

Installation and Administration Guide

VMware Virtual Desktop Manager 2.1

Installation and Administration Guide

Revision: 20080619

Item: VDM-ENG-Q208-450

You can find the most up-to-date technical documentation on our Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2008 VMware, Inc. All rights reserved. Protected by one or more 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.

VMware, Inc.

3401 Hillview Ave.

Palo Alto, CA 94304

www.vmware.com

Contents

About This Book	7
1 VDM Quick Start Guide	9
Hardware Requirements	10
Prerequisites	10
Preinstallation Checklist	11
Prepare Desktop Virtual Machines	11
Installing the VDM Connection Server	13
Single-Server Installation	13
One-Time Configuration	14
Creating Desktops	15
Creating an Individual Desktop	15
Entitling a Desktop	17
Connecting to Desktops	17
2 VDM Introduction and System Requirements	19
VDM Overview	19
System Requirements	21
VDM Connection Server	21
Connection Server Hardware Requirements	21
Connection Server Supported Operating Systems	22
VDM Client	22
VDM Client Supported Operating Systems	22
VDM Web Access	23
VDM Agent Virtual Desktop	24
Prerequisites	24
Upgrading VDM	25
3 Installing and Configuring VDM	27
Prepare Desktop Virtual Machines	28
Using the VDM Agent on Virtual Machines with Multiple NICs	30
Installing the VDM Connection Server	30

- Single-Server Installation 30
- Multiserver Installation 32
- One-Time Configuration 33
 - Enabling and Disabling a VDM Connection Server 34
- End-to-End Configuration 35
 - Configuration for a Pooled Desktop 36
 - VirtualCenter Permissions for VDM 37
 - Advanced Pool Settings 42
 - Advanced Pooling Example Scenarios 43
 - Entitling a Desktop 45
 - Connecting to Desktops 45
 - Changing End User Passwords 47
 - Setting the Default Desktop for Thin Client Users 47
 - Setting an Externally Resolvable Name on a Connection Server 48
- VDM Administrator User Interface 49
 - Inventory Page 49
 - Configuration Page 51
 - Events Page 52
- Searching Desktops and Entitled Users and Groups 52
 - Working with Active Sessions 53
- Global Configuration Settings 54
- Viewing Events 56
- RSA SecurID 56
- Deleting VDM Objects 57
- Installing SSL Certificates 58
 - Creating the CSR 59
- Load Balancing 62
 - Load Balancing in a Non-DMZ Deployment 63
 - Session Setup and Load Balancing 63
 - DNS Requirements for a Load-Balanced Solution 64
 - Load-Balancing Solution 64
- DMZ Deployment 65
 - DMZ Installation 65
 - Load Balancing in a DMZ Deployment 67
 - Configuring Firewall Ports for DMZ Deployments 67
- Exporting and Importing VDM Configuration Data 69
- Client Command-Line Parameters 69
- Collecting VDM Diagnostic Information 70
 - Using the VDM Support Tool to Collect Diagnostic Information 70
 - Using the VDM Support Script to Collect Diagnostic Information 71

Updating Support Requests	72
Troubleshooting VDM	72
A VDM Client Advanced Active Directory RDP Settings	73
Using Active Directory Group Policies for Advanced Settings	76
B VDM Group Policy Objects	77
Computer Configuration	77
VDM Agent Configuration	77
VDM Client Configuration	78
VDM Server Configuration	79
VDM User Configuration for VDM Client	80
Glossary	83
Index	87

About This Book

This manual, the *Installation and Administration Guide* describes setting up, installing, and configuring VMware® Virtual Desktop Manager, including how to install the various software components, how to deploy servers, and how to configure and connect to virtual desktops. It also describes how to set up load balancing and security, supported operating systems, and thin client devices.

This chapter includes these topics:

- “Intended Audience” on page 7
- “Document Feedback” on page 7
- “Technical Support and Education Resources” on page 8

Intended Audience

This manual is intended for anyone who wants to install, administrate, or configure VDM. The information in this manual is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to:

docfeedback@vmware.com

Technical Support and Education Resources

The following sections describe the technical support resources available to you. You can access the most current versions of this manual and other books by going to:

<http://www.vmware.com/support/pubs>

Online and Telephone Support

Use online support to submit technical support requests, view your product and contract information, and register your products. Go to <http://www.vmware.com/support>.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

Find out how VMware support offerings can help meet your business needs. Go to <http://www.vmware.com/support/services>.

VMware Education Services

VMware courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. For more information about VMware Education Services, go to <http://mylearn1.vmware.com/mgreg/index.cfm>.

VDM Quick Start Guide

1

This chapter describes the VDM administrator user interface and basic installation instructions. It describes general guidelines to perform basic configuration and to create virtual desktops and introduces basic administration tasks.

VDM is part of the VMware Virtual Desktop Infrastructure which enables enterprises to host desktop virtual machines in their data center using VMware software and provide users access from a PC or thin client using a remote display protocol. VDM provides the software tools for setting up and configuring your virtual desktop environment.

This chapter includes these topics:

- “Hardware Requirements” on page 10
- “Prerequisites” on page 10
- “Preinstallation Checklist” on page 11
- “Prepare Desktop Virtual Machines” on page 11
- “Installing the VDM Connection Server” on page 13
- “One-Time Configuration” on page 14
- “Creating Desktops” on page 15
- “Connecting to Desktops” on page 17

Hardware Requirements

VDM requires a dedicated physical or virtual server with following specifications for running VDM:

- As a minimum, a Pentium IV 2.0Ghz processor. VMware recommends dual processors.
- As a minimum, 2GB RAM. VMware recommends 3GB RAM for deployments of 50 or more desktops.
- A minimum of one 10/100Mbps NIC. VMware recommends a 1Gbps NIC.

VDM Connection Server can be installed on either 32-bit or 64-bit hardware.

For DMZ deployments, VDM requires an additional dedicated hardware or software server with similar specifications.

For high availability deployments, each VDM Connection Server requires a dedicated physical or virtual server with similar specifications.

Prerequisites

VDM Connection Server has the following prerequisites:

- VMware Infrastructure
VMware Infrastructure 3.5 (current versions of ESX Server and Virtual Center) with at least one ESX host and one VirtualCenter instance is recommended. VMware Infrastructure 3.02 is supported.
- Servers running VDM Connection Server standard or replica instances that are joined to an Active Directory domain

NOTE VDM Connection Server does not make nor require any schema or configuration updates to Active Directory.

- Microsoft Sysprep tools installed on your VC Server
- A customization specification that permits cloned virtual machines to join the AD domain (optional)
- A valid license key for VDM

The VDM Agent, VDM Client, and VDM Web Access have the following prerequisites:

- For Windows guest desktops and Windows clients, you must have administrative privileges to install the VDM Client and the VDM Agent.

- ActiveX controls and Internet Explorer 6 or above are required for Windows client users who access their desktops using VDM Web Access.
- Web Access using Linux or Mac OS X requires Java JRE version 1.5.0 or 1.6.0.
- Microsoft Remote Desktop Connection 6.0 recommended (not required)

VMware recommends that you upgrade VDM Client machines to use Microsoft Remote Desktop Connection (RDC) 6.0. This recommendation applies to machines running Windows XP and Windows XPe. Windows 2000 does not support RDC 6.0. Windows Vista comes with RDC 6.0 installed.

RDC 6.0 can be downloaded at the Microsoft Web site.

- If connecting to a Windows Vista desktop using a Linux client, you must install the rdesktop remote desktop protocol client version 1.5.0, which you can download from the rdesktop Web site.

After you download rdesktop, follow the instructions in the readme file.

Preinstallation Checklist

Before you install VDM, consult the following checklist.

- The machine that is to act as the connection server is in the Windows domain.
- You can ping the FQDN of the connection server.
- Any previous versions of VDM are uninstalled.

Prepare Desktop Virtual Machines

Before you install the VDM software, prepare desktop virtual machines for use. Where changes in VirtualCenter are required, see the latest VirtualCenter documentation for specific steps.

Make sure that the following prerequisites are in place:

- The base desktop virtual machine to deploy to users is identified, and the latest operating system and application Service Packs and patches are installed. For Windows XP desktop virtual machines, ensure that the patch specified by Microsoft KB article 323497 (required by VDM) is installed. Information about Microsoft KB articles can be found on the Microsoft Web site.
- The latest VMware Tools are installed (provided with VI 3.5).
- Networking settings (proxies, and so forth) are properly configured in the desktop virtual machine.

- VDM Agent is installed.

NOTE For automated updating of VDM Agent in large environments, VMware recommends using standard Windows update mechanisms such as Altiris, SMS, LanDesk, BMC, or other systems management software.

- You have administrative rights to the desktop virtual machine.

To install VDM Agent

- 1 Download the VDM installer file from the VMware secure Web site to a local drive.

For information about the location of the secure Web site, contact your VMware representative.

- 2 Run `VMware-vdmagent-2.1.0-<xxx>.exe`

<xxx> is the build number of the software component you are installing in the desktop virtual machine.

The Installation wizard opens.

- 3 Click **Next**.
- 4 Accept the license terms and click **Next**.
- 5 Choose your custom setup options as follows:

- Install the VDM Authentication GINA component to restrict direct RDP connections. By default, RDP connections to the virtual machine from any source are allowed. If the VDM Authentication GINA is installed, RDP connections are only allowed if the connection goes through the VDM Connection Server.

You must install the GINA component to enable single sign on (SSO). With SSO, end users only need to enter their user credentials one time. When users enter their user credentials into the connection server, they are automatically logged into desktops to which they are entitled.

- Install the USB Redirection component to allow virtual desktop users access to locally connected USB devices with their virtual desktops.
- 6 Accept or change the destination folder and click **Next**.
 - 7 Click **Install** to begin the installation process.
 - 8 Click **Finish**.

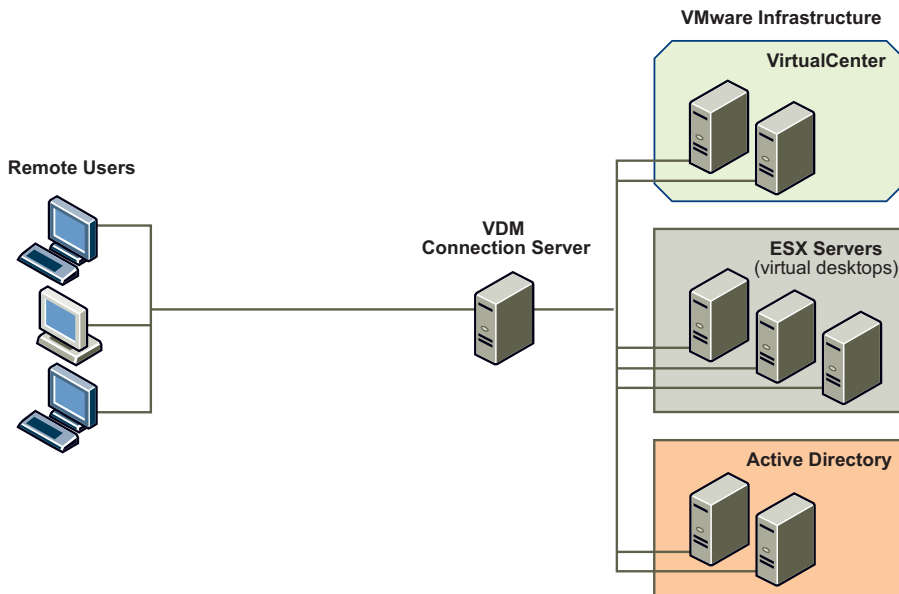
Installing the VDM Connection Server

The VDM connection server must be running Windows 2003 Server and be either a physical server dedicated to connection brokering or a standalone virtual machine. Optionally, you can obtain an SSL certificate to use for that server.

Single-Server Installation

The most basic type of deployment is single-server deployment. Figure 1-1 shows a single-server deployment with a client device, a connection server, Web-based administration, Active Directory, and VMware Virtual Infrastructure.

Figure 1-1. VDM Single Server Deployment



To perform a single server installation

- 1 Run `VMware-vdmconnectionserver-2.1.0-<xxx>.exe` on the machine that is to act as the connection server.
 <xxx> is the build number of the software component you are installing.
 The Installation wizard opens.
- 2 Click **Next**.
- 3 Accept the VMware license terms and click **Next**.

- 4 Accept or change the destination folder and click **Next**.
- 5 Choose the **Standard** deployment option.
- 6 Click **Next > Install > Finish**.

See “Installing the VDM Connection Server” on page 30.

One-Time Configuration

Perform a one-time configuration on your VDM Connection Server so that it is set up to perform deployment tasks.

To perform a one-time configuration

- 1 Go to https://<hostname_or_ipaddress>/admin to launch VDM Administrator.

<hostname_or_ipaddress> is the hostname or IP address of the VDM Connection Server, or load balancer.
- 2 Log in using the appropriate credentials.

Initially, all domain users who are members of the local administrators group on the VDM Connection Server can log into the VDM administrator user interface. Use the interface to change the list of VDM administrators later.

The first time you log in, the Configuration page appears. Entering the license information causes the Inventory page to display when you log in.
- 3 Click the **Configuration** button to change to the Configuration page if it is not displayed at log in.
- 4 On the Configuration page, perform the following actions:
 - a In **Access and Security Settings**, enter the VMware VDM license key.
 - b In **VirtualCenter Servers**, click **Add** and complete the details for the VirtualCenters to use with VDM.

