RSA SECURID® ACCESS
Implementation Guide

VMware Horizon View 7.2

Daniel R. Pintal, RSA Partner Engineering
Last Modified: September 14, 2017

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.

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 Features	
VMware Horizon View 7.2	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	-
SSO	
SAML SSO	-
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	-

Supported Authentication Methods by Integration Point

This section indicates which authentication methods are supported by integration point. The next section (Configuration Summary) contains links to the appropriate configuration sections for each integration point.

VMware Horizon View integration with RSA Cloud Authentication Service

Authentication Methods	IDR SAML	Cloud SAML	HFED	REST	RADIUS
RSA SecurID	-	-	-	-	✓
LDAP Password	-	-	-	-	✓
Authenticate Approve	-	-	-	-	✓
Authenticate Eyeprint ID	-	-	-	-	✓
Authenticate Fingerprint	-	-	-	-	✓
Authenticate Tokencode	-	-	-	-	✓
FIDO Token	-	-	-		

VMware Horizon View integration with RSA Authentication Manager

Authentication Methods	UDP Agent	TCP Agent	REST	RADIUS
RSA SecurID	✓	-	-	✓
AM RBA	-			-

✓ Supported
- Not supported
n/t Not yet tested or documented, but may be possible

Configuration Summary

All of the supported use cases of RSA SecurID Access with VMware Horizon View require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – VMware Horizon View can be integrated with RSA Cloud Authentication Service in the following way(s):

RADIUS Client

Cloud Authentication Service RADIUS Configuration
VMware Horizon View RADIUS Configuration

RSA Authentication Manager – VMware Horizon View can be integrated with RSA Authentication Manager in the following way(s):

UDP Agent

Authentication Manager UDP Agent Configuration
VMware Horizon View UDP Agent Configuration

RADIUS Client

Authentication Manager RADIUS Configuration
VMware Horizon View RADIUS Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

RADIUS

To configure RADIUS for Cloud Authentication Service for use with a RADIUS client, you must first configure a RADIUS client in the RSA SecurID Access Console.

Logon to the RSA SecurID Access console and browse to **Authentication Clients** > **RADIUS** > **Add RADIUS Client** and enter the **Name**, **IP Address** and **Shared Secret**. Click **Publish** to push your configuration change to the RADIUS server.

RSA Cloud Authentication RADIUS server listens on port UDP 1812.

RSA Authentication Manager Configuration

UDP Agent

To configure your RSA Authentication Manager for use with a UDP-based agent, you must create an agent host record in the Security console of your Authentication Manager and download its configuration file (sdconf.rec).

- Hostname: Configure the agent host record name to match the hostname of the agent.
- IP Address: Configure the agent host record to match the IP address of the agent.

> **Important: Authentication Manager must be able to resolve the IP address from the hostname.**

RADIUS

To configure your RSA Authentication Manager for use with a RADIUS Agent, you must configure a RADIUS client and a corresponding agent host record in the Authentication Manager Security Console.

The relationship of agent host record to RADIUS client in the Authentication Manager can 1 to 1, 1 to many or 1 to all (global).

RSA Authentication Manager RADIUS server listens on ports UDP 1645 and UDP 1812.

Partner Product Configuration

Before You Begin

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

VMware Horizon View is normally implemented on multiple servers to provide high availability and to meet scalability requirements. Each VMware Horizon View server can be individually configured for RSA SecurID authentication. If RSA SecurID is not enabled, the user is authenticated using just Microsoft Active Directory credentials (username, password, and domain name).

If RSA SecurID is enabled on a VMware Horizon View server, then users of the server are first required to supply their RSA SecurID username and passcode. If they are not authenticated at this level, access is denied. If they are correctly authenticated with RSA SecurID, they continue as normal and are then required to enter their Active Directory credentials.

It is possible in a multi-server VMware Horizon View deployment to have some servers enabled for RSA SecurID authentication and to have others disabled. This scenario can be used to force RSA SecurID authentication for users accessing the VMware Horizon View environment remotely over the Internet.

VMware Horizon View Configuration

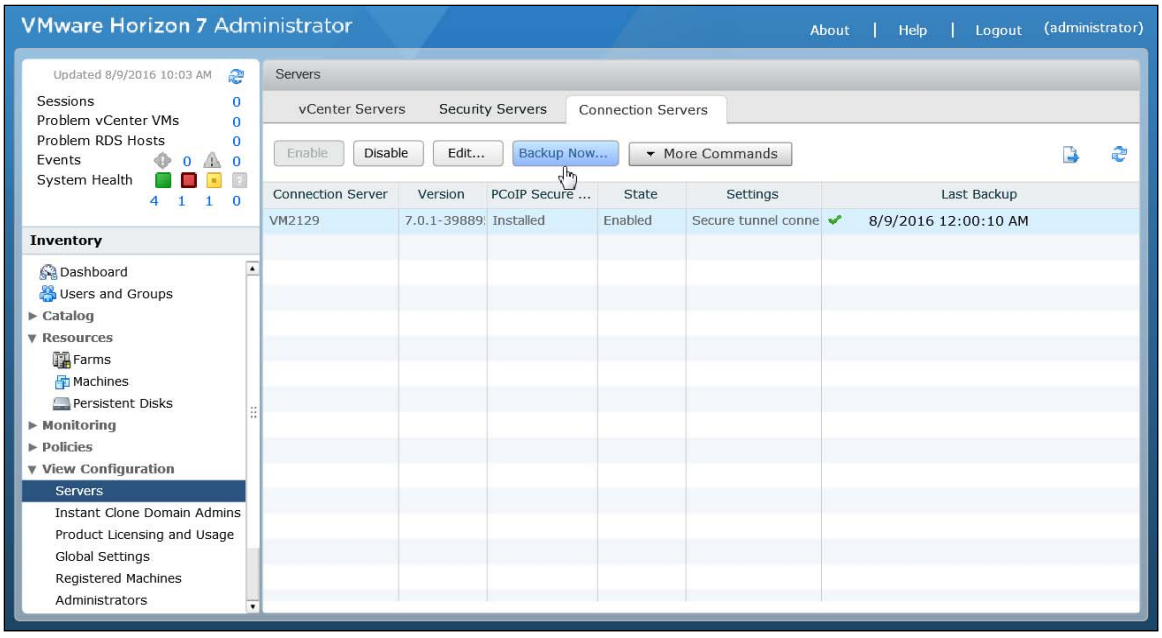
Configuration Overview

The following steps to configure each VMware Horizon View server for RSA SecurID, RADIUS and SecurID Access authentication are carried out using the web browser based Horizon View Administrator application.

