RSA SecurID Ready Implementation Guide

Last Modified: January 15, 2008

Partner Information

Product Information	
Partner Name	VMware Inc.
Web Site	www.vmware.com
Product Name	Virtual Desktop Manager
Version & Platform	2.0 (build 378)
Product Description	VMware Virtual Desktop Manager 2 is an enterprise-class connection broker that provides secure connectivity between remote clients and centralized virtual desktops.
Product Category	Remote Access

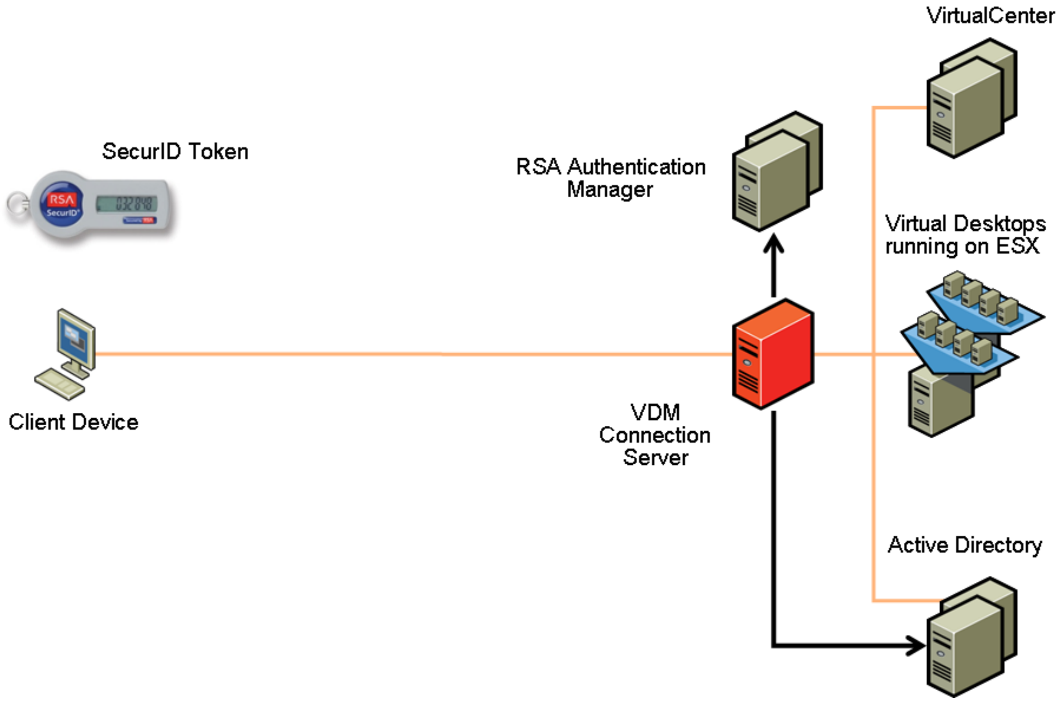
Solution Summary

VMware Virtual Desktop Infrastructure (VDI) delivers end-to-end desktop control and manageability while providing a familiar user experience. VMware Virtual Desktop Manager (VDM) 2 is an enterprise-class connection broker that provides secure connectivity between remote clients and centralized virtual desktops.

Working in conjunction with VMware VirtualCenter, VDM 2 provides optimized management and control of desktop operating systems running on VMware ESX.

By default, VMware VDM 2 authenticates users using Microsoft Active Directory credentials (user name, password and domain name). As an option, VDM 2 servers can be configured so that users are first required to authenticate using RSA SecurID. VDM 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 VDM 2.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication
List Library Version Used	5.0.3
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
RSA Authentication Agent Host Type	Net OS
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



Product Requirements

This document assumes that VMware VDM 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 VDM.

Note: The information given here in the Product Requirements and Agent Host Configuration sections should only be used as a guide.

Software product requirements may change from time to time. Please refer to the appropriate RSA Security and VMware VDM documentation for complete and up to date product requirements, installation and configuration details.