If you enter a server using a DNS name or URL, no DNS lookup is performed to verify whether or not the server has previously been entered using its IP address. A conflict will arise if a VirtualCenter server is added with both its DNS name and its IP address.
 - c Under **Administrators**, click **Add** and complete the details for each AD user who requires login access to VDM Administrator.
- 5 Enable the VDM Connection Server by selecting it from the list of VDM Servers and clicking **Enable**.

Creating Desktops

After you have installed the VDM connection server, create the virtual desktops and entitle users to access them.

Creating an Individual Desktop

Create desktops so that end users can access the VDM service.

To create an individual desktop

- 1 Click the **Inventory** tab.
- 2 In **All Desktops**, click the **Desktops** tab and click **Add**.
- 3 In **Select desktop type**, click **Individual desktop** and click **Next**.
- 4 Enter the **Desktop ID** and the **Desktop Display Name**.

The desktop ID is the name that VDM uses to identify the desktop. The desktop display name is what the end user sees when logging in to the desktop. The desktop ID must be unique for each desktop, but the display name does not need to be unique. Correlate the desktop ID and display name to something within your environment (department name or location, for example). If you do not specify a display name, users see the desktop ID.

- 5 (Optional) enter a description for the desktop.

Use a maximum of 1024 alphanumeric characters, including spaces, in the description. The description is only visible in the Administrator user interface and not to end users.

- 6 Click **Next**.
- 7 Set the desktop parameters as follows:
 - **Desktop state – Enabled** means that the desktop is automatically enabled after it is created. Setting it to **Disabled** means that you must manually change the setting to **Enabled** in order to activate the desktop after it is created.
 - **Virtual machine power policy** – Select **Remain on** for the desktop to remain powered on until it is shut down by an end user or administrator. The desktop remains powered off until it is manually powered back on when this setting is selected. Select **Always powered on** if you want the desktop to stay powered on, even if an end user or administrator attempts to power it off. The

desktop powers on automatically after a power failure when this setting is selected. Select **Suspend when not in use** for the desktop to be suspended when the user is not logged in. Select **Power off when not in use** for the desktop to power off when not in use.

The power policy is applied to individual desktops when users reconnect after logging off or disconnecting.

- **Automatic logoff after disconnect** – Select **Immediately** for desktop users to be logged off as soon as they disconnect, select **Never** for users to never be logged off, or select **After** and enter the number of minutes after which users are logged off when they disconnect.
- **Allow users to reset their desktop** – Select this check box to give desktop users the ability to reset their own desktops without going through the administrator. A reset means that the desktop virtual machine powers off and powers back up. This feature is available on persistent desktops and non-persistent desktops where a user has an active session.

8 Click **Next**.

9 From the list of VirtualCenter servers, choose the VirtualCenter server that the desktop is to use and click **Next**.

10 In the table on the Virtual Machine Selection page, select the virtual machine that the desktop is to use.

All available virtual machines that are running a supported guest operating system and that another virtual desktop is not using appear in the table, including those that are suspended or not powered on.

11 Click **Next**.

12 Review the information in **Ready to Complete** and click **Finish** to accept it or **Back** to make corrections.

13 Click **Finish**.

For information about creating desktop pools, see “Configuration for a Pooled Desktop” on page 36.

Entitling a Desktop

Grant desktop users access to individual or pooled desktops by entitling them to their assigned desktops.

To entitle a desktop to an AD user or group

- 1 In **All Desktops** on the **Inventory** tab, choose the desktop that you want to entitle.
- 2 Click **Entitle**.
- 3 Click **Add**.
- 4 In the **Select object type** section, choose **Users**, **Groups**, or both.
- 5 Choose a domain in which the object you are entitling resides or choose **Entire Directory** to search the entire Active Directory domain forest.
You can search by name or description.
- 6 Choose the object to add to the entitlement.
- 7 Click **OK**.
- 8 In **Entitlement**, click **OK**.

Connecting to Desktops

VDM provides the VDM Client or VDM Web Access for connecting to the desktop virtual machine. Make sure you have administrative rights to the client machine.

To connect to desktops using the VDM Client

- 1 Download and run `VMware-vdmclient-2.1.0-<xxx>.exe`.
<xxx> is the build number of the software component you are installing.
The Installation wizard opens.
- 2 Click **Next**.
- 3 Accept the VMware license terms and click **Next**.
- 4 Choose one of the following the Custom Setup options:
 - Click **Next** to accept the default settings. The default settings install the client and the USB redirection feature.
 - Select **USB Redirection** and select **This feature will not be available** to prevent installation of this feature. Having this feature installed requires space on your hard drive so not installing it frees the required space.

- 5 Click **Next** to accept the default destination folder or click **Change** to use a different destination folder and then click **Next**.
- 6 (Optional) Enter the default server to which the client will connect and click **Next**.
This entry is the IP address or FQDN of the server.
- 7 Configure shortcuts for the VDM Client or, to not use shortcuts, deselect all choices.
- 8 Click **Next > Install > Finish**.
- 9 Start the VMware VDM Client.
- 10 In the **VDM Server** drop-down menu, enter the host name or IP address of the VDM Server.
- 11 Click **Connect**.
- 12 Enter the entitled user's credentials, choose the domain and click **Login**.
- 13 Choose the entitled desktop and click **OK**.

The desktop virtual machine is connected.

To connect to desktops using VDM Web Access

- 1 Start the browser and navigate to the VDM Connection Server URL.
For example, navigate to `https://<hostname_or_ipaddress>`, where `<hostname_or_ipaddress>` is the host name or IP address of the VDM Connection Server.
- 2 Enter an entitled user's name and password and choose the correct domain from the drop-down menu.
- 3 Click **Login**.
- 4 When Access Status is Ready, choose a desktop from the list and click **Connect**.
The desktop is connected.

VDM Introduction and System Requirements

2

This chapter introduces VDM and describes the system requirements for installing and running it. VDM is a connection broker for VMware Virtual Desktop Infrastructure. It connects users to virtual desktops running on VMware Virtual Infrastructure, and plays a critical role in security, access control, and overall desktop management.

This chapter discusses these topics:

- “VDM Overview” on page 19
- “System Requirements” on page 21
- “Prerequisites” on page 24
- “Upgrading VDM” on page 25

VDM Overview

VDM integrates with Active Directory and VMware VirtualCenter to manage and deploy desktops to end users. VDM also provides a client that enables users to connect to virtual desktops using either a Windows PC, thin client, Linux desktop, or Macintosh computer. VDM provides a secure environment for deploying and accessing virtual desktops and uses existing Active Directory functionality for authentication and user and user group management.

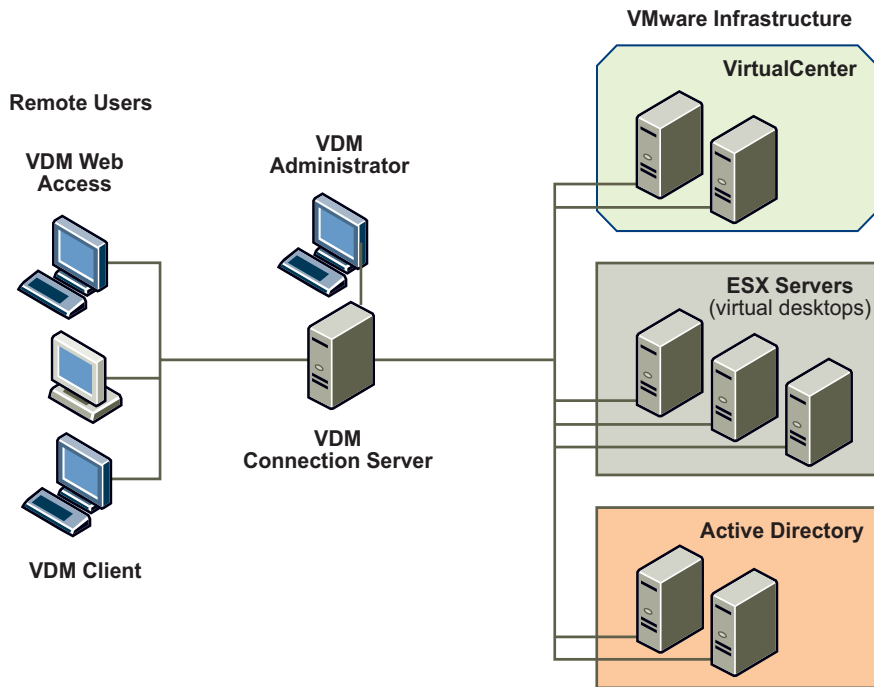
VDM has the following main components:

- VDM Client – User-facing component that connects to VDM Connection Server to connect to virtual desktops. It is a feature-rich, native windows application.

- VDM Web Access – User-facing component that connects to VDM Connection Server to connect to virtual desktops. VDM Web Access installs the client (on a Windows client) the first time you connect and connects to virtual desktops using a Web browser.
- VDM Administrator – Web application that is the primary mechanism for configuring VDM and managing users and desktops.
- VDM Connection Server – Software that acts as a connection broker and provides management and user authentication for virtual desktops. The VDM Connection Server directs incoming remote desktop user requests to the appropriate virtual desktop and enhances the user experience.
- VDM Agent – Software that installs on desktop virtual machines and enables features such as RDP connection monitoring, remote USB support, and single sign on. All guests (desktop virtual machines) require the agent to be installed to run VDM.

VDM uses existing AD infrastructure for authentication and user management. VDM integrates with VMware VirtualCenter to manage virtual desktops running on VMware ESX servers.

Figure 2-1 shows a high-level view of a VDM environment and its main components. These components are described in more detail in later sections of this book.

Figure 2-1. High-Level View of a VDM Environment

System Requirements

The following sections describe the hardware requirements for the VDM connection server and supported operating systems for the VDM Connection Server, the VDM Client, and the VDM Agent.

VDM Connection Server

The VDM Connection Server requires the following hardware and software.

Connection Server Hardware Requirements

The VDM Connection Server requires the following hardware:

- Dedicated physical or virtual server with the following specifications for running VDM.
 - As a minimum, a Pentium IV 2.0Ghz processor. Dual processors are recommended.

- As a minimum 2GB RAM. 3GB RAM is recommended for deployments of 50 or more desktops.
- A minimum of one 10/100Mbps NIC. 1Gbps NIC is recommended.

VDM Connection Server can be installed on either 32-bit or 64-bit hardware.

For DMZ deployments, VDM requires an additional dedicated physical or virtual server with similar specifications. For more information about DMZ deployments, see “DMZ Deployment” on page 65.

For high availability deployments, each VDM Connection Server requires a dedicated physical or virtual server with similar specifications.

NOTE VDM Connection Server is not supported on servers that have the Windows Terminal Server role installed. Remove the Windows Terminal Server role from any server on which you will be installing VDM Connection Server.

Connection Server Supported Operating Systems

The VDM Connection Server supports the following operating systems:

- Windows Server 2003 R2 Standard Edition with SP2 (English, Japanese, German)
- Windows Server 2003 Standard Edition with SP2 (English, Japanese, German)
- Windows Server 2003 R2 Enterprise Edition with SP2 (English, Japanese, German)
- Windows Server 2003 Enterprise Edition with SP2 (English, Japanese, German)

VDM Client

The VDM Client supports the following operating systems and devices:

VDM Client Supported Operating Systems

The VDM Client supports the following operating systems:

- Windows 2000 Professional with SP4 (English, Japanese)
- Windows XP Professional with SP2 (English, Japanese, German)
- Windows XP Professional with SP3 (English only)
- Windows XP Home with SP2 (English, Japanese, German)
- Windows XP Home with SP3 (English only)
- Windows Vista Home (English, Japanese, German)
- Windows Vista Home Premium (English, Japanese, German)

- Windows Vista Business (English, Japanese, German)
- Windows Vista Ultimate (English, Japanese, German)

Windows XP Client support for MMR

Windows XP Client is the only client operating system that supports multimedia redirection (MMR). MMR supports the following media formats:

- MPEG-1
- MPEG-2
- MPEG-4-part2
- WMV 7/8/9
- WMA
- AC3
- MP3

For Windows Media-supported video files, Windows Media Player 10 and higher is strongly recommended to support MMR and should be installed in both the client and guest.