VMware Horizon View UDP Agent Configuration

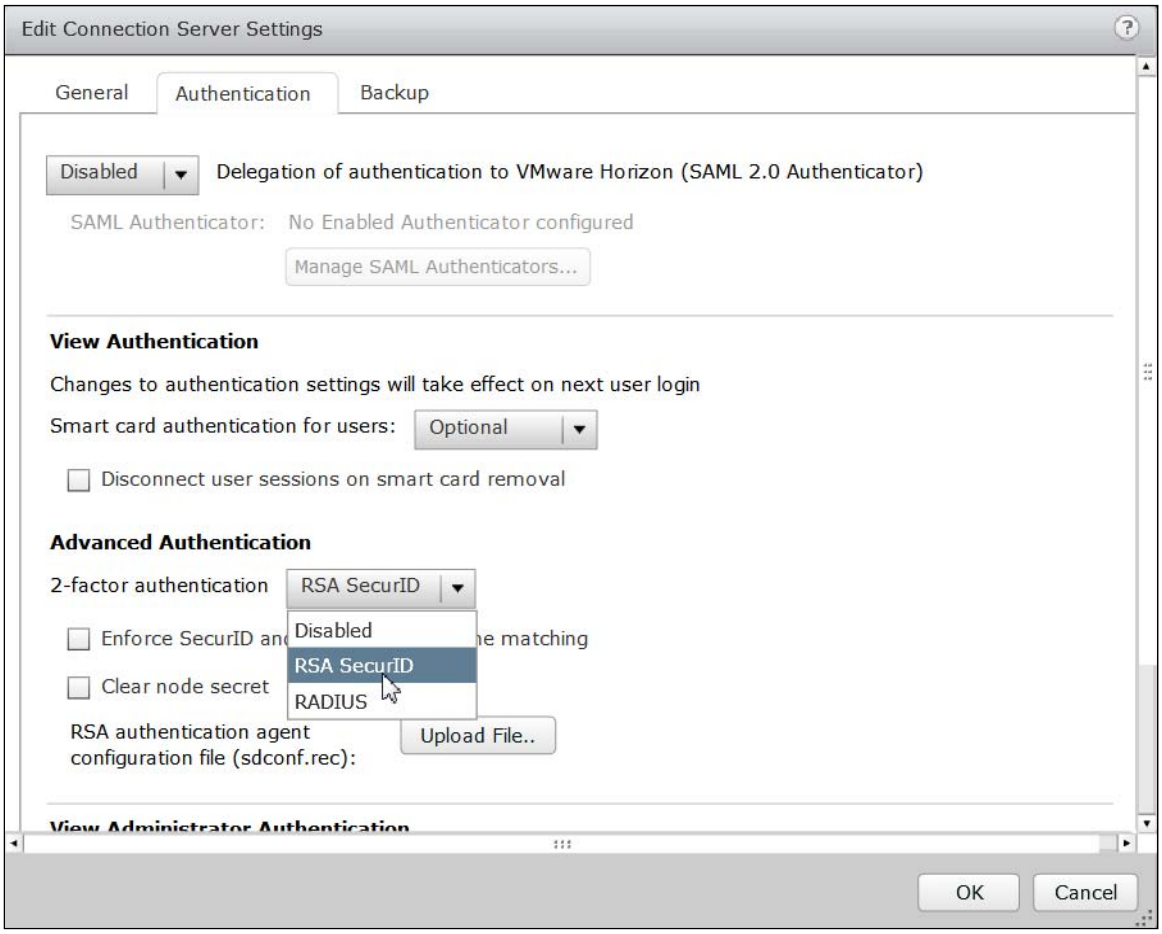
Complete the steps in this section to integrate VMware Horizon View with RSA SecurID Native protocol.

1. Log into the web browser based Horizon View Administrator using an administrator username and password.
2. From the Horizon View Administrator page, expand the View Configuration and select **Servers**. Locate the list of Horizon View Connection Servers on the right hand page, select the appropriate Connection Server and click **Edit**.



3. Within the Edit View Connection Server Settings window locate and select the **Authentication** tab.

4. Under Advanced Authentication, select **RSA SecurID** for the 2-factor authentication setting.



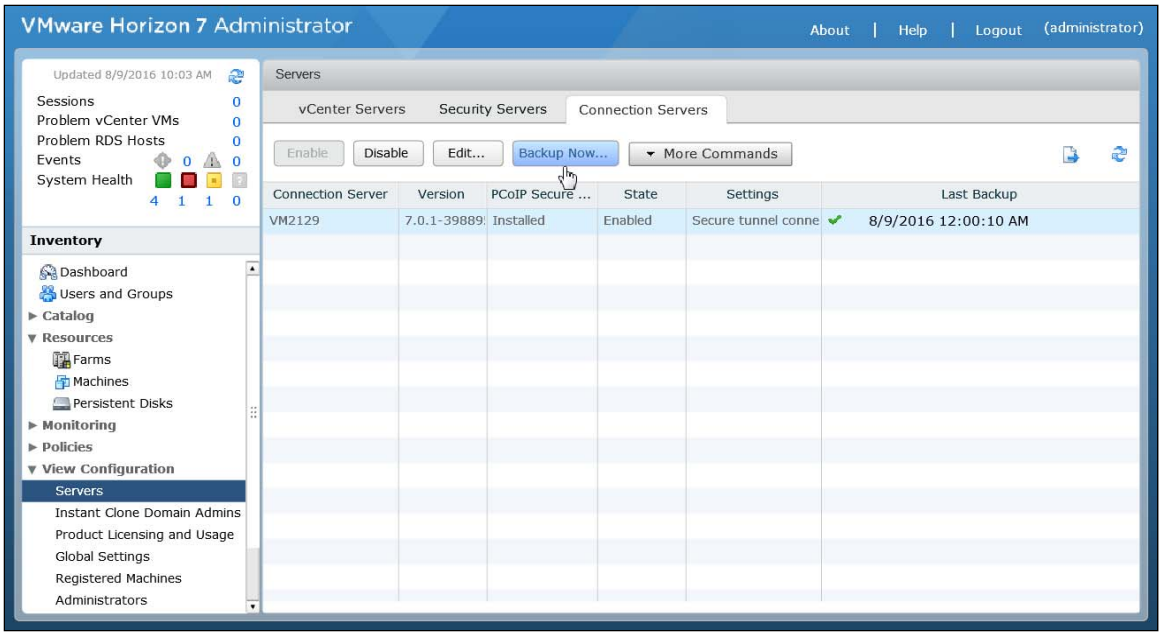
5. Decide if RSA SecurID usernames must match usernames used in Active Directory. If they should be forced to match, then select **Enforce SecurID and Windows user name matching**. In this case, the user will be forced to use the same RSA SecurID username for Active Directory authentication. If this option is not selected, the names are allowed to be different.
6. Upload the sdconf.rec file. Click **Browse** and select the **sdconf.rec** file. The sdconf.rec file was earlier exported from your RSA Authentication Manager.

> **! There is no need to restart VMware Horizon View after making these configuration changes. The necessary configuration files for each View server are automatically distributed and the RSA SecurID configuration takes effect immediately.**

