RSA SECURID® ACCESS

Standard Agent Implementation Guide

VMware Horizon View Client 6.2

Daniel R. Pintal, RSA Partner Engineering
Last Modified: August 9th, 2016

RSA READY

Solution Summary

VMware Horizon View delivers end-to-end desktop control and manageability while providing a familiar user experience. VMware Horizon View is an enterprise-class connection broker that provides secure connectivity between remote clients and centralized virtual desktops.

Working in conjunction with VMware vCenter, VMware Horizon View provides optimized management and control of desktop operating systems running on VMware ESX.

By default, VMware Horizon View authenticates users using Microsoft Active Directory credentials (username, password, and domain name). As an option, VMware Horizon View can be configured so that users are first required to authenticate using RSA SecurID. VMware Horizon View authentication works in conjunction with RSA Authentication Manager. Two-factor authentication provides enhanced security for access to virtual desktops and is a standard feature of VMware Horizon View.

RSA SecurID Access Supported Features	
VMware Horizon View Client 6.2	
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
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No

RSA Software Token Supported Features	
Windows Automation	No
SID800 Automation	No
OS X Automation	No
iOS Automation	Yes
Android Automation	Yes
File-based Provisioning	Yes
CT-KIP Provisioning	Yes
CTF Provisioning	Yes

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the VMware Horizon View Client to provision RSA Authentication Manager resources. 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 View Client components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Provisioning

Windows

The VMware Horizon View Windows Desktop and Web client provides support for RSA SecurID authentication and requires the user to enter the RSA token code or passcode manually.

Mobile Clients

The VMware Horizon View Mobile client provides support for RSA SecurID authentication and either manually entering the RSA token or passcode or through token automation. Token automation requires the user or administrator to provision an RSA Software token from the RSA Authentication Manager by one of the three supported methods of provisioning; SDTID, CT-KIP or CTF.

Note: For more details related to provisioning and importing of RSA Software Tokens please reference the RSA Authentication Manager Administrators guide and the VMware Horizon View Client guides.

VMware Horizon View Configuration

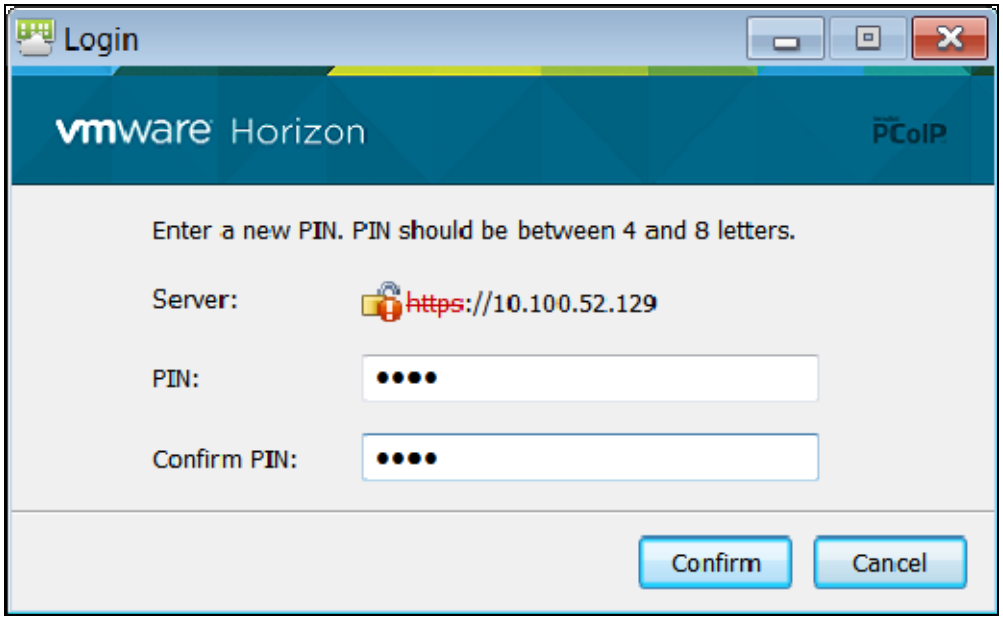
No modification to the client is required, RSA SecurID authentication is implemented using the process outlined within the **VMware_Horizon_View_6_2_RSA_SecurID_Access_8.2_Standard_Agent** implementation guide. VMware Horizon View Agents adhere to the authentication policy configured within the VMware Horizon View Connection server.

