

VMware Virtual Desktop Manager User Authentication Guide

VMware Virtual Desktop Manager

The purpose of this guide is to provide details of user authentication in VMware® Virtual Desktop Manager (VDM). It explains how users log in to VDM and describes the infrastructure that supports user authentication.

This guide is intended for architects and system administrators who need more information about user authentication in VDM. This guide covers user authentication options using Microsoft Active Directory and RSA SecurID and includes deployment scenarios within an enterprise infrastructure.

The screenshots in this guide are from VDM Client. The user interface for VDM Web Access and thin client devices is similar but are not shown in this guide.

- [VDM Overview](#)
- [VDM User Authentication](#)
- [Active Directory Authentication](#)
- [RSA SecurID Authentication](#)

VDM is a key component in the VMware Virtual Desktop Infrastructure (VDI) solution. VDM is an enterprise class virtual desktop manager that securely connects authorized users to centralized virtual desktops. It works with VMware Virtual Infrastructure 3 to provide a complete, end-to-end VDI solution that improves control and manageability and provides a familiar desktop experience.

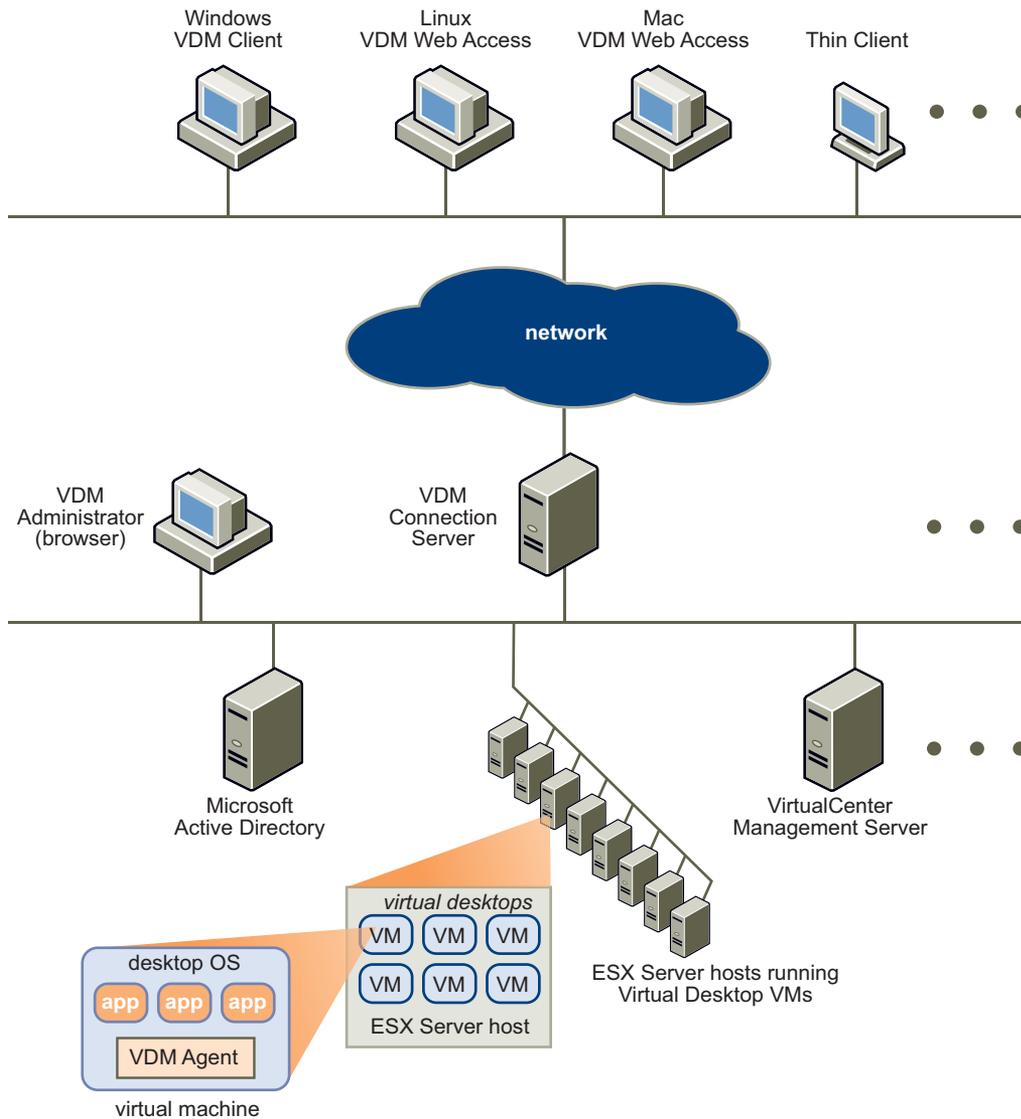
VDM Overview

VDM includes the following key components:

- VDM Connection Server
- VDM Agent
- VDM Client
- VDM Web Access
- VDM Administrator

Figure 1 shows the physical topology of a VDI infrastructure with VDM and shows the relationship between the main VDM components.

Figure 1. VMware VDI Infrastructure with VDM - Physical Topology



VDM Connection Server

The VDI connection broker that manages secure access to virtual desktops and works with VirtualCenter to provide advanced management capabilities. It is installed on Microsoft Windows Server 2003 on a server that is part of an Active Directory domain.

VDM Connection Server is installed as one of the following instances:

- Standard—This instance appears in [Figure 1](#). It provides stand-alone functionality and is used as the only VDM Connection Server (or the first of a group of VDM Connection Servers that act as part of a high-availability, fully replicated group).
- Replica— This instance is installed as a second or subsequent VDM server in a high-availability group. Configuration data is initialized from an existing VDM Server and is automatically replicated between VDM group members.
