RSA SECURID® ACCESS

Standard Agent Implementation Guide

VMware Inc., NSX Edge 6.2.1 SSL VPN-Plus

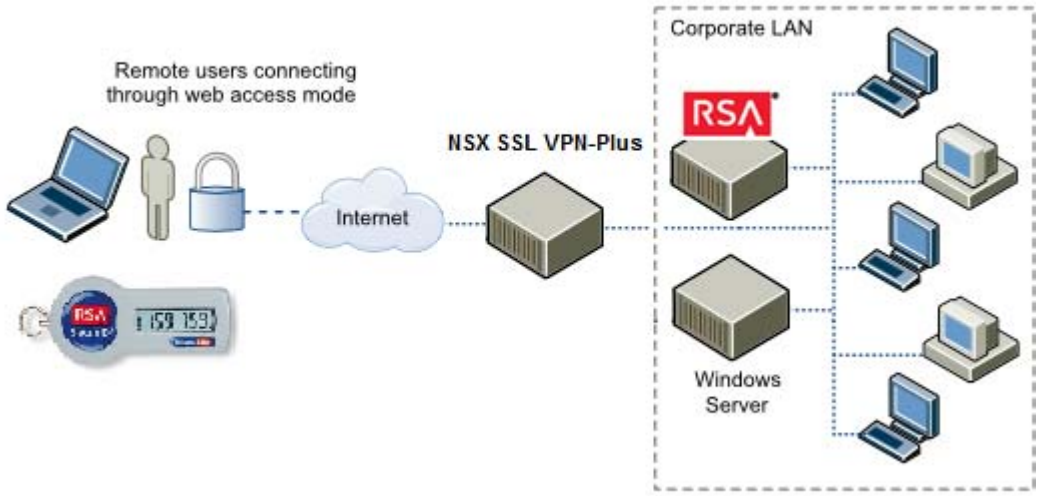
Daniel R. Pintal, RSA Partner Engineering
Last Modified: December 16, 2016

RSA READY

Solution Summary

VMware NSX Edge 6.2.1 SSL VPN-Plus users can authenticate 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 SecurID Access Supported Features	
VMware NSX Edge 6.2.1 SSL VPN-Plus	
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
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes



Partner Product Configuration

Before You Begin

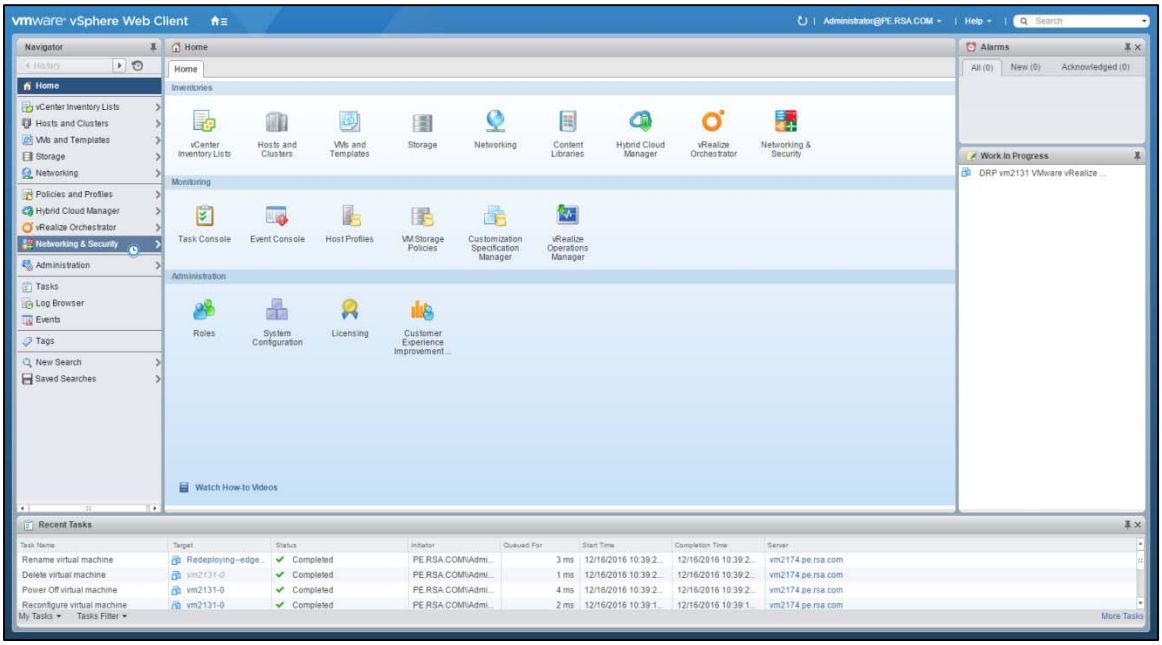
This section provides instructions for configuring the VMware NSX Edge 6.2.1 SSL VPN-Plus with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

