# VMware, Inc.
## View Connection Server 4

# RSA SecurID Ready Implementation Guide

Last Modified: November 19, 2009

## Partner Information

| Product Information | |
|---|---|
| **Partner Name** | VMware, Inc. |
| **Web Site** | www.vmware.com |
| **Product Name** | View Connection Server |
| **Version & Platform** | 4.0 |
| **Product Description** | VMware View Connection Manager 4 is an enterprise-class connection broker that provides secure connectivity between remote clients and centralized virtual desktops. |
| **Product Category** | Remote Access |

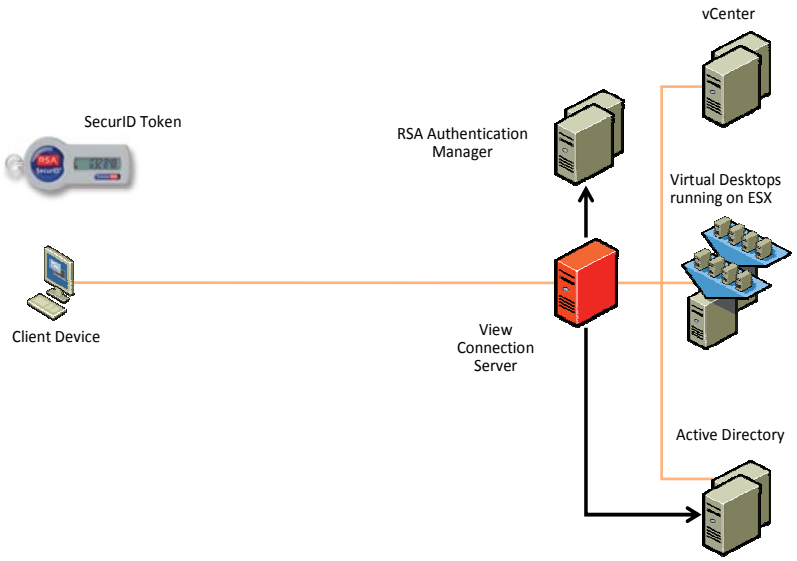
## Solution Summary

VMware View delivers end-to-end desktop control and manageability while providing a familiar user experience. VMware View Connection Server 4 is an enterprise-class connection broker that provides secure connectivity between remote clients and centralized virtual desktops.

Working in conjunction with VMware vCenter, View Connection Server 4 provides optimized management and control of desktop operating systems running on VMware ESX.

By default, VMware View Connection Server 4 authenticates users using Microsoft Active Directory credentials (username, password, and domain name). As an option, View Connection Server 4 can be configured so that users are first required to authenticate using RSA SecurID. View Connection Server RSA SecurID authentication works in conjunction with RSA Authentication Manager. This optional two-factor authentication provides enhanced security for access to virtual desktops and is a standard feature of View Connection Server 4.

| **Partner Integration Overview** | |
|---|---|
| **Authentication Methods Supported** | Native RSA SecurID Authentication |
| **RSA SecurID Library Version Used** | 5.03 |
| **RSA Authentication Manager Replica Support *** | Full Replica Support |
| **Secondary RADIUS Server Support** | No |
| **RSA Authentication Agent Host Type for 7.1** | Standard Agent |
| **RSA SecurID User Specification** | Designated Users, All Users, Default Method |
| **RSA SecurID Protection of Administrative Users** | No |
| **RSA Software Token and RSA SecurID 800 Automation** | No |
| * = Mandatory Function when using Native SecurID Protocols | |



# Product Requirements

This document assumes that VMware View Connection Server is installed in an environment that is properly protected by RSA Authentication Manager and that the reader has a basic functional knowledge of RSA Authentication Manager and VMware View Connection Server.

