RSA SECURID® ACCESS
Implementation Guide

Cisco AppDynamics

Gina Salvalzo, RSA Partner Engineering
Last Modified: April 26, 2018

RSA READY

Solution Summary

Cisco AppDynamics provides application performance (APM) and IT Operations Analytics (ITOA) in a cloud service. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. AppDynamics support user auto-provisioning.

RSA SecurID Access Features	
Cisco AppDynamics	
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 AppDynamics 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 – AppDynamics 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
AppDynamics 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 AppDynamics 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

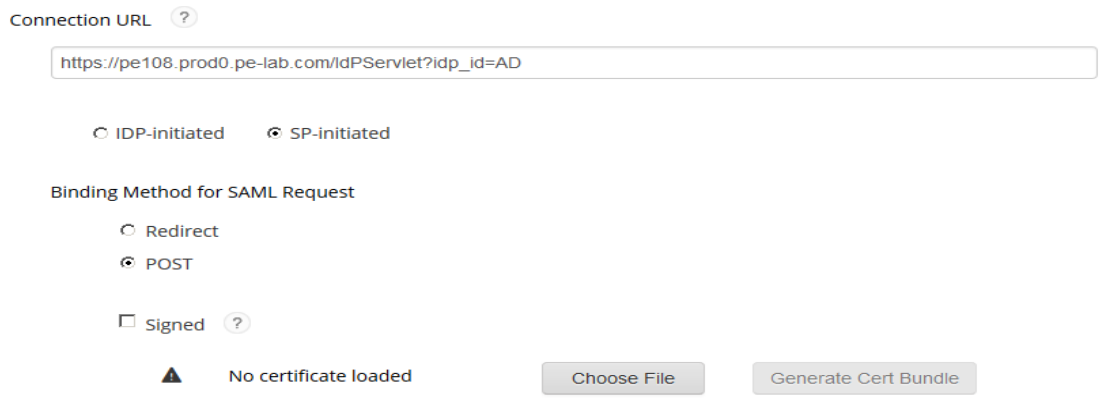
Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the SAML application that you wish to add.

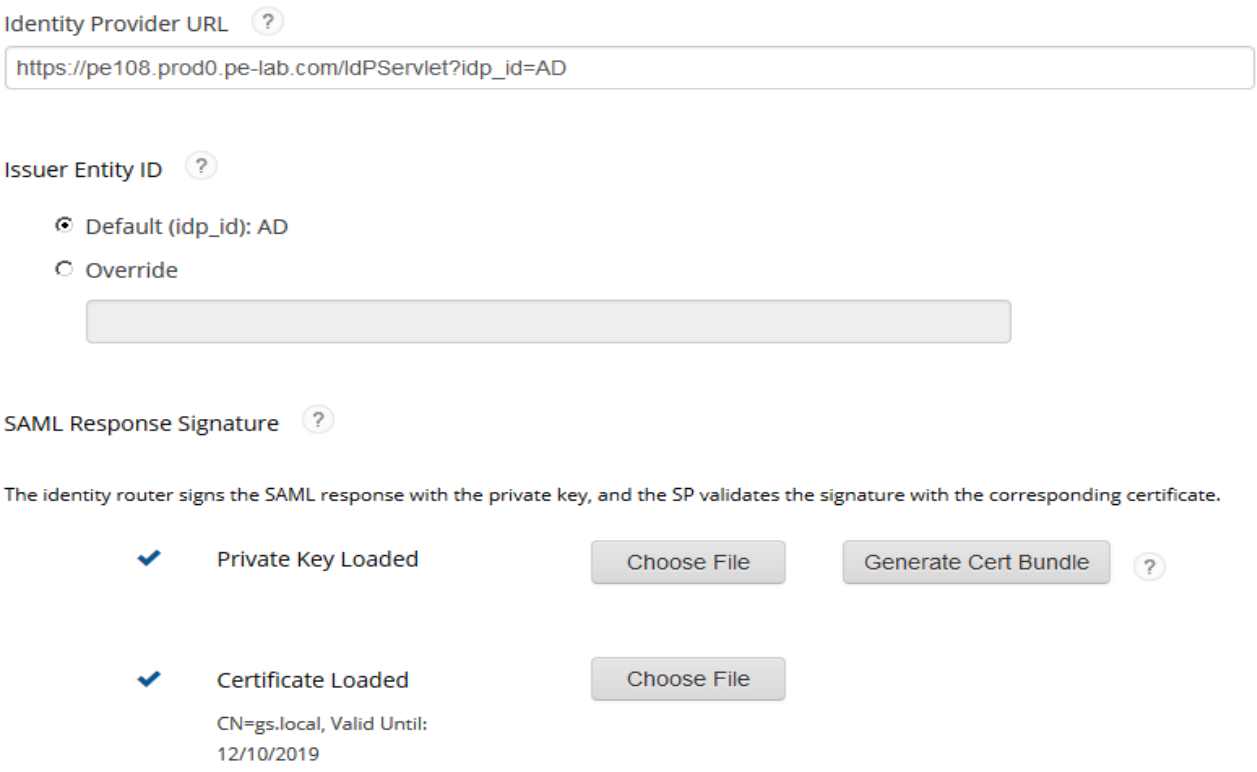
3. On the Basic Information page, specify the application name and click **Next Step**.

