

# **RSA SECURID<sup>®</sup> ACCESS**

## **Implementation Guide**

### **Zoho**

# **ManageEngine Password Manager Pro**

John Sammon, RSA Partner Engineering  
Last Modified: February 28, 2018

## Solution Summary

---

ManageEngine Password Manager Pro (PMP) stores encrypted administrative passwords for enterprise resources. It enables IT managers to maintain a central repository of passwords, enforce standard password policies and control unauthorized user access to shared passwords. ManageEngine Password Manager Pro supports Active Directory, LDAP, local authentication and single sign-on. Single sign-on is supported via SAML using a SP initiated authentication flow. The PMP integration with RSA Authentication Manager introduces an extra level of security by enabling RSA SecurID two-factor authentication.

<b>RSA SecurID Access Features</b>	
<b>ManageEngine Password Manager Pro 7.6</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	✓

## Supported Authentication Methods by Integration Point

This section indicates which authentication methods are supported by integration point. The next section (Configuration Summary) contains links to the appropriate configuration sections for each integration point.

### ManageEngine Password Manager Pro integration with RSA Cloud Authentication Service

Authentication Methods	REST	IDR SAML	Cloud SAML	HFED	RADIUS
RSA SecurID	-	✓	n/t	-	-
LDAP Password	-	✓	n/t	-	-
Authenticate Approve	-	✓	n/t	-	-
Authenticate Tokencode	-	✓	n/t	-	-
Device Biometrics	-	✓	n/t	-	-
SMS Tokencode	-	✓	n/t	-	-
Voice Tokencode	-	✓	n/t	-	-
FIDO Token	-	✓	n/t	-	-

### ManageEngine Password Manager Pro integration with RSA Authentication Manager

Authentication Methods	REST	RADIUS	UDP Agent	TCP Agent
RSA SecurID	-	-	✓	-
AM RBA	-	-	-	-

- ✓ Supported
- Not supported
- n/t Not yet tested or documented, but may be possible

## Configuration Summary

---

All of the supported use cases of RSA SecurID Access with ManageEngine PMP 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** – ManageEngine PMP 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  
ManageEngine Password Manager Pro SAML Configuration](#)**

**RSA Authentication Manager** – ManageEngine Password Manager Pro can be integrated with RSA Authentication Manager in the following way:

UDP Agent

**[Authentication Manager UDP Agent Configuration  
ManageEngine Password Manager Pro UDP Agent Configuration](#)**

## RSA SecurID Access 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 ManageEngine Password Manager Pro 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.

1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for ManageEnginePMP 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, enter the value of your ManageEngine PMP server Hostname and Port.
  - b. Choose **SP-initiated**.
  - c. Select checkbox **Signed**. Click on **Choose File** and select [public certificate](#) of your ManageEngine Password Manager Pro server.

#### Initiate SAML Workflow

Connection URL ?

IDP-initiated  SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?

Certificate Loaded ?  
CN=win7, Valid Until:  
01/06/2028

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

### SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp\_id): zda00vr0g7px  
 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:  
08/11/2019

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**.

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

### Service Provider

Assertion Consumer Service (ACS) URL 

https://<HOSTNAME>:<PORT>/saml2

Audience (Service Provider Entity ID) 

7d7ce31f1cc04dfd812b2e4678a8874

6. In the **Assertion Consumer Service (ACS) URL** field, replace <HOSTNAME> and <PORT> with your ManageEngine Password Manager Pro server Site Hostname and Port.
7. In the **Audience (Service Provider Issuer ID)** field, provide the value as per received with service provider.
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 **Next Step**.

12. 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 

13. Click **Next Step**.
14. On the **Portal Display** page, select **Display in Portal**.
15. Click **Save and Finish**.
16. Click **Publish Changes**.

**Publish Changes**

Status:  Changes Pending

Refer to the [ManageEngine Password Manager Pro SAML Configuration](#) section for instructions on how to configure the service provider for SAML SSO.