### View Connection Server 4 SecurID Authentication Requirements

RSA SecurID authentication is a standard feature of VMware View Connection Server 4. An RSA Authentication Manager is required and must be directly IP network accessible from each View Connection Server. To use RSA SecurID token authentication, each user must have a SecurID token that is registered with the RSA Authentication Manager.

| **Operating System** | |
|---|---|
| **Microsoft Windows Server 2003 Standard** | SP2 |
| **Microsoft Windows Server 2003 R2 Standard** | SP2 |
| **Microsoft Windows Server 2003 Enterprise** | SP2 |
| **Microsoft Windows Server 2003 R2 Enterprise** | SP2 |
| **Additional Software Requirements** | |
| **Active Directory** | All Patch Levels Supported |

# Authentication Agent Configuration

To facilitate communication between the VMware View Connection Server 4 and the RSA Authentication Manager / RSA SecurID Appliance, an Authentication Agent record must be added to the RSA Authentication Manager database. The Authentication Agent record identifies the VMware View Connection Server 4 within its database and contains information about communication and encryption.

To create the Authentication Agent record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Authentication Agent Record, you should configure the View Connection Server 4 as Standard Agent. This setting is used by the RSA Authentication Manager to determine how communication with the View Connection Server 4 will occur.

**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 Security documentation for additional information about creating, modifying, and managing Authentication Agent records.

# RSA SecurID files

| RSA SecurID Authentication Files | |
|---|---|
| **Files** | **Location** |
| sdconf.rec | %SystemRoot%\System32\sdconf.rec |
| Node Secret | %SystemRoot%\System32\securid |

# VMware View Connection Server 4 Configuration

## *Before You Begin*

This section provides instructions for integrating VMware View Connection Server 4 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 vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

VMware View Connection Server is normally implemented on multiple servers to provide high availability and to meet scalability requirements. Each View Connection 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 View Connection 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.

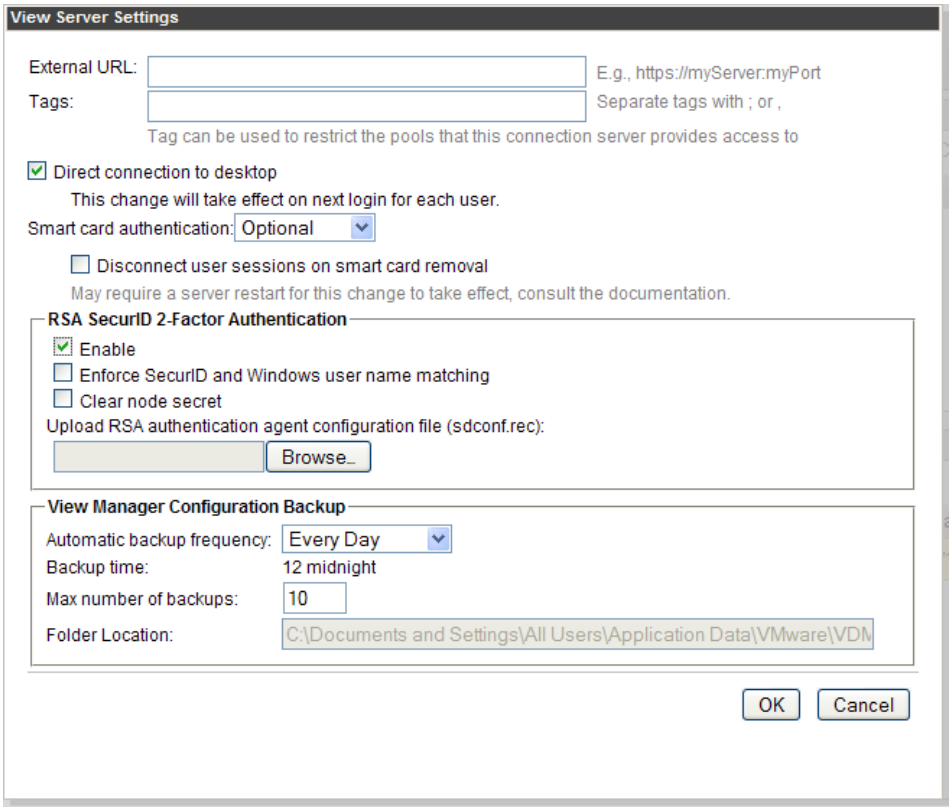
It is possible in a multi-server View Connection Server deployment to have some servers enabled for RSA SecurID authentication and to have others disabled. This scenario can be used to force RSA SecurID authentication for users accessing the View Connection Server environment remotely over the Internet.

