



RSA SecurID Ready Implementation Guide

Last Modified: May 22, 2013

Partner Information

Product Information	
Partner Name	VMware
Web Site	www.vmware.com
Product Name	Horizon Connector
Version & Platform	1.5.1
Product Description	The Horizon Connector provides Federated Security on the client premise to VMware cloud hosted applications.

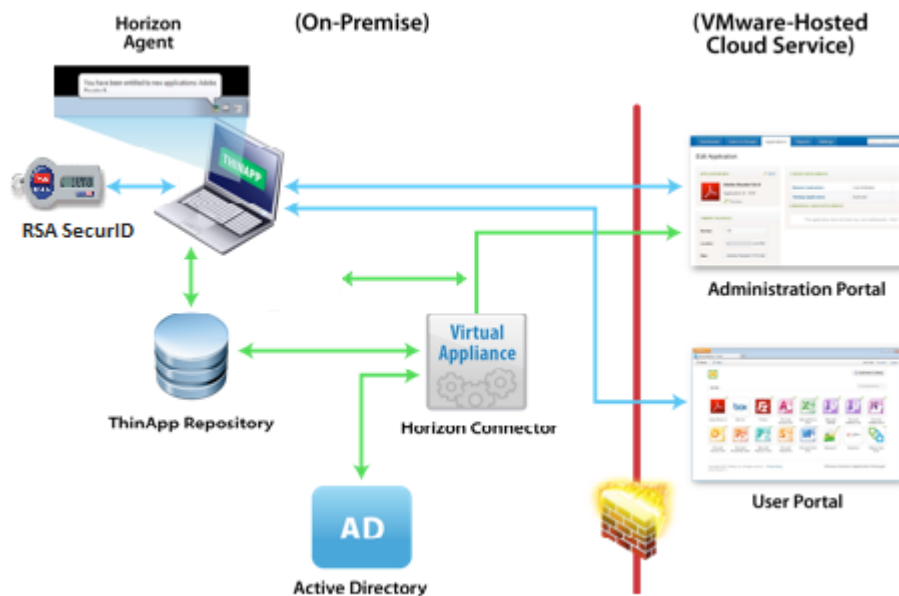


Solution Summary

VMware Horizon Connector uses RSA SecurID for two factor authentication into Horizon cloud based hosted applications.

The Horizon Connector logon page can optionally be customized to take advantage of RSA Risk-Based Authentication (RBA). RBA allows administrators to strengthen authentication attempts with step-authentication comprised of security questions or out-of-band tokencode delivery to an email address or SMS address. RSA Authentication Manager will challenge users when its adaptive risk engine determines the user is attempting a high-risk logon attempt.

RSA Authentication Manager supported features VMware Horizon Connector 1.5.1	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	No
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	Yes
Risk-Based Authentication with Single Sign-On	Yes
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces


Set the Agent Type to “Standard Agent” when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with VMware Horizon Connector 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 documentation for additional information about creating, modifying and managing Authentication Agents.

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	/opt/vmware/c2
Node Secret	/opt/vmware/c2
sdstatus.12	/opt/vmware/c2
sdopts.rec	/opt/vmware/c2

 **Note: The appendix of this document contains more detailed information regarding these files.**

Risk-Based Authentication Integration Script

To protect a web-based application with Risk-Based Authentication (RBA), you must generate an integration script using the RSA Security Console, and deploy it to the application's default logon page. The script redirects the user from the web-based application's default logon page to a customized logon page that allows RSA Authentication Manager to authenticate the user with RBA.

The following steps should be taken prior to generating the integration script.

- Download the integration script template for VMware Horizon Connector from the following link:
<https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=903434085&arg12=downloaddirect&transaction=signon&quiet=true>
- Verify that the most recent RBA integration script template is installed on your Authentication Manager system by comparing the header of the installed integration script template to the header of the downloaded integration script template.
- Install the downloaded integration script template if it is newer than the installed script template, or if the script template for your agent is not installed.