VDM 2 SecurID Authentication Requirements

RSA SecurID authentication is a standard feature of VMware VDM 2. An RSA Authentication Manager server is required and must be directly IP network accessible from each VDM 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 Support

VDM 2 Connection Server must be installed on a server running Microsoft Windows Server 2003. This server must be joined to an Active Directory domain.

Agent Host Configuration

To facilitate communication between the VMware VDM 2 server 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 VDM Connection Server within its database and contains information about communication and encryption.

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

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the VMware VDM 2 Server as a **Net OS Agent** type. This setting is used by the RSA Authentication Manager to determine how communication with the VMware VDM 2 server will occur.

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

In a multi-server VDM deployment involving a standard instance and replica instances you must add an Agent Host record for each VDM Connection Server that is configured for RSA SecurID authentication.

VMware VDM 2 Server Configuration

Configuration Overview

This section provides instructions for integrating VMware VDM 2 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.

VDM Connection Server is normally implemented on multiple servers to provide high availability and to meet scalability requirements. Each VDM 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 (user name, password and domain name).

If RSA SecurID is enabled on a VDM Connection Server then users of this server are first required to supply their RSA SecurID user name 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 VDM deployment to have some servers enabled for RSA SecurID authentication and to have others disabled. For example, this scenario can be used to force RSA SecurID authentication for users accessing the VDM environment remotely over the Internet.

Before You Begin

All VMware VDM 2 components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

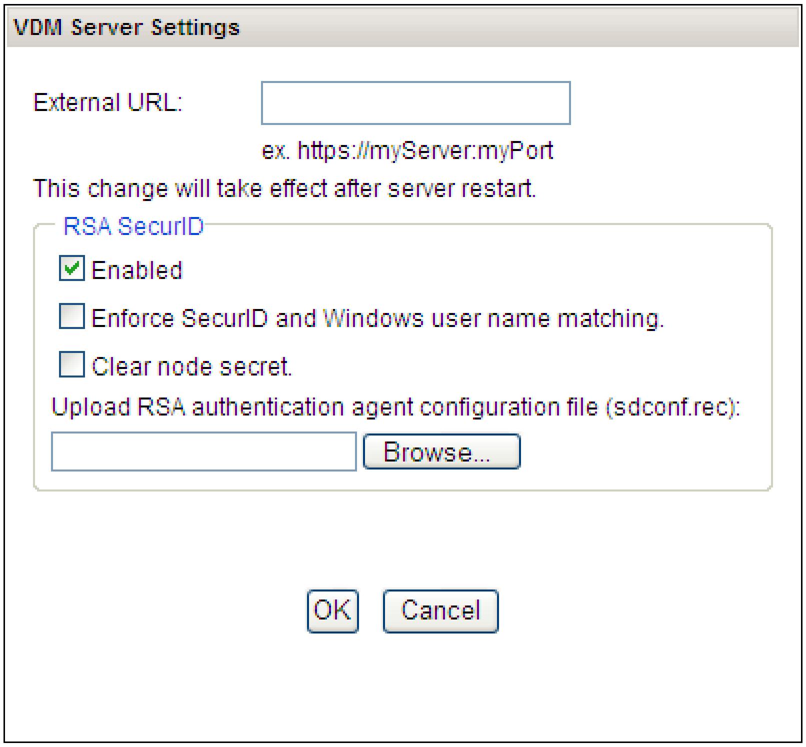
Ensure that the RSA Authentication Manager is configured correctly. Specifically, ensure that there is an Agent Host entry for every VDM Connection Server. The procedure for this is described in the previous section.

For user authentication with RSA SecurID, user entries must first be added to RSA Authentication Manager and each user must have an assigned RSA SecurID token or password.

Enable VDM RSA SecurID Authentication

The following steps to configure each VDM Connection Server for RSA SecurID authentication, are carried out using the Web based VDM Administrator application.

1. Log in to the Web based VDM Administrator using an administrator username and password.
2. From the VDM Administrator Configuration page, select a VDM Connection Server (listed under VDM Servers) and click Edit.
3. Under RSA SecurID, select the Enabled checkbox as shown below.



