

RSA SECURID® ACCESS Implementation Guide

ParkMyCloud

Gina Salvazo, RSA Partner Engineering
Last Modified: March 28, 2018



Solution Summary

ParkMyCloud is a SaaS platform that automatically identifies and eliminates public cloud resource waste, reducing spending. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. ParkMyCloud support user auto-provisioning.

RSA SecurID Access Features	
ParkMyCloud	
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 ParkMyCloud 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 – ParkMyCloud 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
ParkMyCloud 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 ParkMyCloud 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 ParkMyCloud 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, keep the field blank.
 - b. Choose **IdP-initiated**.

 Note: The following IdP-initiated configuration works for SP-initiated as well.

Initiate SAML Workflow

Connection URL 


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect


POST


Signed 

 No certificate loaded

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


SAML Identity Provider (Issuer)

Identity Provider URL 


Issuer Entity ID 

Default (idp_id): pmc


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:

Dec 10, 2019 09:57 AM


EST

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 **Choose File** and upload the private key.
- c. Select **Choose File** to import the public signing certificate.
- d. Select the checkbox for **Include Certificate in Outgoing Assertion**.

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

Service Provider

Assertion Consumer Service (ACS) URL 

`https://console.parkmycloud.com/saml/sso/<NAME>`

Audience (Service Provider Entity ID) 

`https://console.parkmycloud.com/saml/sso/<NAME>`

6. In the **Assertion Consumer Service (ACS) URL** field, replace <NAME> with your ParkMyCloud organization name used in step 5 page 11.
7. In the **Audience (Service Provider Issuer ID)** field, replace <NAME> with your ParkMyCloud organization name used in step 5 page 11.
8. 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

Email Address

Identity Source

AD20

Property 

mail







Attribute Hunting 

NameID Attribute Hunting

10. Click **Show Advanced Configuration**.

- In the Attribute Extension section, verify that the variables FirstName, LastName and NameID are correct for your environment.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property		
Identity Sc ▼	FirstName	AD20 ▼	givenName ▼		
Identity Sc ▼	LastName	AD20 ▼	sn ▼		
Identity Sc ▼	NameID	AD20 ▼	mail ▼		
+ ADD					

- 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 ?

No Access Allowed ▼

- 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.

Publish Changes

Status:  Changes Pending



Partner Product Configuration

Before You Begin

This section provides instructions for configuring ParkMyCloud 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 ParkMyCloud components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

ParkMyCloud SAML Configuration

Procedure

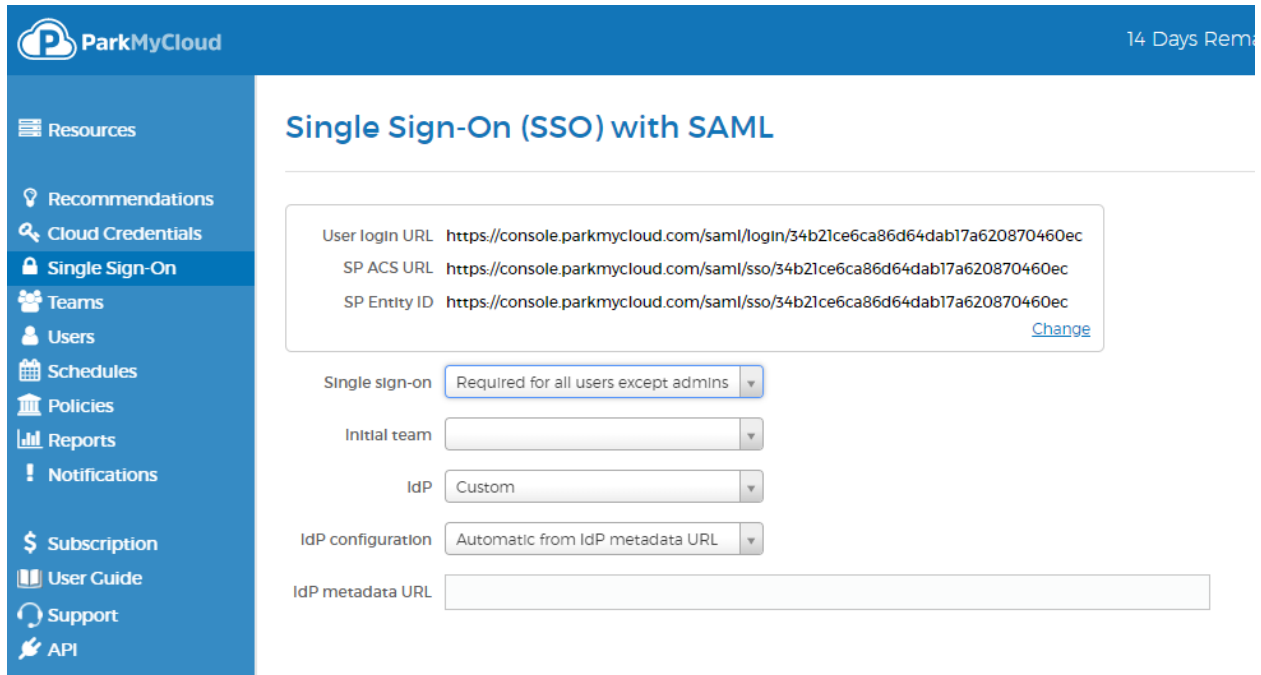
1. Login to ParkMyCloud as an administrator. <https://console.ParkMyCloud.com>
2. Navigate to **Single Sign-On**.