- Security Server—This instance implements a subset of the VDM Connection Server functionality and is used in a demilitarized zone (DMZ) deployment. A VDM security server does not need to be in an Active Directory domain. The standard and replica instances automatically include the Security Server functionality.

The instance type is selected during VDM Connection Server installation.

High-availability and DMZ deployments of VDM Connection Server using replica and security server instances are described in *Introduction to Virtual Desktop Manager*.

Configuration data is stored in an embedded LDAP directory on each Standard and Replica instance.

VDM Agent

VDM Agent runs on each virtual desktop and is used for session management and single sign-on. With VDM Client, this component supports optional USB device redirection. VDM agent can be installed on a virtual machine template so that virtual desktops created from that template automatically include the VDM Agent.

Place virtual desktops in one of these Active Directory domains:

- The same domain to which VDM Connection Servers are joined
- A domain with a trust agreement with the VDM Connection Server domain

When users connect to their virtual desktop, they are automatically logged on using the same credentials they use to log on to their domain. During installation, VDM Agent can disable this single sign-on feature. If the virtual desktop is not part of a domain or is part of a domain with which it has no trust agreement, and single sign-on is not available, the user must manually log on to the virtual desktop.

VDM Client

VDM Client runs on a Windows PC as a native Windows application and allows users to connect to their virtual desktops through VDM. This component connects to a VDM Connection Server and allows the user to log on using any of the supported authentication mechanisms. After users log on, they can select from the list of virtual desktops for which they are authorized. This step provides remote access to their virtual desktops and provides users with familiar desktop experiences.

VDM Client also works closely with VDM Agent to provide enhanced USB support. Basic USB support (such as USB drives and USB printers) is supported without VDM USB support, but VDM extends this support to include additional USB devices. You can specify VDM USB support in VDM Client during the installation.

