RSA SECURID® ACCESS
Standard Agent Implementation Guide

VMware Horizon View 6.2

Daniel R. Pintal, RSA Partner Engineering

Last Modified: August 9th, 2016

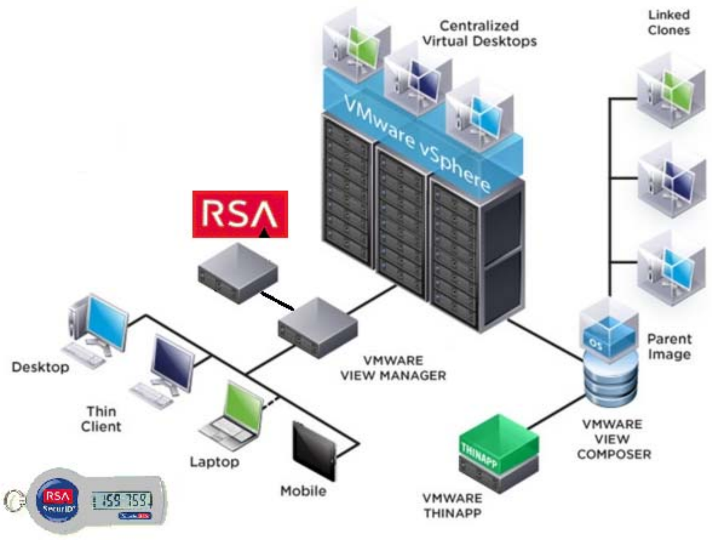
Solution Summary

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 Authentication Manager supported features	
VMware Horizon View 6.2	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	No
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	No
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	No
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No



RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between the VMware Horizon View and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the VMware Horizon View and contains information about communication and encryption.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

! Important: The UDP-based authentication agent's hostname must resolve to the IP address specified.

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 VMware Horizon View will occur.

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.

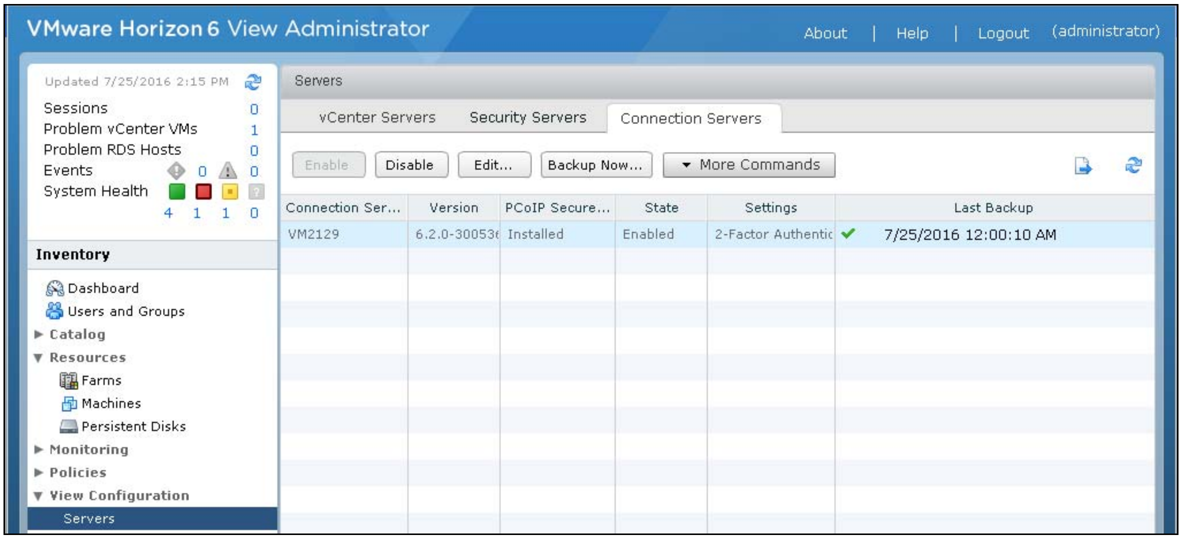
It is possible in a multi-server VMware Horizon View deployment to have some servers enabled for RSA SecurID authentication and to have others disabled. This scenario can be used to force RSA SecurID authentication for users accessing the VMware Horizon View environment remotely over the Internet.