VDM Web Access

VDM Web Access supports the following operating systems:

- Windows XP Professional with SP2 which requires IE6 SP1 or higher (English, Japanese, German)
- Windows XP Professional with SP3 which requires IE6 SP1 or higher (English only)
- Windows XP Home with SP2 which requires IE6 SP2 or higher (English, Japanese, German)
- Windows XP Home with SP3 which requires IE6 SP2 or higher (English only)
- Windows Vista Home which requires IE7 (English, Japanese, German)
- Windows Vista Home Premium which requires IE7 (English, Japanese, German)
- Windows Vista Business which requires IE7 (English, Japanese, German)
- Windows Vista Ultimate which requires IE7 (English, Japanese, German)
- RHEL 5.0, Update 1 which requires Java JRE 1.5.0 or 1.6.0 and Firefox 1.5 or 2.0 (English only)

- SLES 10 with SP1 which requires Java JRE 1.5.0 or 1.6.0 and Firefox 1.5 or 2.0 (English only)
- Ubuntu 7.10 which requires Java JRE 1.5.0 or 1.6.0 and Firefox 2.0 (English only)
- Mac OS/X 10.4 Tiger (experimental) which requires Java JRE 1.5.0, RDC 1.0, and Safari (English only)
- Mac OS/X 10.5 Leopard (experimental) which requires Java JRE 1.5.0, RDC 1.0, and Safari (English only)

VDM Agent Virtual Desktop

The VDM Agent supports the following operating systems (32-bit) for virtual desktops:

- Windows XP Professional with SP2 (English, Japanese, German)
- Windows XP Professional with SP3 (English only)
- Windows Vista Business Edition (English, Japanese, German)
- Windows Business Ultimate Edition (English, Japanese, German)

Prerequisites

VDM Connection Server has the following prerequisites:

- VMware Infrastructure
VMware Infrastructure 3.5 (current versions of ESX Server and Virtual Center) with at least one ESX host and one VirtualCenter instance is recommended. VMware Infrastructure 3.02 is supported.
- Servers running VDM Connection Server standard or replica instances that are joined to an Active Directory domain

NOTE VDM Connection Server does not make nor require any schema or configuration updates to Active Directory.

- Microsoft Sysprep tools installed on your VC Server
- A customization specification that permits cloned virtual machines to join the AD domain (optional)
- A valid license key for VDM

The VDM Agent, VDM Client, and VDM Web Access have the following prerequisites:

- For Windows guest desktops and Windows clients, you must have administrative privileges to install the VDM Client and the VDM Agent.
- The use of ActiveX controls and Internet Explorer 6 or above are required for Windows client users who access their desktops using VDM Web Access.
- Web Access using Linux or Mac OS X requires Java JRE version 1.5.0 or 1.6.0
- Microsoft Remote Desktop Connection 6.0 recommended (not required)

It is recommended that you upgrade VDM Client machines to use Microsoft Remote Desktop Connection (RDC) 6.0. This recommendation applies to machines running Windows XP and Windows XPe. Windows 2000 does not support RDC 6.0. Windows Vista comes with RDC 6.0 installed.

RDC 6.0 can be downloaded at the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=26F11F0C-0D18-4306-ABCF-D4F18C8F5DF9&displaylang=en>

- If connecting to a Windows Vista desktop using a Linux client, you must install the rdesktop remote desktop protocol client version 1.5.0, which you can download from the following URL:

<http://www.rdesktop.org/>

After you download rdesktop, follow the instructions in the readme file.

- VDM Web Access requires that you install the full VDM Client to use the USB redirection feature.
- If using USB redirection, make sure you install the USB redirection feature when you install the VDM Client.

Upgrading VDM

Upgrading VDM software is no different than performing any other type of installation. You should upgrade the VDM Client and VDM Agent at the same time you upgrade the VDM Connection Server to ensure the same version is installed on all VDM components. Upgrading to a newer version of software preserves existing configuration data.

Installing and Configuring VDM

3

VDM installation consists of installing VDM software components and preparations in VirtualCenter. This document describes in detail how to install VDM components but assumes that the administrator is familiar with VMware Virtual Infrastructure administration. VMware recommends that administrators run an end-to-end test before deploying VDM to end users.

Before installing VDM, see Chapter 2, “VDM Introduction and System Requirements,” on page 19 to obtain system requirements and hardware and device support. This chapter covers these topics:

- “Prepare Desktop Virtual Machines” on page 28
- “Installing the VDM Connection Server” on page 30
- “One-Time Configuration” on page 33
- “End-to-End Configuration” on page 35
- “VDM Administrator User Interface” on page 49
- “Searching Desktops and Entitled Users and Groups” on page 52
- “Global Configuration Settings” on page 54
- “Viewing Events” on page 56
- “RSA SecurID” on page 56
- “Deleting VDM Objects” on page 57
- “Installing SSL Certificates” on page 58
- “Load Balancing” on page 62

- “DMZ Deployment” on page 65
- “Exporting and Importing VDM Configuration Data” on page 69
- “Client Command-Line Parameters” on page 69
- “Collecting VDM Diagnostic Information” on page 70
- “Troubleshooting VDM” on page 72

Prepare Desktop Virtual Machines

Before you install the VDM software, prepare desktop virtual machines for use. Where changes in VirtualCenter are required, see the latest VirtualCenter documentation for specific steps.

Make sure that the following prerequisites are in place:

- Identify the base desktop virtual machine to deploy to users, and install the latest operating system and application Service Packs and patches. For Windows XP desktop virtual machines, ensure that the following Microsoft patch that VDM requires is installed:

<http://support.microsoft.com/kb/323497>

- The latest VMware Tools are installed (provided with VI 3.5).
- Make sure that networking settings (proxies, and so forth) are properly configured in the desktop virtual machine.
- VMware VDM Agent is installed.

NOTE For automated updating of VDM Agent in large environments, VMware recommends using standard Windows update mechanisms such as Altiris, SMS, LanDesk, BMC, or other systems management software.

- Make sure that you have administrative rights to the desktop virtual machine.

To install VMware VDM Agent

- 1 Download the VDM installer file from the VMware secure Web site to a local drive.

For information about the location of the secure Web site, contact your VMware representative.

- 2 Run `VMware-vdmagent-2.1.0-<xxx>.exe`

<xxx> is the build number of the software component you are installing in the desktop virtual machine.

The VMware Installation wizard opens.

- 3 Click **Next**.
- 4 Accept the VMware license terms and click **Next**.
- 5 Choose your custom setup options.

Install the VDM Authentication GINA component to restrict direct RDP connections. By default, RDP connections to the virtual machine from any source are allowed. If the VDM Authentication GINA is installed, RDP connections are only allowed if the connection goes through the VDM Connection Server. Installing the VDM Authentication GINA also enables single sign on (SSO).

Install the USB Redirection component if virtual desktop users need to access locally connected USB devices with their virtual desktops.

- 6 Accept or change the destination folder and click **Next**.
- 7 Click **Install** to begin the installation process.
- 8 Click **Finish**.

To create a desktop virtual machine template

- 1 In VirtualCenter, convert the desktop virtual machine to a template.
You must create a desktop virtual machine template to use desktop pools in VDM.
- 2 (Optional) In VirtualCenter, create a guest customization specification.
Use DHCP for the specification and set the computer name to the virtual machine name. Cloned virtual machines also need to be able to join AD domains if the VDM single sign-on feature is required.
- 3 As a test, deploy a virtual machine from the template to validate that customization is successful.
Make sure that AD domain join and authentication works.
- 4 If a folder was not automatically created, create one in the Virtual Machines and Templates Inventory view.

Using the VDM Agent on Virtual Machines with Multiple NICs

For Guest Virtual Machines with more than one virtual NIC, you need to configure the subnet that the VDM Agent will use. This determines which network address the VDM Agent provides to the VDM Server for client RDP connections. To configure this subnet, create the following REG_SZ registry value in the virtual machine on which the VDM Agent is installed:

```
HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m  
(REG_SZ)
```

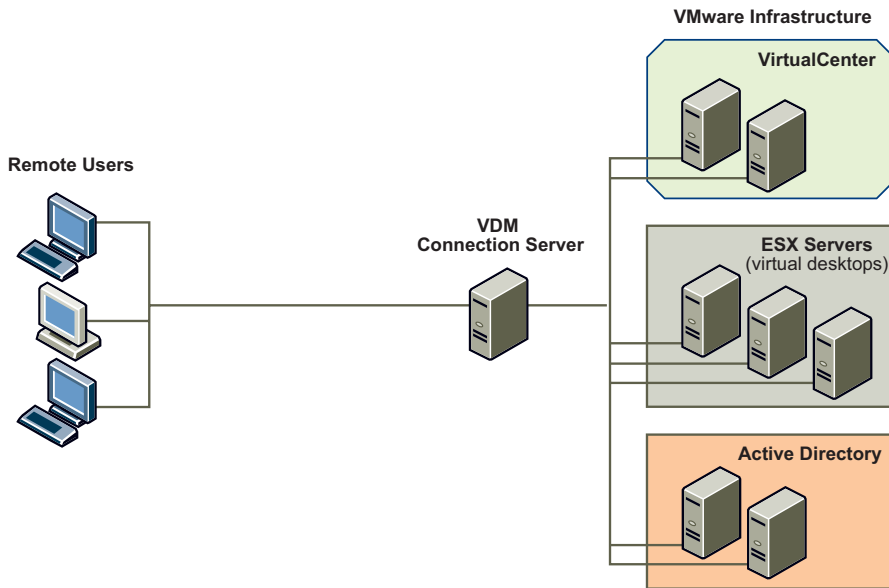
In the registry value, n.n.n.n is the TCP/IP subnet and m is the number of bits in the subnet mask.

Installing the VDM Connection Server

The VDM Connection Server must be running on Windows 2003 Server and be located on either a physical or virtual server dedicated to connection brokering. Do not have the connection server perform any other functions or roles (for example, do not designate the same server to be the VirtualCenter server). The connection server must be joined to the domain (but cannot be a domain controller) and it is recommended that each connection server has a static IP address assigned to it. The domain user account used to install the connection server must have administrative privileges on that server. The connection server administrator also needs to know the VirtualCenter credentials. It is recommended that you obtain an SSL certificate to use for that VDM Connection Server. For more information about SSL certificate installation, see “Installing SSL Certificates” on page 58.

Single-Server Installation

The most basic type of deployment is single-server deployment. The following diagram shows a single-server deployment with a client device, a connection server, Web-based administration, Active Directory, and VMware Virtual Infrastructure.

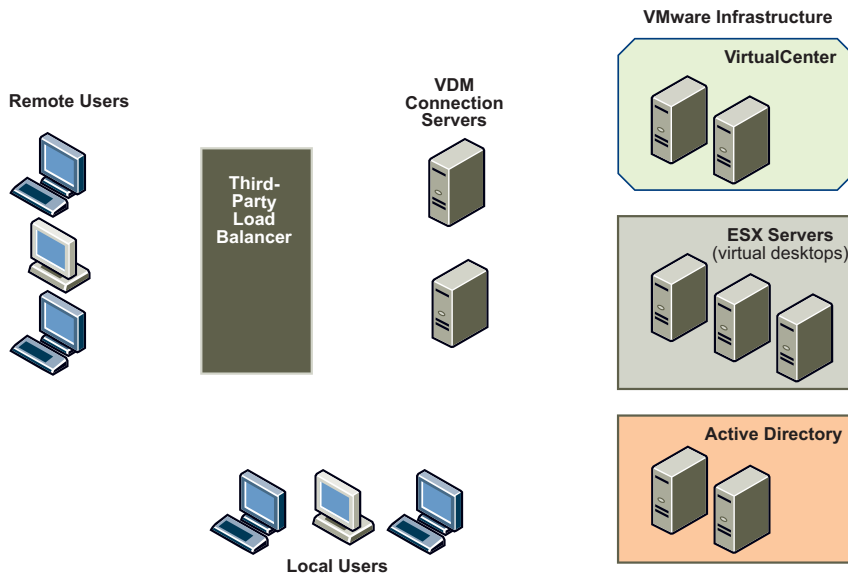
Figure 3-1. VDM Single Server Deployment**To perform a single server installation**

- 1 Run `VMware-vdmconnectionserver-2.1.0-<xxx>.exe` on the machine that is to act as the connection server.
 <xxx> is the build number of the software component you are installing.
 The VMware Installation wizard opens.
- 2 Click **Next**.
- 3 Accept the VMware license terms and click **Next**.
- 4 Accept or change the destination folder and click **Next**.
- 5 Choose the **Standard** deployment option.
- 6 Click **Next > Install > Finish**.

Multiserver Installation

VDM Connection Server can also be deployed in a multiserver configuration for high availability and load balancing. The following high-level diagram shows a multiserver deployment, connection servers, a load balancer, Web-based administration, Active Directory, and VMware Virtual Infrastructure (which includes ESX servers hosting the virtual desktops).

Figure 3-2. VDM Multiserver Deployment



NOTE Multi-server installation assumes that one other instance of VDM Connection Server is installed using the standard deployment option. Multi-server installation is performed on second, or subsequent, servers. See “Single-Server Installation” on page 30 for more information.

To perform a multiserver installation

- 1 Run `VMware-vdmconnectionserver-2.1.0-<xxx>.exe` on the machine that is to act as the connection server.

<xxx> is the build number of the software component you are installing.

The VMware Installation wizard opens.

- 2 Click **Next**.
- 3 Accept the VMware license terms, and click **Next**.
- 4 Accept or change the destination folder, and click **Next**.
- 5 Choose the **Replica** deployment option.
- 6 Enter the host name or IP address of the existing connection server that you replicate.
- 7 Click **Next**.
- 8 Click **Install**.
- 9 Click **Finish**.

One-Time Configuration

Perform a one-time configuration on your VDM Connection Server so that it is set up to perform deployment tasks.

To perform a one-time configuration

- 1 Go to https://<hostname_or_ipaddress>/admin to launch VDM Administrator.

<hostname_or_ipaddress> is the hostname or IP address of the VDM Connection Server, or load balancer.
- 2 Log in using the appropriate credentials.

Initially, all domain users who are members of the local administrators group on the VDM Connection Server are allowed to login to the VDM administrator user interface. You can use the interface to change the list of VDM administrators later.