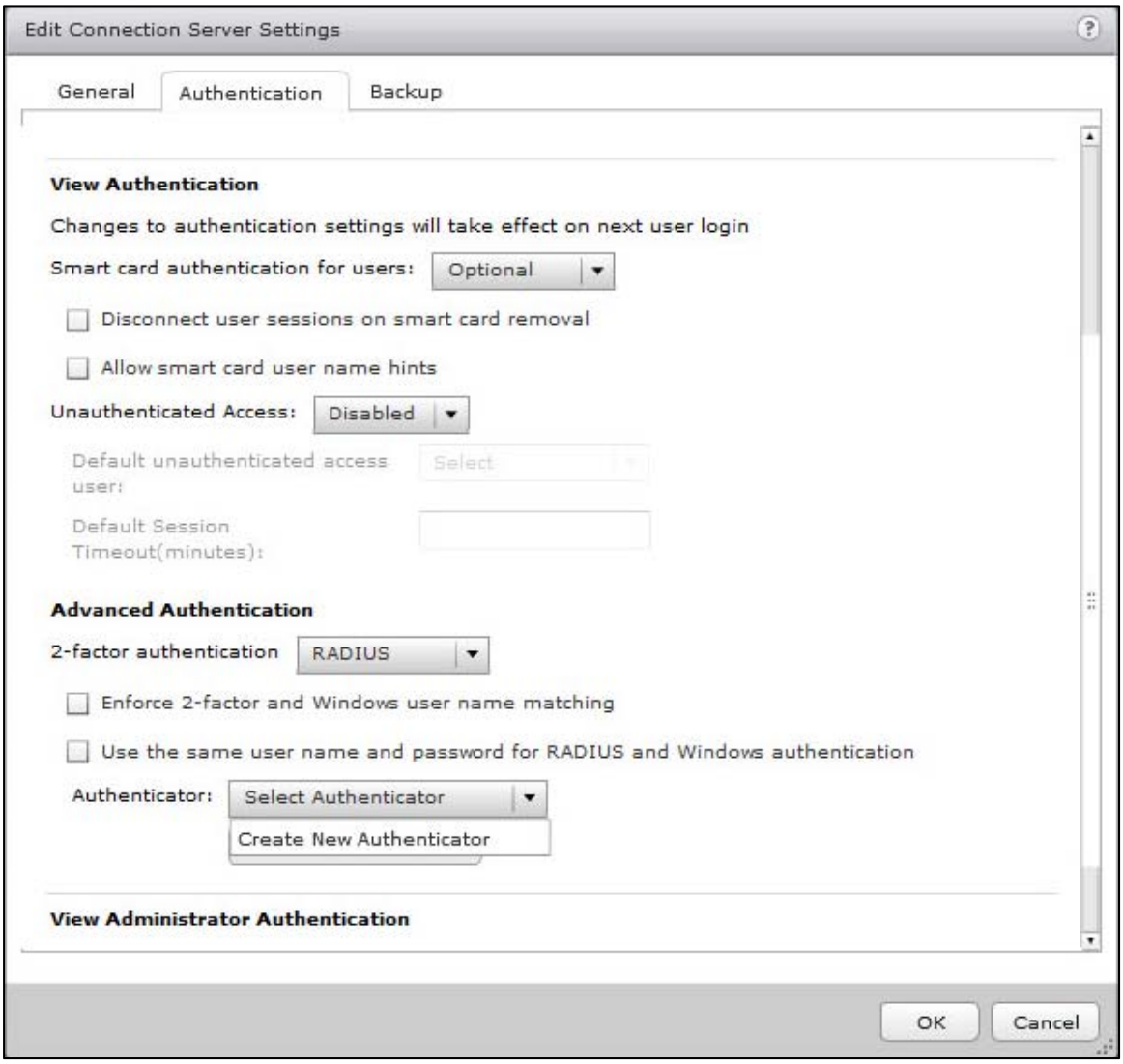
VMware Horizon View RADIUS Configuration

Complete the steps in this section to integrate VMware Horizon View with RSA SecurID Suite/Access using the RADIUS authentication protocol.

1. Log into the web browser based Horizon View Administrator using an administrator username and password.
2. From the Horizon View Administrator page, expand the View Configuration and select **Servers**. Locate the list of Horizon View Connection Servers on the right hand page, select the appropriate Connnection Server and click **Edit**.

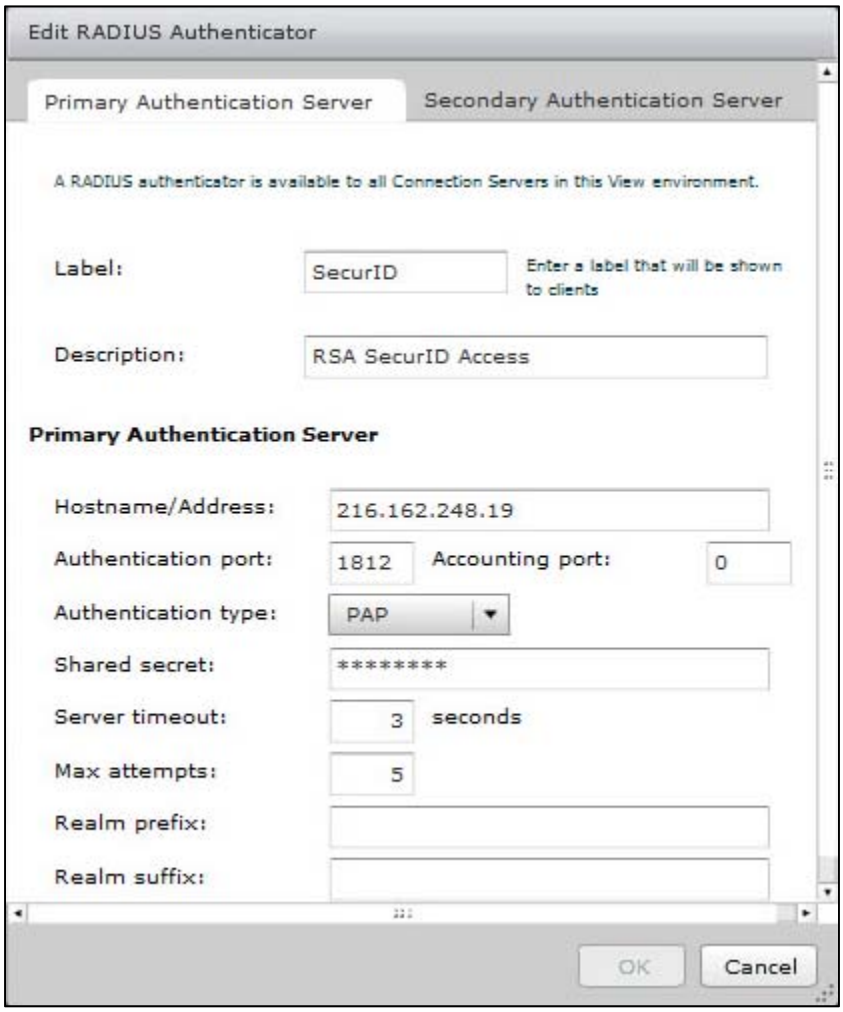


3. Within the Edit View Connection Server Settings window locate and select the **Authentication** tab.
4. Under Advanced Authentication, select **RADIUS** for the 2-factor authentication setting.