> **Note: The following SP-initiated configuration works for both SP-initiated and IDP- initiated connections.**

4. On the Connection Profile page, choose **SP–initiated.**
5. Enter the Identity Provider URL from step 7 into the Connection URL field.
6. Select binding method **POST**.

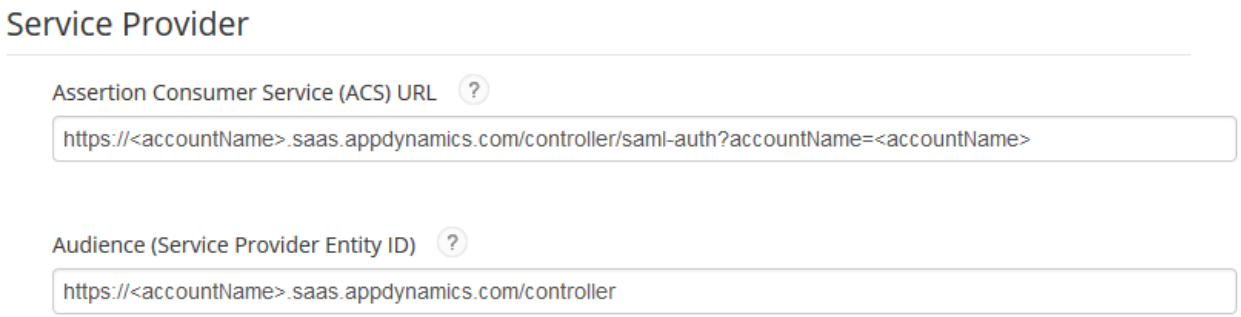


7. Scroll down to the SAML Identity Provider (Issuer) section.



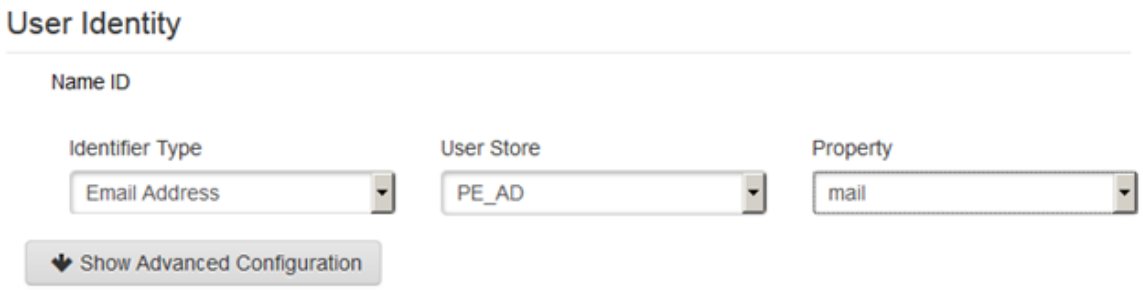
a. Select **Choose File** and upload the private key.
b. Select **Choose File** and upload the public certificate.