## RSA Authentication Manager Configuration

### UDP Agent

To configure your RSA Authentication Manager for use with a UDP-based agent, you must create an agent host record in the Security console of your Authentication Manager and download its configuration file (sdconf.rec).

- Hostname: Configure the agent host record name to match the hostname of the agent.
- IP Address: Configure the agent host record to match the IP address of the agent.

---

**! > Important: Authentication Manager must be able to resolve the IP address from the hostname.**

---

## Partner Product Configuration

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

This section provides instructions for configuring the ManageEngine Password Manager Pro 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.

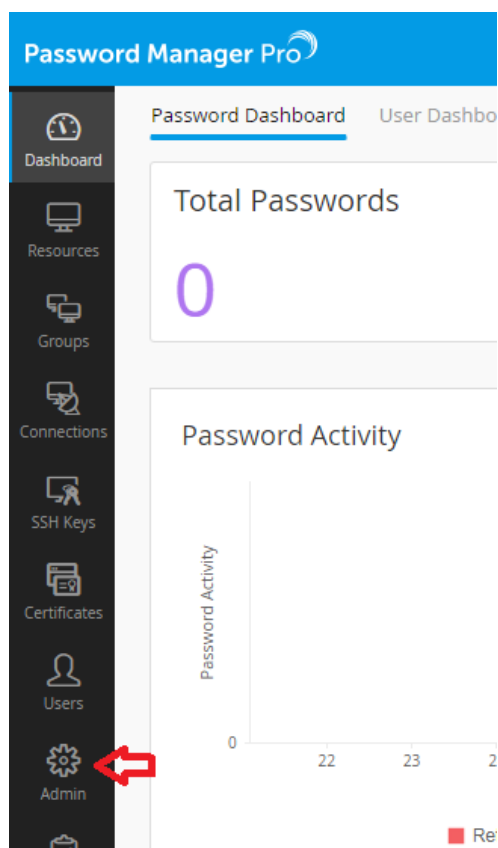
All ManageEngine Password Manager Pro components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### ***ManageEngine Password Manager Pro Configuration***

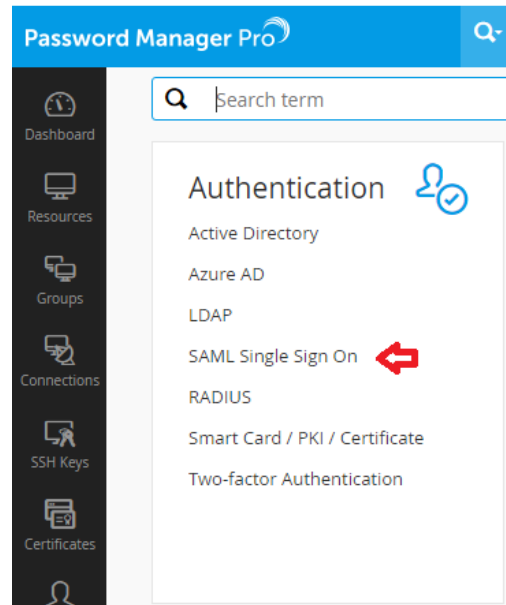
#### **ManageEngine Password Manager Pro SAML Configuration**

Complete the steps in this section to integrate ManageEngine Password Manager Pro with RSA SecurID Access using SAML authentication protocol.

1. Login to your ManageEngine Password Manager Pro server as an Administrator.
2. On the displayed page, in the left panel, click on **Admin**.



3. On the Displayed page, in the *Authentication* section, click on **SAML Single Sign on**.



4. On the displayed page, in the first *Service Provider Details* section, note down the value of **Entity ID** and **ACS URL**. Download *SP certificate file* which will be used in IDP configuration.

### 1 Service Provider Details

Use these details for integrating PMP with your IdP.

Entity Id : 7d7ce31f1cc04dfd812b2e4678a8874

Assertion Consumer URL : <https://win7:7272/saml2>

Download SP certificate file. : [spcert.cer](#)

Download SP metadata file. : [metadata.xml](#)

5. In the second *Configure Identity Provider Details* section, select **Configure IdP information manually**.

## 2 Configure Identity Provider Details

You need to provide details about the SAML IdP here. Here, you have the option either to enter the details manually or auto-fill the details by supplying the metadata file of the IdP. In case you choose to fill the details manually, collect details such as issuer id, login URL and logout URL from the IdP.

