Hewlett-Packard
HP Network Automation

RSA SecurID Ready Implementation Guide

Last Modified: December 28, 2009

Partner Information

Product Information	
Partner Name	Hewlett-Packard
Web Site	www.hp.com
Product Name	HP Network Automation
Version & Platform	7.6
Product Description	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. 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.
Product Category	Networks and Communication, Web Applications & ERP

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.

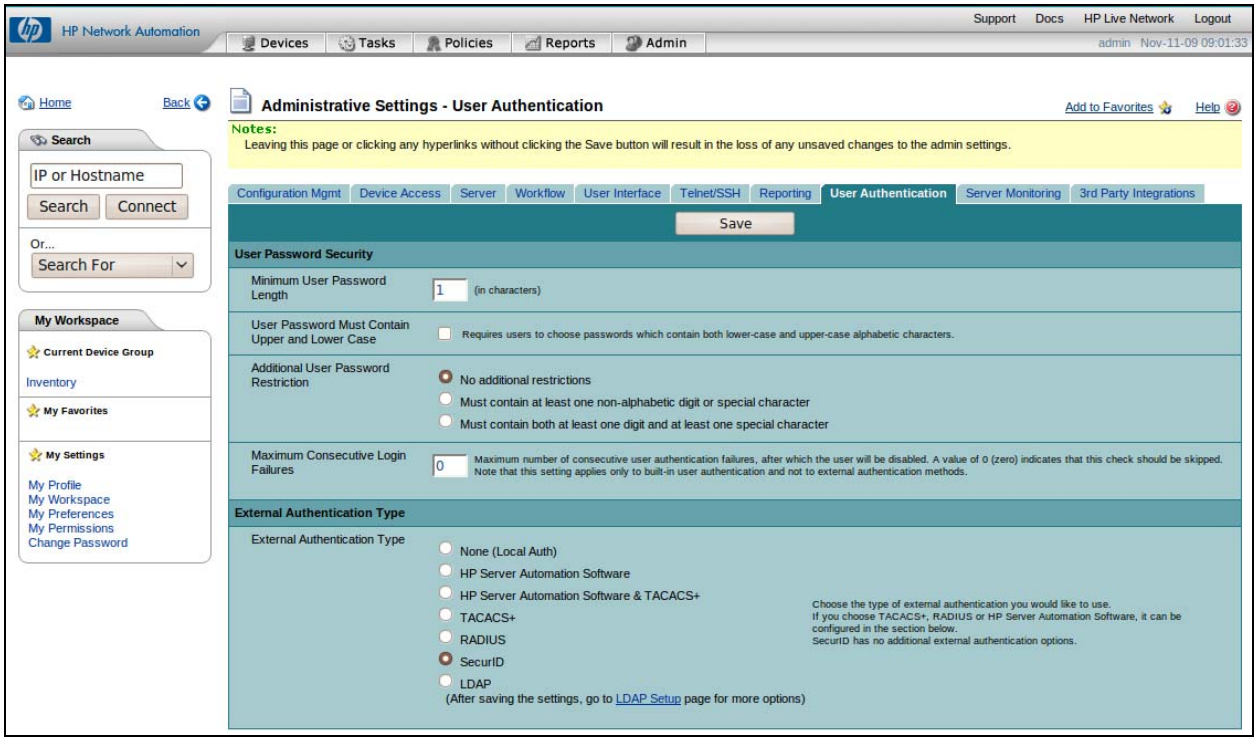
Configuring RSA SecurID Authentication in HP Network Automation

