



RSA SecurID Ready Implementation Guide

Last Modified: December, 19, 2008

Partner Information

Product Information	
Partner Name	AdventNet, Inc
Web Site	www.adventnet.com
Product Name	ManageEngine PasswordManager Pro
Version & Platform	6.0 & JAVA
Product Description	ManageEngine Password Manager Pro (PMP) is a software solution to securely store, access and administer shared administrative passwords. It enables IT managers to maintain a central repository of passwords, enforce standard password policies and control unauthorized user access to shared passwords.
Product Category	General Security Utility



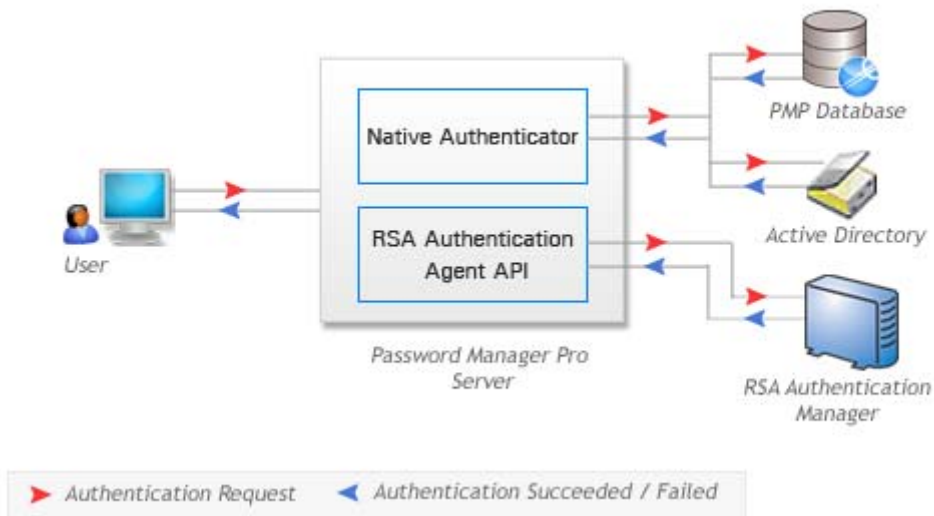


Solution Summary

ManageEngine Password Manager Pro (PMP) stores sensitive, administrative passwords of enterprise resources in encrypted form. Access to the data is restricted by a single level of authentication – local authentication of PMP or the authentication of third party identity stores like ActiveDirectory or LDAP. To introduce an extra level of security, PMP provides two factor authentication with RSA SecurID.

For RSA SecurID authentication, PMP communicates with RSA Authentication Manager using the RSA Authentication Agent APIs. PMP sends the user's credentials to RSA Authentication Manager, which validates and sends back the status to the PMP server.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	5.0.3.172(API version)
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	No
RSA Authentication Agent Host Type	Communication Server, UNIX
RSA SecurID User Specification	All Users
* = Mandatory Function when using Native SecurID Protocols	





Product Requirements

AdventNet Software Requirements:

Software	Comments
PMP 6.0 and above	Earlier versions of this product do not support RSA SecurID authentication

Operating System Support

Platform	Required Patches
MS Windows Server 2003/XP/Vista/Professional	All Patch Levels Supported
LINUX – RedHat Linux 8.0 /9.0/CentOS 4.4/ Suse Linux 10.1; Mandrake Linux 10.0	All Patch Levels Supported

RSA Agent Host Configuration

To facilitate communication between PMP and the RSA Authentication Manager/RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies PMP within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information:|

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure PMP as either a UNIX Agent or Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with PMP will occur.

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	%PMP_HOME%/bin/
Node Secret	%PMP_HOME%/bin/
sdstatus.12	File normally is stored in the same location as the Node Secret
sdopts.rec	Not implemented



Partner Product Configuration

Before You Begin

This section provides instructions for integrating AdventNet Password Manager Pro with RSA SecurID authentication. 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 documentation for all products in order to install the required components. All products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuration

Installation steps for integrating PMP with RSA Authentication Manager:

Install PMP and RSA Authentication Manager. It is not necessary for both to be installed on the same server. Follow the steps detailed below to do the integration.

1. Download RSA Authentication Agent API from RSA download server and unzip it under **%PMP_HOME%/PMP/lib**.
2. Configure RSA Agent Host record.
 - Register the PMP server as an Agent Host in the RSA Authentication Manager.
 - Generate the RSA Authentication Manager **sdconf.rec** file and copy it to the default application directory (**%PMP_HOME%/PMP/bin**).
 - If a Node Secret file, exists, copy it to **%PMP_HOME%/PMP/bin** as well.
 - 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.



Two-factor Authentication Flow of Events

Before authentication can take place, use the RSA Security Console to enter all desired PMP users into RSA Authentication Manager, assign tokens to them and activate them on the appropriate Agent Host.

The following sequence describes a typical PMP – RSA SecurID authentication process. Note that users must authenticate twice: first with their local LDAP or Active Directory passwords, and then with their RSA SecurID tokens.

1. A user tries to access PMP web-interface
2. PMP authenticates the user via ActiveDirectory or LDAP or locally.



3. PMP prompts for the user for a username and RSA SecurID passcode and forwards the credentials to RSA Authentication Manager through the RSA Runtime API.



4. RSA Authentication Manager authenticates the user and returns a message to PMP.
5. PMP grants the user access to the requested resource.

Note that the RSA Server may request that the user sets a new PIN (or accepts one generated by the system), or that the user waits for the tokencode to change and enter a



new passcode. These options and their frequencies are configured via the RSA Security Console.

Certification Checklist For RSA Authentication Manager v6.1

Date Tested: 12/18/2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows 2003 Standard Edition SP2
RSA Authentication Agent API	5.0.3.172	-
ManageEngine Password Manager Pro	6.0	Mandrake Linux

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input type="checkbox"/> N/A
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/> N/A
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
Credential Functionality			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/> N/A
Set Credential	<input type="checkbox"/> N/A	Set Credential	<input type="checkbox"/> N/A
Retrieve Credential	<input type="checkbox"/> N/A	Retrieve Credential	<input type="checkbox"/> N/A

JGS / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function



Certification Checklist For RSA Authentication Manager 7.1

Date Tested: 18/12/2008

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003 Standard Edition SP2
RSA Authentication Agent API	5.0.3.172	-
ManageEngine Password Manager Pro	6.0	Mandrake Linux

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input type="checkbox"/> N/A
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input type="checkbox"/> N/A
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input type="checkbox"/> N/A
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input type="checkbox"/> N/A
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input type="checkbox"/> N/A
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input type="checkbox"/> N/A
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input type="checkbox"/> N/A
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input type="checkbox"/> N/A
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input type="checkbox"/> N/A
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input type="checkbox"/> N/A
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input type="checkbox"/> N/A
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

JGS / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function



Appendix

RSA SecurID file locations:

sdconf.rec – stored as a file in %PMP_HOME%/bin/
Node Secret – stored as a file in %PMP_HOME%/bin/
sdstatus.12 – stored as a file in %PMP_HOME%/bin/
sdopts.rec - not implemented