- Upload IdP metadata file.  Configure IdP information manually.

Issuer :  ⓘ  
IdP Login URL :  ⓘ  
Protocol Binding :  ▾  
IdP Logout URL :

Save

- a. In **Issuer** field, enter your **IDP ID**.
  - b. In the **IdP Login URL** field, enter **IDP URL**.
  - c. In the **Protocol Binding** section, select *HTTP-Post*.
  - d. In the **IdP Logout URL** section, enter login URL of IDP.
  - e. Click on **Save**.
6. Scroll down to the third section. Select **Upload IdP Cert File now** option. Click on **Browse** to select your **IDP public certificate**. Click on **Save**.

## 3 Import IdPs Certificate

You need to supply PMP the certificate of the IdP. Collect the certificate from the IdP and upload it here. Alternatively, if you are already managing the certificate in PMP, you may choose the other option and specify the details.

- Upload IdP Cert File now  Use IdP Cert File from PMP File Store or Key Store

Import Certificate:

7. In the fourth section, Click on Enable Now to enable SAML authentication.

④ Enable / Disable SAML Single Sign On.

At any point, you may enable or disable SAML SSO through this step.

Current status : Disabled



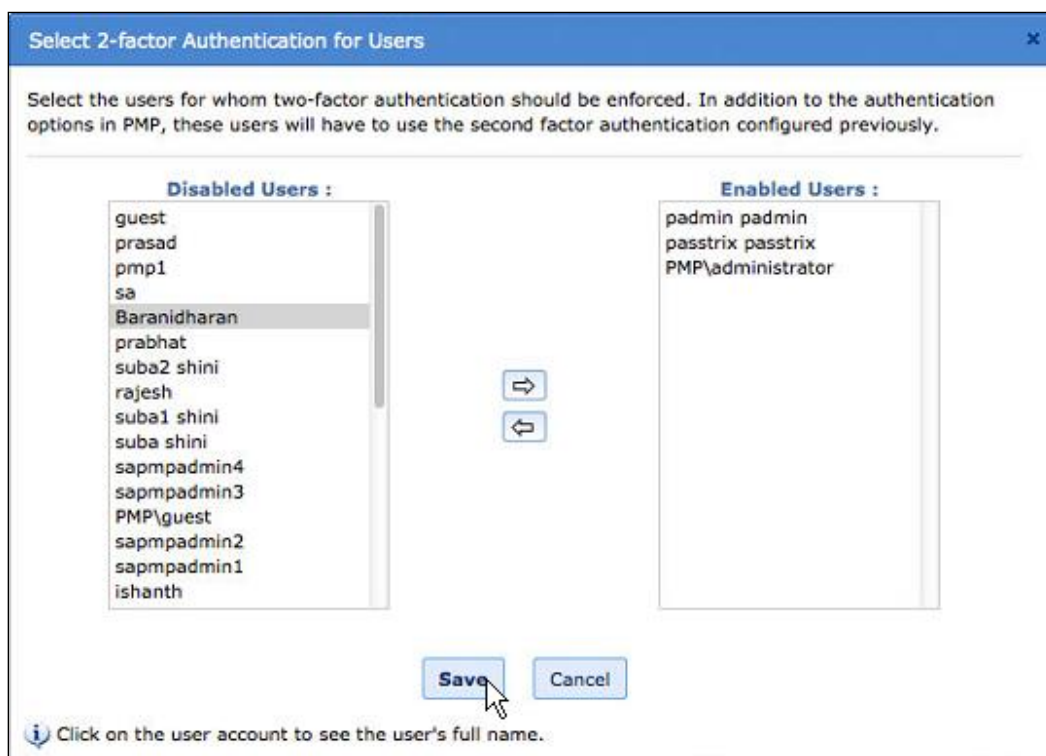
Enable Now

8. Your ManageEngine Password Manager Pro account is now enabled for SAML Single Sign on.

