VMware Inc.
vCloud Networking and Security

RSA SecurID Ready Implementation Guide

Last Modified: March 25, 2013

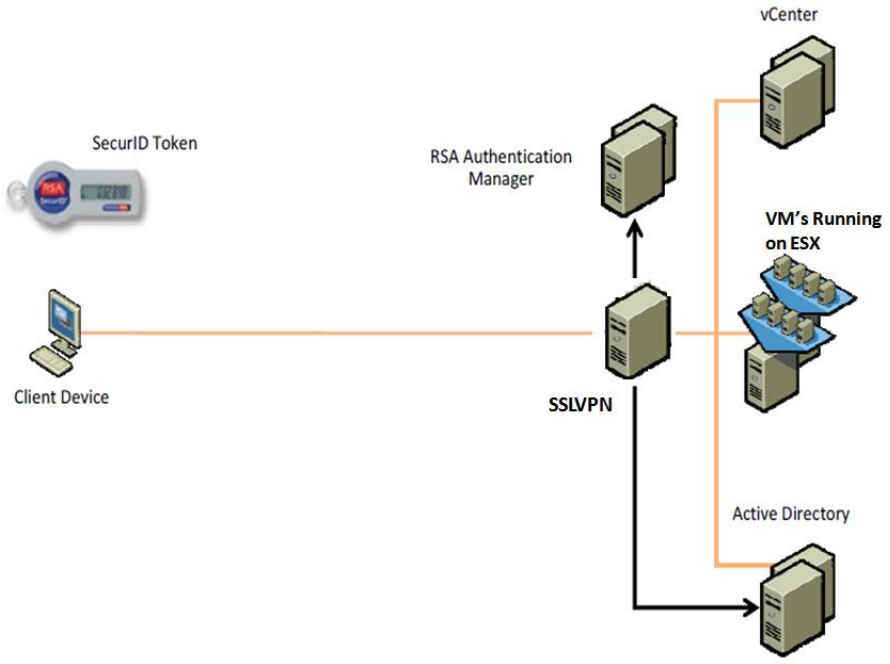
Partner Information

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.

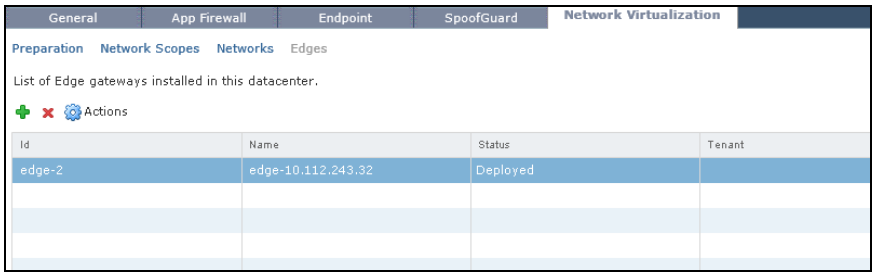
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.

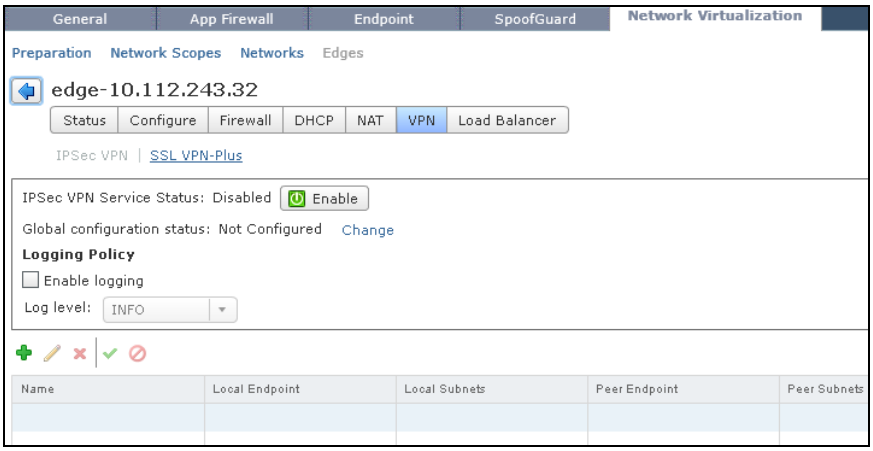
Enable SecurID Authentication for SSLVPN