Screens

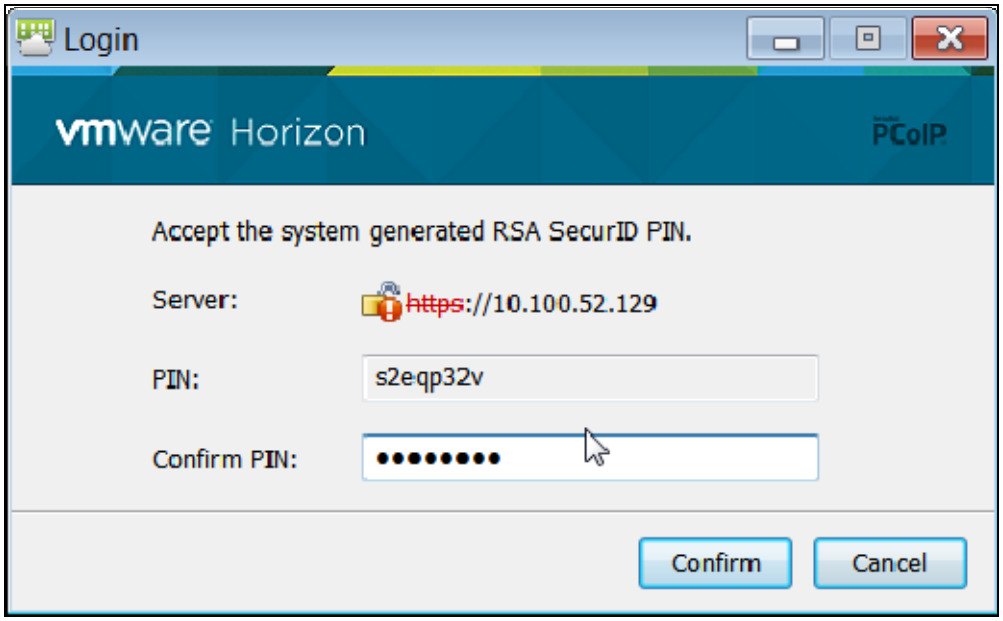
Windows and MAC Desktop

Login screen:

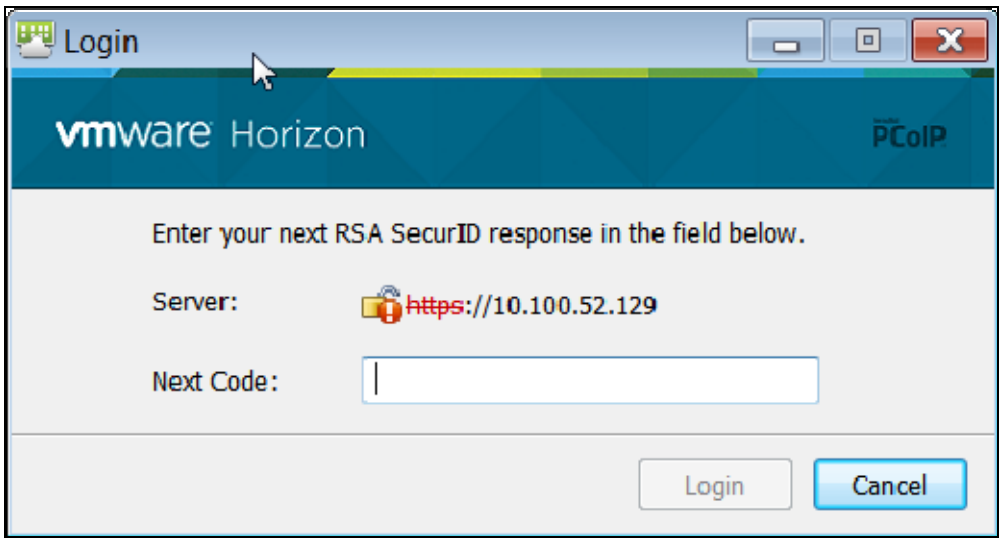
User-defined New PIN:



System-generated New PIN:

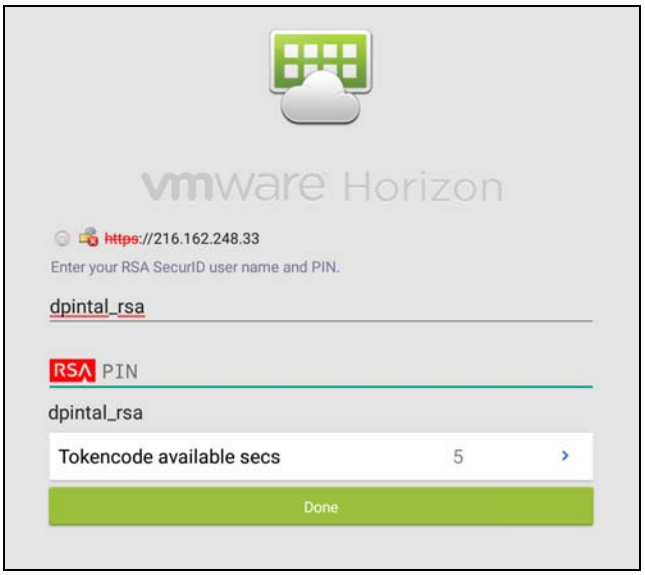


Next Tokencode:

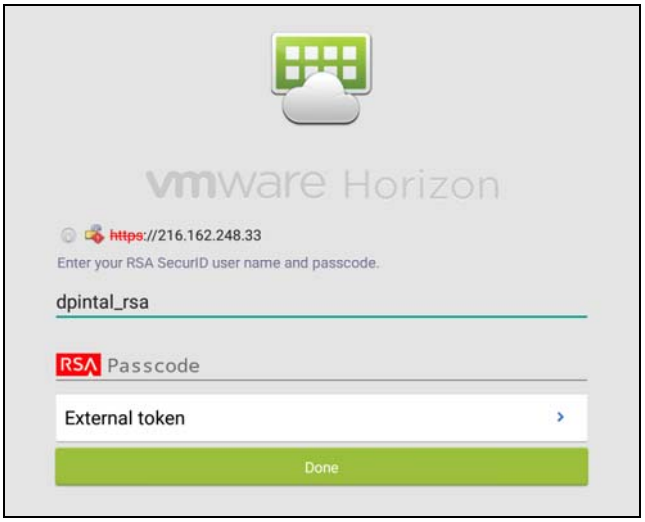


Mobile (Android)

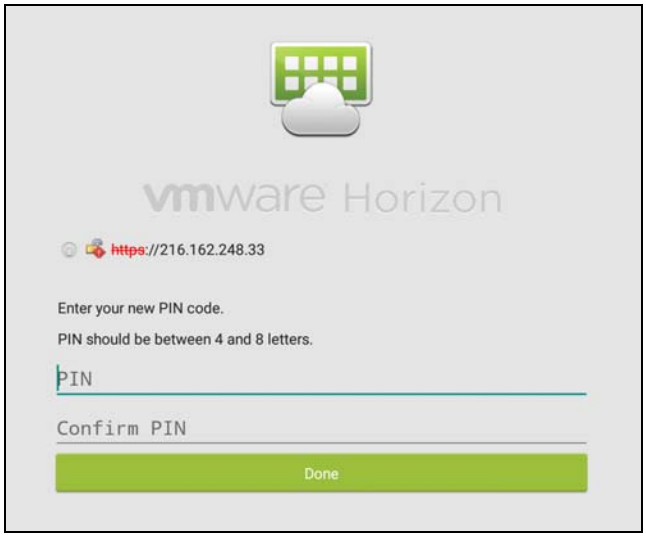
Software Token PIN Prompt:



Login screen:

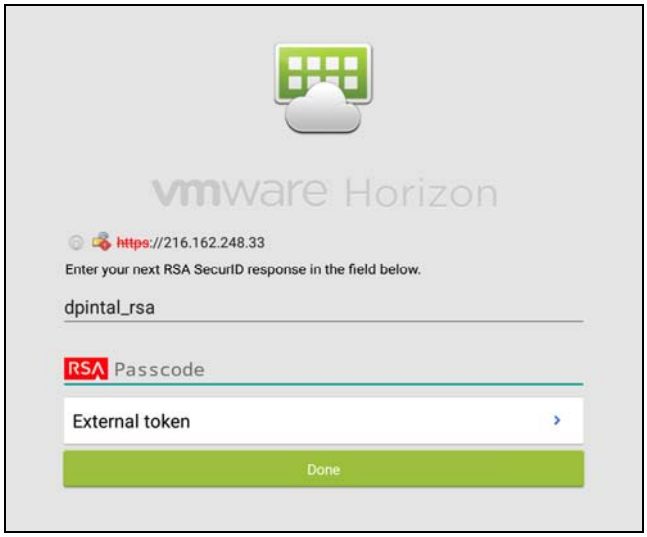


User-defined New PIN:



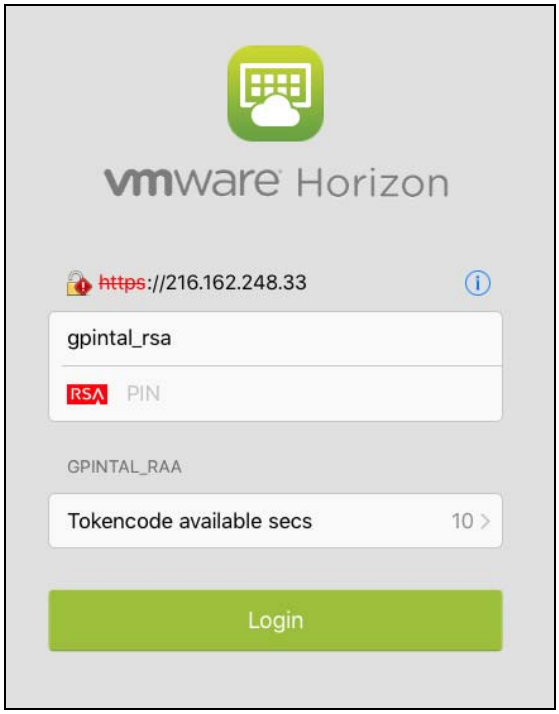
System-generated New PIN:

Next Tokencode:

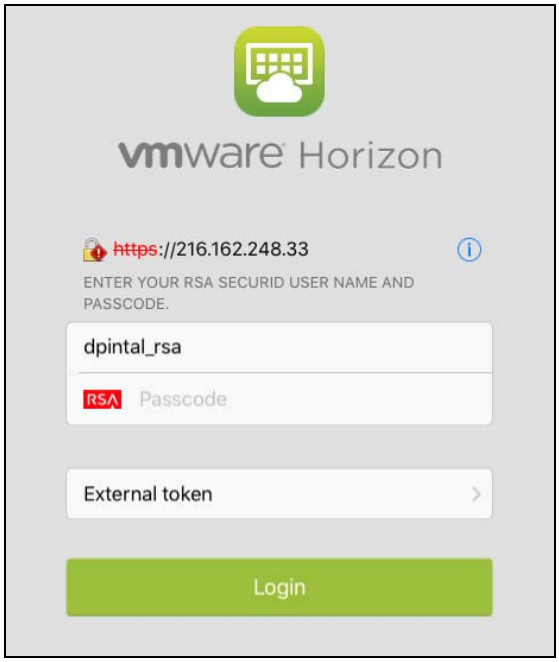


Mobile (iOS)

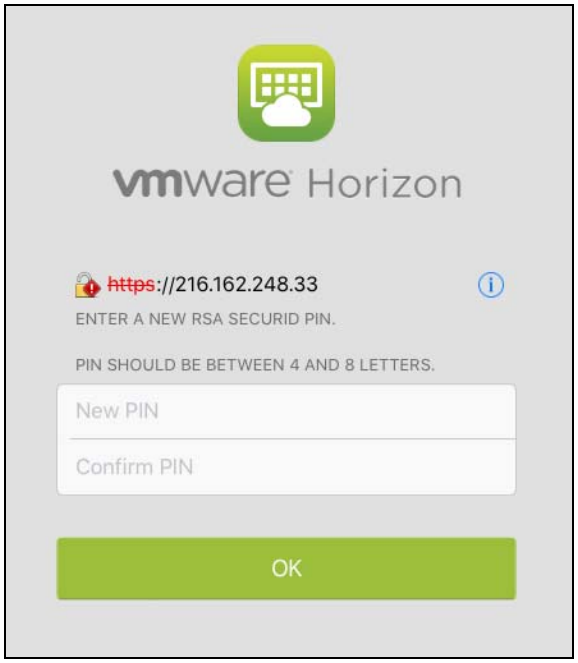
Software Token PIN Prompt:



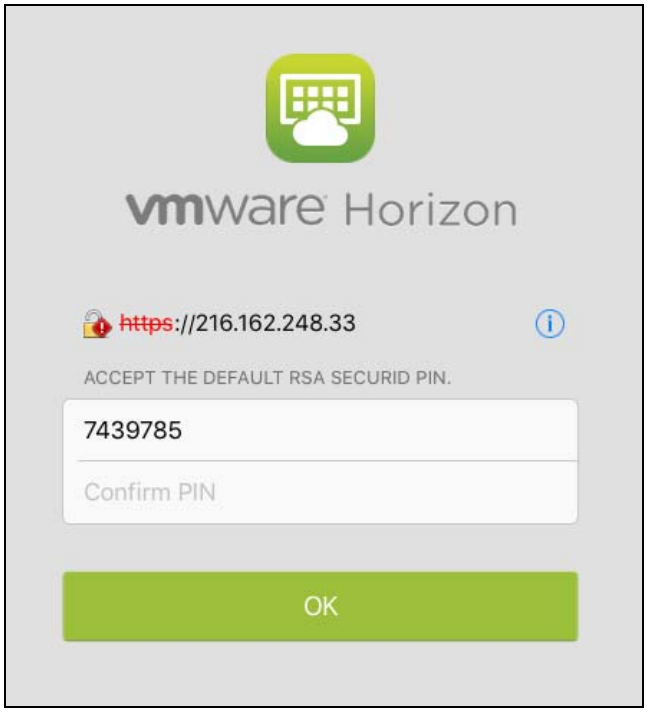
Login screen:



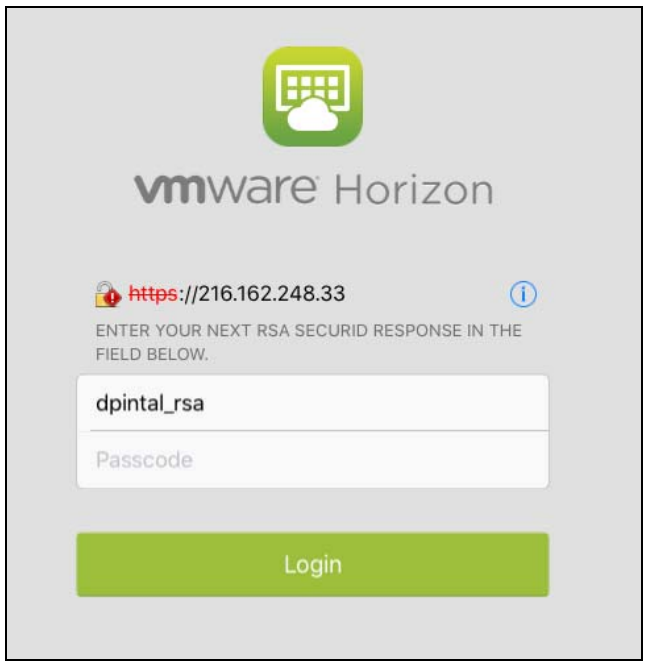
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA SecurID Access

Date Tested: August 9th, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
VMware Horizon View	6.2	Microsoft Windows Server 2012 R2 x64
VMware Horizon View HTML Access	2.4	Microsoft Windows Server 2012 R2 x64
VMware Windows Client	4.01	Microsoft Windows 7 x64
VMware MAC Client	4.1.0	MAC OS X 10.11.6
VMware iOS Mobile Client	4.1	iOS 9.3.3
VMware Android Mobile Client	1.8	Android 6.0.1
VMware Horizon View Agent	6.2	Windows 10

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

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

Certification Checklist for RSA SecurID Access

RSA Software Token Automation – RSA Native Protocol					
	Windows	**OS X**	**Android**	**iOS**	**Other**
PINless Token					
Next Tokencode Mode	N/A	N/A	✓	✓	N/A
PINpad-style Token					
Deny Alphabetic PIN	N/A	N/A	✓	✓	N/A
Next Tokencode Mode	N/A	N/A	✓	✓	N/A
Fob-style Token					
16-Character Passcode	N/A	N/A	✓	✓	N/A
Alphanumeric PIN	N/A	N/A	✓	✓	N/A
Next Tokencode Mode	N/A	N/A	✓	✓	N/A
Other					
Password-Protected Token	N/A	N/A	✓	✓	N/A
System-Generated PIN	N/A	N/A	✓	✓	N/A

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

Appendix

RSA Software Token SDK Integration Details			
	Android	**iOS**	**Other**
RSA Software Token SDK			
RSA Software Token SDK Version	2.0	2.1	N/A
RSA Software Token Data			
Display Token Serial Number	✓	✓	N/A
Display Token Expiration Date	✓	✓	N/A
Number of Tokens Supported	10	10	N/A
Provisioning			
File-Based	✓	N/A	N/A
CT-KIP	✓	✓	N/A
CTF	✓	✓	N/A

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