## ManageEngine Password Manager Pro UDP Agent Configuration

### Configure the Password Manager Pro for RSA SecurID Authentication

1. Contact RSA to get a copy of the RSA Authentication Agent API and copy the API jar files and the *rsa\_api.properties* file to the *%PMP\_HOME%/PMP/lib* directory.
2. Open the *%PMP\_HOME%/PMP/bin/rsa\_api.properties* file and set the *RSA\_AGENT\_HOST* property value to the PMP server hostname or IP Address.
3. Log in to the PMP admin console, click the **Admin** tab and select the **Two Factor Authentication** menu.
4. Select the **RSA SecurID** radio button and click the **Save** button.
5. Click the **Admin** tab, select the **Users** menu and click the **Set 2-factor authentication** button.
6. Scroll to the **Disabled Users** list, select all of the users who will be required to authenticate with RSA SecurID and click the right arrow button. The users you selected should appear in the **Enabled Users** list.



7. Click the **Save** button.

## Login Screenshots

---

Login screen:

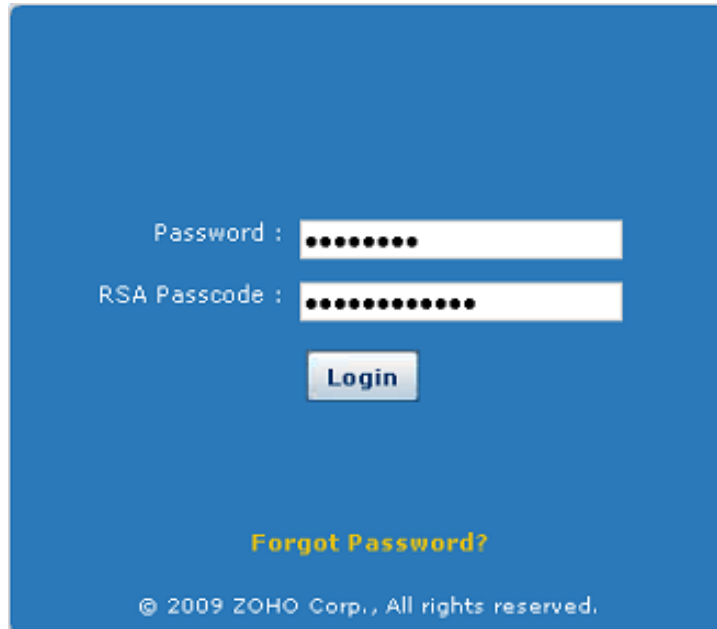


User Name :

**Next**

**Forgot Password?**

© 2009 ZHOHO Corp., All rights reserved.



Password :

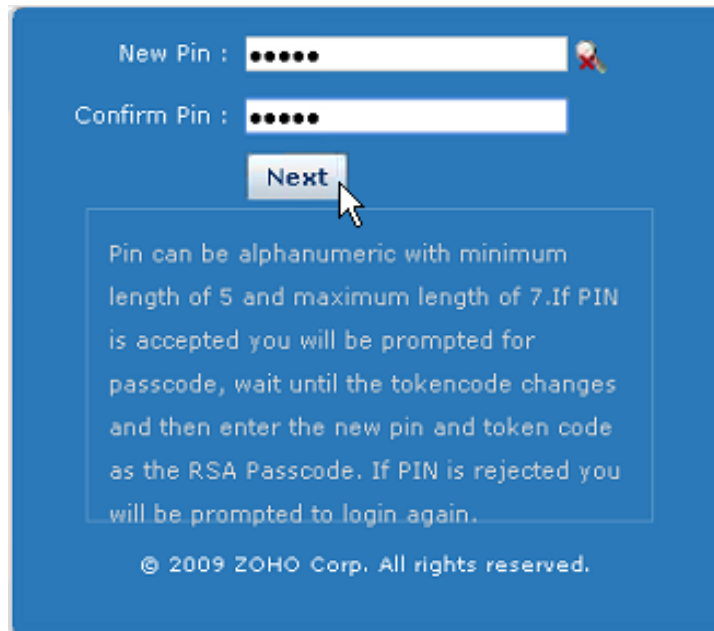
RSA Passcode :

**Login**

**Forgot Password?**

© 2009 ZHOHO Corp., All rights reserved.

