

# **RSA SECURID<sup>®</sup> ACCESS**

## **Implementation Guide**

**Robin**

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

## Solution Summary

---

Robin is a meeting room booking system that simplifies your day. Robin makes scheduling meetings a snap with easy calendar integration, usage analytics and room displays. Robin delivers a single sign on experience to the user through SAML. This integration supports both IdP and SP initiated authentication flows.

RSA SecurID Access Features	
Robin	
<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	-
Identity Assurance	
Collect Device Assurance and User Behavior	✓

## Configuration Summary

---

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




Robin  
SAML Direct




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

The screenshot shows the 'Robin' configuration interface. At the top, there is a header with a gear icon, the word 'Robin', and buttons for 'Cancel' and 'Next Step'. Below the header is a sidebar with a section titled 'Add Connection' and 'Type: Robin'. The sidebar contains four steps: '1. Basic Information >', '2. Connection Profile', '3. User Access', and '4. Portal Display'. The main content area is titled 'Basic Information' and contains the following fields: 'Name' (with 'Robin' entered), 'Description (optional)' (empty), and a 'Disabled' checkbox. At the bottom right, there are 'Cancel' and 'Next Step' buttons.

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:** The following IdP-initiated configuration works for SP-initiated Robin connections as well.

## Initiate SAML Workflow

Connection URL 


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): 1m8c86hqbitmz  
 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   ?

cert.pem   
Certificate valid until: Sun Jul 11 08:29:30 UTC 2021

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) ?

- a) In the [Assertion Consumer Service \(ACS\) URL](#) field, provide the value as per received with service provider metadata.
- b) In the [Audience \(Service Provider Issuer ID\)](#) field, provide the value as per received with service provider metadata.

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. 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 Soi"/>	<input type="text" value="Email"/>	<input type="text" value="AD20"/>	<input type="text" value="mail"/>	
<span>+</span> ADD				

- Under Uncommon Formatting SAML Response Options, in the Relay State URL Encoding section, check **Include Issuer NameID Format** and from the NameID Format dropdown select **Persistent Identifier**.

### Uncommon Formatting SAML Response Options

#### Sign Outgoing Assertion

- Entire SAML response     Assertion within response

Signature Algorithm       Digest Algorithm

Encrypt Assertion ?

 No certificate loaded     

Encryption Algorithm       Encryption Key Transport

#### Relay State URL Encoding

Send encoded URL in outgoing assertion ?

Include Issuer NameID Format

NameID Format

- Click **Next Step**.
- 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 ?

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

Status:  Changes Pending



# Partner Product Configuration

## Before You Begin

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

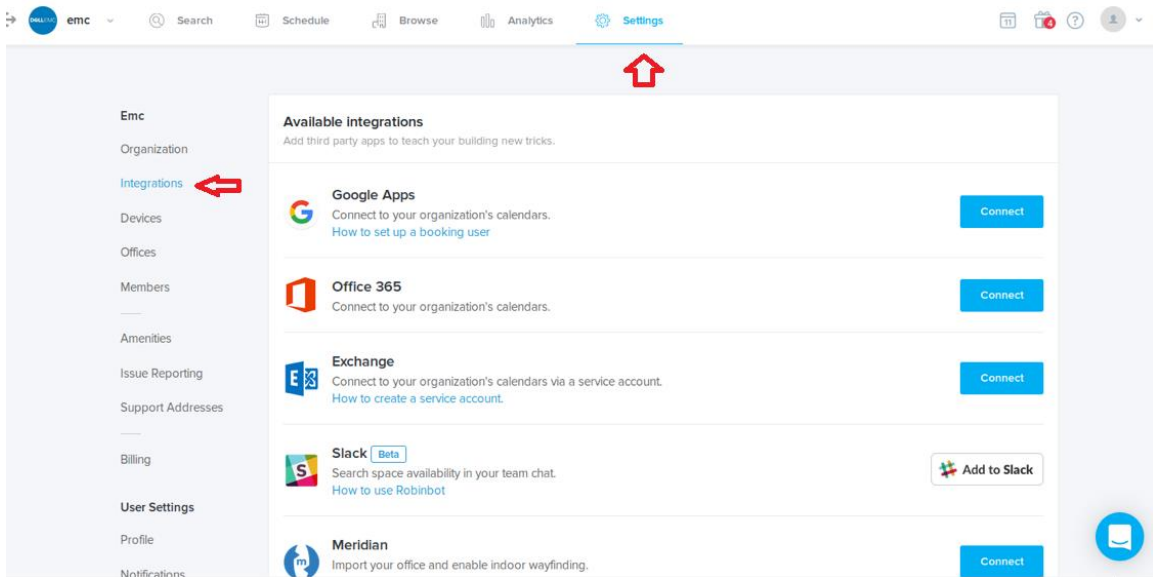
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

