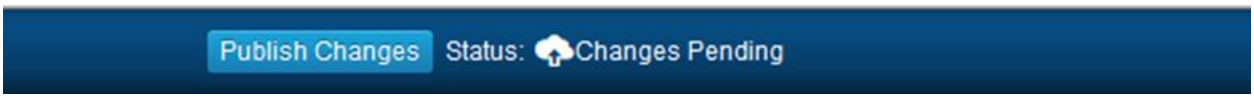
- Set Attribute Source to **Identity Source**.
- Set Attribute Name to **PersonImmutableID**.
- Set the **Identity Source** to the user store containing your ADP users.
- Set the **Property** field to the attribute in your user store that contains the ADP username.

8. Click **Next Step**.

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



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



Partner Product Configuration

ADP SAML Configuration

Procedure

Contact ADP for configuration instructions for ADP services with RSA SecurID Access.

Note: The Issuer Key and certificate configured in the ADP SP service must match the Identity Provider Entity ID and certificate that are configured in step 4 on page 5 of this document.