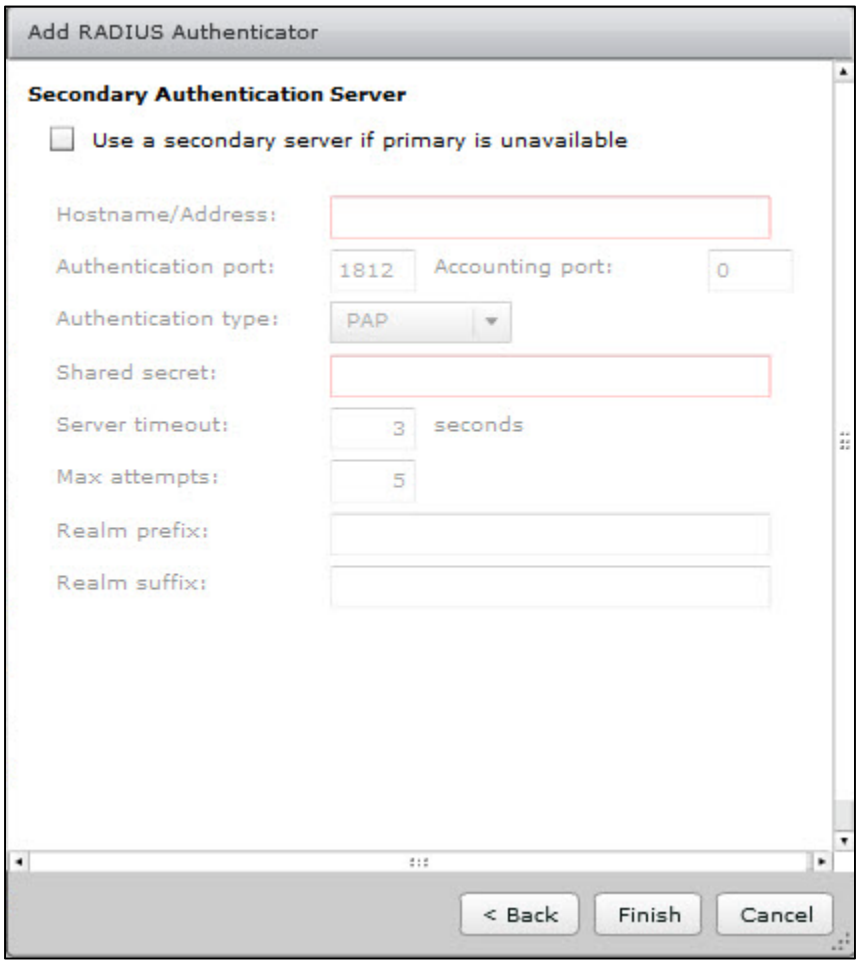


5. Under Advanced Authentication, use the **Select Authenticator** pulldown to select **Create New Authenticator** and configure the new RADIUS Host.

6. In the Edit RADIUS Authenticator window, provide a **Label**, **Description**, **Hostname/Address** and **Shared secret** of the RADIUS Host.



7. Continue with step 8 only if a secondary RADIUS Authenticator exists, otherwise skip to step 9.
8. Check the **Use a secondary server if primary is unavailable** and enter the details of the secondary RADIUS Host.



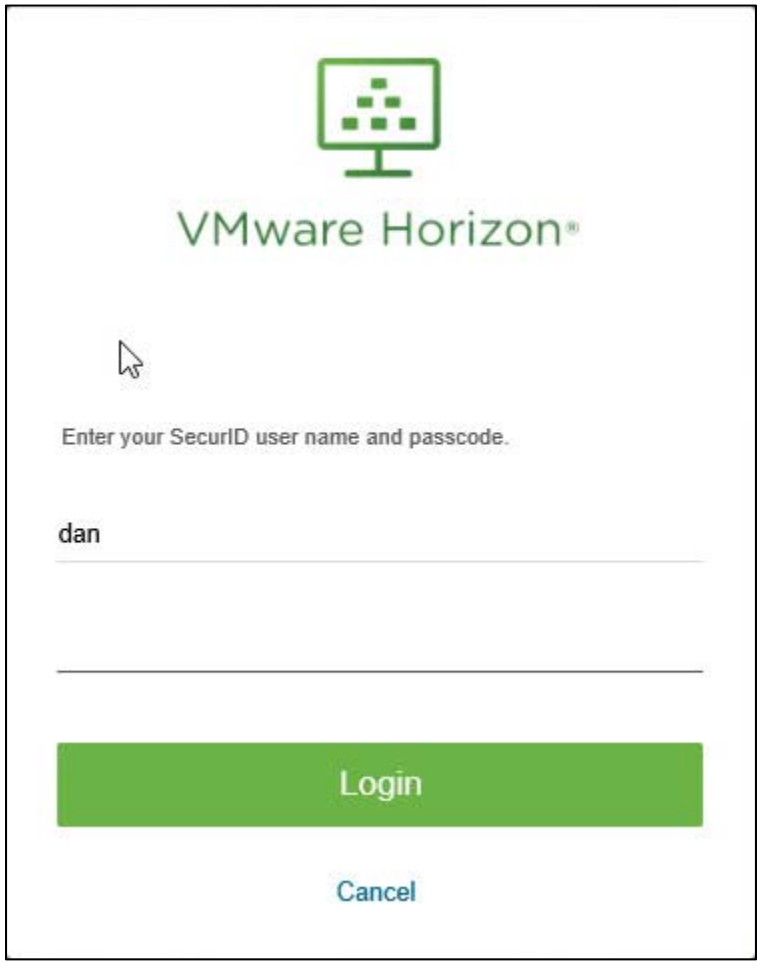
9. Select **Finish**.

! There is no need to restart VMware Horizon View after making these configuration changes.

RSA SecurID Login with VMware Horizon View Web Client

This section provides details about the end user interface for VMware Horizon View when configured for RSA SecurID authentication. This section shows dialogs from the VMware Horizon View Web Client, which is a native client for VMware Horizon View.

When a user connects to VMware Horizon View Web, which is enabled for RSA SecurID authentication, the user is presented with a specific VMware Horizon View RSA SecurID login prompt as shown below.

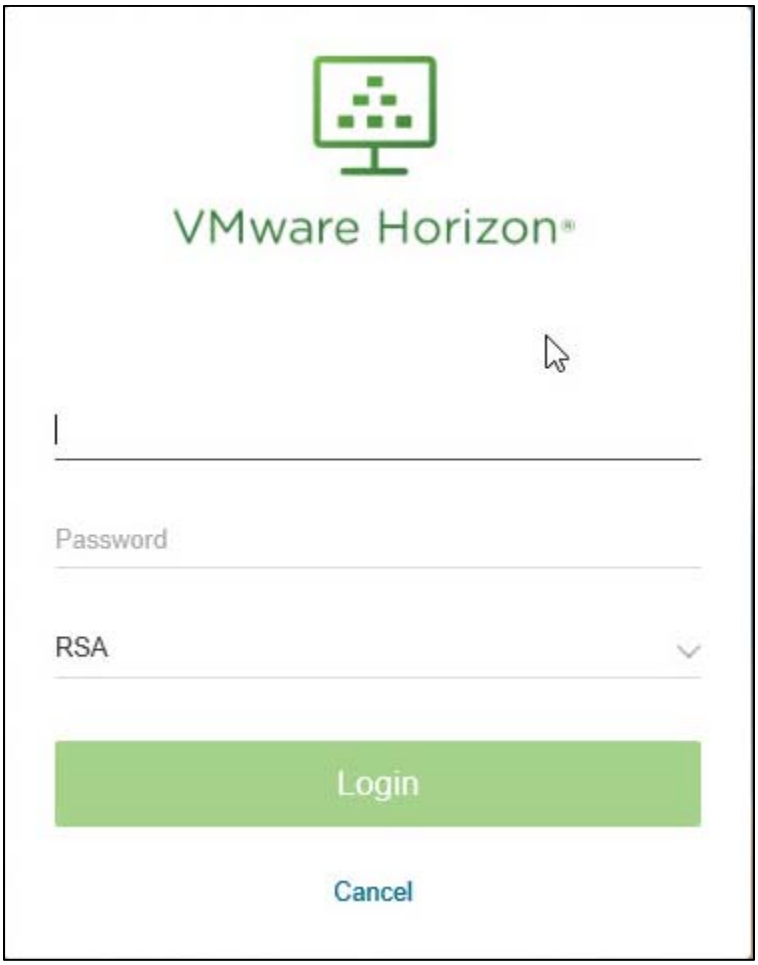


Users enter their RSA SecurID username (which may be the same as their Active Directory username). Users enter their passcode and click **Log In**. An RSA SecurID passcode is normally made up of a PIN followed by a tokencode.

If the users are required to enter a new RSA SecurID PIN after entering their RSA SecurID username and passcode, they are presented with a new PIN prompt. Users choose a new PIN and click **OK**. After users set a new PIN, they are prompted to re-enter the next tokencode.