## *Enable View Connection Server RSA SecurID Authentication*

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

1. Log into the web browser based **View Administrator** using an administrator username and password.
2. From the **View Administrator** Configuration page, select a View Connection Server (listed under Servers->View Servers) and click **Edit**.

3. Under **RSA SecurID 2-Factor Authentication**, select the **Enable** checkbox as shown below.




4. 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.
5. Upload the sdconf.rec file for this server. Click **Browse** and select the sdconf.rec file. The sdconf.rec file was earlier exported from the RSA Authentication Manager. It is important that the sdconf.rec file imported is the correct files for this particular server.

> **Note: There is no need to restart the View Connection Server after making these configuration changes. The necessary configuration files for each View Connection Server are automatically distributed and the RSA SecurID configuration takes effect immediately.**

## *RSA SecurID Login with VMware View Client for Windows*

This section gives details about the end user interface for VMware View 4 when configured for RSA SecurID authentication. This section shows dialogs from the VMware View Client for Windows, which is a native Windows client for View Connection Server 4. View Connection Server 4 also supports a web browser based View Web Access client application. View Web Access uses similar dialogs for RSA SecurID authentication but they are presented through a browser interface.

When a user connects to a View Connection Server that has RSA SecurID authentication enabled, they are presented with a specific 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 **OK**. 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 presented with a new PIN prompt. Users choose a new PIN and click **OK**. After users set a new PIN, they are prompted to wait for the next tokencode before being able to log in.

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

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

# Certification Checklist for RSA Authentication Manager 7.x

Date Tested: November 19, 2009

| Certification Environment | | |
|---|---|---|
| **Product Name** | **Version Information** | **Operating System** |
| **RSA Authentication Manager** | 7.1 | Microsoft Windows Server 2003 |
| **VMware View Connection Server** | 4.0 | Microsoft Windows Server 2003 |

| Mandatory Functionality | | | |
|---|---|---|---|
| **RSA Native Protocol** | | **RADIUS Protocol** | |
| **New PIN Mode** | | | |
| Force Authentication After New PIN | ✓ | Force Authentication After New PIN | N/A |
| System Generated PIN | ✓ | System Generated PIN | N/A |
| User Defined (4-8 Alphanumeric) | ✓ | User Defined (4-8 Alphanumeric) | N/A |
| User Defined (5-7 Numeric) | ✓ | User Defined (5-7 Numeric) | N/A |
| Deny 4 and 8 Digit PIN | ✓ | Deny 4 and 8 Digit PIN | N/A |
| Deny Alphanumeric PIN | ✓ | Deny Alphanumeric PIN | N/A |
| Deny Numeric PIN | ✓ | Deny Numeric PIN | N/A |
| PIN Reuse | ✓ | PIN Reuse | N/A |
| **Passcode** | | | |
| 16 Digit Passcode | ✓ | 16 Digit Passcode | N/A |
| 4 Digit Fixed Passcode | ✓ | 4 Digit Fixed Passcode | N/A |
| **Next Tokencode Mode** | | | |
| Next Tokencode Mode | ✓ | Next Tokencode Mode | N/A |
| **Load Balancing / Reliability Testing** | | | |
| Failover (3-10 Replicas) | ✓ | Failover | N/A |
| No RSA Authentication Manager | ✓ | No RSA Authentication Manager | N/A |
| **Additional Functionality** | | | |
| **RSA Software Token Automation** | | | |
| System Generated PIN | N/A | System Generated PIN | N/A |
| User Defined (8 Digit Numeric) | N/A | User Defined (8 Digit Numeric) | N/A |
| Next Tokencode Mode | N/A | Next Tokencode Mode | N/A |
| **RSA SecurID 800 Token Automation** | | | |
| System Generated PIN | N/A | System Generated PIN | N/A |
| User Defined (8 Digit Numeric) | N/A | User Defined (8 Digit Numeric) | N/A |
| Next Tokencode Mode | N/A | Next Tokencode Mode | N/A |

DRP / PAR

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