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.

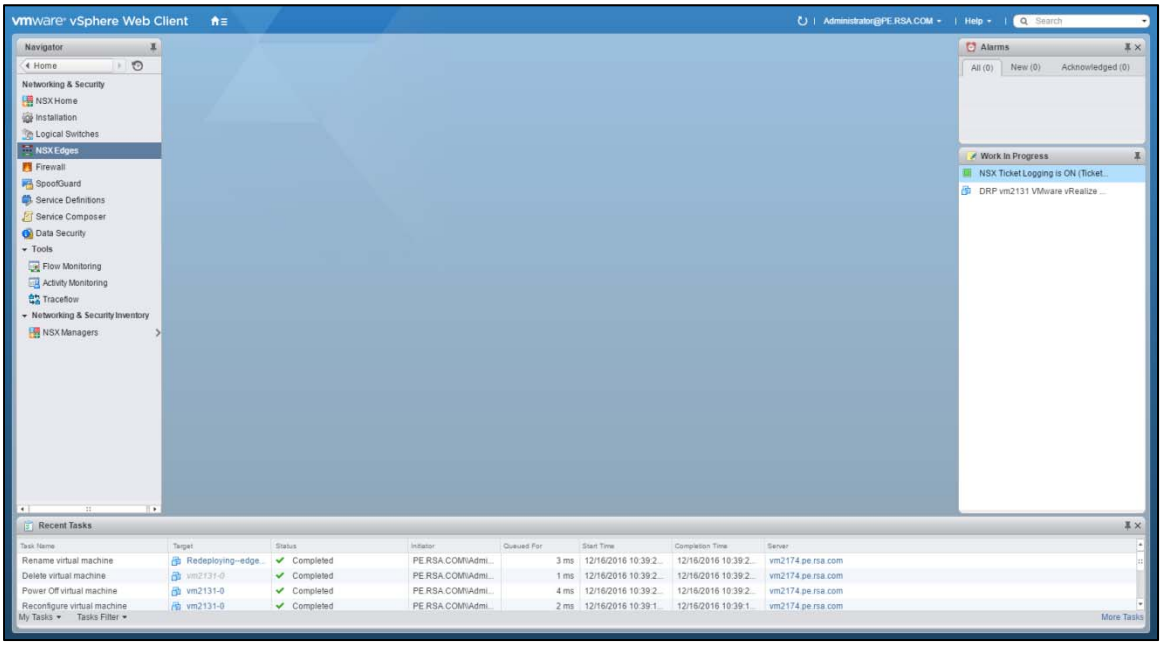
All VMware NSX components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