VMware Horizon View Configuration

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

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 server and click **Edit**.



VMware Horizon 6 View Administrator — About | Help | Logout (administrator)

Updated 7/25/2016 2:15 PM

Sessions	0
Problem vCenter VMs	1
Problem RDS Hosts	0
Events	◆ 0 ⚠ 0
System Health	🟩 4 🟥 1 🟨 1 ? 0

Inventory

- Dashboard
- Users and Groups
- ▶ Catalog
- ▼ Resources
  - Farms
  - Machines
  - Persistent Disks
- ▶ Monitoring
- ▶ Policies
- ▼ View Configuration
  - Servers

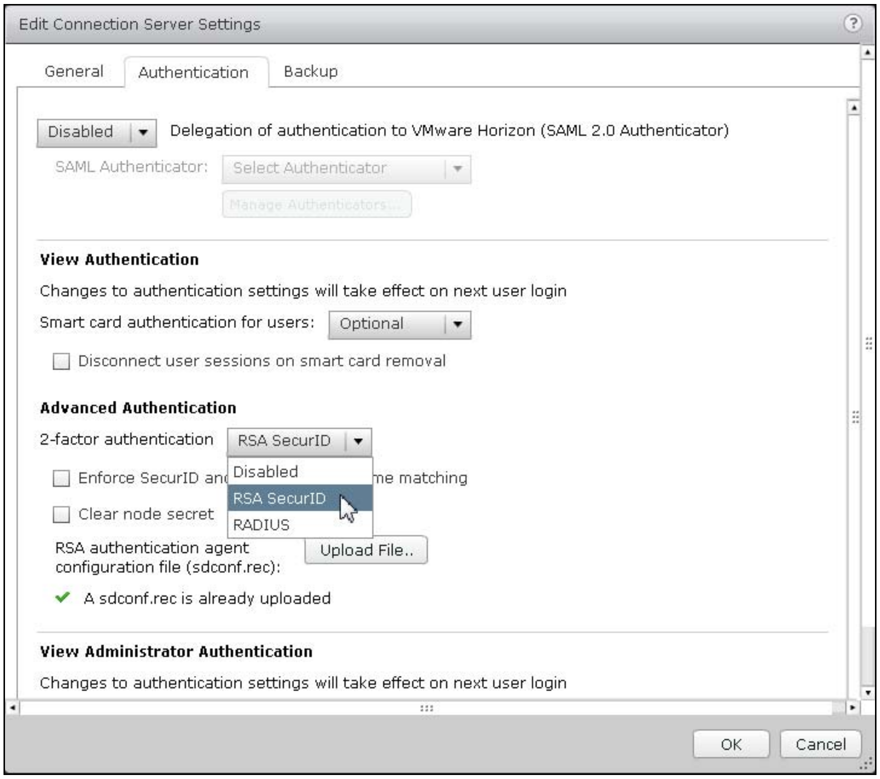
Servers

vCenter Servers | Security Servers | Connection Servers

Enable | Disable | Edit... | Backup Now... | ▼ More Commands

Connection Ser...	Version	PCoIP Secure...	State	Settings	Last Backup
VM2129	6.2.0-30053(	Installed	Enabled	2-Factor Authentic ✓	7/25/2016 12:00:10 AM

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.



Edit Connection Server Settings

General | Authentication | Backup

Disabled ▼ Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)

SAML Authenticator: Select Authenticator ▼

Manage Authenticators...

View Authentication

Changes to authentication settings will take effect on next user login

Smart card authentication for users: Optional ▼

□ Disconnect user sessions on smart card removal

Advanced Authentication

2-factor authentication: RSA SecurID ▼ (Disabled / RSA SecurID / RADIUS)

□ Enforce SecurID an[d ...]me matching

□ Clear node secret

RSA authentication agent configuration file (sdconf.rec): Upload File..