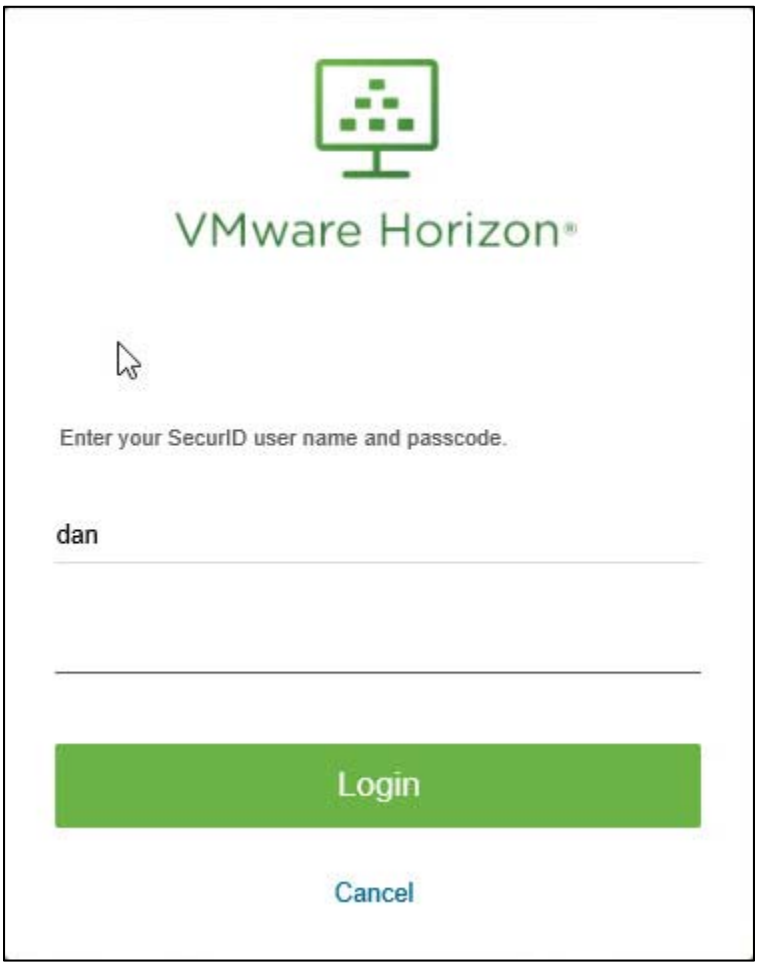
System generated PINs are also supported. If the RSA Authentication Manager is set up to use system generated PINs, users are presented with a new PIN when they first log in.

If the RSA SecurID credentials are correct as validated against RSA Authentication Manager, the user then gets a second VMware Horizon View prompt to enter their Microsoft Active Directory credentials.

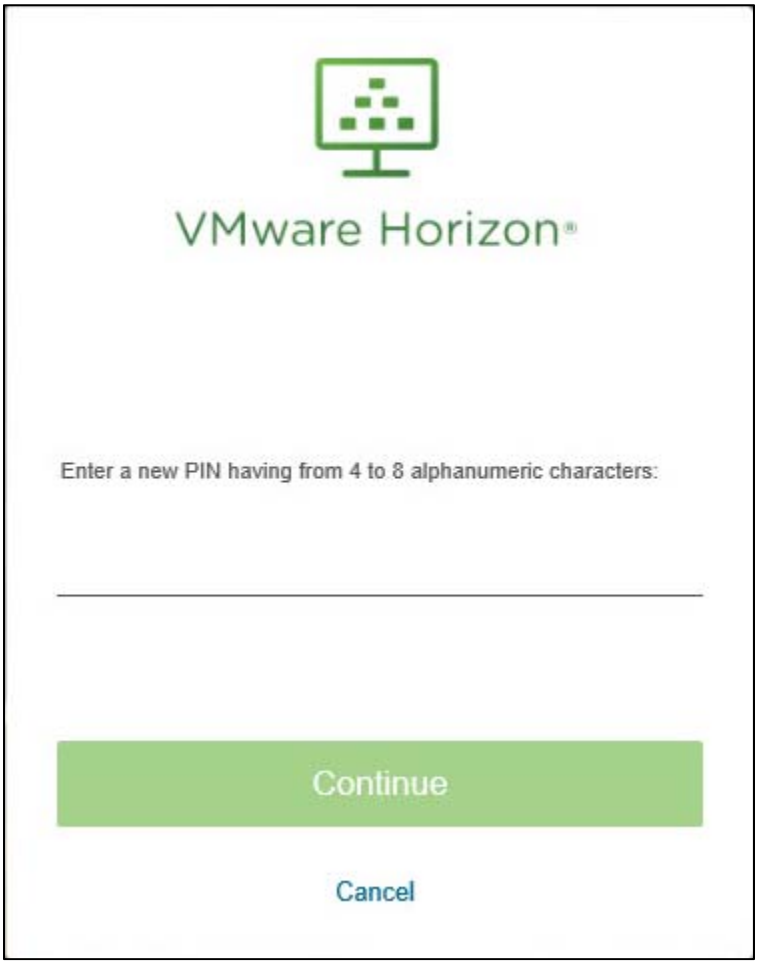


RSA SecurID Suite/Access Web Based Login Screenshots

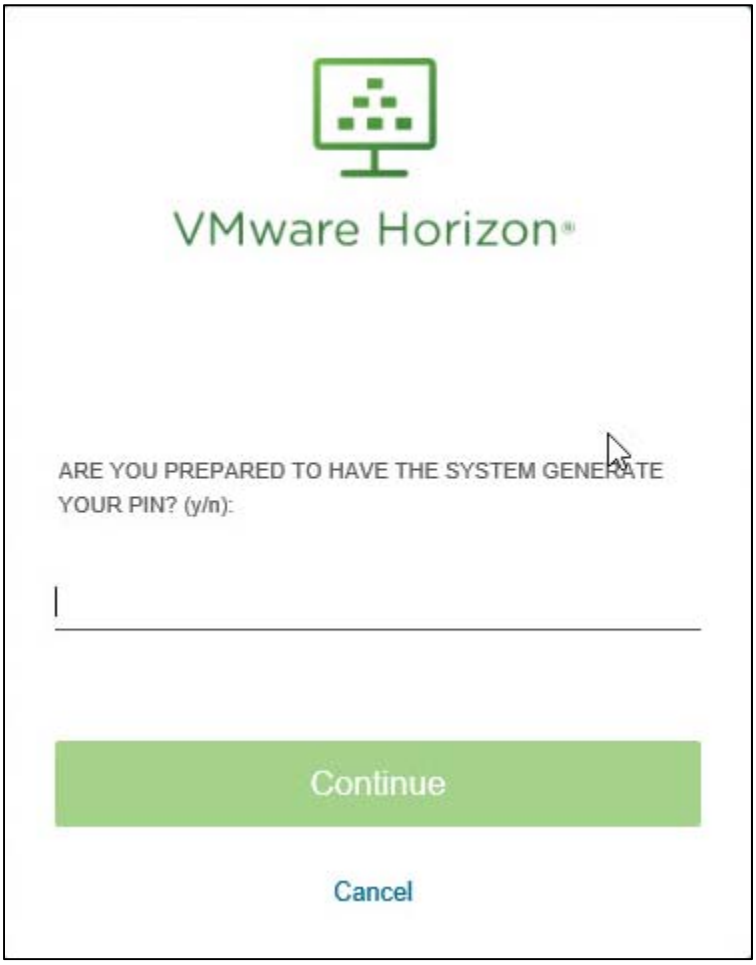
Login screen (Suite/Access):



