

RSA SECURID[®] ACCESS

Implementation Guide

Cisco AppDynamics

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



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.



Cisco AppDynamics
SAML Direct

+ 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**.

Connection URL ?

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect
 POST
 Signed ?

▲ No certificate loaded



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

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): AD

Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.



Private Key Loaded



Certificate Loaded

CN=gs.local, Valid Until:
12/10/2019

Include Certificate in Outgoing Assertion

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



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

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<accountName>.saas.appdynamics.com/controller/saml-auth?accountName=<accountName>

Audience (Service Provider Entity ID) ?

https://<accountName>.saas.appdynamics.com/controller

- 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**.

User Identity

Name ID

Identifier Type

Email Address

User Store

PE_AD

Property

mail

Show Advanced Configuration

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.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc	emailAddress	AD20	mail	
Identity Sc	accountName	AD20	company	
+ ADD				

12. Click **Next Step**.



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

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


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.

Publish Changes

Status:  Changes Pending



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.

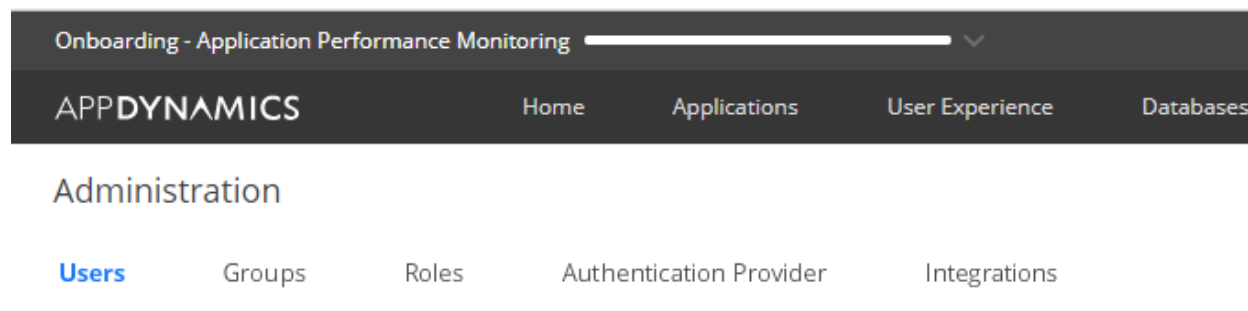
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.





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

Administration

Users Groups Roles **Authentication Provider** Integrations

Provider Password Requirements

Authentication Provider

AppDynamics
 LDAP
 SAML

SAML Configuration

Login URL	<input type="text" value="https://portal.sso2.pe-lab.com/ldpServlet?idp_id=Adtest"/>	ⓘ
Logout URL	<input type="text" value="https://portal.sso2.pe-lab.com/LogServlet"/>	ⓘ
Certificate	<input type="text" value="A1UEAxMIZ3MubG9yYVwwggEiMA0GCsqGSIb3DQEBAAUAA4IBDwAwggEKAoIBAQCrlwDFChHPvUdV8VIV89DbTUjRWDZ1bwQjRydL/kkyqU3GFXSdaHFMccLdWa7FAnG WJ/+WAPoIZbwNb3gztH4s3dCOZBCCGs12+MunUA3RFggwceyTh6r5gwl1SvNBB4e kKwl5ndkch56/j6Z4v/Bji39jCBiqc0RYLnwXb3qU0syXYDBKFN1MEqUKHqF5jr IMtV2TSKILDy86u7C3QIOeqN64gXRvRv8w/dE0V45dohzxAfjuvv17pk45Qq/G Jnp14BewAETdOOWKJQvr+19YqC1DfnN1pEFKRRqMjg3Arp5ZHxchXhoNxFb66O14 pJFpgclZxKHPjllrxZjAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAdbZPSzcYC6T mDoLi1gr2wOLKOEu63WY0KaF/0i0Mx91fgOXLSPyrylJ95RqQlelshUWM5wsC PEFGXCDL1nD5v034t60FC13kE70lyjCQRByl5lz0908MEv5G1+qVUH+C7sjwvy7b HK06dCpPW2+JbfnTsWDOH5HkeZMDbl9c+GahrgYa4cvLDWk9g7fsCncWg3fr9W XVFEVgqK3fYc1rU7Q7xRVhkMUyW/Z8aqCjpDTmho5peceqDdzYI9D6ZuaIZat9 XI8OP0uB6s+gxwRnAJTqXa48/2i8QbPZV85Le5113TVvG5L48wCpxwBsoLbM0l5r XeoN8j2YCO0= -----END CERTIFICATE-----"/>	ⓘ

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

SAML Attribute Mappings

Username Attribute	<input type="text" value="emailAddress"/>
Display Name Attribute	<input type="text" value="Display Name"/>
Email Attribute	<input type="text" value="emailAddress"/>

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