The first time you log in, the Configuration page appears. After you enter the license information, the Inventory page displays when you log in.
- 3 Click the **Configuration** button to change to the Configuration page if it is not displayed at log in.

- 4 On the Configuration page, perform the following actions:
 - a In **Access and Security Settings**, enter the VMware VDM license key.
 - b In **VirtualCenter Servers**, click **Add** and complete the details for the VirtualCenters to use with VDM.

If you enter a server using a DNS name or URL, no DNS lookup is performed to verify whether or not the server has previously been entered using its IP address. A conflict will arise if a VirtualCenter server is added with both its DNS name and its IP address.

- c Grant Administrative rights to AD users who have login access to VDM Administrator.

Enabling and Disabling a VDM Connection Server

Enable the VDM Connection Server so that users can log in. Disable the VDM Connection Server to prevent users from logging in. Currently logged in users are not affected when you disable the VDM Connection Server. Disabling the VDM Connection Server is useful if you need to take it out of service for any reason. When a VDM Connection Server is disabled, end users who attempt to log in see a message stating that the VDM Server Connection failed and the VDM Server is currently disabled.

To enable a VDM Connection Server

- 1 Click the **Configuration** tab.
- 2 Select the VDM Connection Server from the list of VDM Servers and click **Enable**.

To disable a VDM Connection Server

- 1 Click the **Configuration** tab.
- 2 Select the VDM Connection Server from the list of VDM Servers and click **Disable**.

Disabling a VDM Connection Server does not affect the current active desktop sessions nor will it prevent new desktop sessions from being established.

End-to-End Configuration

Perform an end-to-end configuration on new installations to ensure that installation and configuration issues can be easily resolved. This section refers to both individual and pooled desktops.

To perform a configuration for an individual desktop

- 1 Click the **Inventory** tab.
- 2 In **All Desktops**, click the **Desktops** tab and click **Add**.
- 3 In **Select desktop type**, click **Individual desktop** and click **Next**.
- 4 Enter the **Desktop ID** and the **Desktop Display Name**.

The desktop ID is the name that VDM uses to identify the desktop. The desktop display name is what the end user sees when logging in to the desktop. The desktop ID must be unique for each desktop, but the display name does not need to be unique. The desktop ID and display name should correlate to something within your environment (department name or location, for example). If you do not specify a display name users see the desktop ID.

- 5 (Optional) enter a description for the desktop.

You can use any alphanumeric characters in the description and the description can contain a maximum of 1024 characters, including spaces. The description is only visible in the Administrator user interface and not to end users.

- 6 Click **Next**.
- 7 Set the desktop parameters as follows:
 - **Desktop state – Enabled** means that the desktop is automatically enabled after it is created. Setting it to **Disabled** means that you must manually change the setting to **Enabled** in order to activate the desktop after it is created.
 - **Virtual machine power policy** – Select **Remain on** for the desktop to remain powered on until it is shut down by an end user or administrator. The desktop remains powered off until it is manually powered back on when this setting is selected. Select **Always powered on** if you want the desktop to stay powered on, even if an end user or administrator attempts to power it off. The desktop powers on automatically after a power failure when this setting is selected. Select **Suspend when not in use** for the desktop to be suspended when the user is not logged in. Select **Power off when not in use** for the desktop to power off when not in use.

The power policy is applied to individual desktops when users reconnect after logging off or disconnecting.

- **Automatic logoff after disconnect** – Select **Immediately** for desktop users to be logged off as soon as they disconnect, select **Never** for users to never be logged off, or select **After** and enter the number of minutes after which users are logged off when they disconnect.
- **Allow users to reset their desktop** – Select this check box to give desktop users the ability to reset their own desktops without going through the administrator. A reset means that the desktop virtual machine powers off and powers back up. This feature is available on persistent desktops and non-persistent desktops where a user has an active session.

8 Click **Next**.

9 From the list of VirtualCenter servers, select the VirtualCenter server that the desktop is to use and click **Next**.

10 In the table on the Virtual Machine Selection page, select the virtual machine that the desktop is to use.

All available virtual machines that are running a supported guest operating system and that another virtual desktop is not using appear in the table, including those that are suspended or not powered on.

11 Click **Next**.

12 Review the information in **Ready to Complete** and click **Finish** to accept it or **Back** to make corrections.

13 Click **Finish**.

After a desktop is added, entitle it to an AD user or group. See “Entitling a Desktop” on page 45.

For information about testing the desktop launch, see “Connecting to Desktops” on page 45.

Configuration for a Pooled Desktop

Perform a configuration on new installations to ensure that installation and configuration issues can be easily resolved. Deploy a single virtual machine from the template to make sure virtual machines can deploy from this template.

Before you deploy pooled desktops, create a template and a customization specification (if using customization) in VirtualCenter. Make sure you can manually create virtual machines and customize them by using the customization specification. To ensure that single sign (SSO) functions, the customization specification must use dynamic address assignment (specifically, DHCP), the computer name needs to be set to the virtual machine name and the virtual machine automatically joined to the domain. For information about creating templates and customization specifications, see the most recent VirtualCenter documentation.

After you complete these template and customization specification items, ensure that the virtual machine successfully joined the domain. Finally, make sure that all guest virtual machine names, including those deployed from the template for the pooled desktop, are registered in DNS. Because you are using dynamically assigned IP addresses, use AD-integrated DNS and let the DHCP client register virtual machines with the dynamic DNS.

NOTE Test individual desktops before testing pools.

VirtualCenter Permissions for VDM

To use VirtualCenter with VDM, VDM administrators must have permissions for certain operations in VirtualCenter. These permissions are granted by creating and assigning VirtualCenter roles to the VDM administrator. Assign VDM administrators the role of administrator for a datacenter or cluster where pools will be created so that they can make the required changes. Assign a role that will allow them to read global customization specifications. These permissions are required for VDM to work with VirtualCenter.

To create the VDM administrator role for VirtualCenter

- 1 In VirtualCenter, Click the **Administration** button.
- 2 If it is not already selected, click the **Roles** tab and click **Add Role**.
- 3 Enter a name for the role (VDM Administrator, for example).
- 4 In the list of **Privileges**, expand **Folder** and select **Create Folder** and **Delete Folder**.
- 5 Expand **Virtual Machine** and perform the following steps:
 - a Expand **Inventory** and select **Create** and select **Remove**.
 - b Expand **Interaction** and click **Power On**, **Power Off**, **Suspend**, and **Reset**.

- c Expand **Configuration** and select **Add new disk**, **Add or Remove Device**, **Modify Device Settings**, and **Advanced**.
 - d Expand **Provisioning** and select **Customize**, **Deploy Template**, and **Read Customization Specifications**.
- 6 Expand **Resource** and select **Assign Virtual Machine to Resource Pool**.
 - 7 Click **OK**.

The new role appears in the list of roles.

To assign the administrator or VDM administrator VirtualCenter roles

- 1 In VirtualCenter, select the datacenter or cluster.
- 2 Click the **Permissions** tab.
- 3 Right-click on the page anywhere below the list of **Users and Groups**.
- 4 Click **Add Permission**.
- 5 In **Users and Groups**, click **Add**.
- 6 In the **Domain** drop-down menu, select the administrator's domain.
- 7 In **Users and Groups**, select an administrator from the list.
- 8 Click **Add** and **OK**.
- 9 In **Assigned Role**, select a role.

Select **Administrator** to give full control over the datacenter or cluster. The Administrator role is preconfigured in VirtualCenter.

Select **VDM Administrator** to give the user the more restrictive access and permissions that the VDM Administrator role that you created.

- 10 Click **OK**.

To create a VirtualCenter role for reading customization specifications

- 1 In VirtualCenter, click **Administration**.
- 2 Click the **Roles** tab and click **Add Role**.
- 3 Enter a name for the role (for example, Read Only Customization Specifications).
- 4 In the list of privileges, select **Virtual Machine**.
- 5 Expand **Provisioning**, and select **Read Customization Specifications**.
- 6 Click **OK**.

To assign VirtualCenter roles for VDM

- 1 In VirtualCenter, in the Inventory view, click **Hosts and Clusters**.
- 2 Click the **Permissions** tab.
- 3 Right click on the page anywhere below the list of **Users and Groups**.
- 4 Click **Add Permission**.
- 5 In **Users and Groups**, click **Add**.
- 6 In the **Domain** drop-down menu, select the administrator's domain.
- 7 In **Users and Groups**, select an administrator from the list.
- 8 Click **Add** and **OK**.
- 9 In **Assigned Role**, select **Global Read Only Custom Spec** and click **OK**.

NOTE Test individual desktops before testing pools.

To perform a configuration for a pooled desktop

- 1 Click the **Inventory** tab.
- 2 In **Desktops**, click the **Desktops** tab and **Add**.
- 3 In **Select desktop type**, select either **Desktop pool - persistent** or **Desktop pool - non-persistent**.

Persistent desktop pools allow users to log into the same desktop every time. Users can save documents and files on persistent desktops because they return to the same desktop.

Non-persistent pools are available to users when they log in but are returned to the pool when users log off. Users log in to a different desktop each time and cannot save documents or files on the desktop.

- 4 Click **Next**.
- 5 Enter the **Desktop ID** and the **Desktop Display Name**.

The desktop ID is the name that VDM uses to identify the desktop (in this case, the desktop pool). The user sees the desktop display name when logging in to the desktop. The desktop ID must be unique for each desktop, but the display name does not need to be unique. The desktop ID and display name do not need to correlate to anything specific within your environment. If you do not specify a display name, users see the desktop ID.

- 6 (Optional) enter a description for the pooled desktop.

You can use any alphanumeric characters in the description and the description can contain a maximum of 1024 characters, including spaces. The description is only visible in the Administrator user interface and not to end users.

- 7 Click **Next**.

- 8 Set up the desktop parameters:

- **Desktop state – Enabled** means that the pool is automatically enabled after it is created and ready for use by end users. **Disabled** means that you must manually change the setting to **Enabled** to activate the pool after it is created. **Disabled** is used for such things as upgrading virtual machines or taking desktops offline to perform maintenance.
- **Provision – Enabled** means that virtual machines are created for the pool as soon as you finish the steps add a pooled desktop. **Disabled** means that you must manually change the setting to **Enabled** to create virtual machines for the pool after the pool is created.
- **Pool size** – Set to the number of desired virtual desktops.
- **Stop provisioning on error** – Stops the provisioning of virtual machines when an error is detected.
- **Virtual machine power policy – Remain on** sets the virtual machines to always remain on. **Always powered on** sets the assigned virtual machines to remain powered on. **Suspend when not in use** sets the virtual machines to be suspended when the user is not logged in. **Power off when not in use** sets virtual machines to power off when not in use.

The power policy is applied to assigned persistent pooled desktops when users reconnect after logging off or disconnecting. Power policy for persistent and non-persistent pooled desktops in the idle state is applied the next time users reconnect.

- **Prefix for virtual machine names** – Set this to a value for each pool that identifies virtual machines as part of that pool. Virtual machines created for this pool have names that begin with this prefix.
- **Power off and delete virtual machine after first use** (for non-persistent pools only) – Deletes the virtual machine when the user logs out after first use. If necessary, a new virtual machine is cloned to maintain a specific pool size after virtual machines are deleted.

- **Automatic logoff after disconnect** – Select **Immediately** if you want desktop users to be logged off as soon as they disconnect, select **Never** if you want users to never be logged off, or select **After** and fill in the number of minutes after which users are logged off when they disconnect.
- **Allow users to reset their desktop** – Select this check box if you want to allow desktop users to reset their own desktops without going through the administrator.
- **Allow multiple sessions per user** (for non-persistent pools only) – Select this check box if you want to allow a desktop user to simultaneously use multiple desktops in a pool from different client devices.

9 Click **Next**.

10 From the list of VirtualCenter servers, select the VirtualCenter server that the desktop is to use and click **Next**.

If multiple VirtualCenter servers are running in your environment, make sure that another VirtualCenter server is not using the VirtualCenter unique ID. By default, an ID value is randomly generated but it is editable. For details about editing VirtualCenter unique ID values, see the latest VirtualCenter documentation.

11 In **Template Selection**, select a template from which to deploy virtual machines for the desktop pool.

12 Select the virtual machine folder location.

VDM creates a folder with the same name as the desktop ID and puts the newly created virtual machines in the folder.

13 Select a host or cluster on which to run the virtual machines that this desktop uses and click **Next**.

14 Select a resource pool in which to run the virtual machines that this desktop uses, and click **Next**.

15 Select either a single datastore or multiple datastores to store the virtual machine files and click **Next**.

Ensure that sufficient free space is available to store the new virtual machines in the datastores that you select. The amount of free space displays beneath the list of available datastores. The amount of free space increases with each datastore that you select. If you do not have sufficient space available, you must add free space by selecting another datastore.

16 Select a customization specification to customize the guest operating system for virtual machines used in this desktop and click **Next**.

- 17 Review the information in **Ready to Complete** and click **Next** to accept it or **Back** to make revisions.

- 18 Click **Finish**.

After the pooled desktop is added, entitle it to an AD user or group. See “Entitling a Desktop” on page 45.

For information about testing the desktop launch, see “Connecting to Desktops” on page 45.

Advanced Pool Settings

Use advanced pool settings to override the default pool settings and determine how your pooled desktops are deployed and managed. The advanced pool settings are an option when you are creating either a persistent or non-persistent pool in the Desktop Settings in the Add Desktop wizard.