VDM Web Access

VDM Web Access is similar to VDM Client but provides a VDM user interface through a Web browser. VDM Web Access is included automatically during the VDM Connection Server installation. VDM Web Access is supported on Linux and Apple Mac OS/X, but this Web access does not support VDM USB extensions. All necessary VDM software is installed automatically on the client through the Web browser. VDM Web Access on Linux uses rdesktop and on Apple Macintosh OS/X uses Microsoft Remote Desktop Connection Client for Mac.

VDM Web Access can also be used on a Windows client with VDM Client. A user obtains the required software on their client device by accessing a VDM Connection Server with a Web browser. If the VDM Client software is installed with USB support by a user with administrative rights, VDM Web Access on Windows has complete VDM USB support.

VDM Administrator

VDM Administrator provides VDM administration through a Web browser. It is used by VDM administrators to make configuration changes and manage virtual desktops and entitlements of desktops of Windows users and groups

VDM Administrator also provides an interface to monitor log events on a VDM Server and is installed with VDM Connection Server. For more information on the VDM Connection Server components and their relationship with other VDM components, see *Introduction to Virtual Desktop Manager*.

VDM User Authentication

To log in to VDM, users enter their Microsoft Windows credentials at the login prompt to validate their identity and access their virtual desktops.

As an added level of security, VDM can be configured to require RSA SecurID authentication that requires the use of a SecurID token for each user. As part of the login process, users must enter their SecurID user name with their SecurID PIN and tokencode. After their SecurID credentials are verified, users are prompted for their Windows credentials.

Active Directory Authentication

VDM Connection Server must be joined to an Active Directory domain, which can be Windows Server 2000 or Windows Server 2003 Active Directory.

During the installation of VDM Connection Server (standard and replica instances), a check is made to ensure that the server is joined to an Active Directory domain and that the current domain trust relationship is valid. Before connecting to their virtual desktops, VDM must authenticate users with their Active Directory domain credentials.

After users enter their domain credentials using VDM Client, VDM Web Access, or a thin client device, VDM Connection Server performs an authentication check. This check is performed by VDM Connection Server against Active Directory. The domain is selected from a drop-down menu that contains the domains to which the VDM Server is joined and all domains with which a trust relationship exists.

By authenticating users against existing Active Directory infrastructure, an organization can simplify the operational management of VDM by ensuring that the management of all user accounts is handled in Active Directory. For example, if a user account is disabled in Active Directory, that user cannot log into VDM. Also, account policies (such as restricting the permitted hours of login, password expiration, and so on) are handled through existing Active Directory operational procedures.

When users establish a session to a virtual desktop, VDM automatically logs them on to that desktop operating system using the same Active Directory credentials that they used to log on to VDM Connection Server. This single sign-on capability works whenever the virtual desktop is joined to the same Active Directory domain as the VDM Connection Server or to a domain that has a trust relationship with the VDM Connection Server domain. If the virtual desktop is joined to another domain or workgroup, the user must log into the virtual desktop operating system manually.

Active Directory Multi-Domain Authentication

For multi-domain Active Directory environments, a VDM user can authenticate to the domain of the VDM Connection server and any domains with which a trust relationship exists. If no Active Directory trusts or limited trusts exist between domains, it might be necessary to deploy multiple VDM Connection Server environments so that all users can use VDM.