SSL VPN-Plus SecurID Authentication Requirements

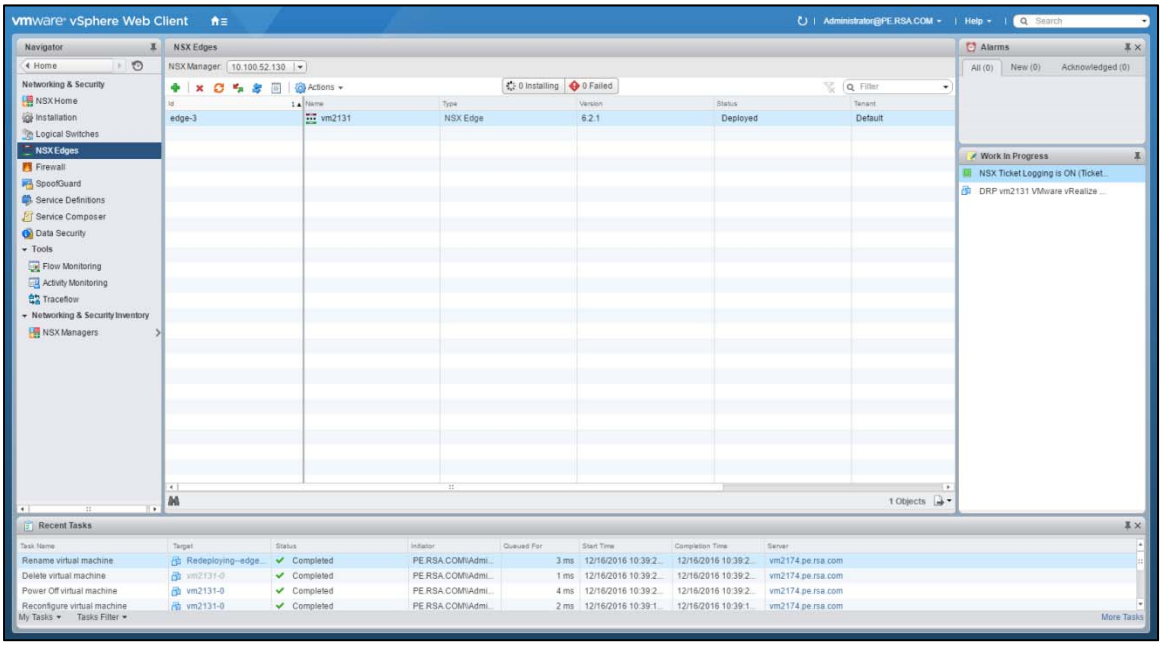
1. Login to the VMware vSphere Web Client.
2. Click on **Networking & Security.**



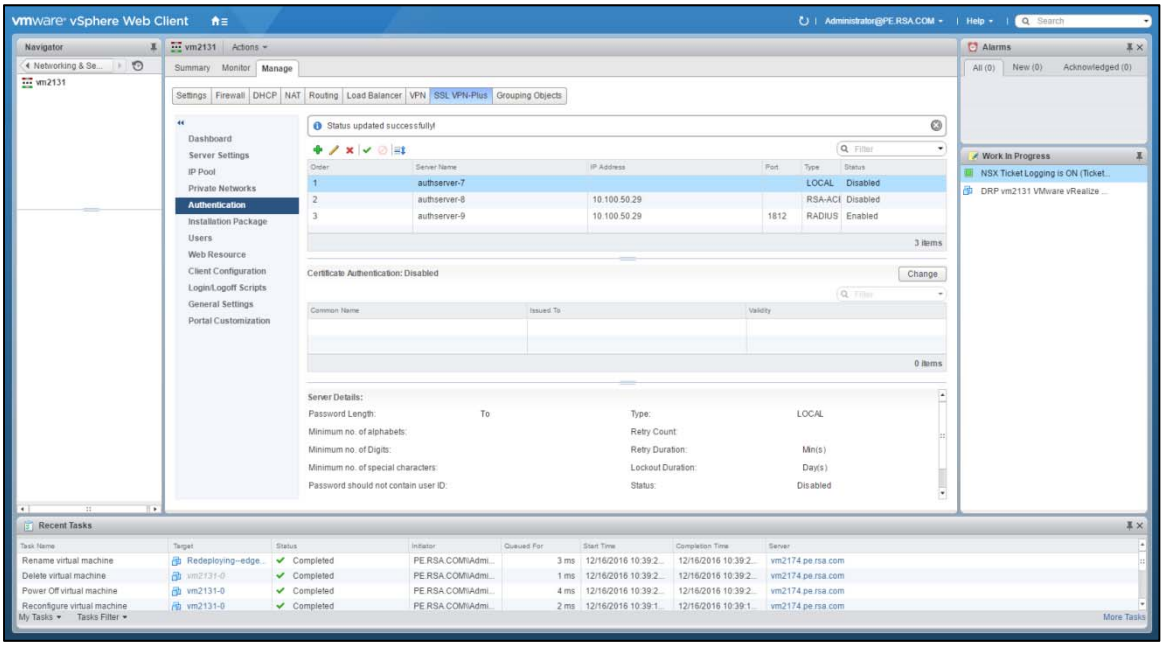
3. Click on **NSX Edges**.