When you are configuring desktop settings, access and enable the advanced settings by expanding **Advanced Settings** and selecting **Enable Advanced Pool Settings**. The advanced pool settings include the following options:

- **Minimum number of virtual machines** – Overrides the default minimum number of virtual machines available for a pool. Set this number to the minimum number of anticipated virtual machines upon first deployment.
- **Maximum number of virtual machines** – Overrides the default maximum number of virtual machines available for a pool. Set this number to the maximum number of virtual machines that are to be deployed in the pool at any point. This setting is necessary to prevent over burdening of hardware resources.
- **Number of available virtual machines** – Overrides the default number of available virtual machines for a pool. This setting determines how many virtual machines are available for immediate use. If the power policy dictates, available virtual machines over this limit will be suspended or powered off as needed. For non-persistent pools, this setting determines how many virtual machines are provisioned (added) as new users log in to virtual desktops. For persistent pools, this setting must match the rate at which users are added to the environment (in other words, if you add two users a day, set this number to 2 for persistent pools).

You can further specify virtual machine behavior for desktops that use a specific VirtualCenter Server using the advanced VirtualCenter settings on the Configuration page. On that page, you can control the maximum number of concurrent provisioning (desktop virtual machine creation) operations and the maximum number of concurrent power operations.

Advanced Pooling Example Scenarios

VDM pooling is flexible and offers many possible combinations of settings. The following example scenarios show some possible combinations of settings and illustrate how VDM behaves.

Pooling Example 1

Pooling example 1 has the following settings:

- **Type of pool** – Non-persistent
- **Minimum number of virtual machines** – 100
- **Maximum number of virtual machines** – 200
- **Number of available virtual machines** – 20
- **Virtual machine power policy** – Suspend when not in use

In this example, the pool initially clones and customizes 100 virtual machines. After 20 virtual machines, a virtual machine is suspended for each new cloned virtual machine so that the available count (in other words, powered up and ready for use) did not exceed 20. The minimum and maximum values only affect the cloning and not the number of available virtual machines.

As users log in, the number of available virtual machines setting powers up more virtual machines to keep them at the right level. When the eightieth user logs in, the setting initiates a cloning operation. As users log out, virtual machines are suspended (based on the power policy) to keep the available number of virtual machines down.

Pooling Example 2

Pooling example 2 has the following settings:

- **Type of pool** – Persistent
- **Minimum number of virtual machines** – 100
- **Maximum number of virtual machines** – 200
- **Number of available virtual machines** – 20
- **Virtual machine power policy** – Suspend when not in use

The actions are the same as in Example 1, except that when users log off, their virtual machines are suspended. The used virtual machines are not returned to the pool because they are now assigned.

Pooling Example 3

Pooling example 3 has the following settings:

- **Type of pool** – Non-persistent
- **Minimum number of virtual machines** – 100
- **Maximum number of virtual machines** – 200
- **Number of available virtual machines** – 20
- **Virtual machine power policy** – Remain on

The pool initially clones and customizes 100 virtual machines. These virtual machines are left running. As the eightieth and subsequent users log in, the available count restarts cloning to maintain the capacity.

Pooling Example 4

Pooling example 4 has the following settings:

- **Type of pool** – Non-persistent
- **Minimum number of virtual machines** – 200
- **Maximum number of virtual machines** – 200
- **Number of available virtual machines** – 20
- **Virtual machine power policy** – Remain on

The pool clones 200 virtual machines. No more virtual machines are ever cloned. The power policy means that virtual machines are not powered off.

Pooling Example 5

Pooling example 5 has the following settings:

- **Type of pool** – Non-persistent
- **Minimum number of virtual machines** – 200
- **Maximum number of virtual machines** – 200
- **Number of available virtual machines** – 20
- **Virtual machine power policy** – Suspend when not in use

The pool clones 200 virtual machines. After the twentieth clone, the pool manager starts to suspend virtual machines to maintain the available count at 20. As users log in, virtual machines are resumed to maintain the spare count.

Entitling a Desktop

After an individual or pooled desktop is added, entitle AD users or groups to it.

To entitle a desktop to an AD user or group

- 1 In **All Desktops** on the Inventory tab, choose the desktop that you want to entitle.
- 2 Click **Entitle** and **Add**.
- 3 In **Select object type**, select **Users** or **Groups**.
- 4 Choose the domain where the object you are entitling reside, or choose **Entire Directory** to search across the entire Active Directory domain forest.

You can search by name or description.

- 5 Choose the object to add to the entitlement.

You can entitle multiple users and groups to a desktop. If you entitle multiple users or groups to a desktop, the desktop behaves like a nonpersistent pool. For information about non-persistent pools, see “Configuration for a Pooled Desktop” on page 36.

- 6 Click **OK**.
- 7 In **entitlement**, click **OK**.

Connecting to Desktops

VDM provides the VDM Client or VDM Web Access for connecting to the desktop virtual machine.

NOTE Make sure you have administrative rights to the client machine.

To connect to desktops using the VDM Client

- 1 Download and run `VMware-vdmclient-2.1.0-<xxx>.exe`.
 <xxx> is the build number of the software component you are installing.
 The Installation wizard opens.
- 2 Click **Next**.
- 3 Accept the VMware license terms and click **Next**.

- 4 Choose one of the following the Custom Setup options:
 - Click **Next** to accept the default settings. The default settings install the client and the USB redirection feature.
 - Select **USB Redirection** and choose **This feature will not be available** to prevent installation of this feature. Having this feature installed requires space on your hard drive so not installing it frees the required space.
- 5 Click **Next** to accept the default destination folder or click **Change** to use a different destination folder and then click **Next**.
- 6 (Optional) Enter the default server to which the client will connect and click **Next**. This entry is the IP address or FQDN of the server.
- 7 Configure shortcuts for the VDM Client or, to not use shortcuts, deselect all choices.
- 8 Click **Next > Install > Finish**.
- 9 Start the VMware VDM Client.
- 10 In the **VDM Server** drop-down menu, enter the host name or IP address of the VDM Server.
- 11 Click **Connect**.
- 12 Enter the entitled user's credentials, select the domain and click **Login**.
- 13 Choose the entitled desktop and click **OK**.

The desktop virtual machine is connected.

To connect to desktops using VDM Web Access

- 1 Start the browser and navigate to the VDM Connection Server URL.
For example, navigate to `https://<hostname_or_ipaddress>`, where `<hostname_or_ipaddress>` is the host name or IP address of the VDM Connection Server.
- 2 Enter an entitled user's name and password and select the correct domain from the drop-down menu.
- 3 Click **Login**.
- 4 When Access Status is Ready, choose a desktop from the list and click **Connect**.
The desktop is connected.

To connect to desktops using VDM Web Access

- 1 Start the browser and go to the VDM Connection Server URL.
For example: `https://<hostname or ipaddress>`, where `<hostname or ipaddress>` is the host name or IP address of the VDM Connection Server.
- 2 The VDM Client installs automatically if you are logging on using a Windows client.
- 3 Enter the entitled user's name and password and make sure that you select the correct domain from the drop-down menu.
- 4 Click **Login**.
- 5 When the **Access Status** is **Ready**, select a desktop from the list and click **Connect**.
The desktop is connected.

Changing End User Passwords

VDM supports password policies from the AD domain. If AD group policy is set so that passwords expire or an AD administrator requires users to change their passwords, the users are prompted to do so when logging on to VDM using the Client or Web Access. The password the user enters must conform to, and will be checked against, any AD group policy that has been set.

Setting the Default Desktop for Thin Client Users

VDM administrators can set the default desktop that thin client users log into using the `VDMAdmin.EXE` command-line command on the VDM Connection Server. This utility is only available on US English systems.

To set the default desktop for a thin client user

- 1 Open a command prompt on the VDM Connection Server.
- 2 From the command line, run this command:

```
C:\Program Files\VMware\VMware VDM\Server\bin\vdmin -D -d
mydesktop -u <Domain>\<Username>
```

Running the command creates an entry in LDAP to ensure that thin client users who are entitled to multiple desktops only have access to the default desktop after this command is run. Users can set their own default desktops but only after logging into the thin client.

Setting an Externally Resolvable Name on a Connection Server

If VDM clients cannot directly access a VDM Connection Server by using `https://<hostname>` where `<hostname>` is the host name of the VDM Connection Server, you must specify an externally resolvable name for the VDM Connection Server. If the VDM Connection Server is accessed from the Internet, set the name to something that resolves on the Internet. This name can be something like `https://vdmservername.mycompany.com`. Whenever this situation arises, you must set the name for each VDM Connection Server that is unresolvable.

The process of setting the name is not the same for all installation types. For standard or replica installations, you can set the name by using the Administrator user interface. For a security server installation, you must edit or create a file with the settings and save it on the security server.

To set the name on a standard or replica installation

- 1 On the Configuration page, in **VDM Servers**, choose the VDM Connection Server.
- 2 Click **Edit**.
- 3 Enter a name in the **External URL** field and click **OK**.
- 4 Restart the VDM Connection Server service so that the changes take effect.
- 5 Click **Start > Administrative Tools > Services** and select the VMware VDM Connection Server from the list of services.

If the service is running, click **Restart the service**. If the service is not running, click **Start the service**.

To set the name on a security server installation

- 1 Create or edit the properties file (`locked.properties`) so that it contains entries for the externally resolvable name of the security server, the port number and the client protocol.

The properties file is a text file. If it already exists, it is located at `C:\Program Files\VMware\VMware VDM\Server\sslgateway\conf\locked.properties`. always save this file in the same place, whether it already exists or not.

As an example, if the security server's externally resolvable name is `vdmservname.mycompany.com`, the port number is 443, and the client protocol is HTTPS, you use a text editor to edit or create the properties file with the following entries:

- `clientHost=vdmservname.mycompany.com`
- `clientPort=443`
- `clientProtocol=https`

If a properties file already exists containing entries with these key words, replace the entries with new entries from this list.

- 2 Save the file.
- 3 Restart the VDM Security Server service so that the changes take effect.
- 4 Click **Start > Administrative Tools > Services** and select the VMware VDM Security Server from the list of services.

If the service is running, click **Restart the service**. If the service is not running, click **Start the service**.

VDM Administrator User Interface

The VDM Administrator user interface is where you perform all of the configuration, deployment, and administrative tasks for VDM. The **Inventory**, **Configuration**, and **Events** buttons always appear at the top of the Administrator user interface. These buttons allow you to navigate to other areas of the interface and perform administration and configuration tasks. This section describes the pages that each button opens and the options associated with them.

When you click a button in the administrator user interface and you select a tab on the page that opens, the background becomes white. Tabs that are not selected have a purple background.

Inventory Page

The Inventory page opens when you log in to the VDM Administrator user interface (except the first time you log in, when the Configuration page opens). The Inventory page is where you access all of your virtual machines and deploy and make changes to virtual desktops. The **Show** drop-down menu allows you to change between the **Desktops** and **Entitled Users and Groups** views.

The Inventory page allows you to search and filter information about desktops, virtual machines, and active sessions and to scroll between pages if multiple pages exist (each page contains 200 objects).

- **Desktops** view – Choose among the **Desktops**, **Virtual Machines**, or **Active Sessions** tabs. On the **Desktops** tab, you can add, edit, entitle, enable, disable, or delete desktops or desktop pools. On the **Virtual Machines** tab, you can view and delete virtual machines. On the **Active Sessions** tab, you can view, disconnect, or reboot active sessions.

You can filter the information in the tables that are associated with each tab. You can also choose which columns to filter and search when the **Desktops** view is selected.

- **Desktops** tab – Filter and search the **Desktop ID** or **Type** columns.
- **Virtual Machines** tab – Filter and search the **Virtual Machine Name**, **IP Address**, **User**, or **Status** columns.
- **Active Sessions** tab – Filter and search the **User** or **Desktop** columns.

When you are in the **Desktops** view, you can choose between the **Inventory** and **Search** tabs on the left side of the page.

- **Inventory** – All of the desktops appear in a list on that tab. Selecting a desktop from the list displays information about that desktop on the right side of the page. The right side of the page also displays the **Summary**, **Users and Groups**, **Virtual Machines**, and **Active Sessions** tabs.
- **Search** – The **Search for Desktops** field appears. Enter search text in this field to search for desktops. You can use the **In these categories** check boxes to choose the search criteria. Selecting a desktop from the list displays information about that desktop on the right side of the page. In addition, the right side of the page displays the **Summary**, **Users and Groups**, **Virtual Machines**, and **Active Sessions** tabs.

The Inventory page uses a different icons for each type of desktop. Individual desktop icons have a solid border containing one blue square, persistent pool desktop icons have a solid border containing two blue squares, and nonpersistent pool desktop icons have a dotted border containing two blue squares.

- **Entitled Users and Groups** view

In the Entitled Users and Groups view, you can choose between the **Entitled Users and Groups** and **Active Sessions** tabs. You can view the entitled users and groups for virtual desktops or pools of desktops and disconnect active sessions here.

You can filter the information in the tables that are associated with each tab. You can also choose which columns to filter and search when the tabs in the **Entitled Users and Groups** view are selected:

- On the **Entitled Users and Groups** tab, you can choose to filter and search the Display Name or Domain columns.
- On the **Active Sessions** tab, you can choose to filter and search the User or Desktop columns.