1. Login to VMware vShield Manager.

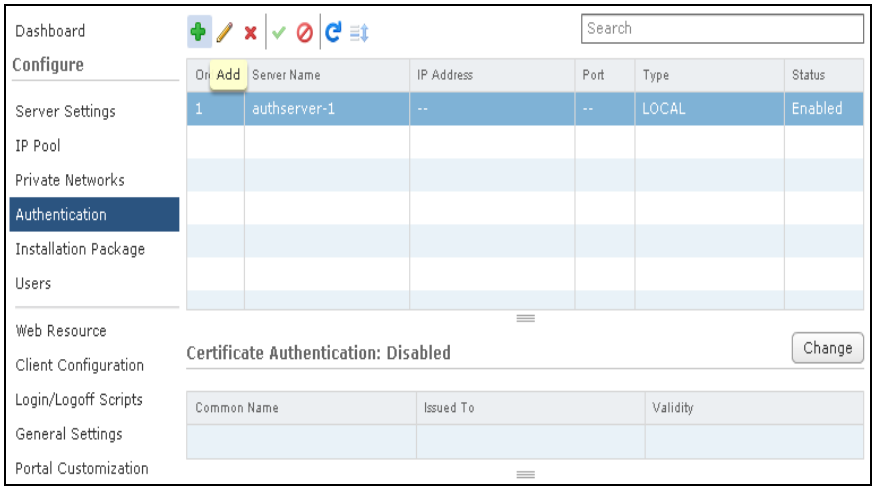
2. Select the **Network Virtualization** tab and click on the deployed Edge gateway.



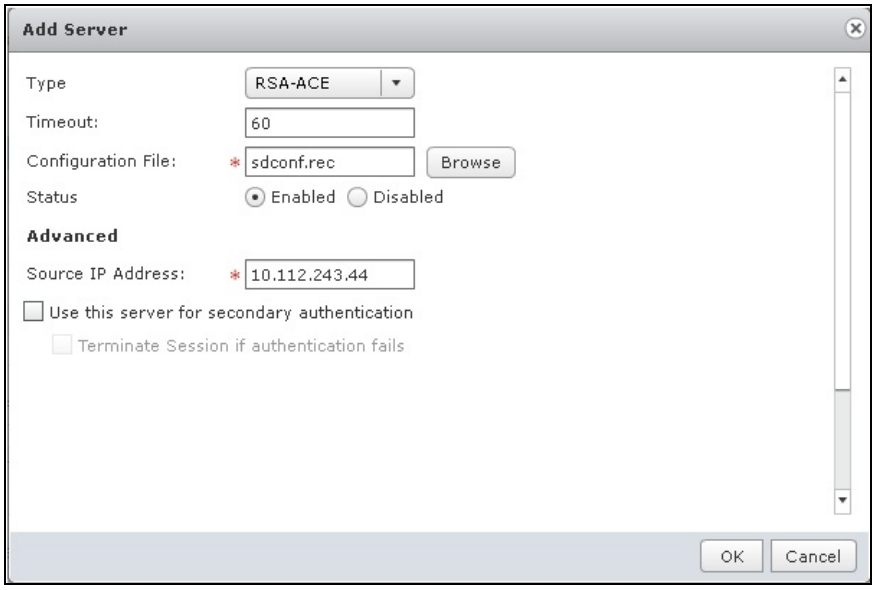
3. Select **VPN** and then click the **SSLVPN-Plus** link.