Please refer to RSA documentation for more information on RBA integration scripts.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the VMware Horizon Connector 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 the product documentation for all products in order to install the required components.

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

Configuring SecurID for the Horizon Connector

1. Browse to <https://{HorizonConnectorIP}:8443> and login as the Horizon Connector Administrator and select **SecurID** from the toolbar.

The screenshot shows the VMware Horizon Connector administration console. On the left is a sidebar menu with options: About, Configuration, Directory, User Attributes, Join Domain, Windows Auth, SecurID (highlighted), Internal Access, External Access, Directory Sync, Sync Safeguards, Windows Apps, and Change Password. The main content area is titled 'SecurID' and contains the text 'Enable SecurID' followed by an unchecked checkbox and a green 'Save' button. On the right is a 'Help' panel with the following text: 'You can configure RSA SecurID authentication for users. Provide the requested information to enable the Connector to access RSA Authentication Manager. If you clear or regenerate the node secret on the RSA SecurID server, you must update the new node secret value on the SecurID page.' At the bottom left, the footer reads 'Copyright © 2012 VMware, Inc. All rights reserved. Horizon Connector Build 1.5.1.800560'. At the bottom right, it reads 'VMware Horizon'.

2. Select the **Enable SecurID** checkbox and complete the remainder of the form by entering the **Connector Address**, **Agent IP Address** and the **Server Configuration** (sdconf.rec).


The screenshot shows the VMware Horizon Connector web interface for configuring SecurID. On the left is a navigation sidebar with options: About, Configuration, Directory, User Attributes, Join Domain, Windows Auth, **SecurID**, Internal Access, External Access, Directory Sync, Sync Safeguards, Windows Apps, and Change Password. The main content area is titled 'SecurID' and contains the following configuration fields:

- Enable SecurID:** A checked checkbox.
- Connector Address:** A text input field containing '192.168.232.128'. Below it is the text: 'Local hostname or IP address of this connector instance'.
- Agent IP Address:** A text input field containing '192.168.232.128'. Below it is the text: 'IP Address of this connector instance as specified in the SecurID server's agent configuration'.
- Server Configuration:** A 'Choose File' button next to the text 'sdconf.rec'. Below it is the text: 'Upload the server configuration file after you have downloaded the compressed configuration file from the RSA SecurID server and extracted the file, default name is sdconf.rec.'
- Node Secret:** A 'Choose File' button next to the text 'No file chosen'. Below it is the text: 'Clear won't take effect until you save.' and 'Uploading node secret is optional, but clearing should be coordinated with SecurID server'.

At the bottom of the form is a green 'Save' button. On the right side, there is a 'Help' box with the following text: 'You can configure RSA SecurID authentication for users. Provide the requested information to enable the Connector to access RSA Authentication Manager. If you clear or regenerate the node secret on the RSA SecurID server, you must update the new node secret value on the SecurID page.'

At the bottom of the page, the footer contains: 'Copyright © 2012 VMware, Inc. All rights reserved. Horizon Connector Build 1.5.1.800560' on the left and 'VMware Horizon' on the right.

Customizing Connector login page for Risk-Based Authentication

 **Note:** Horizon Connector must be configured for SecurID authentication in order to use RSA Risk-Based Authentication. Verify that this is true, and that SecurID Authentication works properly before continuing.

3. Download the RBA integration script for the Horizon Connector from the RSA Authentication Manager Security Console. Save this file as **am_integration.js**.
4. Enable SSH on the Horizon Connector if it is not already enabled.
5. Using an scp client, copy **am_integration.js** to **/opt/vmware/c2/c2instance/webapps/ROOT/static/js/**.
6. Using an scp client, copy **/opt/vmware/c2/c2instance/webapps/ROOT/WEB-INF/views/jspf/login_end.jspf** to your local workstation so you can edit it. Make a backup of the original file by copying the file with a new name, such as **login_end.jspf.orig**.
7. Add the following two lines of code to the bottom of **login_end.jspf**, right before the closing body and html tags.


```
<script type="text/javascript"
src="{contextPath}/static/js/am_integration.js"></script>
<script>window.onload=redirectToIDP(); </script>
</body>
</html>
```
8. Copy the modified **login_end.jspf** to **opt/vmware/c2/c2instance/webapps/ROOT/WEB-INF/views/jspf/**.
9. Restart the Horizon Connector appliance. Once the appliance restarts, users accessing the Horizon Connector login page will be redirected to the RSA Secure Logon Page, where they must successfully complete Risk-Based Authentication to be granted access.