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

1. **Enable SecurID as the Eternal Authentication Method**
2. **Add Users**

Enable SecurID as the External Authentication Method

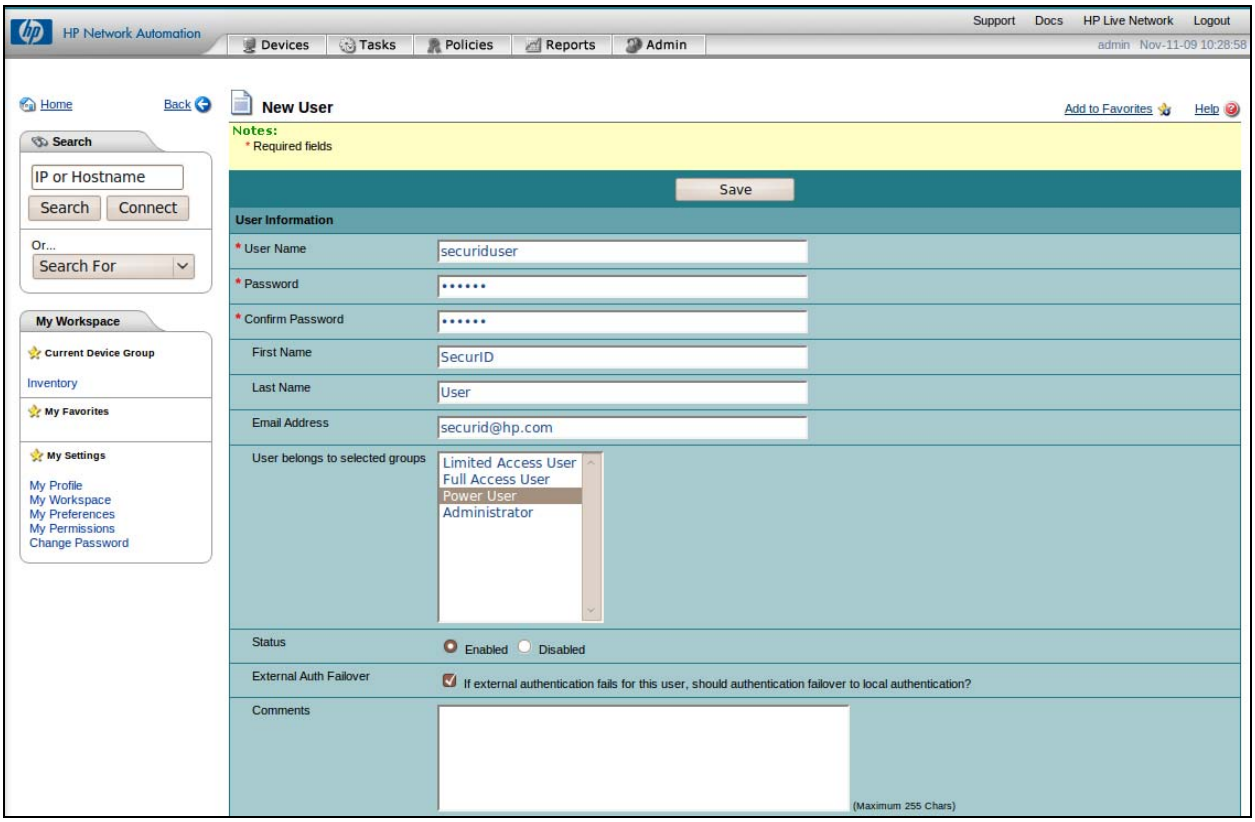
1. In HP NA go to ***Admin->Administrative Settings->External Authentication*** and choose the ***SecurID*** radio button. This will enable RSA SecurID authentication for all locally configured users. See the **Add Users** section for more information.



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.

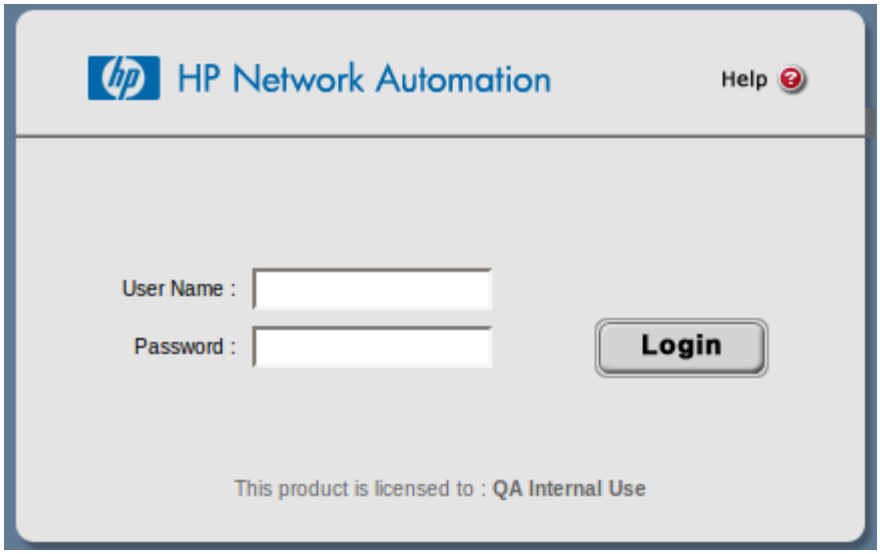
Add Users

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.