When you are in the **Entitled Users and Groups** view, you can choose between the **Inventory** and **Search** tabs on the left side of the Inventory page.

- When you select the **Inventory** tab, all of the entitled users and groups appear in a list on the tab. Selecting a user or group from the list displays information about that user or group on the right side of the page. In addition, the right side of the page displays three tabs: **Summary**, **Desktops**, and **Active Sessions**.

When you select the **Search** tab, the **Search for Desktops:** field displays. Enter search text in this field to search for users or groups. Select the search criteria using the check boxes in **In these categories**.

Configuration Page

The Configuration page opens when you log in to the VDM Administrator user interface for the first time (before adding your license information). It is the same page that is opened when you click **Configuration**. The Configuration page contains the following fields:

- **Access and Security Settings** – Edit license serial number information.
- **VirtualCenter Servers** – Add, edit, or delete VirtualCenter servers for the connection server to use.
- **VDM Servers** – Enable or disable VDM servers (VDM Connection Servers), edit VDM server settings, and enable RSA SecurID.

- **Global Settings** – Enable direct connection to virtual desktops so that connections to desktops are made directly from the client to the virtual machine, enable USB redirection, which allows you to use a locally connected USB devices on a virtual desktop, set SSL for security server that determines if you use HTTP or HTTPS for communication between the client and the VDM Connection Server, and set the session timeout to determine the overall duration of the session before it times out.
- **Administrators** – Add or delete administrators for the connection server and search Active Directory for users or groups and add them as administrators.

Events Page

Use the Events page to view events that an individual connection server generates. You can enter text in the **Contains** field and search by type of message, the time of the message or the message text itself. You can also determine the number of days of messages to display.

Searching Desktops and Entitled Users and Groups

Use the Inventory page to search for information about desktops and entitled users and groups. You can either search by using the columns in the tables that appear on the right side of the page or search by using the categories that appear on the left side of the page.

To search columns in the Desktops Inventory view

- 1 On the Inventory page, choose **Desktops** from the **Show** menu.
- 2 In the **Desktops** field (on the right side of the page), click the **Desktops**, **Virtual Machines**, or **Active Sessions** tab.
- 3 Click the arrow after **Contains** and select the checkboxes for the appropriate columns.
- 4 Click **Done**.
- 5 Enter search text and click **Go**.

To search categories in the Desktops Search view

- 1 On the Inventory page, choose **Desktops** from the **Show** menu.
- 2 In the **Search for desktops** field (on the left side of the page), enter search text.
- 3 In the **In these categories** field, select **Display Name**, **Desktop ID**, **Type**, **User**, or **Virtual Center Name** to search that category.
- 4 Click **Search**.

To search columns in the Entitled Users and Groups Inventory view

- 1 On the Inventory page, select **Entitled Users and Groups** from the **Show** menu.
- 2 In the **Entitled Users and Groups** field (on the right side of the page), click the **Entitled Users and Groups** or **Active Sessions** tab.
- 3 Click the arrow after **Contains** and select the check boxes for the appropriate columns.
- 4 Click **Done**.
- 5 Enter search text and click **Go**.

To search categories in the Entitled Users and Groups Search view:

- 1 On the Inventory page, select **Entitled Users and Groups** from the **Show** menu.
- 2 In the **Search for users** field (on the left side of the page), enter search text.
- 3 In the **In these categories** field, select **Common name**, **Given Name**, **Description**, **Email**, **Display Name**, or **Domain Name** to search that category.
- 4 Click **Search**.

Working with Active Sessions

After you connect to a virtual desktop or desktop pool, active sessions are in the inventory. You can access active sessions on the Inventory page.

To view, disconnect, or reboot active sessions

- 1 Click the **Inventory** tab.
- 2 In **Desktops**, click **Active Sessions**.

You can view the user, desktop ID, DNS name of the VM, start time, duration, and server state (connected or disconnected) for each active session.

- 3 Click anywhere in an active session.

The **Disconnect Session** and **Restart Virtual Machine** options become available.

- 4 Click **Disconnect Session** to disconnect the selected active session or click **Restart Virtual Machine** to restart the active session.

Global Configuration Settings

Use global configuration settings to set VDM behavior, depending on your specific requirements. Table 3-1 lists the global configuration settings.

Table 3-1. Global Configuration Settings

Option	Description
Session timeout (in minutes)	Overall session time limit that starts when a user logs in to the connection server. It is the total amount of time that a user is allowed to be logged in before the session terminates.
Direct connect to virtual desktop	<p>If selected, remote desktop sessions are established directly between the VDM Client and the desktop virtual machine, bypassing the VDM Connection Server (in other words, they do not use tunneled connection).</p> <p>The initial connection is still made to the VDM Connection Server for users to authenticate and select appropriate desktops they are entitled to.</p> <p>This option is appropriate only for deployments inside a corporate network, because RDP traffic is sent unencrypted over the connection between the client and desktop virtual machine.</p> <p>This setting is disabled by default.</p> <p>Changes to this setting take effect for each user upon the next login.</p>
USB redirection	<p>If selected, causes the native client to disable all USB functionality when activated.</p> <p>Changes to this setting take effect for each user upon the next desktop launch.</p>
Require SSL for client connections	<p>If Require SSL for client connections is selected, HTTPS is used as the communication protocol between the client and the VDM Connection Server. Clients who attempt to connect using HTTP are automatically redirected to HTTPS.</p> <p>Changes to this setting require that the VDM Connection Server be restarted to take effect.</p>

Table 3-1. Global Configuration Settings (Continued)

Option	Description
Reauthenticate after network interruption	<p>If selected, determines whether or not user credentials need to be reauthenticated after a network interruption. When this setting is selected, users must reenter their credentials and reauthenticate them against Active Directory. This setting is not available when the Direct connect to virtual desktop setting is selected.</p> <p>If this setting enabled, the client terminates and the user must log on again to the VDM Connection Server (session remains in disconnected state).</p> <p>Requires a restart of the VMware VDM Connection Server to take effect.</p>
Pre-login message	<p>If selected, Client and Web Access users see a disclaimer or login message with information or instructions entered by the administrator.</p>

To configure global settings

- 1 In **Global Settings** on the Configuration tab, click **Edit**.
- 2 Set the session timeout.

Determine how long users are allowed to keep sessions open after they log in to the connection server and enter this value in minutes. The **Session timeout** field must contain a value.
- 3 Set the optional global settings.
 - Select **Direct Connect to Virtual Desktop** to enable connections directly from the client to the virtual machine.
 - Select **USB Redirection** to cause the native client to disable all USB functionality.
 - Select **Require SSL for client connections** to enable HTTPS as the communication protocol between the client and the connection server.

Uncheck the check box to enable HTTP.

- Select **Reauthenticate after network interruption** to force users of virtual desktops to reenter their Active Directory credentials after a network interruption.
- Select **Show a pre-login message to users upon login** if administrators need to configure a message for Web Access or Client users when they log in.

After selecting this check box, type the message into the text field.

- 4 Click **OK**.

Viewing Events

VDM provides a page for viewing events for an individual connection server. You can use the information on the **Events** page for diagnosing problems or viewing activity on the server.

To view events

Click the **Events** tab.

The Events page opens and lists the name of the server for the events that are displayed.

To search events

- 1 Click the arrow after **Contains** and select the columns to search (**Messages**, **Time**, **Type**).
- 2 From the list, choose the number of days of messages to show in the Events table.
- 3 Click **Done**.
- 4 Enter search text in the text box.
- 5 Click **Go**.

Search results appear in the **Events** table. Click (**more**) at the end of each message to display more details about the event.

RSA SecurID

VDM supports RSA SecurID as an additional method for user authentication. RSA SecurID provides strong, two-factor authentication when you access virtual desktops, in addition to the authentication provided when using AD credentials.

If you are using RSA SecurID, you must first enable it by editing your VDM server settings. After you install the RSA SecurID software on your VDM servers, you can edit RSA settings in the VDM administrator user interface.

To enable or edit RSA SecurID

- 1 Click the **Configuration** tab.
- 2 In VDM Servers, click **Edit**.
- 3 In the RSA SecurID dialog box, configure the desired RSA settings:
 - **Enabled** enables RSA SecurID authentication for end users accessing virtual desktops.
 - **Enforce SecurID and Windows user name matching** SecurID checks names against Windows user names and denies access to names that do not match.
 - **Clear node secret** refers to the node secret on the VDM Agent.
For more information about this setting, see the RSA Authentication Manager user documentation.
- 4 In the **Upload RSA authentication agent configuration file (sdconf.rec)** field, enter the location of the `sdconf.rec` file or click **Browse** to search for the file.
For more information about the `sdconf.rec` file, refer to the RSA Authentication Manager user documentation.
- 5 Click **OK**.

Deleting VDM Objects

Delete VDM objects (VirtualCenter, VDM servers, and desktops) by using the administrator user interface.

To remove a VirtualCenter server from a VDM server

- 1 Click the **Configuration** tab.
- 2 In **VirtualCenter Servers**, click **Remove**.
If desktops are using this VirtualCenter server, an error message tells you that you must first delete the desktops using this VirtualCenter before you can delete the VirtualCenter.
If no desktops are using this VirtualCenter server, a warning message tells you that you can no longer access virtual machines managed by this virtual center.
- 3 Click **OK**.
The VirtualCenter server is deleted.

To delete a desktop from a VDM server

- 1 Click the **Inventory** tab.
- 2 In **All Desktops**, click the **Desktops** tab.
- 3 Select a desktop to delete and click **Delete**.

You are given the option to remove the virtual machines from the connection broker only, which means they are still visible in VirtualCenter, or to delete them from disk, which means they are no longer visible in VirtualCenter.

If the desktop has active sessions, you are given the option to disconnect the users, which means users lose their connected desktops, or to leave the users connected, which means users do not lose their connected desktops.

To delete a virtual machine from a VDM desktop

- 1 Click the **Inventory** tab.
- 2 In **All Desktops**, select the desktop containing the virtual machine to delete.
- 3 Click the **Virtual Machines** tab.
- 4 Click **Delete**.

You are given the option to remove the virtual machines from the connection broker only, which means they are still visible in VirtualCenter, or to delete them from disk, which means they are no longer visible in VirtualCenter and deleted from the datastore.

If the desktop has active sessions, you are given the option to disconnect the users (if remove from the connection broker is chosen), which means users lose their connected desktops, or to leave the users connected, which means users do not lose their connected desktops.

Installing SSL Certificates

The VDM Connection Server includes a self-signed SSL certificate that you can use the first time you connect. This certificate is not trusted by clients and does not have the correct name for the service, but it does allow connectivity.

Replace these initial certificates with properly constructed certificates for the service. This removes the certificate check messages that users see and allows thin client devices to connect.

To install certificates, follow these high-level steps:

- 1 Create a suitable Certificate Signing Request (CSR).
- 2 Submit the request to your Certificate Authority (CA) and receive the new certificate.
- 3 Import the certificate into the keystore for the VDM Connection Server.
- 4 Configure the VDM Connection Server to use this new certificate.

Creating the CSR

Deciding what name to bind to a CSR is an important consideration. A certificate binds the name of the service to a cryptographic key pair and, in doing so, assumes ownership of the service and keys. The client can trust the server (and its cryptographic key) because the CA independently determined that the organization that is claiming ownership requested the key.

The most important part of the CSR is the common name (CN) attribute. Use the name that the client computer uses to connect to the VDM Connection Server. In a single-server environment, the name is typically the name of the server. If load balancing is being used, use the load-balanced name.

To create the CSR

- 1 Using the Windows command prompt, create a new keystore containing a public-private key pair:

```
%JAVA_HOME%\bin\keytool -genkey -keyalg "RSA" -keystore keys.p12
-storetype pkcs12 -storepass <secret> -validity 360
```

- 2 Answer the following questions:

- What is your first and last name?

This is the CN attribute. Enter the server name or load-balanced name, for example, server.vmware.com.

- What is the name of your organizational unit?

This is information about where in your organization this server is being deployed. Your CA might have requirements for completing this field. For example, it might require the company's domain name (for instance, vmware.com).

- What is the name of your organization?

This might be your department or company name.

- What is the name of your City or Locality?

Enter your location or leave blank (Unknown).
 - What is the name of your State or Province?

Enter your state information or leave blank (Unknown).
 - What is the two-letter country code for this unit?

Enter your country code (GB, for example).
- 3 Confirm the full name, enter **Yes**, and press **Enter**.