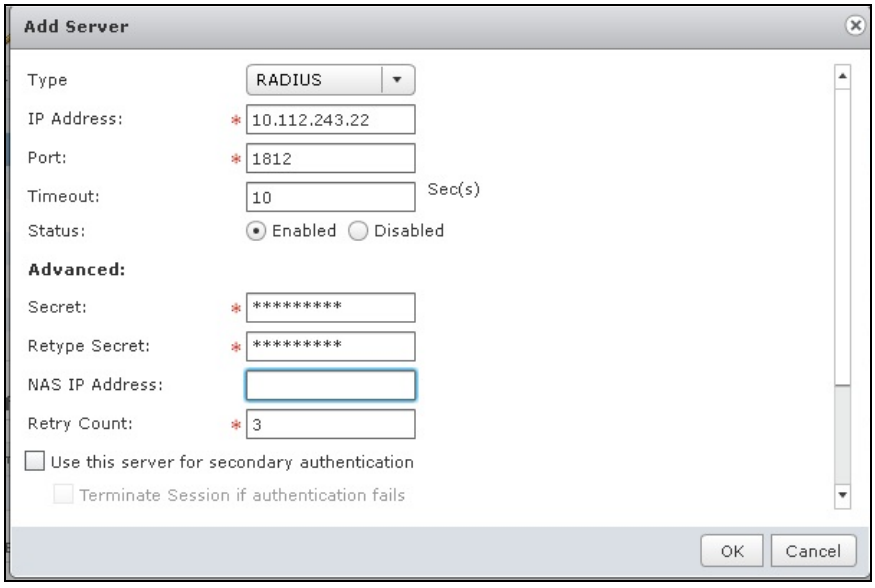
4. Within the SSLVPN-Plus configuration, select the **Authentication** tab and click **Add**.



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.

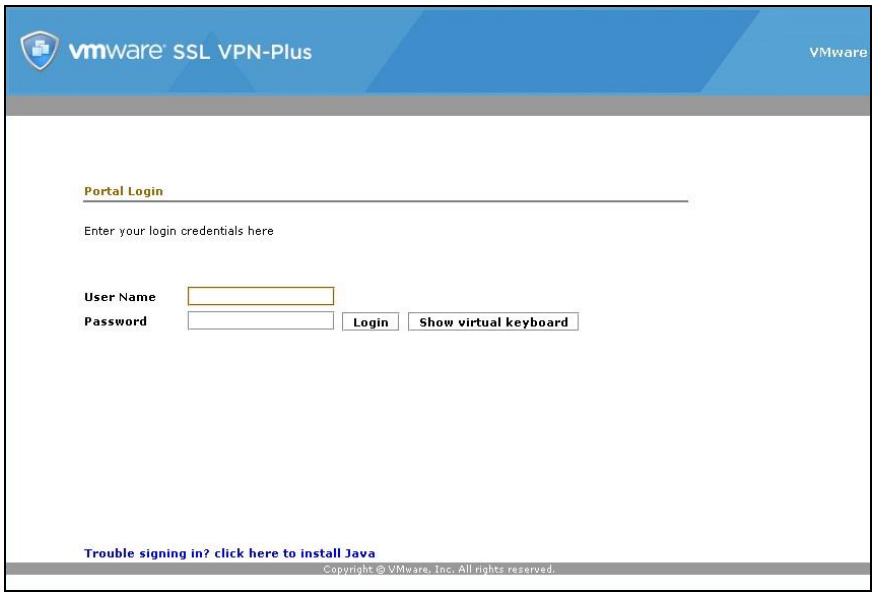


7. Skip this step if you are using the AM's native protocol. Set the server Type to **RADIUS,** set the **IP Address and** the **Port** of the RADIUS server. Enter the Secret and retype to confirm. Enter the number of times to retry attempts before terminating the authentication.