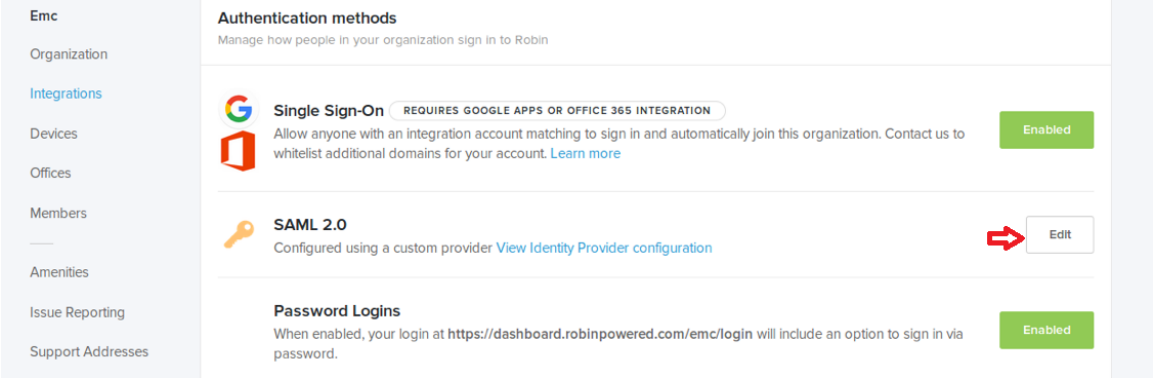
## Robin SAML Configuration

### Procedure

1. Login to your Robin application web account.  
<https://dashboard.robinpowered.com/<domain>/login>
2. Following UI will be displayed. Go to *Settings (gearing icon) → Integrations*.



3. Scroll down to *Authentication methods* > *SAML 2.0*. Click on the **Edit** button.




4. The following UI will be displayed.



### Configure SAML ×

Set up guide for SAML with Robin

---



**Provider**

Custom (Default) ▼

←

---

**SAML SSO URL**

[https://portal.sso4.pe-lab.com/IdPServlet?idp\\_id=1m8c86hqbitmz](https://portal.sso4.pe-lab.com/IdPServlet?idp_id=1m8c86hqbitmz)
←

**Identity Provider Issuer**

1m8c86hqbitmz
 ←

**Public Certificate**

```

-----BEGIN CERTIFICATE-----
MIICpjCCAY6gAwIBAgIGAV0X/QHnMA0GCSqGSIb3DQEBCwUAMBQxEjA
QBgNVBAMT
CWd7hGFILmNvbTAeFw0xNzA3MDYxMzAwNDNaFw0vMTA3MDYxMzAwN

```

←

Advanced Options

Remove

→

Save Configuration

- a) Choose **Custom(Default)** from available drop down options for **Provider** field.
- b) **SAML SSO URL** : Enter the [Identity Provider URL](#) which can be found in *step – 5* on *page 6*. It is of following format :  
[https://<Your Portal URL>?idp\\_id=<Unique IdP ID>](https://<Your Portal URL>?idp_id=<Unique IdP ID>)
- c) **Identity Provider Issuer** : Enter [IDP Issuer Entity ID](#) value received from idp settings.
- d) **Public Certificate** : Paste the RSA SecurID Access IdP public certificate here.
- e) Once sure of all the settings, click on **Save Configuration** button to complete the configurations.