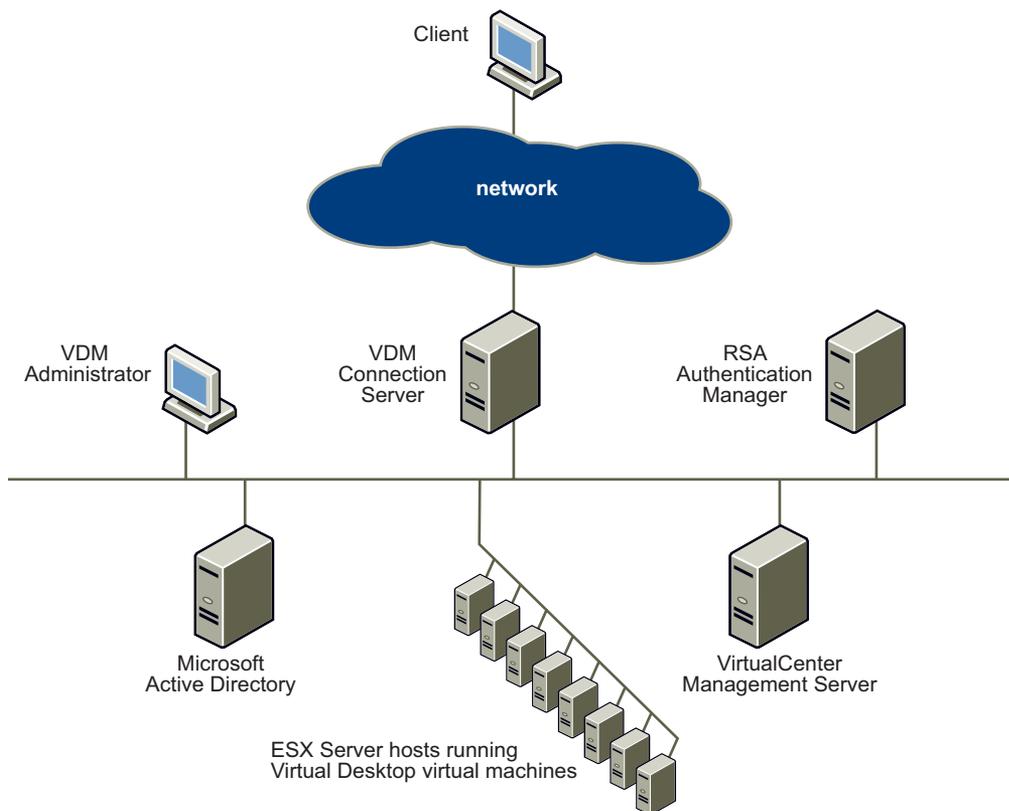
Suppose three domains exist. An Active Directory trust relationship exists between DomainA and DomainB. DomainC is an isolated domain with no trust relationships. A VDM Connection Server joined to DomainA supports VDM user authentication for DomainA and DomainB users but not for DomainC. A second VDM Connection Server environment can be joined to DomainC, so DomainC users can log on to that environment.

RSA SecurID Authentication

VDM servers can be configured so that users must first be authenticated using RSA SecurID. VDM is an RSA Secured product, which means that it has passed RSA certification tests conducted by the RSA Secured Partner program. RSA SecurID authentication is supported for VDM Client and VDM Web Access.

RSA SecurID authentication works with RSA Authentication Manager. This optional authentication provides enhanced security for accessing virtual desktops and is a standard feature of VDM. As shown in [Figure 2](#), a VDM environment with an additional server is used to run RSA Authentication Manager.

Figure 2. VDM Environment with RSA Authentication Manager



Configuring RSA Authentication Manager

Use the Product Requirements and Agent Host Configuration sections as a guide. Software product requirements change from time to time. For more information, see RSA Security and VDM documentation.

To facilitate communication between VDM Connection Server and the RSA Authentication Manager and 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 in its database and contains information about communication and encryption.

To create the Agent Host record, you need the host name and IP addresses for all network interfaces. When adding the Agent Host Record, configure VDM Server as a Net OS Agent type. This setting is used by the RSA Authentication Manager to determine how communication with the VMware VDM server occurs. Host names in the RSA Authentication Manager and RSA SecurID Appliance must resolve to valid IP addresses on the local network.

In a multi-server VDM deployment that involves 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.

To add a Host Agent record for each VDM Connection Server

- 1 On the computer with **RSA Authentication Manager**, choose **Start > All Programs > RSA Security > RSA Authentication Manager Host Mode**.
- 2 Choose **Agent Host > Add Agent Host**.
- 3 In **Name**, enter the fully qualified domain name of the VDM Connection Server.
- 4 In **Network address**, enter the IP Address of the VMware VDM Connection Server.
- 5 In the **Agent Type** drop-down menu, select **Net OS Agent**.
- 6 Leave the **Enable Windows Password Integration** check box deselected.