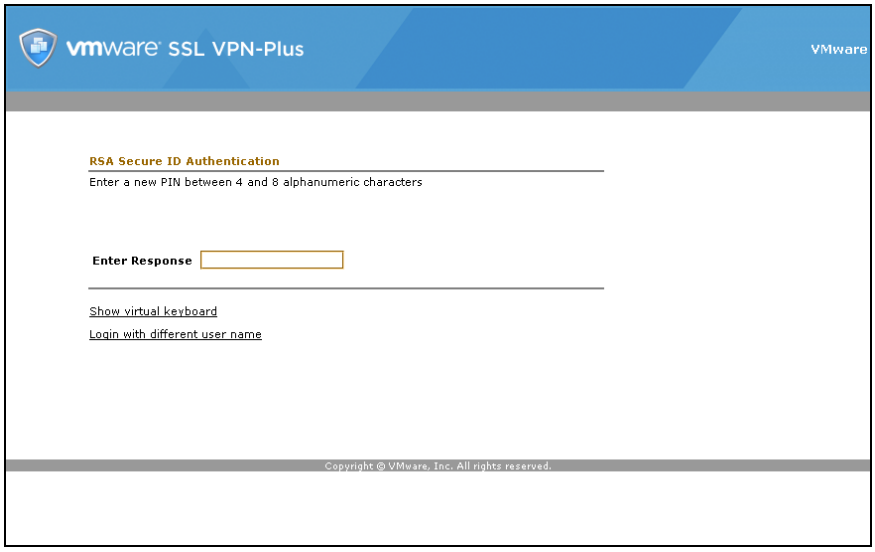


RSA SecurID Login Screens

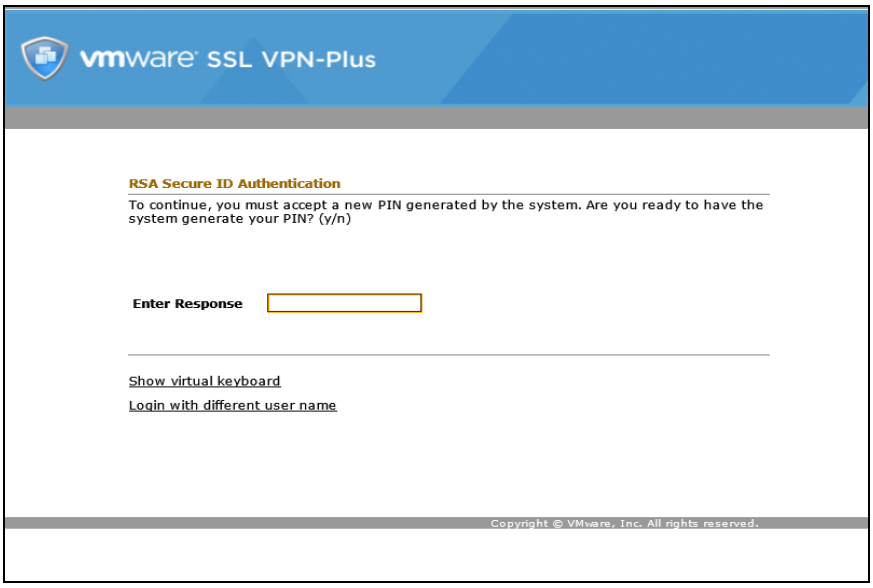
Login screen:



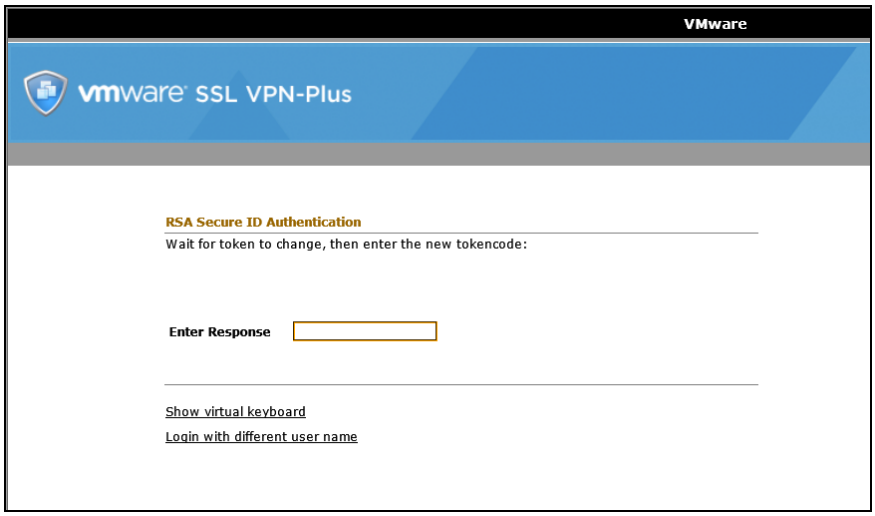
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



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	✓	Force Authentication After New PIN	✓
System Generated PIN	✓	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	✓	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	✓	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	✓
Deny PIN Reuse	✓	Deny PIN Reuse	✓
Passcode			
16-Digit Passcode	✓	16-Digit Passcode	✓
4-Digit Fixed Passcode	✓	4-Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	✓
On-Demand Authentication			
On-Demand Authentication	✓	On-Demand Authentication	✓
On-Demand New PIN	✓	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	✓
No RSA Authentication Manager	✓	No RSA Authentication Manager	✓

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.