



RSA SecurID Ready Implementation Guide

Last Modified: March 25, 2013

Partner Information

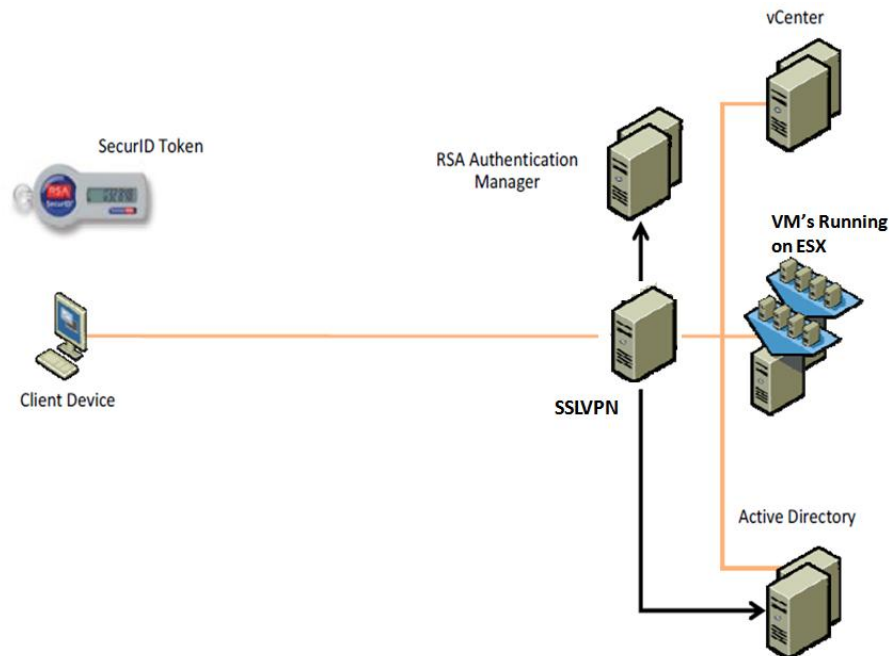
Product Information	
Partner Name	VMware Inc.
Web Site	www.vmware.com
Product Name	vCloud Networking and Security
Version & Platform	vShield Edge 5.1.2
Product Description	The Edge gateway component of VMware vCloud Networking and Security suite offers SSL VPN-Plus as a service. With SSL VPN-Plus, remote users can connect securely to private networks behind a vShield Edge gateway.



Solution Summary

VMware SSLVPN-Plus authenticate users using Microsoft Active Directory, LDAP and Local authentication. As an option, users can be authenticated using RSA SecurID. RSA SecurID authentication works in conjunction with RSA Authentication Manager. This optional two-factor authentication provides enhanced security for access to configured resources.

RSA Authentication Manager supported features vCloud Networking and Security 5.1.2	
RSA SecurID Authentication via Native RSA SecurID Protocol	Yes
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	Yes
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
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 vCloud Networking and Security will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for vCloud Networking and Security to communicate with RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:


- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

 **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 and RADIUS clients.

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	None stored
Node Secret	None stored
sdstatus.12	None stored
sdopts.rec	None stored

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

Partner Product Configuration

Before You Begin

This section provides instructions for configuring vCloud Networking and Security 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 vCloud Networking and Security components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Enable SecurID Authentication for SSLVPN

1. Login to VMware vShield Manager.



2. Select the **Network Virtualization** tab and click on the deployed Edge gateway.

Id	Name	Status	Tenant
edge-2	edge-10.112.243.32	Deployed	

- Select **VPN** and then click the **SSLVPN-Plus** link.