RSA SecurID Login Screens

Login screen:

Login

Enter your username and your passcode (PIN followed by tokencode) for authentication. If you are using the token for the first time, follow the instructions provided with your token.

Username

Passcode

Copyright © 2012 VMware, Inc. All rights reserved.
Horizon Connector Build 1.5.1.800560

VMware Horizon

User-defined New PIN:

Login

Choose a PIN for your token. The PIN will be used to identify you with your token.

Username

PIN

PIN Criteria:
Must be 4-8 characters in length.
May contain letters and numbers

Copyright © 2012 VMware, Inc. All rights reserved.
Horizon Connector Build 1.5.1.800560

VMware Horizon

System-generated New PIN:

Login

Memorize your new PIN: wNpLO. You must provide this PIN every time you log in. In the passcode field, enter your PIN followed by your tokencode.

Username

Passcode

Login

Copyright © 2012 VMware, Inc. All rights reserved.
Horizon Connector Build 1.5.1.800560

VMware Horizon

Next Tokencode:

Login

Wait for your next tokencode, then enter it below (do not include PIN code).

Username

Next Token

Login

Copyright © 2012 VMware, Inc. All rights reserved.
Horizon Connector Build 1.5.1.800560

VMware Horizon

Certification Checklist for RSA Authentication Manager

Date Tested: May 22, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.0	Virtual Appliance
VMware Horizon Connector	1.5.1	Suse Enterprise Linux 11

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 PIN Reuse	<input checked="" type="checkbox"/>	Deny 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
On-Demand Authentication			
On-Demand Authentication	<input checked="" type="checkbox"/>	On-Demand Authentication	<input type="checkbox"/> N/A
On-Demand New PIN	<input checked="" type="checkbox"/>	On-Demand New PIN	<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

DRP ✔ = Pass ✘ = Fail N/A = Not Applicable to Integration

RSA Risk-Based Authentication Functionality			
RSA Native Protocol		RADIUS Protocol	
Risk-Based Authentication			
Risk-Based Authentication	<input checked="" type="checkbox"/>	Risk-Based Authentication	<input type="checkbox"/> N/A
Risk-Based Authentication with SSO	<input checked="" type="checkbox"/>	Risk-Based Authentication with SSO	<input type="checkbox"/> N/A

MRQ ✔ = Pass ✘ = Fail N/A = Not Applicable to Integration

Appendix

Partner Integration Details	
RSA SecurID API	Java API v8.1.1
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes

API Details:

Node Secret:

It is recommended to clear the node secret through the Horizon Connector Administrator login page but can be deleted through the root login at the command line.

sdconf.rec:

Managed through the Horizon Connector administrative interface but can be deleted through the root login at the command line.

sdopts.rec:

Not accessible through the Horizon Connector administrative interface but can be modified and deleted through the root login at the command line.

sdstatus.12:

Not accessible through the Horizon Connector administrative interface but can be deleted through the root login at the command line.

Agent Tracing:

Authentication Agent Event Logging is written to /opt/vmware/c2/. The file rsa_api.log is created and used for informational event logging. When debug logging is enabled a second file rsa_api_debug.log is created.

To set the level of tracing, modify:

```
/opt/vmware/c2/rsa_api.properties
# Enables debug tracing.
RSA_ENABLE_DEBUG=yes
# Sends tracing to a file.
RSA_DEBUG_TO_FILE=yes
```