User-defined New PIN:



New Pin : [.....]

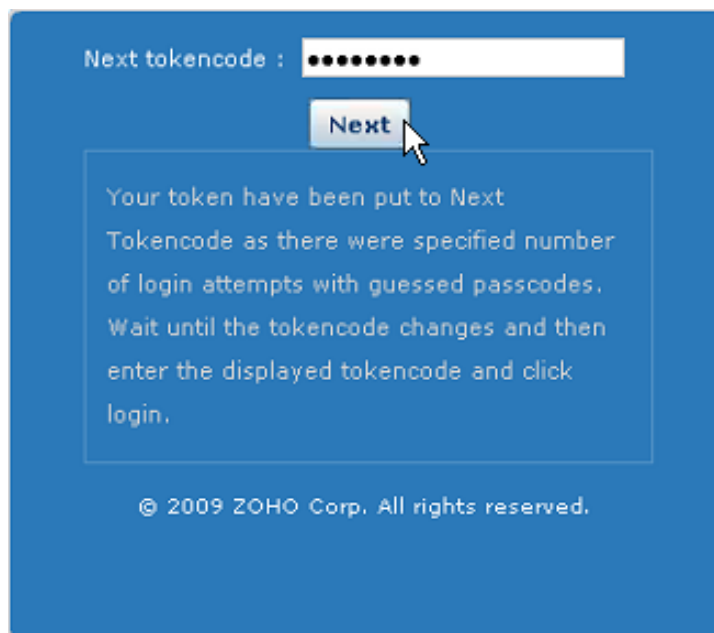
Confirm Pin : [.....]

Next

Pin can be alphanumeric with minimum length of 5 and maximum length of 7. If PIN is accepted you will be prompted for passcode, wait until the tokencode changes and then enter the new pin and token code as the RSA Passcode. If PIN is rejected you will be prompted to login again.

© 2009 Zoho Corp. All rights reserved.

Next Tokencode:



Next tokencode : [.....]

Next

Your token have been put to Next Tokencode as there were specified number of login attempts with guessed passcodes. Wait until the tokencode changes and then enter the displayed tokencode and click login.

© 2009 Zoho Corp. All rights reserved.



## Certification Checklist for RSA SecurID Access

---

### Certification Environment Details:

RSA Authentication Manager 8.1, Virtual Appliance

RSA Authentication Agent 8.1, SUSE Linux Enterprise Server 11 SP3

ManageEngine Password Manager Pro, 7.6, Windows 7

### ***RSA Authentication Manager***

Date Tested: March 27, 2015

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	-	✓	-	-
RSA SecurID Software Token Automation	-	-	-	-
On Demand Authentication	-	-	-	-
Risk-Based Authentication	-	-	-	-

✓ = Passed, ✗ = Failed, - = N/A

## Known Issues

---

At the time of this testing the RSA Authentication Manager API failed to report a character restriction for PIN policies that require alphabetic characters. Instead, the API indicates that the PIN may be alphanumerical. As a result, the integration will prompt the user for an alphanumeric PIN under these circumstances.

Customers should limit their PIN policies to require either numeric or alphanumeric characters.

## Appendix

---

### ***RSA SecurID AccessIntegration Details***

Partner Integration Details	
RSA Authentication Agent API (UDP)	8.1

### ***RSA Authentication Agent Files (C and Java Agents only)***

RSA SecurID Authentication Files	
UDP Agent Files	Location
sdconf.rec	%PMP_HOME%/bin
sdopts.rec	Not implemented
Node secret	%PMP_HOME%/bin
sdstatus.12	The RSA Web agent installation directory.