✓ A sdconf.rec is already uploaded

View Administrator Authentication

Changes to authentication settings will take effect on next user login

OK | Cancel

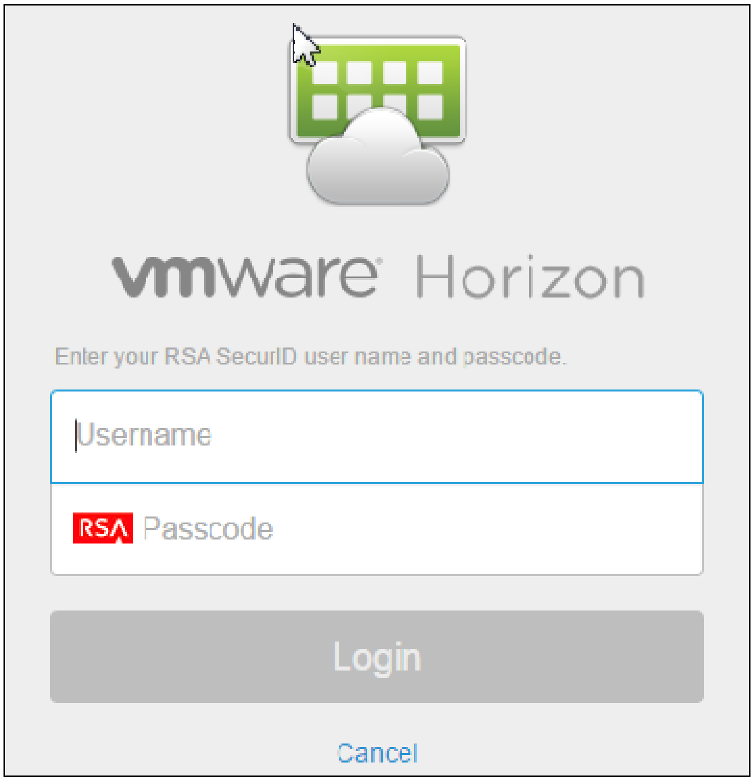
5. Decide if RSA SecurID usernames must match usernames used in Active Directory. If they should be forced to match, then select **Enforce SecurID and Windows user name matching**. In this case, the user will be forced to use the same RSA SecurID username for Active Directory authentication. If this 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.

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.



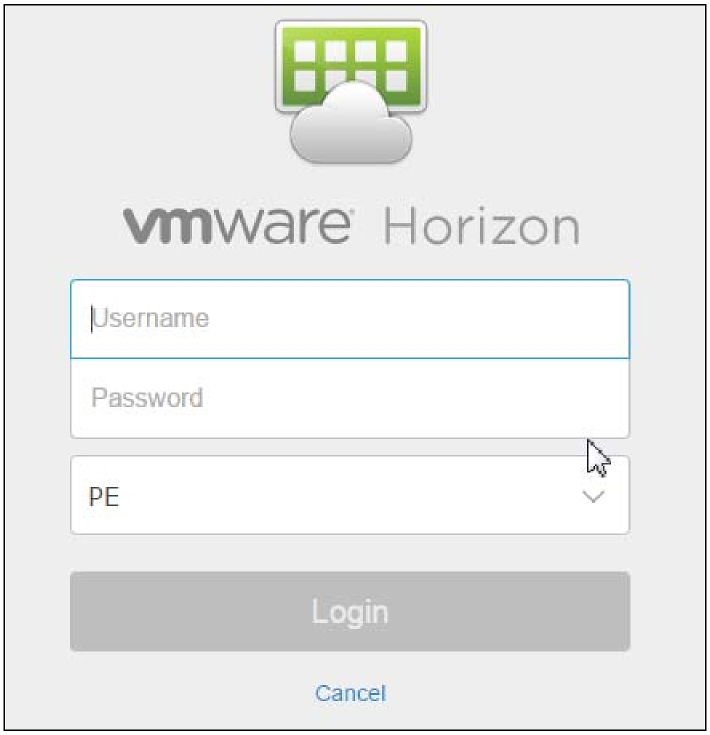
Enter your RSA SecurID user name and passcode.

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.