4. Click on Edge Appliance.

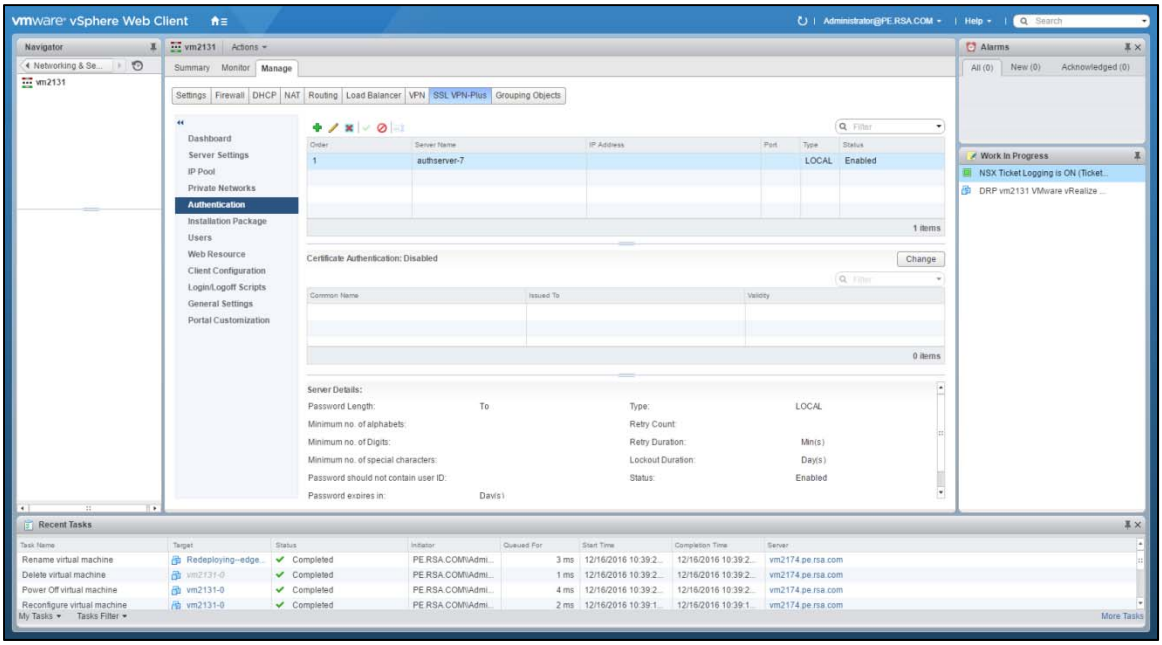


5. Click on **SSLVPN-Plus Tab**.



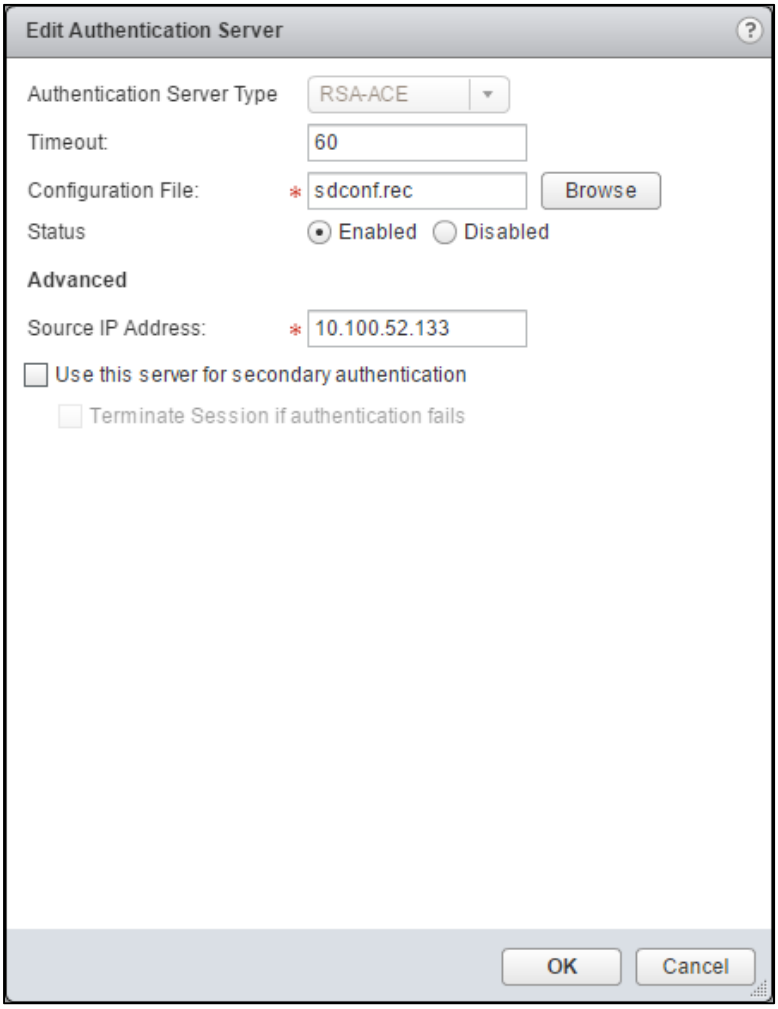
lowercase

6. In SSLVPN-Plus configuration, click on Authentication tab. Click on  to Add an Authentication Server.



RSA SecurID Native Protocol Configuration