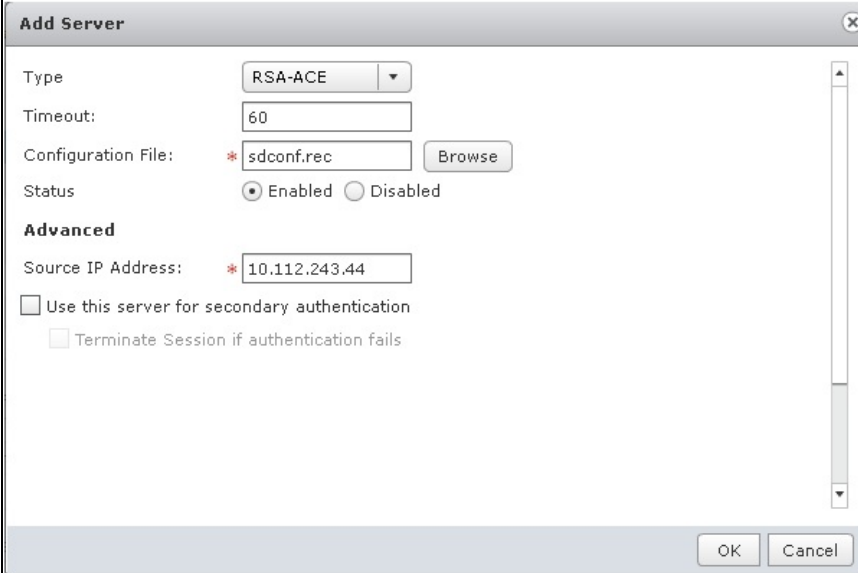
The screenshot shows the configuration page for a VPN endpoint named 'edge-10.112.243.32'. The 'VPN' tab is active, and the 'SSL VPN-Plus' link is highlighted. The interface includes a navigation menu at the top with tabs for General, App Firewall, Endpoint, SpoofGuard, and Network Virtualization. Below the navigation, there are sub-tabs for Preparation, Network Scopes, Networks, and Edges. The main content area shows the VPN configuration options, including a status toggle for 'IPSec VPN Service Status' (currently Disabled) and a 'Global configuration status' of 'Not Configured'. There is also a 'Logging Policy' section with an 'Enable logging' checkbox and a 'Log level' dropdown set to 'INFO'. At the bottom, there is a table with columns for Name, Local Endpoint, Local Subnets, Peer Endpoint, and Peer Subnets.

- Within the SSLVPN-Plus configuration, select the **Authentication** tab and click **Add**.

The screenshot shows the 'Authentication' configuration page for SSLVPN-Plus. The 'Add' button is highlighted in yellow. The interface includes a navigation menu on the left with options like Dashboard, Configure, Server Settings, IP Pool, Private Networks, Authentication (selected), Installation Package, Users, Web Resource, Client Configuration, Login/Logoff Scripts, General Settings, and Portal Customization. The main content area shows a table with columns for ID, Server Name, IP Address, Port, Type, and Status. The 'Add' button is highlighted in yellow. Below the table, there is a 'Certificate Authentication: Disabled' status with a 'Change' button. At the bottom, there is a table with columns for Common Name, Issued To, and Validity.

ID	Server Name	IP Address	Port	Type	Status
1	authserver-1	--	--	LOCAL	Enabled

5. If configuring the server for RADIUS authentication, skip to step 7.
6. Set the server Type to **RSA-ACE**, select **Browse** to locate the sdconf.rec file associated with your RSA Authentication Manager (AM). Set the Source IP address of the interface which will be used to communicate with the AM.

