

RSA SECURID[®] ACCESS

Implementation Guide

ProdPad

Gina Salvazo, RSA Partner Engineering
Last Modified: September 15, 2017

Solution Summary

ProdPad is product management software that helps product managers develop product strategy. Easily manage teams, customers and roadmaps. This integration supports both IdP and SP-initiated authentication flows.

RSA SecurID Access Features	
ProdPad	
On Premise Methods	
RSA SecurID	<input checked="" type="checkbox"/>
On Demand Authentication	<input checked="" type="checkbox"/>
Risk-Based Authentication (AM)	<input type="checkbox"/>
Cloud Authentication Service Methods	
Authenticate App	<input checked="" type="checkbox"/>
FIDO Token	<input checked="" type="checkbox"/>
SSO	
SAML SSO	<input checked="" type="checkbox"/>
HFED SSO	<input type="checkbox"/>

Identity Assurance	
Collect Device Assurance and User Behavior	<input checked="" type="checkbox"/>

Configuration Summary

All of the supported use cases of RSA SecurID Access with ProdPad 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 – ProdPad 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 ProdPad 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 ProdPad 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 ProdPad and click **+Add** to add the connector.



ProdPad
Created From: ProdPad
SAML Direct

Edit ▾

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 as the value is not required.
 - b. Choose **IDP-initiated**.

 **Note:** The following IdP-initiated configuration works for SP-initiated ProdPad 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

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

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): 1g31cc78sht5m

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, Valid Until:
08/16/2021

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 **Override** 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**.

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

Service Provider

Assertion Consumer Service (ACS) URL ?

https://api.prodpad.com/api/v2/sso/saml/acs

Audience (Service Provider Entity ID) ?

https://api.prodpad.com/api/v2/sso/saml/metadata

1. In the **Assertion Consumer Service (ACS) URL** field, provide the value as per received with service provider metadata.
 2. In the **Audience (Service Provider Issuer ID)** field, provide the value as per received with service provider metadata.
6. 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


7. 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 the ProdPad with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

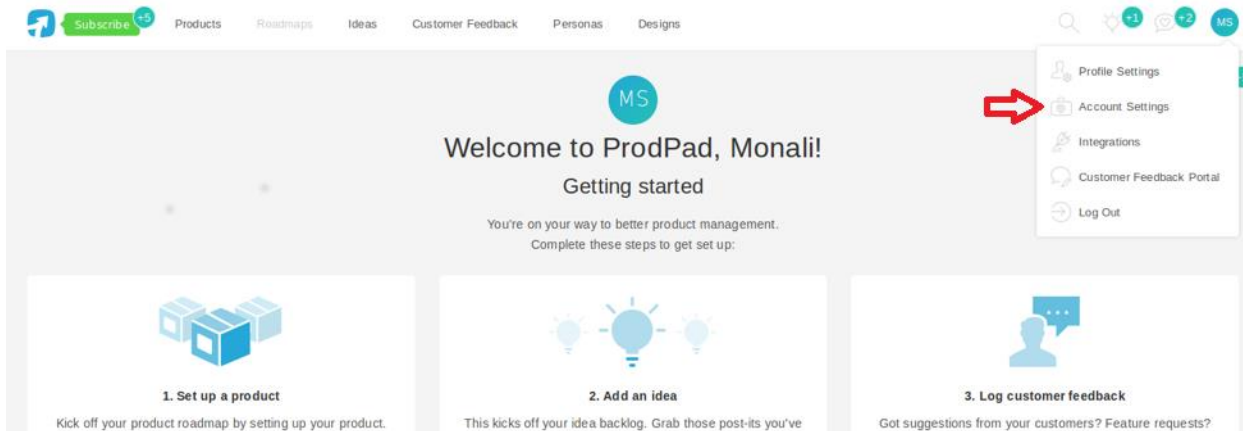
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

