



## RSA SecurID Ready Implementation Guide

Last Modified: December 28, 2009

### Partner Information

Product Information	
Partner Name	Hewlett-Packard
Web Site	<a href="http://www.hp.com">www.hp.com</a>
Product Name	HP Network Automation
Version & Platform	7.6
Product Description	<p>HP NA tracks and regulates configuration and software changes across routers, switches, firewalls, load balancers, and wireless access points. HP NA provides visibility into network changes, maximizing engineers' efficiency and allowing IT staff to identify and correct trends that could lead to problems, while mitigating compliance issues, security hazards, and disaster recovery risks.</p> <p>HP NA captures full audit trail information about each device configuration change. In addition, HP NA can enforce security and regulatory policies at the network level by ensuring configurations comply with pre-defined standards. HP NA mitigates many of the risks inherent in IT operations. The end result is a resilient and maintainable network that is compliant to standards and regulations.</p>
Product Category	<a href="#">Networks and Communication, Web Applications &amp; ERP</a>





## Solution Summary

---

HP Network Automation can be configured to use RSA SecurID two-factor authentication. Once an HP Network Automation administrator enables SecurID as the external authentication method, existing HP users will be required to authenticate with their RSA SecurID tokens.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	5.3
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	Yes
RSA Authentication Agent Host Type	UNIX
RSA SecurID User Specification	All Users
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	No

## Product Requirements

---

Partner Product Requirements: HP NA	
Version	7.6

Operating System	
Platform	Required Patches
Microsoft Windows Server 2003	SP2
Solaris 10	118833-36 or later
Red Hat AS 4 32-bit and 64-bit	
Red Hat AS 5 64-bit	
SuSE Enterprise Linux Server 10.x	

Additional Software Requirements	
Application	Additional Patches
Oracle 10g Standard Edition 10.2.0.2 or 10.2.0.4	
MS SQLServer 2005	
MySQL 5.0.58	



## Agent Host Configuration

---

To facilitate communication between the HP Network Automation Server 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 the HP NA Server 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 the HP NA Server as UNIX. This setting is used by the RSA Authentication Manager to determine how communication with the HP NA server will occur.

---

 **Note: Hostnames within the RSA Authentication Manager/RSA SecurID Appliance must resolve to valid IP addresses on the local network.**

---

Please refer to the appropriate RSA Security documentation for additional information about creating, modifying and managing Agent Host records.

## RSA SecurID files

---

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	C:\WINDOWS\SYSTEM32 or /var/ace
Node Secret	C:\WINDOWS\SYSTEM32 or /var/ace
sdstatus.12	C:\WINDOWS\SYSTEM32 or /var/ace

---

 Please see the [Appendix](#) for more information.

---

# Partner Product Configuration

## Before You Begin

This section provides instructions for integrating HP Network Automation with RSA SecurID. 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 vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

## Configuring RSA SecurID Authentication in HP Network Automation

Follow the steps below to configure HP Network to use RSA SecurID two-factor authentication:

1. [Enable SecurID as the External Authentication Method](#)
2. [Add Users](#)

### Enable SecurID as the External Authentication Method

1. In HP NA go to **Admin->Administrative Settings->External Authentication** and choose the **SecurID** radio button. This will enable RSA SecurID authentication for all locally configured users. See the [Add Users](#) section for more information.

The screenshot shows the HP Network Automation web interface. The main content area is titled "Administrative Settings - User Authentication". A yellow note at the top states: "Leaving this page or clicking any hyperlinks without clicking the Save button will result in the loss of any unsaved changes to the admin settings." Below the note are tabs for "Configuration Mgmt", "Device Access", "Server", "Workflow", "User Interface", "Telnet/SSH", "Reporting", "User Authentication", "Server Monitoring", and "3rd Party Integrations". The "User Authentication" tab is active. The "User Password Security" section includes: "Minimum User Password Length" set to 1; "User Password Must Contain Upper and Lower Case" with an unchecked checkbox; "Additional User Password Restriction" with "No additional restrictions" selected; and "Maximum Consecutive Login Failures" set to 0. The "External Authentication Type" section has "SecurID" selected among other options like "None (Local Auth)", "HP Server Automation Software", "HP Server Automation Software & TACACS+", "TACACS+", "RADIUS", and "LDAP". A note at the bottom right of this section says: "Choose the type of external authentication you would like to use. If you choose TACACS+, RADIUS or HP Server Automation Software, it can be configured in the section below. SecurID has no additional external authentication options." A "Save" button is located above the "External Authentication Type" section.