External URL:

ex. https://myServer:myPort

This change will take effect after server restart.

RSA SecurID

☑ Enabled

□ Enforce SecurID and Windows user name matching.

□ Clear node secret.

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

4. Decide if RSA SecurID user names must match user names used in Active Directory. If they should be forced to match then select this option. In this case the user will be forced to use the same RSA SecurID user name for Active Directory authentication. If this option is not selected, the names are allowed to be different.

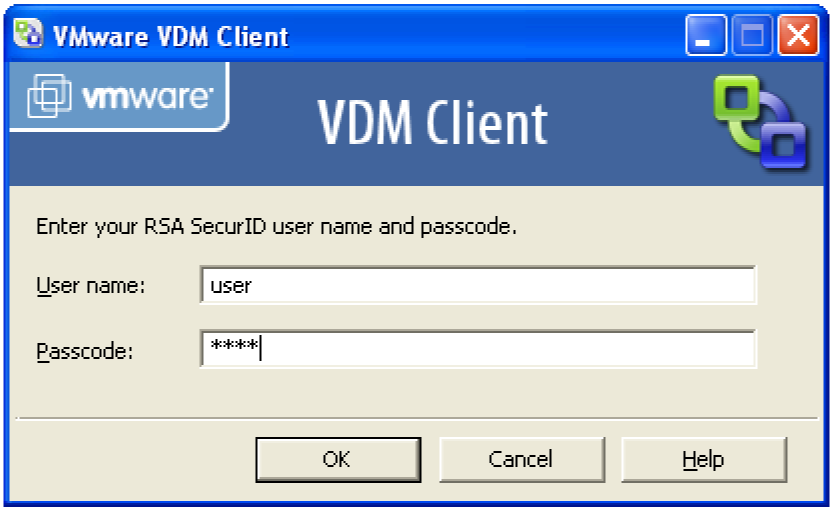
5. Upload the sdconf.rec file for this server. Click Browse and select the sdconf.rec file. The sdconf.rec file was earlier exported from RSA Authentication Manager. It is important that the sdconf.rec file imported is the correct file for this particular server.

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

RSA SecurID Login with VMware VDM Client

This section gives details about the end-user interface for VMware VDM 2 when configured for RSA SecurID authentication. This section shows dialogs from VDM Client, which is a native windows client for VDM 2. VDM 2 also supports a web based VDM Web Access client application. VDM Web Access uses similar dialogs for RSA SecurID authentication but these are presented through a browser interface.

When a user connects to a VDM Connection Server that has RSA SecurID authentication enabled, they are presented with a specific VDM RSA SecurID login prompt as shown below.



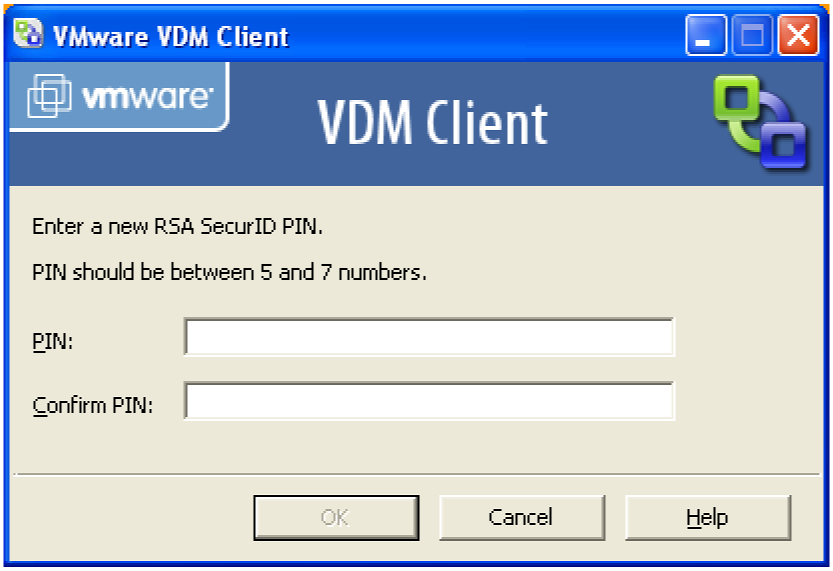
Enter your RSA SecurID user name and passcode.