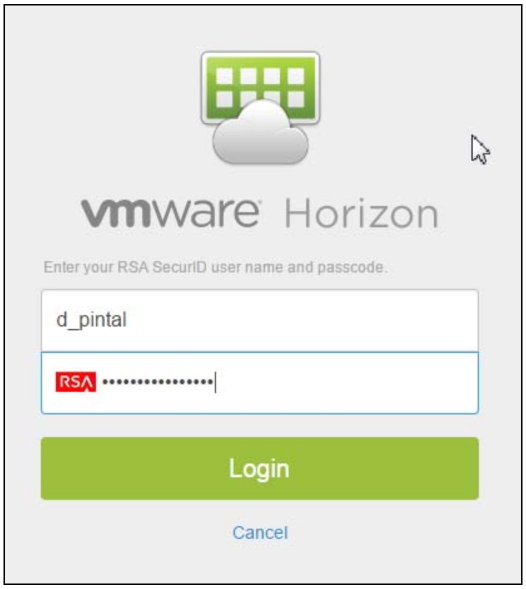
System generated PINs are also supported. If the RSA Authentication Manager is set up to use system generated PINs, users are presented with a new PIN when they first log in.

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 Login Screens

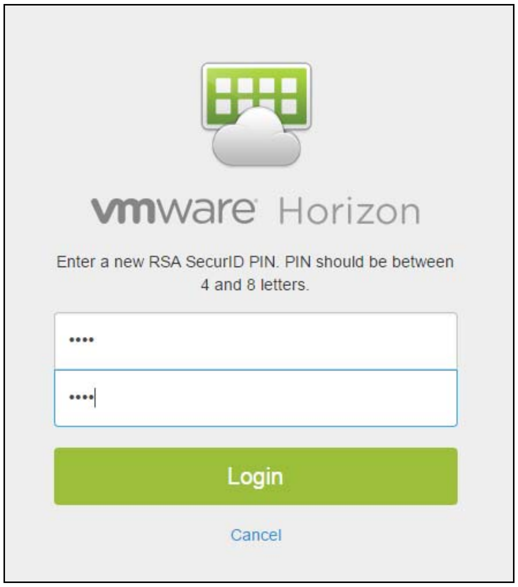
Login screen:



Enter your RSA SecurID user name and passcode.

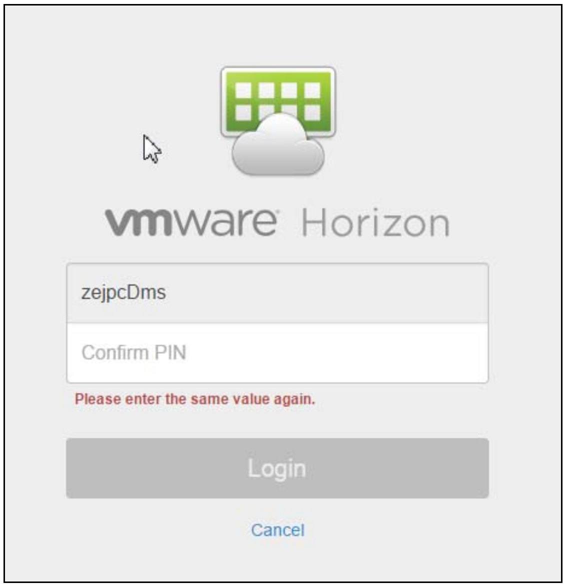
d_pintal

User-defined New PIN:



Enter a new RSA SecurID PIN. PIN should be between 4 and 8 letters.

System-generated New PIN:

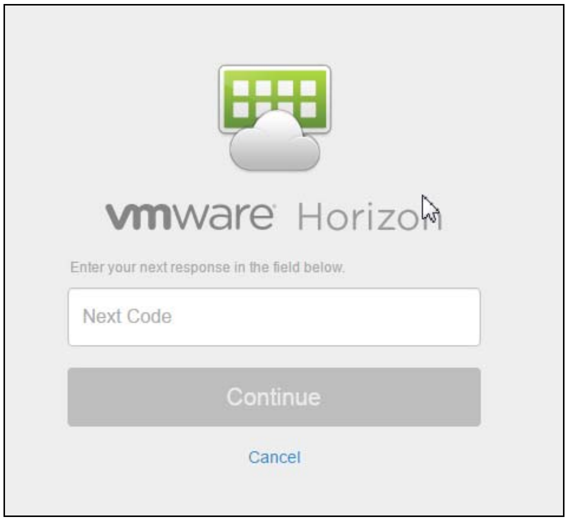


zejpcDms

Confirm PIN

Please enter the same value again.