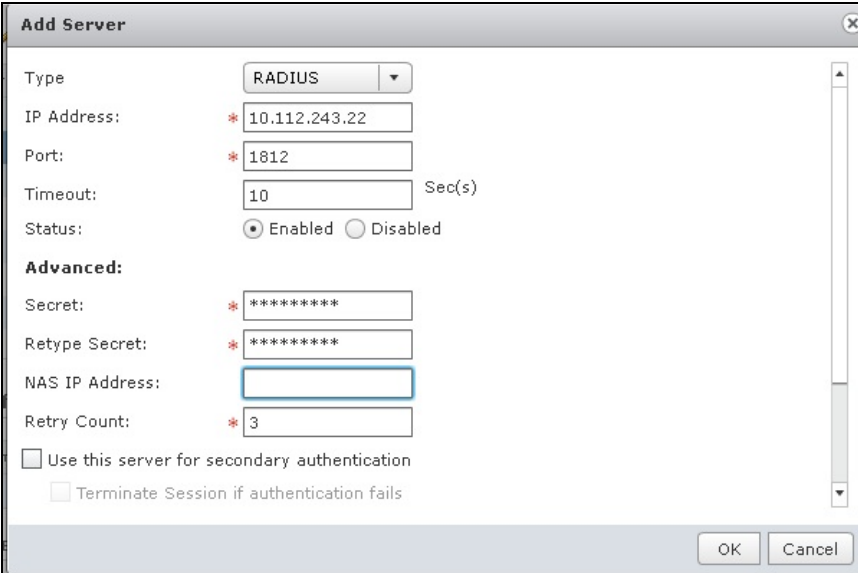


The screenshot shows the 'Add Server' dialog box with the following configuration:

- Type: RSA-ACE
- Timeout: 60
- Configuration File: sdconf.rec (with a 'Browse' button)
- Status: Enabled (radio button selected)
- Advanced:
 - Source IP Address: 10.112.243.44
 - Use this server for secondary authentication
 - Terminate Session if authentication fails

Buttons: OK, Cancel

7. Skip this step if you are using the AM's native protocol. Set the server Type to **RADIUS**, set the **IP Address** and the **Port** of the RADIUS server. Enter the Secret and retype to confirm. Enter the number of times to retry attempts before terminating the authentication.



The screenshot shows the 'Add Server' dialog box with the following configuration:

- Type: RADIUS
- IP Address: 10.112.243.22
- Port: 1812
- Timeout: 10 Sec(s)
- Status: Enabled (radio button selected)
- Advanced:
 - Secret: *****
 - Retype Secret: *****
 - NAS IP Address: (empty field)
 - Retry Count: 3
 - Use this server for secondary authentication
 - Terminate Session if authentication fails

Buttons: OK, Cancel

RSA SecurID Login Screens

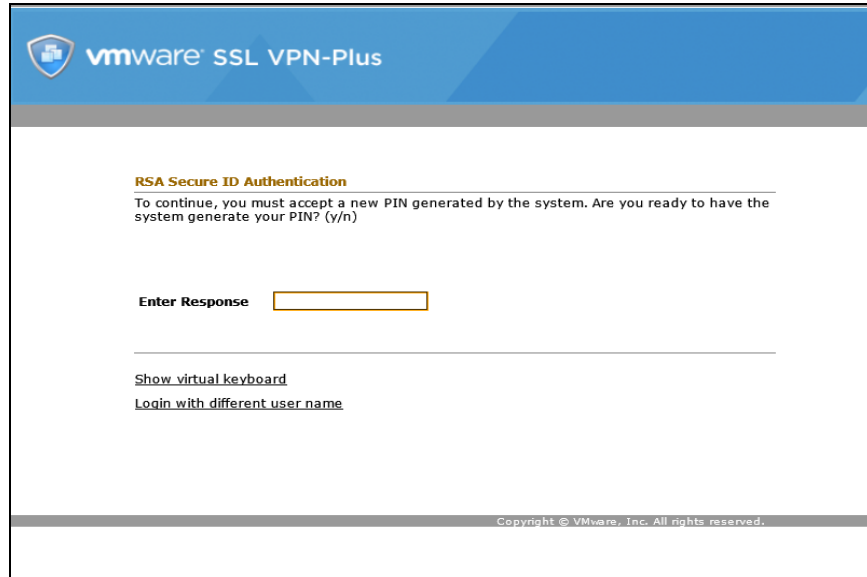
Login screen:

The screenshot shows the VMware SSL VPN-Plus Portal Login screen. At the top, there is a blue header with the VMware logo and the text "vmware SSL VPN-Plus" on the left, and "VMware" on the right. Below the header, the page is titled "Portal Login" and contains the instruction "Enter your login credentials here". There are two input fields: "User Name" and "Password". To the right of the "Password" field are two buttons: "Login" and "Show virtual keyboard". At the bottom of the page, there is a link: "Trouble signing in? click here to install Java" and a small copyright notice: "Copyright © VMware, Inc. All rights reserved."