User name: user

Passcode: ****

Users enter their RSA SecurID user name (which may be the same as their Active Directory user name). 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 user name and passcode, they are presented with a prompt as shown below. Users enter a new PIN in both places and click **OK**.



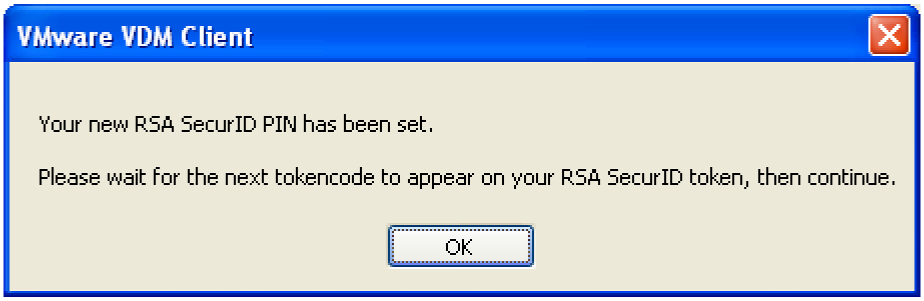
Enter a new RSA SecurID PIN.

PIN should be between 5 and 7 numbers.

PIN:

Confirm PIN:

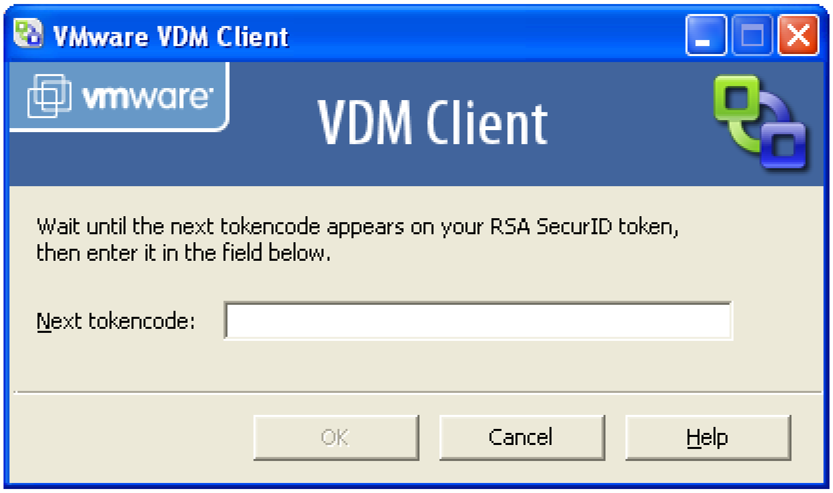
After users set a new PIN, they are prompted to wait for the next tokencode before being able to log in.



Your new RSA SecurID PIN has been set.

Please wait for the next tokencode to appear on your RSA SecurID token, then continue.

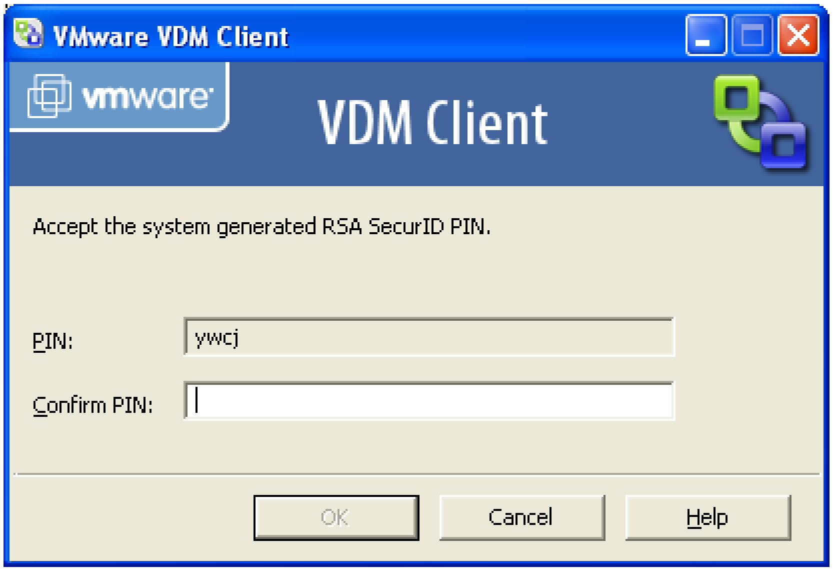
Similarly, if users are required to enter their next RSA SecurID tokencode they are presented with a prompt as follows.