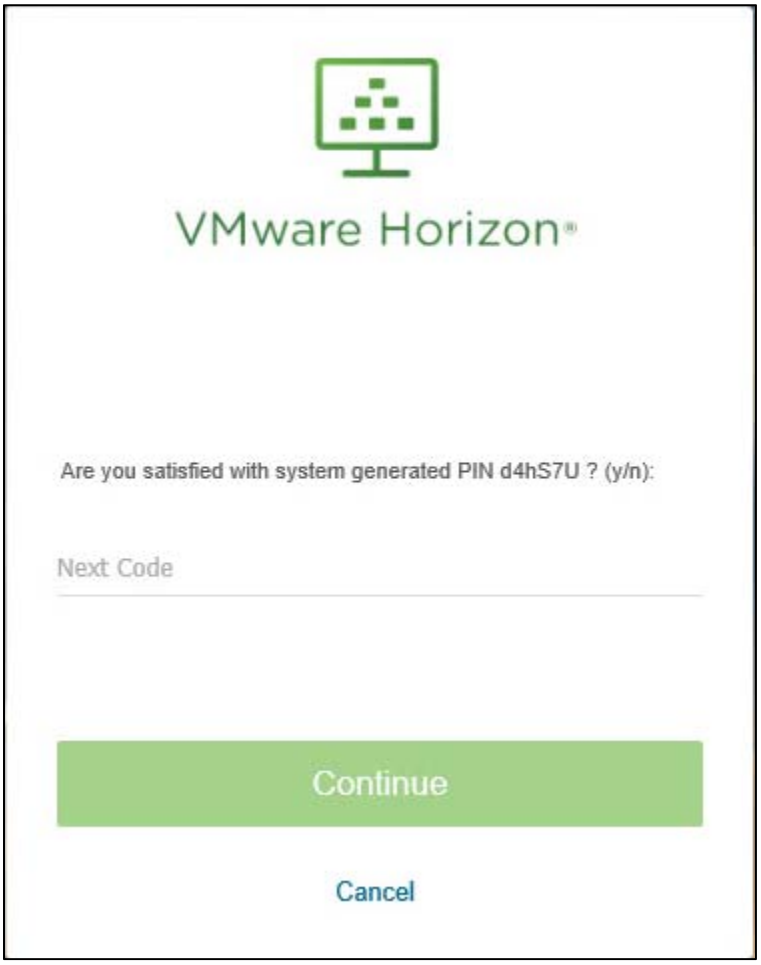
User-defined New PIN (Suite/Access):



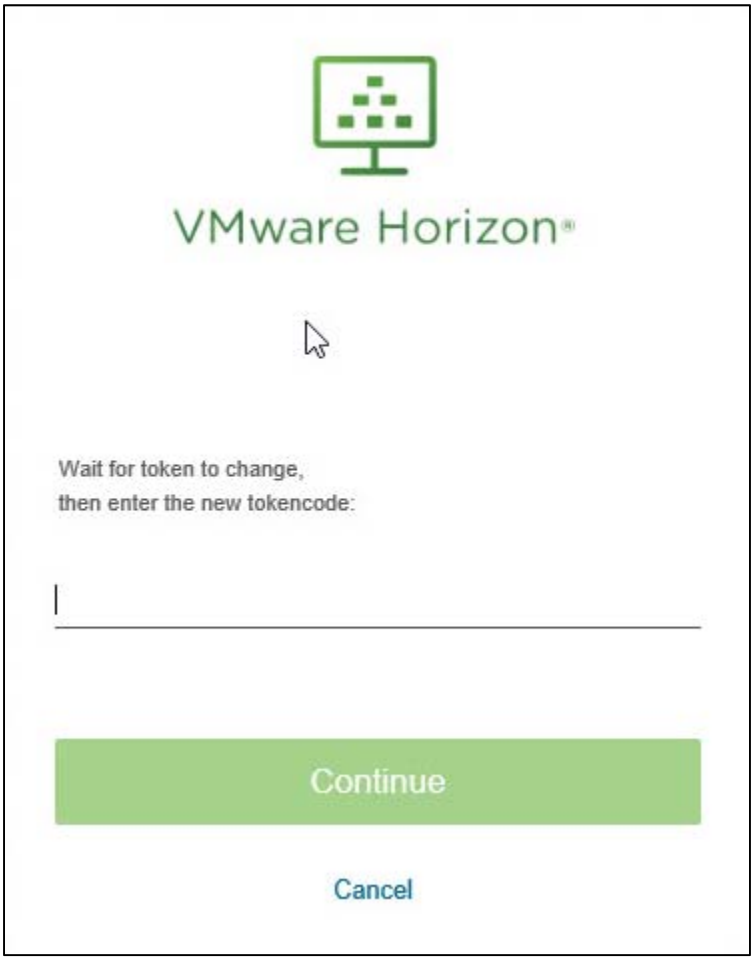
System-generated New PIN Generate (Suite/Access):



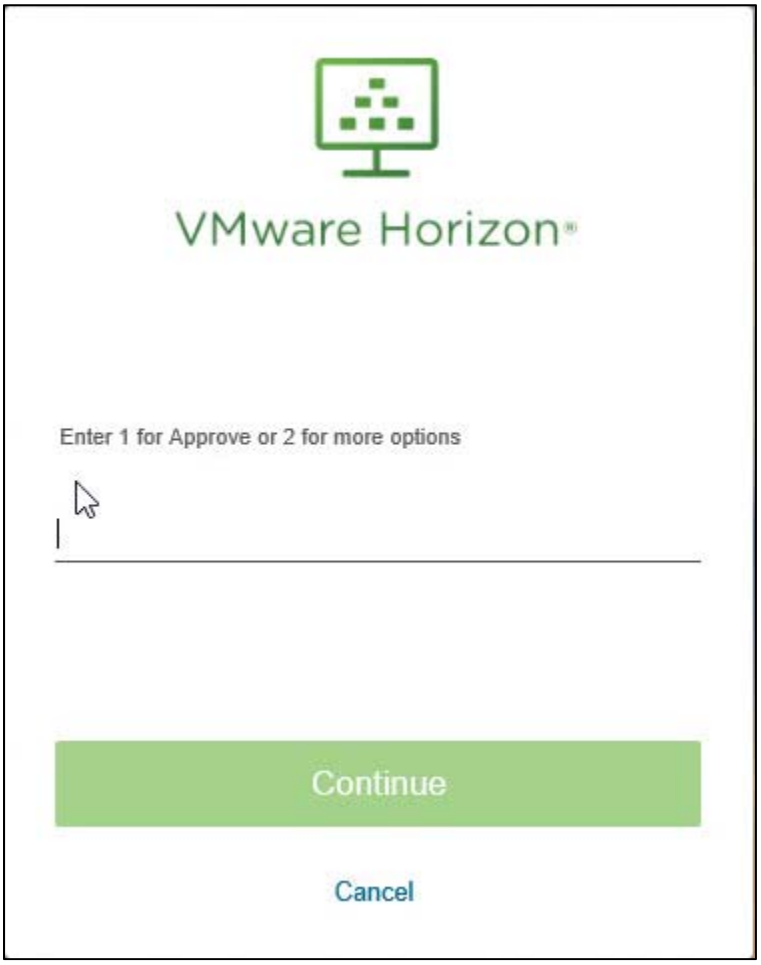
System-generated New PIN Accept (Suite/Access):



Next Tokencode (Suite/Access):



Authentication Method Selection (Access only):



Certification Checklist for RSA SecurID Access

Certification Environment Details:

RSA Authentication Manager 8.2, Virtual Appliance

RSA Authentication Software Token 2.2.4, Android

RSA Remote Authentication 1.5.3, Android

VMWare Horizon View, 7.2, Windows 2012 R2

RSA Authentication Manager

Date Tested: September 13, 2017

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	-	✓	-	✓
RSA SecurID Software Token Automation	-	-	-	-
On Demand Authentication	-	✓	-	✓
Risk-Based Authentication		-		-