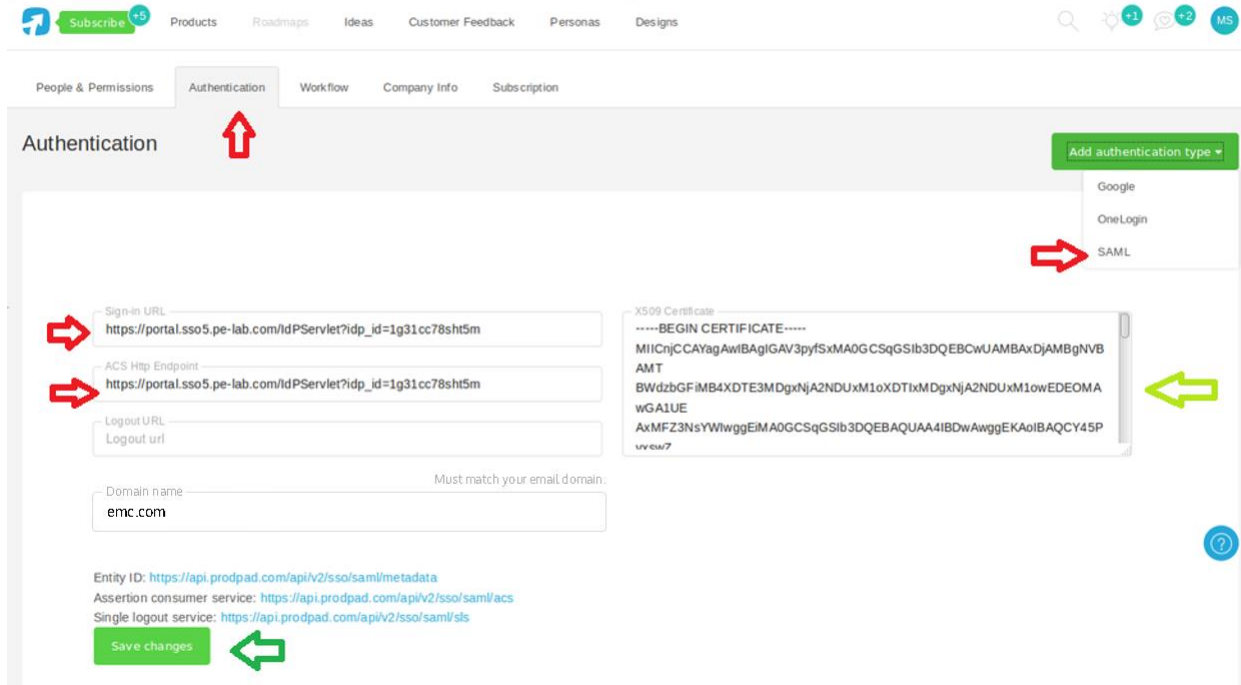
ProdPad SAML Configuration

Procedure

1. Login to your ProdPad application web account.
<https://app.prodpad.com/login>
2. Following UI will be displayed. Go to *Account Settings*.



3. Following UI will be displayed. Go to *Authentication* option. From *Add authentication type* dropdown select *SAML*



- Sign-In URL:** Enter the **Identity Provider URL** which can be found in *step -4* on *page 5*. It is of following format :
https://<Your Portal URL>?idp_id=<Unique IdP ID>
- ACS Help Endpoint :** Enter the **Identity Provider URL** which can be found in *step -4* on *page 5*. It is of following format :
https://<Your Portal URL>?idp_id=<Unique IdP ID>
- X509 Certificate:** Convert the RSA SecurID Access IdP public certificate's to fingerprint format and paste here.
- Enter a domain that will be used. This needs to match your domain of your email. A validation email to confirm ownership will be send to the administrator's email. Click the link in the email to confirm ownership of domain.
- Once sure of all the settings, click on **Save changes** button to complete the configurations.

4. Your ProdPad account is now enabled for SAML SSO authentication.