Next Tokencode:



Enter your next response in the field below.

Next Code

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 Horizon View Client	3.0	Microsoft Windows 7 x64
VMware Horizon View Agent	6.0	Windows 10

RSA SecurID Authentication

Date Tested: August 9th, 2016

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

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

Appendix

RSA SecurID Authentication Files

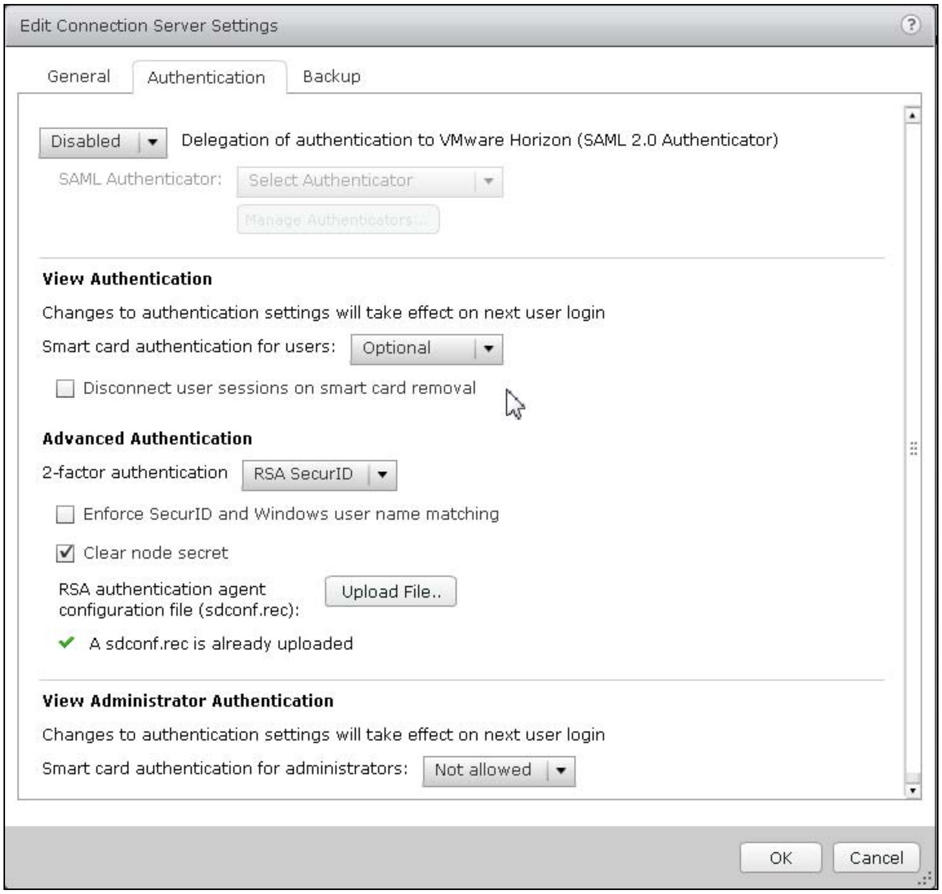
RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	%SystemRoot%\System32
sdopts.rec	%SystemRoot%\System32
Node secret	%SystemRoot%\System32
sdstatus.12 / jastatus.12	%SystemRoot%\System32

Partner Integration Details

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

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**.



Edit Connection Server Settings

Disabled ▾ Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)

SAML Authenticator: Select Authenticator ▾

View Authentication

Changes to authentication settings will take effect on next user login

Smart card authentication for users: Optional ▾

□ Disconnect user sessions on smart card removal

Advanced Authentication

2-factor authentication RSA SecurID ▾

□ Enforce SecurID and Windows user name matching

☑ Clear node secret

RSA authentication agent configuration file (sdconf.rec): Upload File..

✓ A sdconf.rec is already uploaded

View Administrator Authentication

Changes to authentication settings will take effect on next user login

Smart card authentication for administrators: Not allowed ▾

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**.