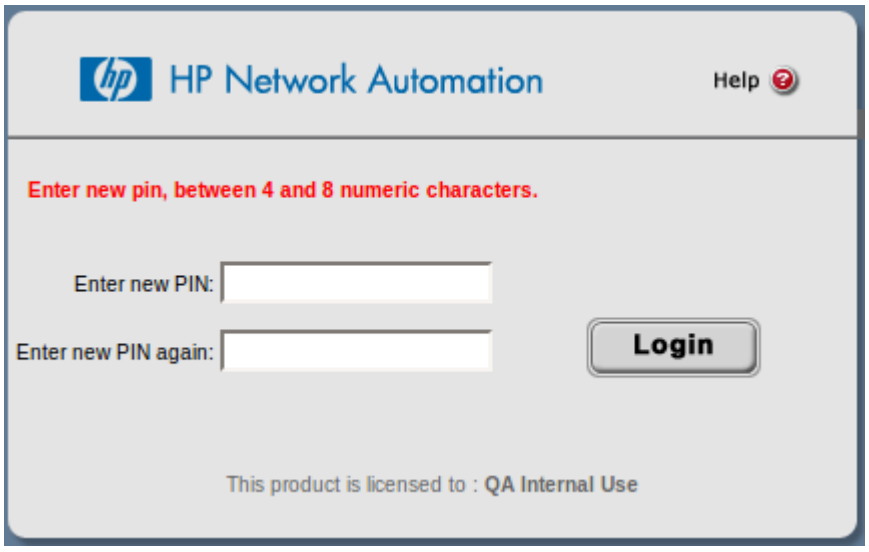


Note there is a failover capability to local authentication in specific cases if needed. See the HP NA documentation for more information. See the HP NA documentation for detailed information about adding users.

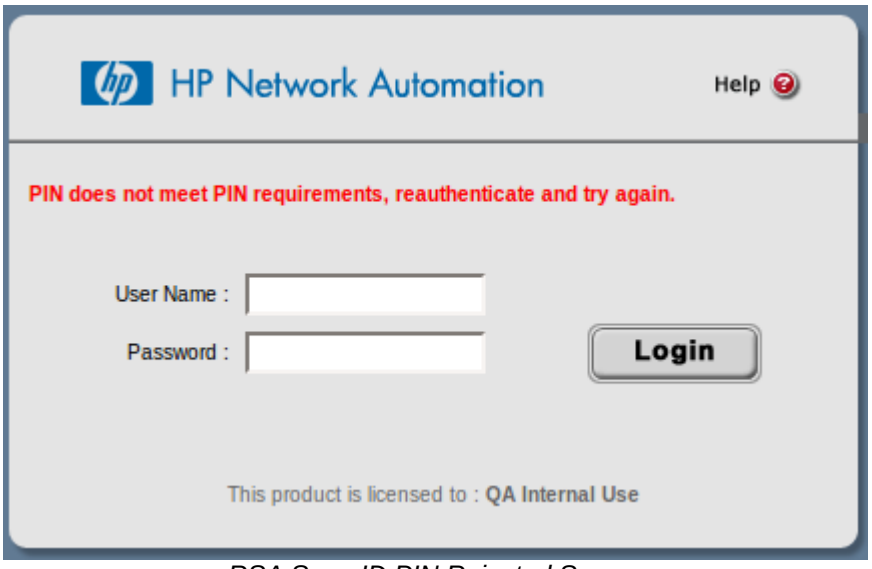
Login Screens



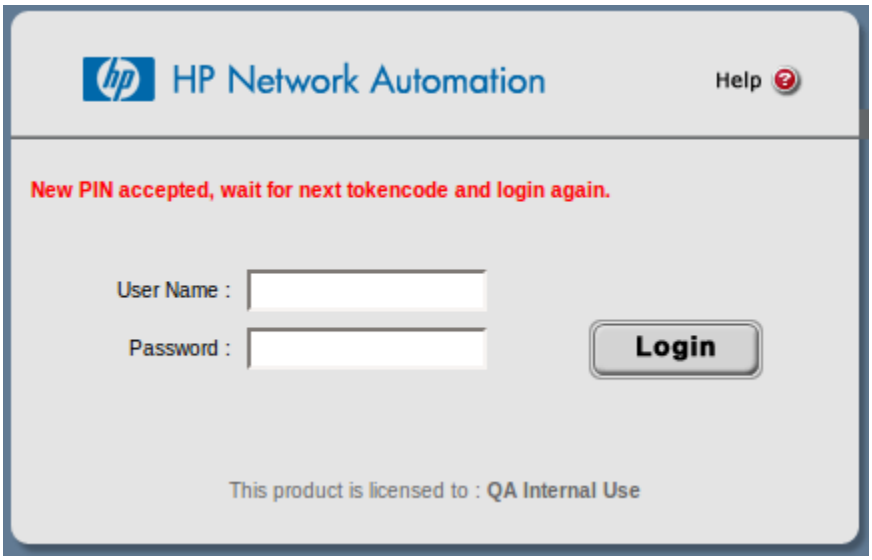
Standard HP Network Automation Login Screen



RSA SecurID New PIN Screen



RSA SecurID PIN Rejected Screen



RSA SecurID PIN Accepted Screen

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

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**	
New PIN Mode			
Force Authentication After New PIN	✓	Force Authentication After New PIN	N/A
System Generated PIN	✓	System Generated PIN	N/A
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	N/A
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Deny Numeric PIN	✓	Deny Numeric PIN	N/A
PIN Reuse	✓	PIN Reuse	N/A
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	N/A
4 Digit Fixed Passcode	✓	4 Digit Fixed Passcode	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
No RSA Authentication Manager	✓	No RSA Authentication Manager	N/A
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
RSA SecurID 800 Token Automation			
System Generated PIN	N/A	System Generated PIN	N/A
User Defined (8 Digit Numeric)	N/A	User Defined (8 Digit Numeric)	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	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.