The Agent Host is added.

- 7 Export a set of configuration files for this host.

The `sdconf.rec` file must be imported to each VDM Connection Server as follows:

- a Run **Agent Host > Generate Configuration Files**
- b Select **One Agent Host** and click **OK**.
- c From the list of servers, select the specific VDM Connection Server to extract the `sdconf.rec` file for this VDM Connection Server.

For more information on creating, modifying, and managing the Agent Host records, see RSA Security documentation.

Configuring VDM for RSA SecurID Authentication

After the RSA Authentication Manager is configured `sdconf.rec` file is exported, VDM Administrator is used to configure each VDM Connection Server for RSA SecurID Authentication.

To Configure VDM for RSA SecurID Authentication

- 1 Log in to the Web-based VDM Administrator with your administrator user name and password.
- 2 From the **VDM Administrator Configuration** page, under **VDM Servers**, select a VDM Connection Server and click **Edit**.
- 3 Under **RSA SecurID**, select the **Enabled** check box.
- 4 (Optional) If RSA SecurID user names need to match user names used in Active Directory, select the **Enforce SecureID and Windows user name matching** check box.

The user is forced to use the same RSA SecurID user name for Active Directory authentication. If this option is not selected, the user name can be different.

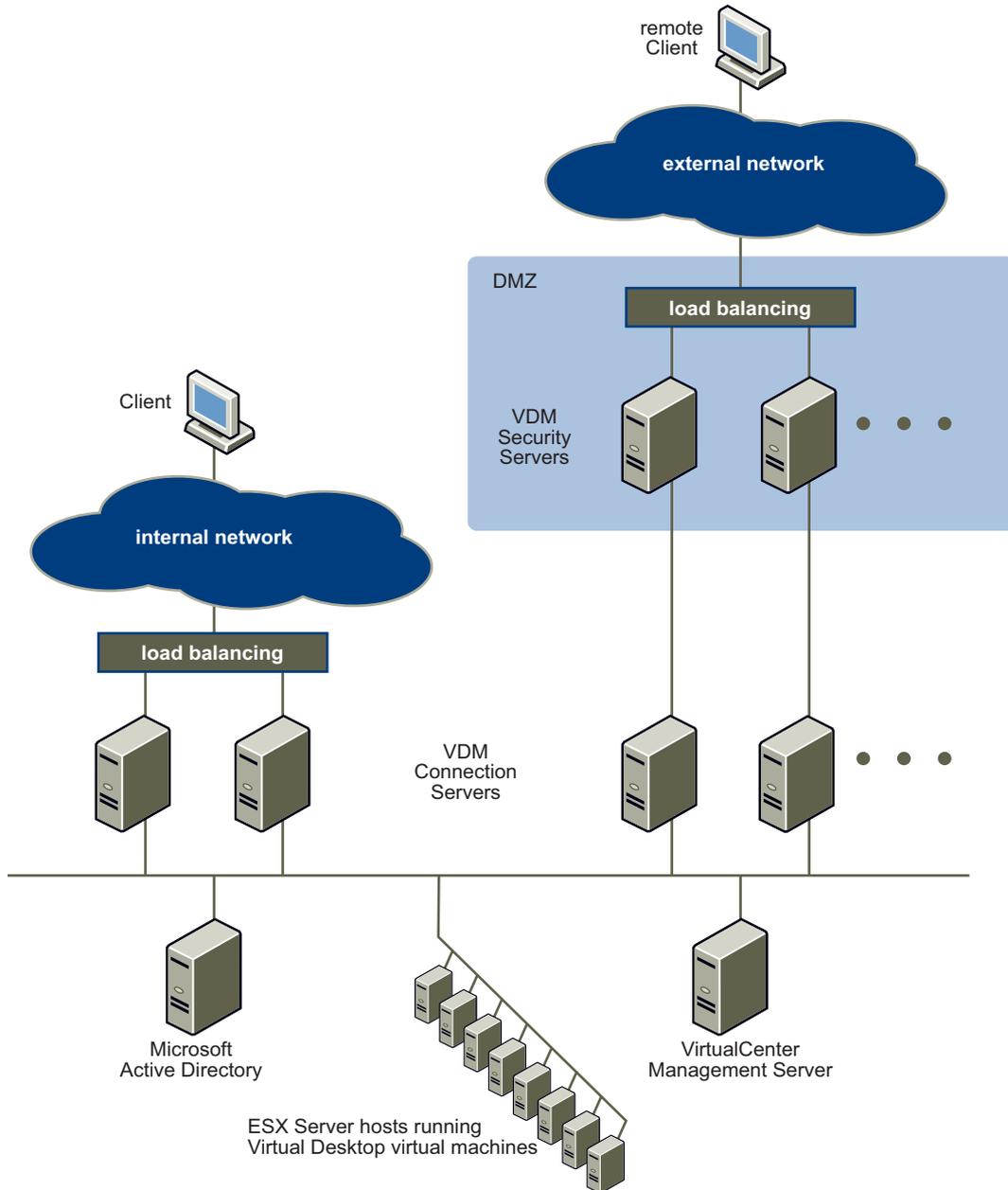
- 5 Upload the `sdconf.rec` file for this server.
- 6 Click **Browse** and select the `sdconf.rec` file.