Wait until the next tokencode appears on your RSA SecurID token, then enter it in the field below.

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 dialog box to confirm the PIN as shown below.

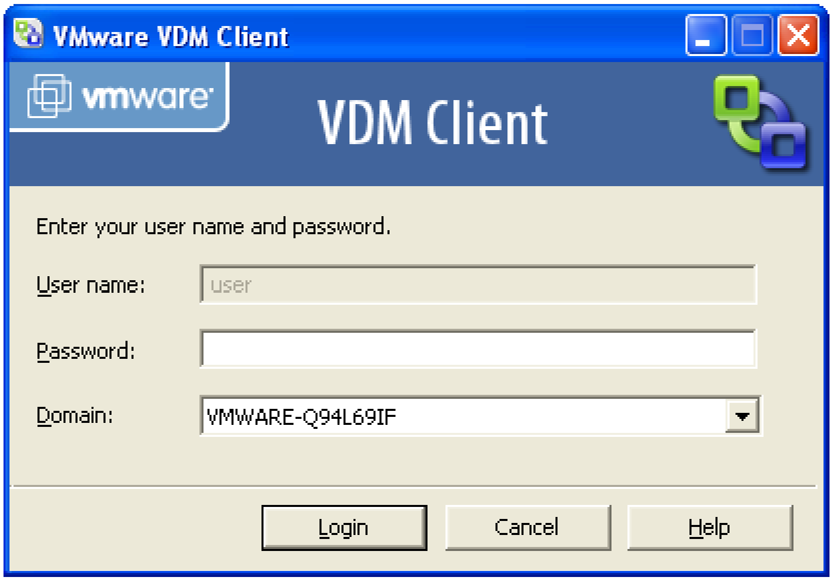


Accept the system generated RSA SecurID PIN.

PIN: ywcj

Confirm PIN:

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.



Enter your user name and password.

User name: user

Password:

Domain: VMWARE-Q94L69IF

Note that the User name is grayed out in the above dialog box and so users cannot change it. This is the case when the VDM Server is configured to force RSA SecurID and Windows username matching. If it is not configured in this way, the users are free to enter a different user name.

Certification Checklist for RSA Authentication Manager

Date Tested: January 9, 2008

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	6.1 [300]	Microsoft Windows Server 2003
RSA Authentication Agent	Java Library Version 5.03	Microsoft Windows Server 2003
VMware Virtual Desktop Manager	2.0	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
User Selectable	✓	User Selectable	N/A
Deny 4 and 8 Digit PIN	✓	Deny 4 and 8 Digit PIN	N/A
Deny Alphanumeric PIN	✓	Deny Alphanumeric PIN	N/A
Passcode			
16 Digit Passcode	✓	16 Digit Passcode	N/A
4 Digit Password	✓	4 Digit Password	N/A
Next Tokencode Mode			
Next Tokencode Mode	✓	Next Tokencode Mode	N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	Failover	N/A
Name Locking Enabled	✓	Name Locking Enabled	
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
User Selectable	N/A	User Selectable	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
User Selectable	N/A	User Selectable	N/A
Next Tokencode Mode	N/A	Next Tokencode Mode	N/A
Credential Functionality			
Determine Cached Credential State	N/A	Determine Cached Credential State	
Set Credential	N/A	Set Credential	
Retrieve Credential	N/A	Retrieve Credential	

INIT / PAR

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