User-defined New PIN:

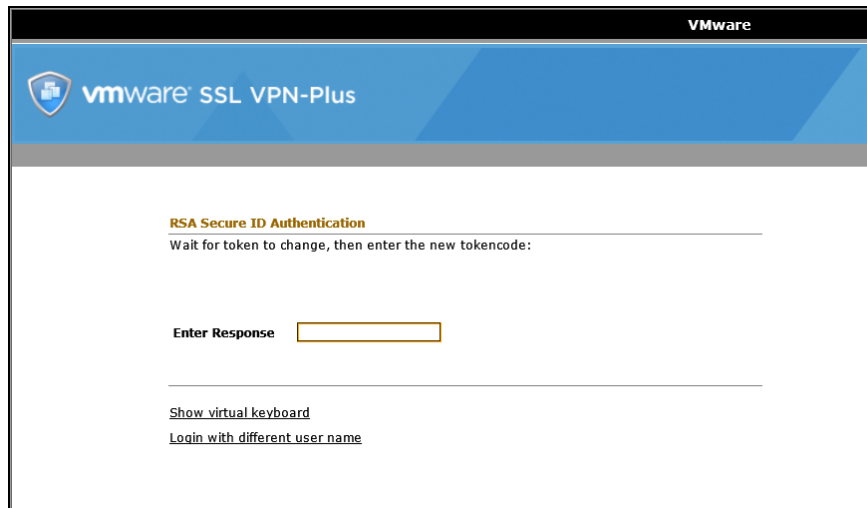
The screenshot shows the RSA Secure ID Authentication screen for defining a new PIN. At the top, there is a blue header with the RSA logo and the text "vmware SSL VPN-Plus" on the left, and "VMware" on the right. Below the header, the page is titled "RSA Secure ID Authentication" and contains the instruction "Enter a new PIN between 4 and 8 alphanumeric characters". There is one input field labeled "Enter Response". Below the input field are two links: "Show virtual keyboard" and "Login with different user name". At the bottom of the page, there is a small copyright notice: "Copyright © VMware, Inc. All rights reserved."

System-generated New PIN:



The screenshot shows the VMware SSL VPN-Plus interface. At the top, there is a blue header with the VMware logo and the text "vmware SSL VPN-Plus". Below the header, the text "RSA Secure ID Authentication" is displayed in bold. Underneath, a message reads: "To continue, you must accept a new PIN generated by the system. Are you ready to have the system generate your PIN? (y/n)". Below this message is a text input field with the label "Enter Response". Underneath the input field are two links: "Show virtual keyboard" and "Login with different user name". At the bottom of the page, there is a small copyright notice: "Copyright © VMware, Inc. All rights reserved."

Next Tokencode:



The screenshot shows the VMware SSL VPN-Plus interface. At the top, there is a black header with the VMware logo and the text "VMware". Below the header, there is a blue banner with the VMware logo and the text "vmware SSL VPN-Plus". Below the banner, the text "RSA Secure ID Authentication" is displayed in bold. Underneath, a message reads: "Wait for token to change, then enter the new tokencode:". Below this message is a text input field with the label "Enter Response". Underneath the input field are two links: "Show virtual keyboard" and "Login with different user name".

Certification Checklist for RSA Authentication Manager

Date Tested: March 25, 2013

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	8.0	Virtual Appliance
VMware vShield Edge	5.1	Linux 2.6.32.36

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 checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny PIN Reuse	<input checked="" type="checkbox"/>	Deny PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16-Digit Passcode	<input checked="" type="checkbox"/>	16-Digit Passcode	<input checked="" type="checkbox"/>
4-Digit Fixed Passcode	<input checked="" type="checkbox"/>	4-Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
On-Demand Authentication			
On-Demand Authentication	<input checked="" type="checkbox"/>	On-Demand Authentication	<input checked="" type="checkbox"/>
On-Demand New PIN	<input checked="" type="checkbox"/>	On-Demand New PIN	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>

DRP

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration

Appendix

Partner Integration Details	
RSA SecurID API	8.1.1
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

Node Secret:

To clear the node secret a new edge must be deployed.

sdconf.rec:

To clear the sdconf.rec a new edge must be deployed.

sdopts.rec:

Sdopts.rec is not supported.