1. Select the Authentication Server Type **RSA-ACE**, select **Browse** to import the **sdconf.rec** file and enter the **Source IP Address** to configured NSX for use with RSA Authentication Manager.



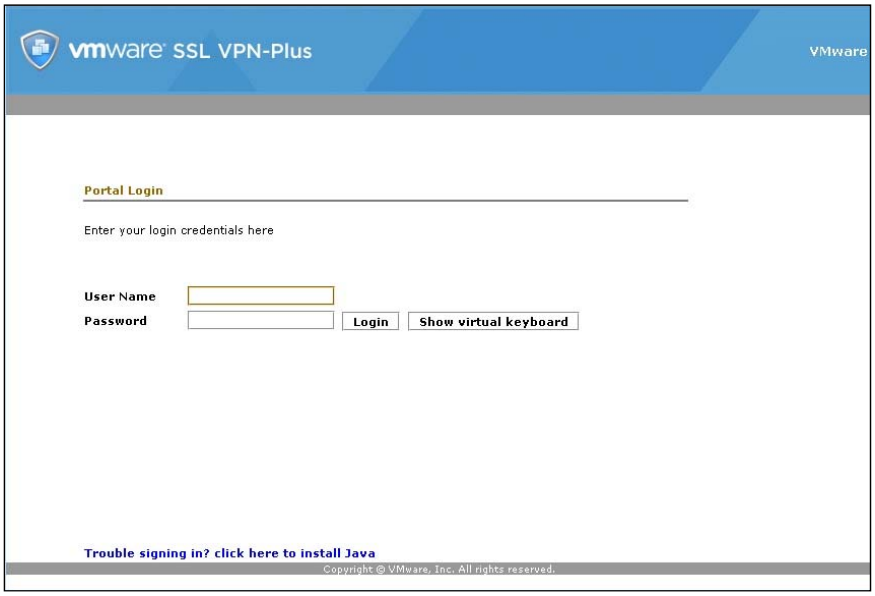
! An sdopts.rec file is created automatically using the NSX Edge's IP Address as the Source IP Address.