✓ = Passed, **X** = Failed, **-** = N/A

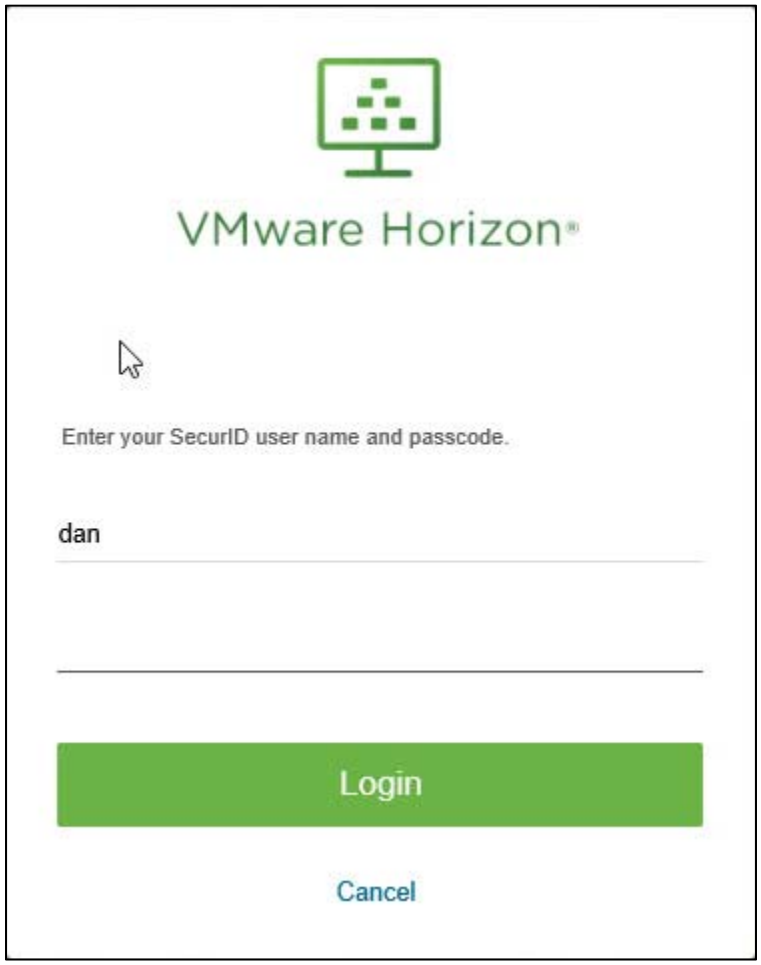
Known Issues

The integration between Horizon View and RSA SecurID Access (RSA Cloud offering supporting RSA SecurID RADIUS & Authenticate), requires a note to administrators and users.

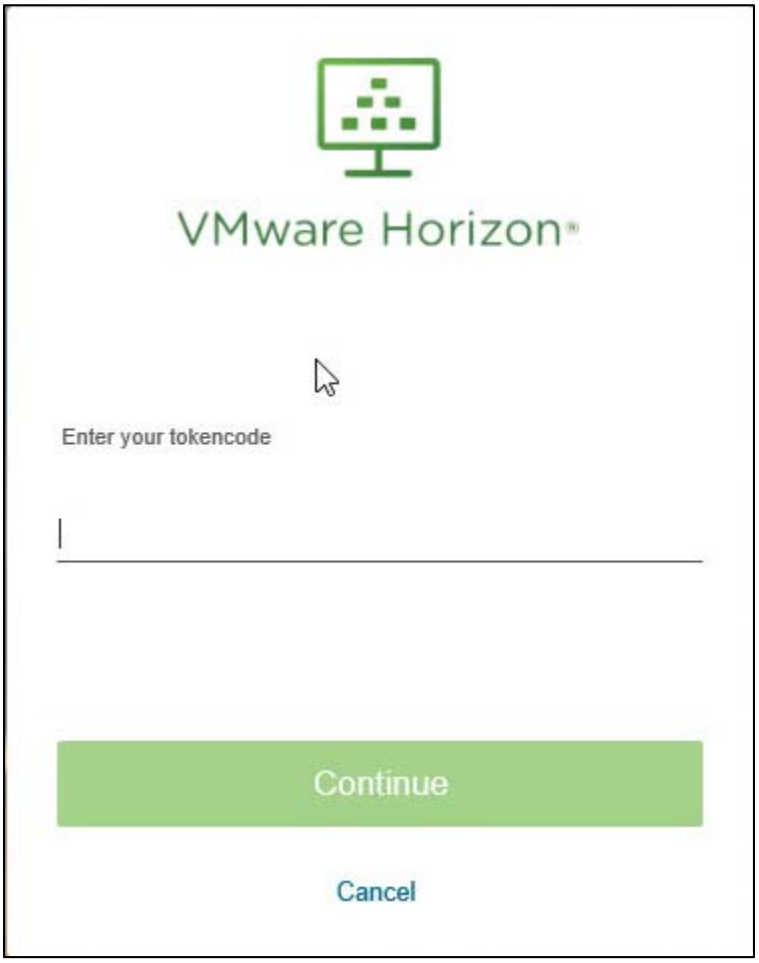
RSA SecurID Access (RADIUS)

The user interaction differs from the RSA Authentication Manager 8.2 in that the user is required to provide their LDAP username/password at the initial logon screen, not SecurID user name and passcode as prompted on the initial login screen (See Login screen below). Once the user correctly enters their LDAP username/password they are subsequently prompted for their tokencode, provided they have set their Token PIN (See Enter the Tokencode below).

Login screen 1:



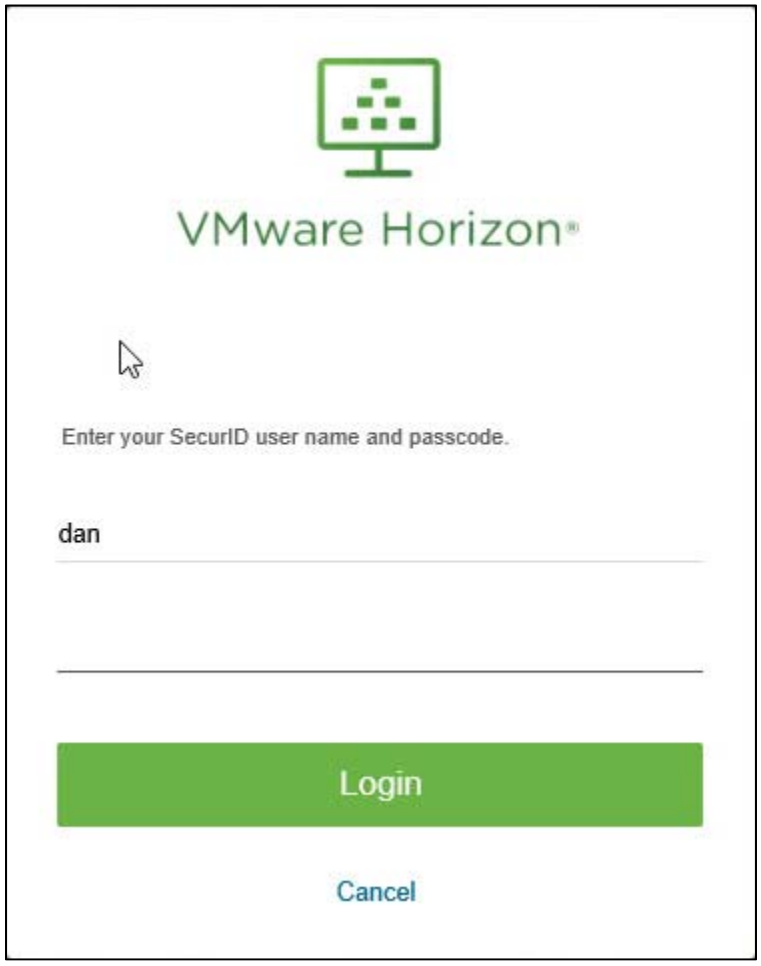
Enter the Tokencode:



