

# **RSA SECURID<sup>®</sup> ACCESS**

## **Implementation Guide**

**Accompa**

Gina Salvazo, RSA Partner Engineering  
Last Modified: August 30, 2017

## Solution Summary

---

Accompa is cloud-based Requirements Management software tool. It is widely used by Business Analysis, Product Management, Engineering, IT teams etc. Accompa delivers a single sign on experience to the user through SAML. This integration supports IdP initiated authentication flows.

<b>RSA SecurID Access Features</b>	
<b>Accompa</b>	
<b>On Premise Methods</b>	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
<b>Cloud Authentication Service Methods</b>	
Authenticate App	✓
FIDO Token	✓
<b>SSO</b>	
SAML SSO	✓
HFED SSO	-
<b>Identity Assurance</b>	
Collect Device Assurance and User Behavior	✓

## Configuration Summary

---

All of the supported use cases of RSA SecurID Access with Accompa 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** – Accompa 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 Accompa 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 Accompa 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** Accompa.



Accompa  
SAML Direct

+ Add

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

Accompa

All fields are required (except where noted)

Basic Information

Name  
Accompa

Description (optional)

Disabled ?

Cancel Next Step →

4. Navigate to **Initiate SAML Workflow** section.
  - a. In the **Connection URL** field, keep the field blank as the value is not required.
  - b. Choose **IDP-initiated**.

 **Note:** Accompa application only supports IdP-initiated SSO scenario as of now.

## Initiate SAML Workflow

Connection URL ?

http://www.example.com


IDP-initiated  SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?

 No certificate loaded

Choose File Generate Cert Bundle

5. Scroll down to **SAML Identity Provider (Issuer)** section.

## SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp\_id): 6imt198ktjjq  
 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=gslab.com, Valid Until:  
08/09/2020

Include Certificate in Outgoing Assertion

- a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
- b. Select **Default (idp\_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
- 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**.

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

## Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

- In the [Assertion Consumer Service \(ACS\) URL](#) field, provide the value as per received.
  - In the [Audience \(Service Provider Issuer ID\)](#) field, provide the value as per received.
7. 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.

## User Identity ?

NameID

Identifier Type

Identity Source

Property ?

Attribute Hunting ?

NameID Attribute Hunting

8. Moving next, select **Show Advanced Configuration**. In the **Attribute Extension** section, add **email**. These are mandatory provisioning attributes needs to be forwarded at the time of SSO.

## Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
<input type="text" value="Identity Sc"/>	<input type="text" value="email"/>	<input type="text" value="AD20"/>	<input type="text" value="mail"/>	
+ ADD				


9. Click **Next Step**.


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

## Access Policy


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

Allow All Authenticated Users

Select Custom Policy 

No Access Allowed 

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.

[Publish Changes](#) Status:  Changes Pending



## Partner Product Configuration

### ***Before You Begin***

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

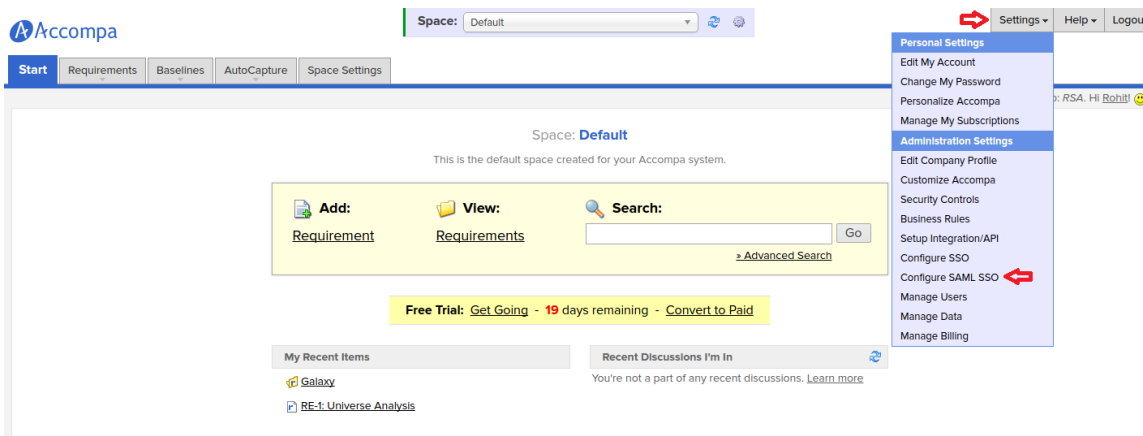
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

### Accompa SAML Configuration

#### Procedure

1. Login to your Accompa application web account. (<https://www.accompa.com/login.html>)
2. Following UI will be displayed. Go to *Settings* → *Configure SAML SSO*.



3. Following UI will be displayed. Navigate to *Configure SAML SSO (Single Sign-On)* section.

The screenshot displays the 'Configure SAML SSO (Single Sign-On)' configuration page. The page includes a sidebar with navigation options like 'Personal Settings' and 'Administration Settings'. The main content area contains the following configuration fields:

- Accompa SSO Login URL:** <https://www.accompa.com/samlsp/module.php/saml/sp/saml2-acs.php/saml-ss0-sp>
- Entity ID:** <https://www.accompa.com/samlsp>
- SAML Version:** 2.0
- SAML SSO Status:** Active (with a green dot and a red arrow icon)
- Restrict to SSO Only:** Radio buttons for 'Users must login using SSO' (selected) and 'Users can login using SSO or Accompa login page'.
- Issuer:** f65ydzgwhb6f
- Identity Provider Certificate:** Choose File (No file chosen)
- Current Certificate:** CN=gslab.com
- Request Signature Method:** RSA-SHA1
- Identity Provider Login URL:** [https://portal.sso4-pe-lab.com/IdPServlet?idp\\_id=f65ydzgwhb6f](https://portal.sso4-pe-lab.com/IdPServlet?idp_id=f65ydzgwhb6f)
- Identity Provider Logout URL:** <https://www.accompa.com/login.html>
- Custom Error URL:** <https://www.accompa.com/login.html>

A green 'Save' button with a right-pointing arrow is located at the bottom right of the configuration area.

- Make a note of **Accompa SSO Login URL** and **Entity ID** values. These will be handy during IdP side SSO configurations.  
**Note :** These values are generated after completion of SAML configuration.
- Select **Users can login using SSO or Accompa login page** radio button for the **Restrict to SSO Only** field so that users will not be locked out to login manually inside account in the scenarios of SSO failures.
- Issuer :** Provide IdP issuer value here received from step 5b page 6.
- Identity Provider Certificate :** Provide public certificate of IDR refer to step 5d page 6.
- Request Signature Method :** Choose appropriate signing mechanism from available drop-down options.
- Identity Provider Login URL :** Enter the Identity Provider URL which can be found in step 5a on page 3. It is of following format :  
[https://<Your Portal URL>?idp\\_id=<Unique IdP ID>](https://<Your Portal URL>?idp_id=<Unique IdP ID>)
- Identity Provider Logout URL :** Provide URL value where users will get redirected after logging out from the account.
- Custom Error URL :** Provide URL value for landing page for the users in case of SSO failure.
- Click on the **Save** button to configure SAML settings.

- Navigate to Settings > Manage Users.
- Add user.