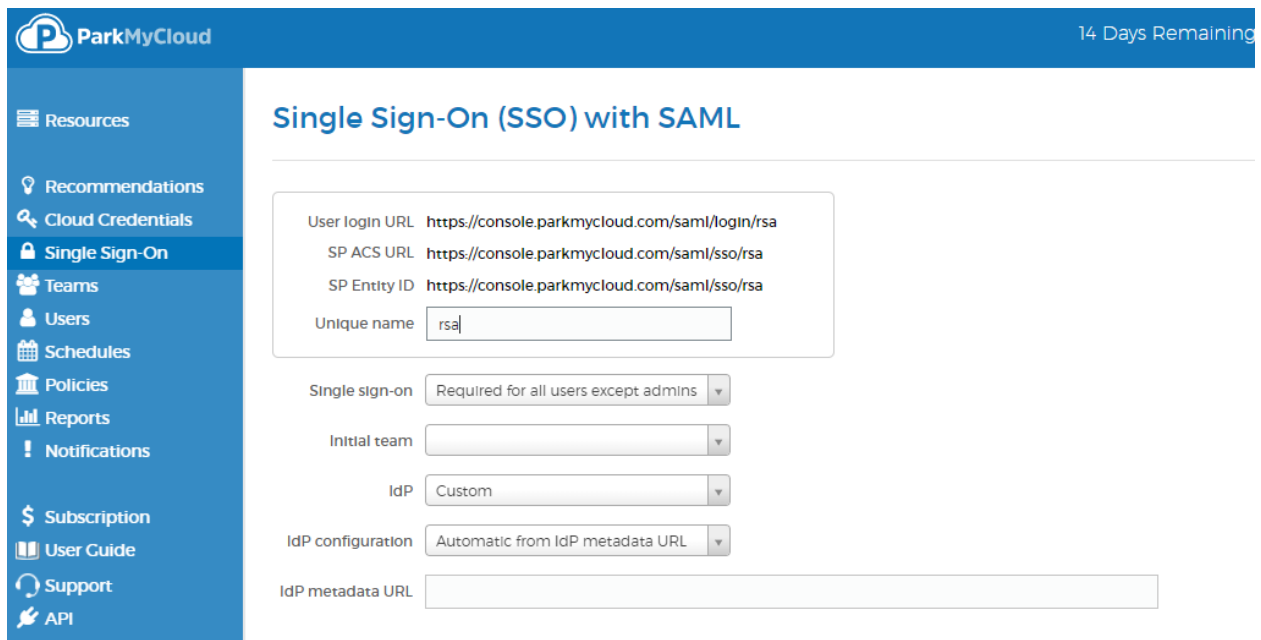
- 3. Select an option from the **Single sign-on** dropdown list. In this example we used **Required for all users except admins**.

The screenshot displays the ParkMyCloud user interface. On the left is a blue sidebar navigation menu with the following items: Resources, Recommendations, Cloud Credentials, Single Sign-On (highlighted in blue), Teams, Users, Schedules, Policies, Reports, Notifications, Subscription, User Guide, Support, and API. The main content area has a blue header with the ParkMyCloud logo and the title 'Single Sign-On (SSO) with SAML'. Below the title, there is a 'Single sign-on' label and a dropdown menu. The dropdown menu is open, showing three options: 'Disabled' (which is highlighted with a blue bar), 'Allowed for all users', and 'Required for all users except admins'.

- Click the **Change** link in the top box.



- Enter a preferred unique name for your organization.



- Take note of both the SP ACS URL and SP Entity ID for it will be needed to configure steps 5 and 6 on page 6.

7. Select the Initial team from the dropdown list. Users automatically provisioned by SSO will be added to this team.
8. Leave IdP set to **Custom**.
9. Select **Manual** from the IdP configuration dropdown list.
10. Enter the Identity Provider URL in the **IdP sign-in URL** field. Refer to page 5.
11. Enter the **IdP entity ID**. Refer to page 5.
12. Paste the public certificate into the IdP certificate field.
13. Click **Save Changes**.

Single Sign-On (SSO) with SAML

User login URL **https://console.parkmycloud.com/saml/login/rsa**

SP ACS URL **https://console.parkmycloud.com/saml/sso/rsa**

SP Entity ID **https://console.parkmycloud.com/saml/sso/rsa**

Unique name

Single sign-on

Initial team

IdP

IdP configuration

IdP sign-in URL

IdP entity ID

IdP certificate

14. For SP initiated login, go to **https://console.ParkMyCloud.com/saml/login/<name>**.