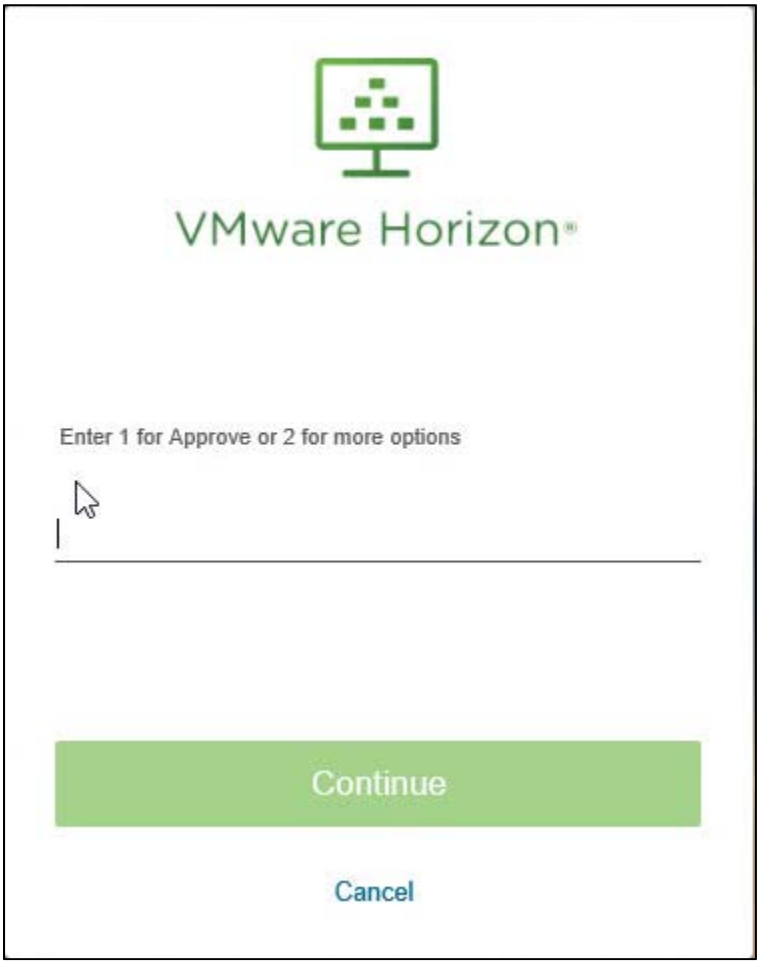
RSA SecurID Access (Authenticate/Swipe)

Similarly, using the Authenticate/Swipe RSA Authentication method the user provides an LDAP username/password, not SecurID user name and passcode as prompted on the initial login screen (See Login screen below). After the user correctly enters their LDAP username/password they are subsequently prompted to enter 1 for Authenticate or 2 for other options (See Authentication Method Selection (Access only) below.

Login screen:



Authentication Method Selection (Access only):



Appendix

RSA SecurID Access Integration Details

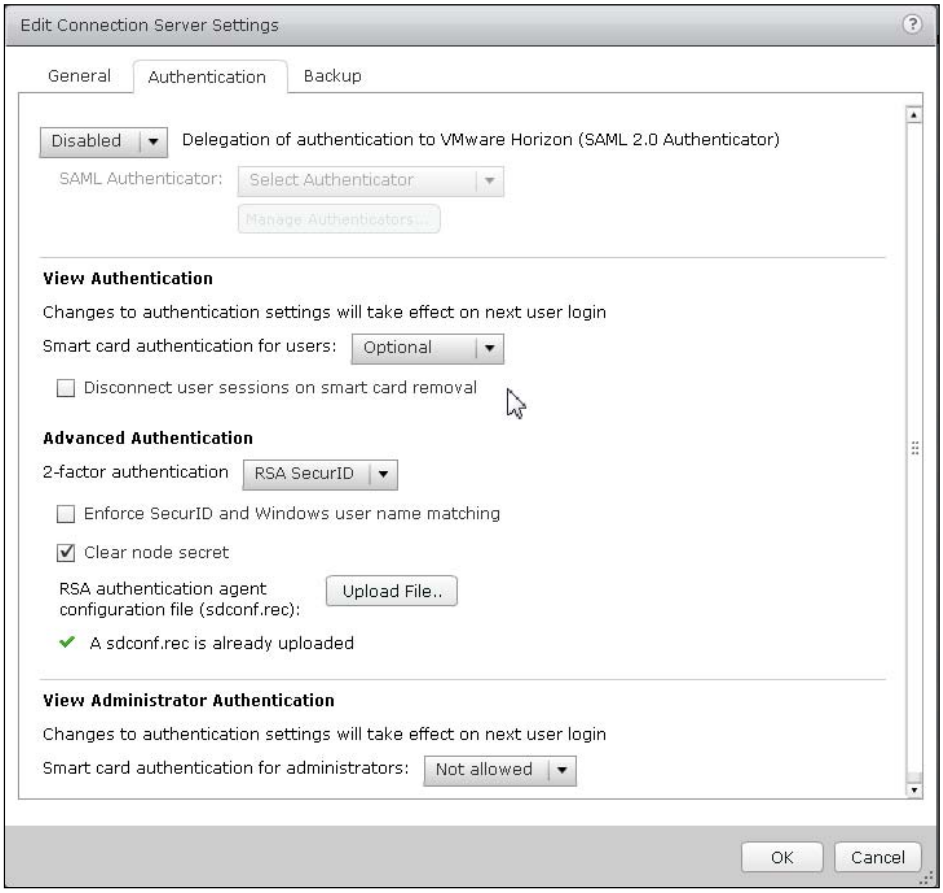
Partner Integration Details	
RSA Authentication Agent API (UDP)	5.0.3.176
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	Yes

RSA Authentication Agent Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	%SystemRoot%\System32
sdopts.rec	%SystemRoot%\System32
Node secret	%SystemRoot%\System32
sdstatus.12 / jastatus.12	%SystemRoot%\System32

Node Secret:

If you need to clear the node secret, use the Horizon View Administrator console and check the **Clear node secret** box and select **OK**.



sdconf.rec:

If you need to clear the *sdconf.rec* it is stored as %SystemRoot%\System32\sdconf.rec. Refer to the graphic above and use the **Upload File** button when importing a new sdconf.rec file.

sdstatus.12:

The sdstatus.12 file is not created either in the file system or within the registry.

Agent Tracing:

Authentication Agent Event Logging is written to [Install Drive]:\Program Files\VMware\VMware View\Server\bin. 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:

[Install Drive]:\Program Files\VMware\VMware View\Server\broker\conf\rsa_api.properties

```
#      Enables debug tracing.
RSA_ENABLE_DEBUG=yes
#      Sends tracing to a file.
RSA_DEBUG_TO_FILE=yes
```

sdopts.rec:

Not accessible through the Horizon View administrative interface but can be added, modified and deleted through the Windows file system at **%SystemRoot%\System32\sdopts.rec**.