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

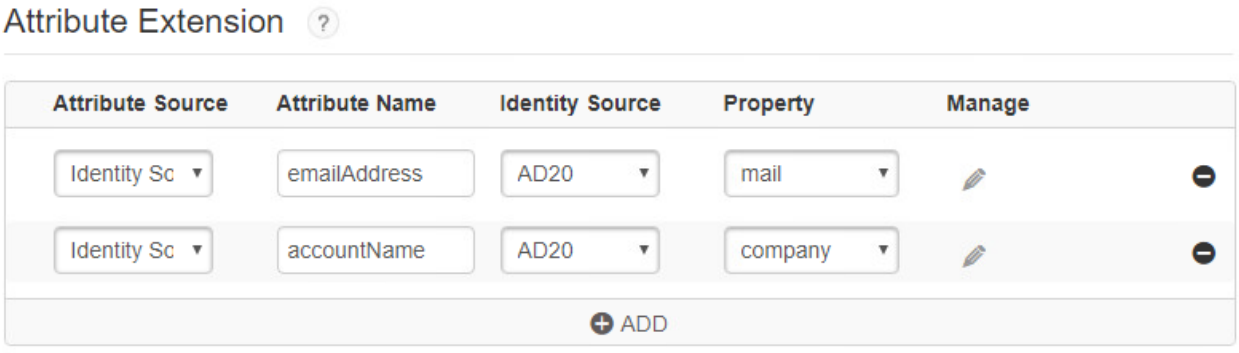


a. In the **Assertion Consumer Service (ACS) URL** field replace **<accountName>** with your company's subdomain on AppDynamics.
b. In the **Audience (Service Provider Entity ID)** field replace **<accountName>** with your company's subdomain on AppDynamics.

9. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email** and **Property** to **mail**.

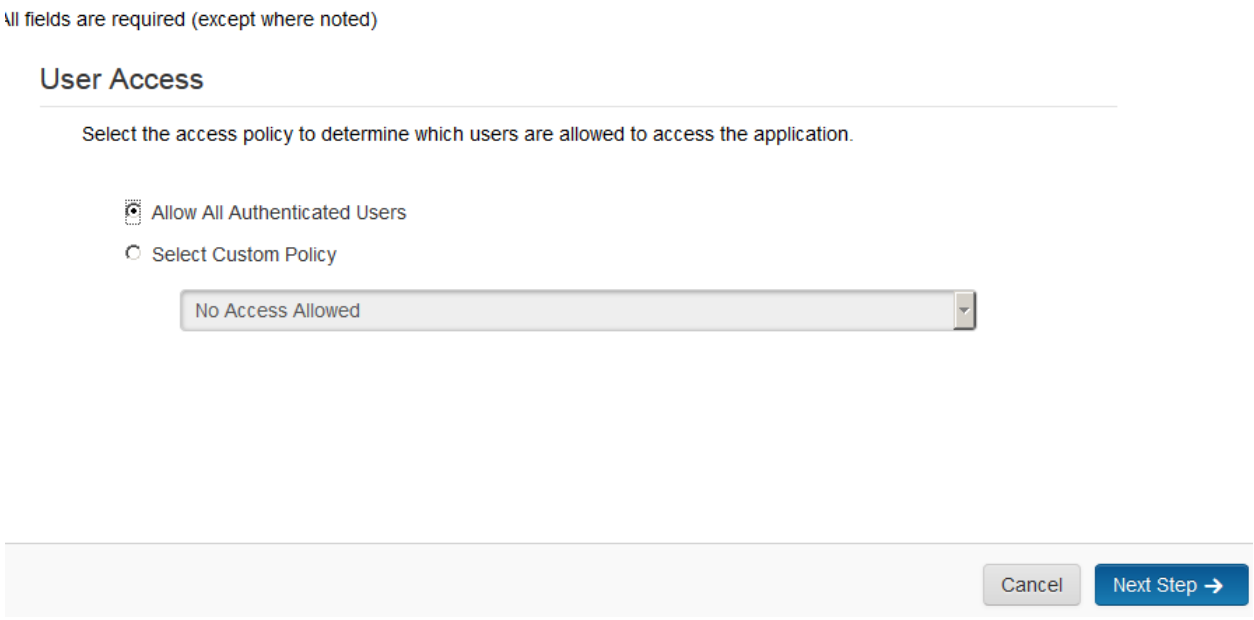


10. Click Show Advanced Configuration.
11. In the Attribute Extension section, add **emailAddress** and **accountName**. Additional attributes may also be added such as First Name, Display Name, and Groups-Membership.