RSA SecurID RADIUS Protocol Configuration

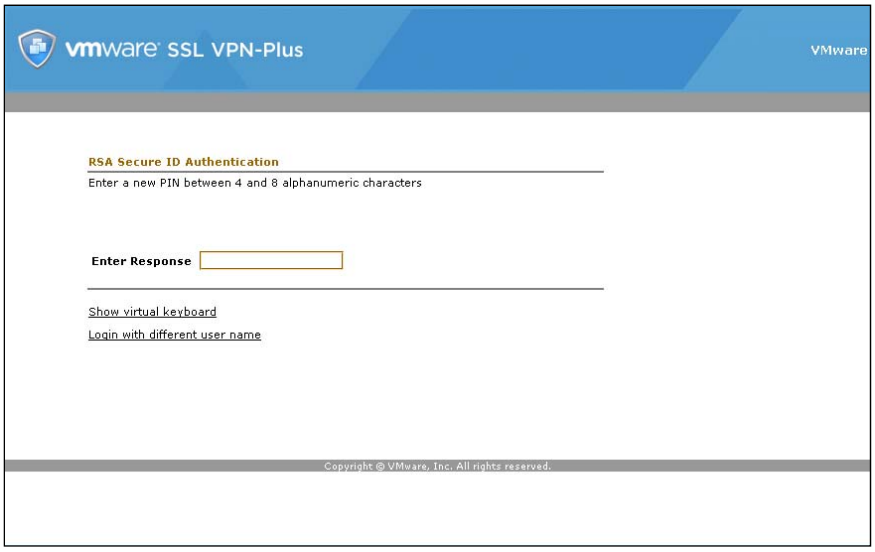
1. Select the Authentication Server Type **RADIUS**, enter the **IP Address, Port, Secret, Retype Secret** and **Retry Count** to configured NSX for use with a RADIUS server.

Screens

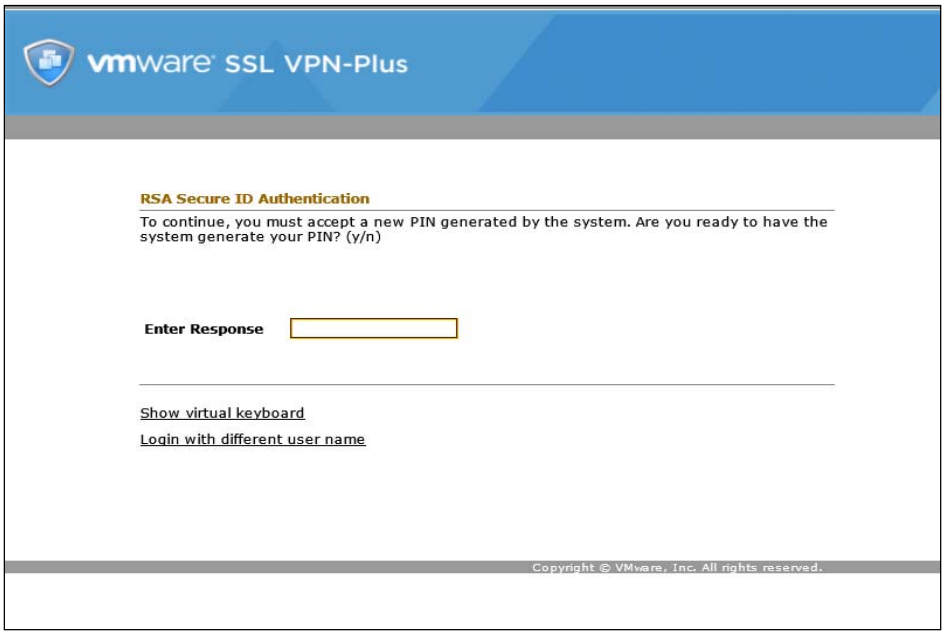
Login screen:



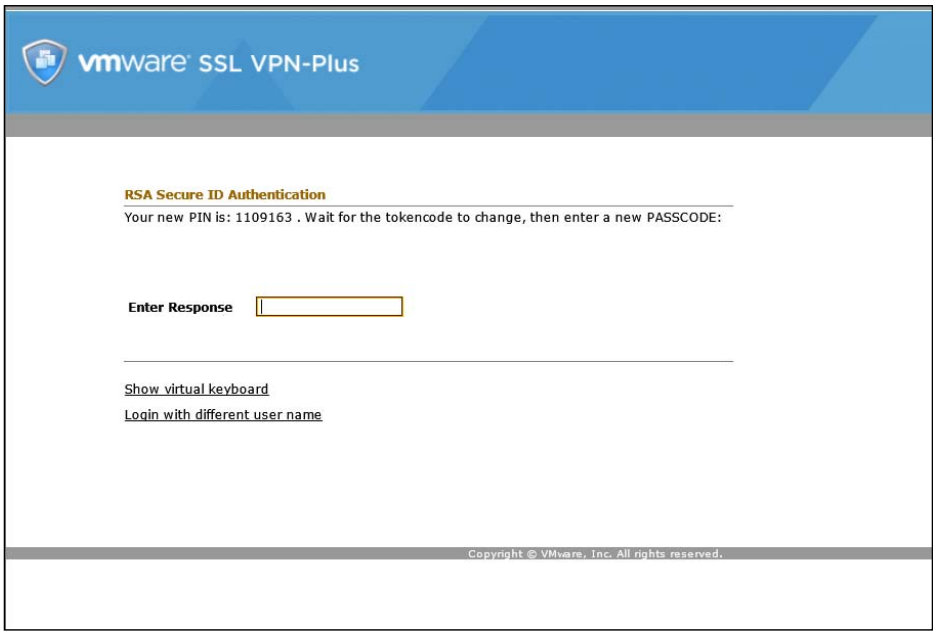
User-defined New PIN:



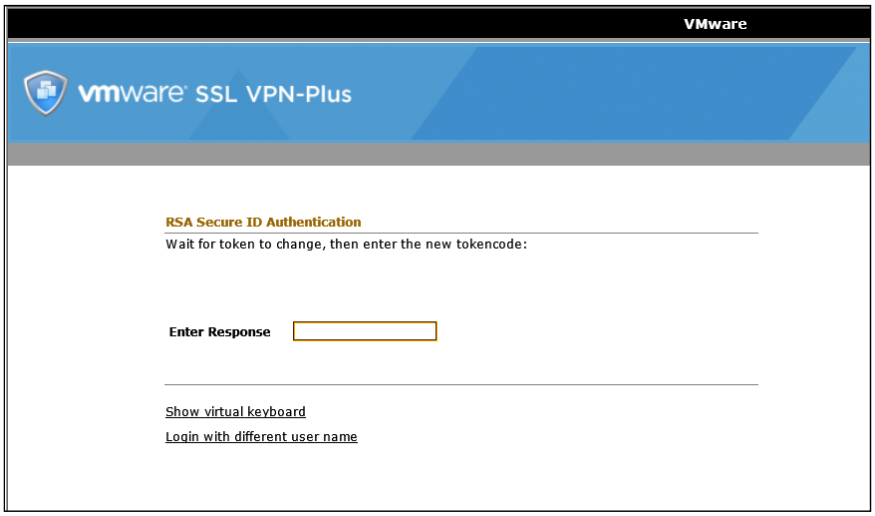
System-generated New PIN:



After entering the response you will see below screen with system generated pin.



Next Tokencode:



Certification Checklist for RSA SecurID Access

Date Tested: December 16, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
VMware NSX Edge SSL VPN-Plus	6.2.1	Virtual Appliance

RSA SecurID Authentication - Native

Date Tested: December 16, 2016

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

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

RSA SecurID Authentication - RADIUS

Date Tested: December 16, 2016

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

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

Appendix

Partner Integration Details	
RSA SecurID 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	No

The sdconf.rec configuration file is uploaded through the vSphere Web Client interface for the NSX Edge. During the RSA Authentication Server configuration an sdopts.rec file will be generated and configured with the NSX Edge Source IP provided during the NSX Edge installation/configuration. The sdconf.rec and sdopts.rec files are deleted when the RSA Authentication sever is deleted from within the vSphere Web Client interface for the NSX Edge.