The `sdconf.rec` file was exported earlier from RSA Authentication Manager. This imported file must be the correct file for this particular VDM Connection Server for RSA SecurID Authentication to work.

Users do not 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.

In a multi-server VDM deployment, users can configure only some VDM Connection Servers for RSA SecurID. This scenario can be used if some VDM Connection Servers are used to support Internet clients and others are used to support internal network clients. If only the Internet-serving VDM Connection Servers are configured for RSA SecurID, then only the Internet clients are required to authenticate with RSA SecurID.

Figure 3. External and Internal Clients Accessing VDM Connection Servers



Using the RSA SecurID Login for VDM Client

When users connect to a VDM Connection Server that has RSA SecurID authentication enabled, they must use the RSA SecurID login to connect from VDM Client or VDM Web Access. The following steps describe how to use the RSA SecureID login to connect to a VDM Connection Sever from VDM Client.

To use the SecurID login for VDM Client

- 1 Enter your RSA SecurID user name.

Your SecurID user name can be the same as your Active Directory user name.

- 2 Enter your passcode and click **OK**.

An RSA SecurID passcode comprises a PIN code and a tokencode. If you need to enter a new RSA SecurID PIN after entering your RSA SecurID user name and passcode, you are prompted to enter this information.

- 3 Enter a new PIN in both fields and click **OK**.

After users create a new PIN, they are prompted to wait for the next tokencode before logging in.

Similarly, if users are required to enter their next RSA SecurID tokencode, they are prompted to do so.

System-generated PINs are also supported. If the RSA Authentication Manager is configured to use system-generated PINs, users are prompted to confirm their PIN.

If the RSA SecurID details are correct as validated against RSA Authentication Manager, users are prompted to reenter their Active Directory credentials.

If VDM Server is configured to force RSA SecurID and Windows user name matching, the **User name** field is dimmed. If VDM Server is not configured this way, users can enter a different user name.

If you have comments about this documentation, submit your feedback to: docfeedback@vmware.com

VMware, Inc. 3401 Hillview Ave., Palo Alto, CA 94304 www.vmware.com

Copyright © 2008 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102, 7,290,253, and 7,356,679; patents pending. VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Revision 20080527 Item: EN-000040-00