12. Click **Next Step**.

13. On the **User Access** page, select the desired user policy from the drop down list.



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

Partner Product Configuration

Before You Begin

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

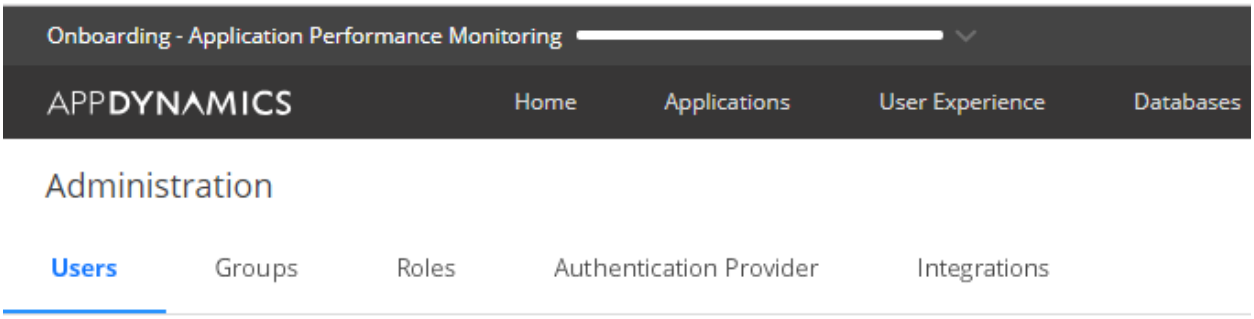
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

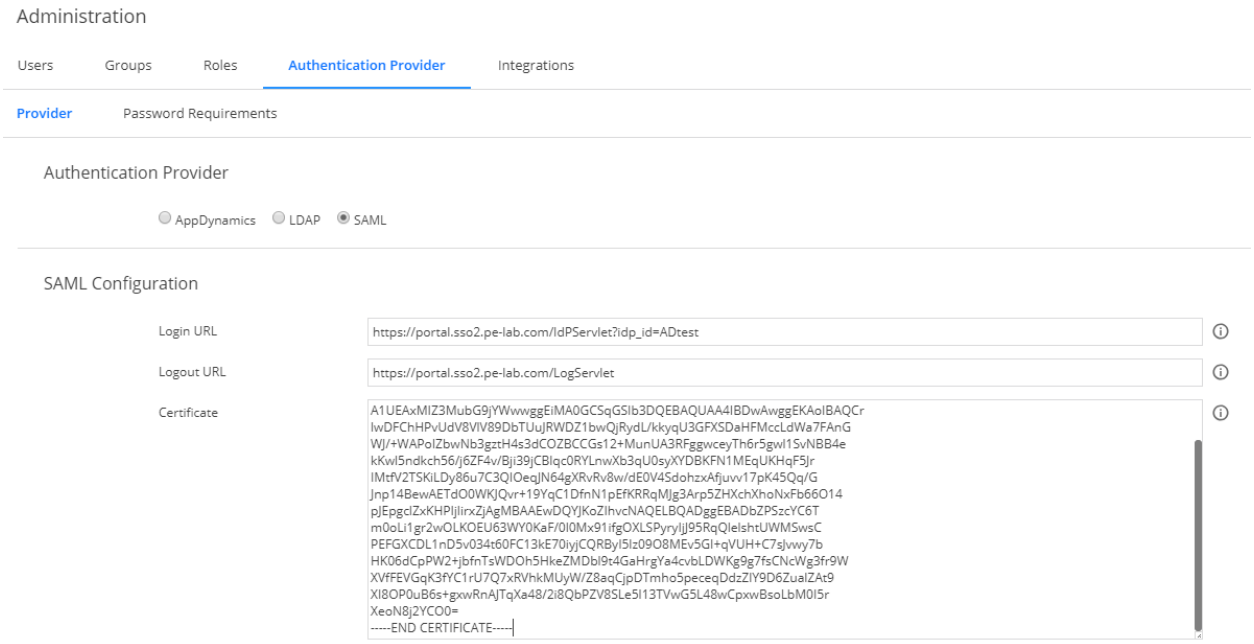
AppDynamics SAML Configuration

Procedure

1. Login to AppDynamics as an administrator. **https://AppDynamics.com/<domain>/login**
2. Navigate to **Setting > Administration**.
3. Click the **Authentication Provider** tab.



4. Under Authentication Provider select the **SAML** radio button.



5. Enter the Issuer Entity ID into the **Login URL** field. Refer to step 7 page 5.
6. Enter a URL into the Logout URL field.
7. Paste the public certificate into the x509 certificate field. Refer to step 7 page 5.

8. Enter the attribute values for Username, Display Name and Email. Refer to step 11 page 6.
9. Click **Save**.