2. Copy the sdconf.rec file from the RSA Authentication Manager Server and install it in the appropriate directory for the OS running HP NA. For Windows, this directory would be %root%system32.

## Add Users

Each RSA SecurID token user must have an HP Network Automation username that matches his/her RSA Authentication Manager username. The screenshot below shows the HP Network Automation **New User** screen.

The screenshot shows the 'New User' form in the HP Network Automation interface. The form is titled 'New User' and includes a 'Save' button. The form fields are as follows:

Field	Value
User Name	securiduser
Password	*****
Confirm Password	*****
First Name	SecurID
Last Name	User
Email Address	securid@hp.com
User belongs to selected groups	Limited Access User, Full Access User, Power User, Administrator
Status	Enabled
External Auth Failover	<input checked="" type="checkbox"/> If external authentication fails for this user, should authentication failover to local authentication?
Comments	(Maximum 255 Chars)

 **Note** there is a failover capability to local authentication in specific cases if needed. See the HP NA documentation for more information. See the HP NA documentation for detailed information about adding users.



## Login Screens



The screenshot shows the standard login interface for HP Network Automation. At the top left is the HP logo followed by the text "HP Network Automation". At the top right is a "Help" link with a question mark icon. Below the header, there are two input fields: "User Name :" and "Password :". To the right of the password field is a "Login" button. At the bottom of the screen, it says "This product is licensed to : QA Internal Use".

*Standard HP Network Automation Login Screen*

The screenshot shows the RSA SecurID New PIN screen. At the top left is the HP logo followed by the text "HP Network Automation". At the top right is a "Help" link with a question mark icon. Below the header, there is a red instruction: "Enter new pin, between 4 and 8 numeric characters." Below this instruction are two input fields: "Enter new PIN:" and "Enter new PIN again:". To the right of the second input field is a "Login" button. At the bottom of the screen, it says "This product is licensed to : QA Internal Use".

*RSA SecurID New PIN Screen*



 **HP Network Automation** Help 

---

**PIN does not meet PIN requirements, reauthenticate and try again.**



User Name :

Password :

**Login**

This product is licensed to : QA Internal Use

*RSA SecurID PIN Rejected Screen*

 **HP Network Automation** Help 

---

**New PIN accepted, wait for next tokencode and login again.**

User Name :



Password :

**Login**

This product is licensed to : QA Internal Use

*RSA SecurID PIN Accepted Screen*



 **HP Network Automation** Help 

---

**Enter next tokencode**

Next tokencode:

**Login**

This product is licensed to : QA Internal Use

*RSA SecurID Next Tokencode Screen*



# Certification Checklist For RSA Authentication Manager v6.1

Date Tested: November 12, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1	Windows Server 2003
RSA Authentication Agent	5.3	Windows Server 2003
RSA Software Token	4.1	Windows Server 2003
HP Network Automation	7.6	Windows Server 2003

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
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
<b>Passcode</b>			
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
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>Load Balancing / Reliability Testing</b>			
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"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input type="checkbox"/> N/A
Additional Functionality			
<b>RSA Software Token Automation</b>			
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
<b>RSA SecurID 800 Token Automation</b>			
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
<b>Credential Functionality</b>			
Determine Cached Credential State	<input type="checkbox"/> N/A	Determine Cached Credential State	<input type="checkbox"/>
Set Credential	<input type="checkbox"/> N/A	Set Credential	<input type="checkbox"/>
Retrieve Credential	<input type="checkbox"/> N/A	Retrieve Credential	<input type="checkbox"/>

JGS / PAR

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



# Certification Checklist For RSA Authentication Manager 7.1

Date Tested: November 12, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows Server 2003
RSA Authentication Agent	5.3	Windows Server 2003
RSA Software Token	4.1	Windows Server 2003
HP Network Automation	7.6	Windows Server 2003

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
<b>New PIN Mode</b>			
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
<b>Passcode</b>			
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
<b>Next Tokencode Mode</b>			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
<b>Load Balancing / Reliability Testing</b>			
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
<b>Additional Functionality</b>			
<b>RSA Software Token Automation</b>			
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
<b>RSA SecurID 800 Token Automation</b>			
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

---

**sdconf.rec** - should be installed in **C:\WINDOWS\SYSTEM32\** for Windows and **/var/ace** for UNIX.

**sdstatus.12** - should be installed in **C:\WINDOWS\SYSTEM32\** for Windows and **/var/ace** for UNIX.

**Node Secret** - should be installed in **C:\WINDOWS\SYSTEM32\** for Windows and **/var/ace** for UNIX.