The keys .p12 file is created in the current directory.
 - 4 Use the following key pair to create a CSR:

```
%JAVA_HOME%\bin\keytool -certreq -keyalg "RSA" -file certificate.csr
-keystore keys.p12 -storetype pkcs12 -storepass secret
```

The `certificate.csr` file is created in the same location. The contents of the file look like the following example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBuDCCASECAQAwDELMAkGA1UEBhMCR0IxEDA0BgNV
BAgTB1Vua25vd24xEDA0BgNVBAcTB1Vua25vd24xFDAS
BgnVBAoTC1ZNd2FyZSBjbWuMRMwEQYDVQQLW2p2bXdh
cmUuY29tMR0wGAYDVQQDExFzZXJ2ZXIudm13YXJlLmNv
bTcBbnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA85iM
2G4J695Nh3LFU0S7eAdXHG51MtRcFR397jj0sjFk2THO
T8Xkeue6pCAG0E9vsRSKiFZiMQL0TSkg0Vwd+bYDMzMx
Uam/baSq7z7JF8irTHXYB/1PXDwdykUI7jYSRVxhjbHm
XU8/2jEUL5DocLDLnysUD2g7cUMYdz/HeECAwEAAA
MA0GCSqGSIb3DQEBBQUAA4GBALq2e5FWHQIE26J0LI dR
FLQqlsu78IsuGF19nvJSxrdnHFUpUvTaTA3auGsz+UJG
/vdHqFt49oSIRIhd7NALLumBo0q4tEywvE3vq0ytUvIE
imJCKsAiAeyWZUydJps+zhVKKhisCGFh60AZp1bmTJgu
AeHnsPs7a1Q0JH60ZvdU
-----END NEW CERTIFICATE REQUEST-----
```
 - 5 (Optional) Back up the `keys.p12` file after the certificate is imported into it in case you need to rebuild the configuration for the server at some point.

To submit the CSR and import the certificate

- 1 Contact your CA and provide the relevant information and a copy of the CSR generated in “To create the CSR” on page 59.
- 2 Request a certificate in PKCS#7 format.

For testing purposes, Thawte provides a free CA at <https://www.thawte.com/cgi/server/try.exe> that generates a 21-day SSL certificate based on an untrusted root. This is slightly better than the get-you-started certificate supplied with VDM because it now uses the correct name. However, clients still issue warnings that the service is not trusted.

- 3 Copy the contents of the generated file into a text editor and save it as `certificate.p7`.

The file looks like the following example:

```
-----BEGIN PKCS7-----
MIIF+AYJKoZIhvcNAQcCoIIF6TCCBeUCAQExADALBgkqhkiG9w0BBwGgggXNMIID
LDCCApWgAwIBAgIQTpY7DsV1n1HeMGgMjMR2PzANBgkqhkiG9w0BAQUFADCBhzEL
...
i7coVx71/lCB0lFmx66NyKlZK5m0bgvd2dlnsAP+nnStyhVHFIPky3nsD04JqrIg
EhCsdpiKSpbtDo18jUubV6z1kQ71CrRQtbi/WtdqxQEETgZCJO2lPoIWMQA=
-----END PKCS7-----
```

- 4 Import the certificate into the keystore using the following command (change the password and replace `secret` with another password):

```
%JAVA_HOME%\bin\keytool -import -keystore keys.p12 -storetype pkcs12
-storepass secret -keyalg "RSA" -trustcacerts -file certificate.p7
```

This operation might generate the following message:

```
... is not trusted. Install reply anyway?
```

This message is generated because the root certificate given to you is not trusted by Java because it is a test certificate and not for production use. Installing this certificate is allowed but might not provide a better user experience than the get-you-started certificate.

To configure the VDM Connection Server to use the new certificate

- 1 Place a new certificate file in the following location on each VDM Connection Server (standard, replica, or security server):

```
C:\Program Files\VMware\VMware VDM\Server\sslgateway\conf
```

- 2 Create or edit the following file on each server:

```
C:\ProgramFiles\VMware\VMwareVDM\Server\sslgateway\conf\
locked.properties
```

- 3 Add the following properties:

- keyfile=keys.p12
- keypass=secret

This changes the values as needed to match what you created in the previous step.

- 4 Restart the VDM service.

Assuming your environment is configured to use SSL, a log message like the following appears:

```
13:57:40,676 INFO <Thread-1> [NetHandler] Using SSL certificate store:
keys.p12 with password of 6 characters
```

This message indicates that the configuration is in use.

Load Balancing

When you set up and configure servers for VDM, load balancing is an important design consideration. Load balancing provides the highest level of scalability and helps avoid any single points of failure. Load balancing addresses the scaling and fault tolerance of your VDM solution.

The VDM Connection Server is the core component of VDM. You can deploy the VDM Connection Server as either a connection server or as a security server. VDM Connection Servers provide session management and handle all incoming client requests and direct them to the appropriate virtual desktop session. The VDM Security Servers ensure secure communication between the client devices and the VDM Connection Servers.

You might already have an existing load-balancing solution in place supporting current business applications and services. You can leverage existing load-balancing services can because the load that VDM uses on the load balancing infrastructure is minimal. In addition to typical hardware-based load-balancing appliances, inexpensive or free software-based products can also be considered as possible load-balancing solutions.

You can deploy load balancing whether you are using a DMZ deployment with security servers deployed inside a DMZ, or a non-security server deployment with end users connecting directly to VDM Connection Servers. See “Load Balancing in a DMZ Deployment” on page 67.

Load Balancing in a Non-DMZ Deployment

In some cases, such as LAN-based deployments, users can connect directly to VDM Connection Servers. In this case, no VDM Security Servers are deployed. You can use tunneled or non-tunneled deployment available for LAN-based connections. When tunneling is enabled, all VDM traffic is encrypted and tunneled through a VDM Connection Server. When tunneling is not enabled, session traffic is not routed through the VDM Connection Servers and therefore is not SSL-encrypted. After a client connects to the virtual desktop that it uses, all communication is between the client and the virtual desktop.

Session Setup and Load Balancing

To configure load balancing, it is important to understand how sessions are set up and how connection information passes between the client and the connection servers.

The initial HTTP or HTTPS TCP session is established between the client and VDM Security Server or VDM Connection Server. The user is authenticated during the initial connection. If authentication is successful, control information is returned to the client. The control information includes a list of virtual desktops to which the user is entitled to connect and the fully qualified domain name (FQDN) of the VDM Connection Server or VDM Security Server.

After the client receives connection information, it initiates a second TCP session for the tunnel to the FQDN (of the connection server). The second TCP session is an SSL tunnel between the client and the security server or VDM Connection Server. After this TCP session starts, the RDP client on the client machine connects to the local host listener and traffic is routed through the tunnel to the security server and then to the virtual desktop.

The VDM secure connection is used for communication in an RDP session. When a client is ready to establish an RDP session with the selected virtual desktop, the client starts a local TCP listener. After it is started, a TCP session is established between the VDM Connection Server and the virtual desktop running on the ESX server. The RDP client on the client machine then connects to the local host, and communication is handled by using the VDM secure connection previously established.

In a load balanced configuration, when a client establishes a TCP session, the TCP session can be established with different hosts. For example, the client's first connection from the client to the load balancer might be to a global DNS name such as `https://vdi-yourcompany.com`. The load balancing infrastructure then forwards the

request to <https://vdm1.example.com>, one of the servers in the VDM Security Server farm. You can use one of several common load balancing methods (proxy, HTTP redirect, NLB cluster, round robin DNS, and so forth) to decide which VDM server is to handle the session.

After the VDM client authenticates with the VDM server, it receives specific instructions to connect directly to <https://vdm1.example.com> and establish an SSL tunnel.

DNS Requirements for a Load-Balanced Solution

Regardless of the load-balancing mechanism you use, a client must be able to connect with each VDM server by its FQDN directly. That is, the client must be able to bypass the load balancing altogether. In cases where VDM Security Servers are deployed inside the DMZ or when VDM Connection Servers are accessed from a local area network, all servers must have valid DNS names.

The load balancer makes the initial decision about which VDM Connection Server is to handle the client session by directing the first TCP session to the chosen VDM Connection Server. The secure tunnel connection is made directly from the client to the VDM Connection Server and as a result does not use the load-balancing infrastructure for this connection, which carries the bulk of network traffic between client and server.

Load-Balancing Solution

You can take several approaches when you implement a load-balancing solution for VDM servers. For example, round-robin DNS, while technically the most simple load-balancing solution to implement, has a significant disadvantage from a failover perspective. If one of the servers fails, it must be removed from the DNS list of records corresponding to the load-balanced domain name. Another issue with a round-robin DNS approach is in the remote-access use case where VDM clients are accessing their virtual desktops across the Internet, through the VDM Security Servers. In this case, the responses of the master DNS server are cached in upstream DNS servers. It can take several hours for a removed DNS name to be replicated to all Internet DNS servers. If a server is out of service, client connections can fail if they are directed to that server during the time it takes for the cached record to expire on all Internet DNS servers.

Support for a redundancy and failover mechanism, typically at the network level, prevents the load balancer from becoming a single point of failure. For example, using the virtual router redundancy protocol (VRRP) to communicate with the load balancer adds redundancy and failover. If the main load balancer fails, another load balancer in the group automatically starts handling connections.

To provide a degree of fault tolerance, a load-balancing solution must be able to remove failed VDM server nodes from the load-balanced group. The way in which failed nodes are detected varies from solution to solution. The solution must ensure that new incoming sessions are not directed to the unresponsive server.

If a VDM server fails or becomes unresponsive during an active session, users do not lose data and desktop states are preserved in the virtual desktop. When users reconnect to a different VDM server in the group, their desktop sessions continue where they were when the failure occurred.

The load balancing solution you choose must support Web session affinity between the client and VDM Connection Server. Web session affinity means that a particular Web session is always directed to the same server.

Many inexpensive and free load-balancing solutions are available that you can use with VMware VDM. Any standards-based load balancer that supports session affinity is acceptable.

Two examples of software-based load balancers are Hercules and Windows Network Load Balancing (NLB). Hercules is a free Linux-based virtual appliance that delivers the open source load balancer called Pen. Windows NLB is a feature available with Windows Server 2003.

DMZ Deployment

VDM also supports DMZ (security server) deployment, which allows greater security when accessing virtual desktops from the Internet. Servers within the DMZ run a subset of the full VDM Connection Server. DMZ deployment adds an additional layer of security and ensures that only authenticated users can attempt a connection to the internal network from the Internet.

DMZ Installation

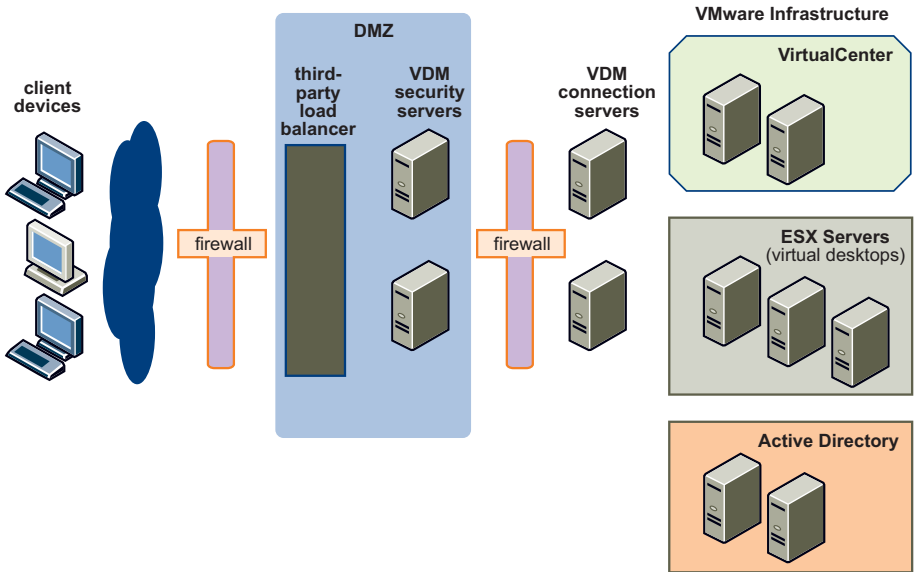
DMZ deployment has the following entities or locations: the Internet, the DMZ, and the internal network. Clients who need access to the virtual desktops reside on the Internet. The virtual desktops are located on the internal network along with the rest of the components that comprise the virtual desktop infrastructure. The DMZ sits between the Internet and the internal network and reduces the risk of the internal network being compromised.

Depending on your particular server configuration, load balancing might be required. You need either a hardware or software load-balancing solution if you have more than one security server.

When you consider firewalls, the stronger approach is to use two firewalls, where the DMZ is between and connected to both firewalls. In this configuration, one firewall is connected to the internal network and the other to the external network.

Figure 3-3 shows a DMZ deployment that allows users to access their desktops from the Internet. It includes a load balancer and firewalls on each side of the DMZ.

Figure 3-3. VDM DMZ Deployment



To perform a DMZ installation for a security server

- 1 Run `VMware-vdmconnectionserver-2.1.0-<xxx>.exe`.
<xxx> is the build number of the software component you are installing.
 The Installation wizard opens.
- 2 Click **Next**.
- 3 Accept the license terms and click **Next**.
- 4 Accept or change the destination folder and click **Next**.
- 5 Choose **Security Server**.

- 6 Enter the FQDN of the connection server (either standard or replica) with which the security server is to communicate.

Each security server is paired with a VDM Connection Server and forwards all traffic to that server.

- 7 Click **Next > Install > Finish**.

Load Balancing in a DMZ Deployment

When you deploy a VDM Security Server inside a DMZ, a link is established with a dedicated VDM Connection Server during the installation process. When VDM Security Servers are deployed inside the DMZ, they must be load balanced inside the DMZ to provide scalability and fault tolerance.

Configuring Firewall Ports for DMZ Deployments

When you set up firewalls in a DMZ deployment, you must configure the firewall rules so that the TCP protocol traffic that needs to pass through the firewall can. The settings described in this section are based on a DMZ deployment where firewall rules are configured from an external network (the Internet, for example) and from the DMZ to the internal network. The settings also assume that clients access VDM from an external network and connect by using VDM Security Servers located within the DMZ and that VDM is set up using default TCP ports for each protocol.

To access a DMZ from an external network and allow client devices to connect to VDM Security Servers within the DMZ, allow TCP ports 80 and 443.

If you connect to the internal network from a DMZ using VDM Security Servers in the DMZ to connect to VDM Connection Servers (standard or replica instances) in the internal network, allow TCP port 8009 for AJP13-forwarded Web traffic and allow TCP port 4001 for JMS messaging traffic.

To connect to the internal network from a DMZ using VDM Security Servers to connect to desktop virtual machines, allow TCP port 3389 for VDM-secured RDP traffic.

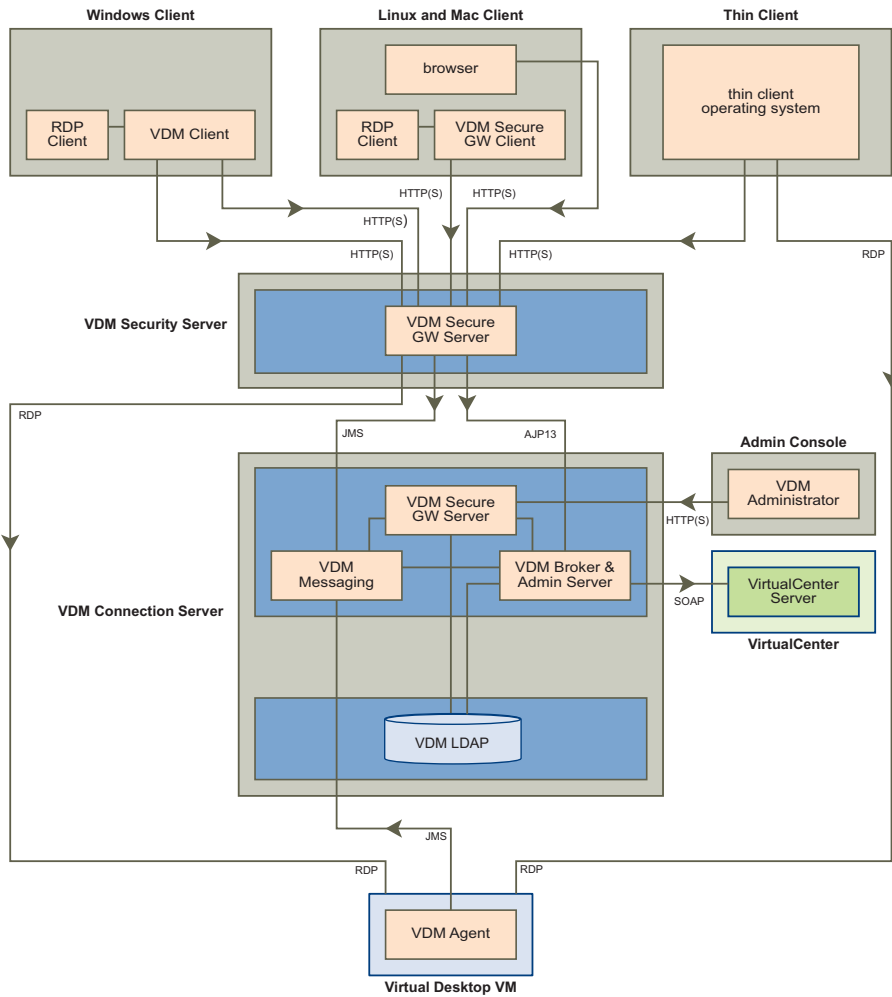
The following default TCP ports are used for each protocol. Use the list of protocols and associated ports as a reference for Figure 3-4.

- JMS – 4001
- AJP13 – 8009
- HTTP – 80
- HTTPS – 443

- RDP – 3389
- SOAP – 80 or 443

Figure 3-4 shows a VDM Security server and shows the relationship with all other VDM components and the protocols used for communication between the components.

Figure 3-4. VDM Component Diagram with Security Server



Exporting and Importing VDM Configuration Data

VDM allows you to export the contents of the primary root of the VDM lightweight directory access protocol (LDAP) data from a VDM Connection Server (standard or replica instance) to preserve this information and import it to other VDM connection servers. The export file format is an LDAP data interchange format (LDIF), which is a standard file format for exchanging LDAP data. If you have multiple VDM connection servers, you only need to export the data from one server because all replicated VDM Connection Servers contain the same VDM configuration data.

To export VDM configuration data

Open a command prompt and run this command:

```
C:\Program Files\VMware\VMware VDM\Server\bin\vdmexport
><MyVDMConfig.LDF>
```

Running this command creates a file called MYVDMConfig.LDF that contains the exported data.

To import VDM configuration data

Open a command prompt and run the following command:

```
LDIFDE -i -f MyVDMConfig.LDF -s 127.0.0.1 -z
```

Client Command-Line Parameters

VDM has settings available through the native client command-line parameters. Administrators can use the command line options to preconfigure VDM client settings.

To display the available command line options, type `wsvc /?` on the command line.

Options are preceded by a hyphen (-) or a forward slash (/). Option text is case-insensitive and can be abbreviated down to its shortest unique form.

For scripting, all scripting parameters except file and languageId can also be specified by AD group policies. They can be order checked as follows: cmdline, machine group policies, user group policies.

The following is a list of the command line options:

- `-serverURL <xxx>` – The URL for the VDM Connection Server to use in the connection dialog box.
- `-userName <xxx>` – User name for the server login dialog box.
- `-domainName <xxx>` – Domain name for the server login dialog box.

- `-password <xxx>` – Password for the server login dialog box.
- `-desktopName <xxx>` – Desktop name for the select desktop dialog box. This is the name as you see it in the select desktop dialog box, not the long desktop id.
- `-screenFull` – Use full-screen desktop mode (only used if `desktopName` is specified).
- `-screenWindow` – Use Window desktop mode (only used if `desktopName` is specified).
- `-screenMulti` – Use full-screen multi-monitor desktop mode (only used if `desktopName` is specified).
- `-nonInteractive` – Used to suppress error message boxes for fully scripted startup.
- `-languageId <xxx>` – A Windows language id to use. If a resource dll is available (for US english), type `0x409`.
- `-file <xxx>` – Text file with additional command line parameter. To simplify repetitive tests, type `wswc /f test1`.

Fully scripted dialog boxes are auto-invoked and are displayed with only the **Cancel** button enabled. If the **Cancel** button is selected, the client exits. The Connect dialog box is fully scripted if the server URL is specified. The Login dialog box is fully scripted if the Connect dialog box is fully scripted and `userName`, `domainName` and `password` are specified. The Select Desktop dialog box is fully scripted if the Login dialog box is fully scripted and `desktopName` is specified.

Collecting VDM Diagnostic Information

Diagnostic information helps VMware Technical Support diagnose and resolve issues with VDM. VDM includes a script called `vdm-support` that collects information for use by VMware Technical Support. Send the file generated by the script with your support request. On the VDM Connection Server you can run the script manually or by using the support tool in the **Start** menu. For VDM Windows Client or Web Access and VDM hosted desktops, you must run the script manually.

Using the VDM Support Tool to Collect Diagnostic Information

The VDM Support tool lets you generate log files and set log levels that determine if you want to generate normal, debug, or full log files for the VDM Connection Server.

To set log levels using the VDM Support Tool

- 1 On the VDM Connection Server, click **Start**, click **All Programs**, and click **VMware**.
- 2 Select **Set VDM Log Levels**.
- 3 In the **Choice** field, type 1 for normal, 2 for debug, or 3 for full and press **Enter**.

To generate log files using the VDM Support Tool

- 1 On the VDM Connection Server, click **Start**, click **All Programs** and click **VMware**.
- 2 Select **Generate VDM Log Bundle**.

The support tool creates a folder called `vdm-sdct` on the desktop of the VDM Connection Server and places the generated log files in it.

Using the VDM Support Script to Collect Diagnostic Information

Use VDM Support Script to generate log files for VDM Connection Servers, Windows Client and Web Access, and VDM hosted desktops.

To collect diagnostic information using the script

- 1 Open a command prompt.
- 2 Change to the VDM program directory.

If you did not install the program in the default directory, use the appropriate drive letter and substitute the appropriate path in the change directory commands, as follows:

- On the VDM Connection Server, run this command: `cd C:\Program Files\VMware\VMware VDM\Server\DCT`
- On VDM Windows Client or Web Access, run this command: `cd C:\Program Files\VMware\VMware VDM\Client\DCT`
- On the VDM hosted desktop, run this command: `cd C:\Program Files\VMware\VMware VDM\Agent\DCT`

- 3 Run the support script:
`cscript vdm-support.vbs`

When the script finishes, it informs you of the output filename and location.

- 4 Copy the script output to another location.

To transfer the compressed output file to another computer, you can use an Secure copy (SCP) or FTP client. If you use an FTP client, make sure that it copies the file in binary mode to ensure the whole file is transferred intact.

WinSCP is an SCP client for Microsoft Windows and is available on the Microsoft Web site. Before you can send the information to VMware Technical Support, file a support request on the Support page of the VMware Web site.

Updating Support Requests

After you file a support request, you might receive an email request from VMware Technical Support asking for the output of the `vdm-support` script. Reply to the email message and attach your script output file to the reply. If the output is too large to include as an attachment (10MB or more), contact VMware Technical Support with your support request number and request FTP upload instructions. You can also update your support request and attach the file at the support Web site.

To update your support request

- 1 Navigate to the Support page at the VMware Web site and log in.
- 2 Click **Support Request History** and find the applicable support request number.
- 3 Update the support request and attach your `vdm-support` script output.

Troubleshooting VDM

The following URLs for VMware Knowledge Base (KB) articles contain troubleshooting information for VDM. The KB articles are continually updated with new troubleshooting information.

- Use the following URL for troubleshooting end user connection issues:
<http://www.vmware.com/info?id=342>
- Use the following URL for troubleshooting pooling issues:
<http://www.vmware.com/info?id=343>
- Use the following URL for troubleshooting USB issues:
<http://www.vmware.com/info?id=346>

VDM Client Advanced Active Directory RDP Settings



The default configuration settings used in the VDM Client are suitable for most situations. However, you can configure some advanced settings in the registry of the client computer that affect the behavior of the VDM Client, particularly advanced RDP connection settings.

You can manage these settings in the client computer registry in several ways. If the settings are not present, the default value is taken for that setting. In most situations, no registry updates are ever required.

Table A-1 describes the settings that you can define in the HKEY_CURRENT_USER directory to override the default behavior. The registry setting names correspond to the Microsoft setting name. For more information about these settings, see the Microsoft TechNet articles.

Table A-1. Client Registry Settings for the Client

Name	Type	Description
Software\VMware, Inc.\VMware VDM\Client\EnableShade	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\InitialPinState	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\DisableSpanChecks	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\ColorDepth	REG_SZ	Defined in bits: 8, 15, 16, 24, or 32.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\DisableWallpaper	REG_SZ	True or false.

Table A-1. Client Registry Settings for the Client (Continued)

Name	Type	Description
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\DisableFullWindowDrag	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\DisableMenuAnimations	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\EnableEnhancedGraphics	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\DisableCursorShadow	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\FontSmoothing	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\DesktopComposition	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\AudioRedirectionMode	REG_SZ	0 = Redirect to Client. 1 = Play in virtual machine. 2 = Disable audio.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\RedirectDrives	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\RedirectPrinters	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\RedirectPorts	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\RedirectSmartcards	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\RedirectClipboard	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\RedirectPlugAndPlayDevices	REG_SZ	True or false.

Table A-1. Client Registry Settings for the Client (Continued)

Name	Type	Description
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\BitmapPersistence	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\ShadowBitmap	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\CachePersistenceActive	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\EnableCompression	REG_SZ	True or false.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\KeyboardHookMode	REG_SZ	0 = Apply key combinations locally. 1 = Send key combinations to VM.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\BitmapCacheSize	REG_SZ	Size in KB, between 1 and 32.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\BitmapVirtualCacheSize	REG_SZ	Size in KB, between 1 and 32.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\BitmapVirtualCache16BppSize	REG_SZ	Size in KB, between 1 and 32.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\BitmapVirtualCache24BppSize	REG_SZ	Size in KB, between 1 and 32.
Software\VMware, Inc.\VMware VDM\Client\RDP Settings\BitmapVirtualCache32BppSize	REG_SZ	Size in KB, between 1 and 32.

Using Active Directory Group Policies for Advanced Settings

Group Policy settings define the components of the user's desktop environment that a system administrator needs to manage. The advanced options are stored in the registry of the client computers and you can manage them by using Group Policy settings in Active Directory.

VDM Connection Server includes an administrative template file (`vdm_client.adm`) that you can load into Active Directory to simplify the management of Group Policy settings on each VDM Client computer. This file is located on each VDM Connection server in `C:\Program Files\VMware\VMware VDM\Server\ADM`.

The Microsoft TechNet article at the following URL provides information about adding this administrative template in Active Directory:

<http://technet2.microsoft.com/windowsserver/en/library/b9546edf-751f-4a09-835a-f3397caef2361033.mspx?mfr=true>

VDM Group Policy Objects

B

Use the VDM group policy objects (GPO) settings to configure the group policies for the VDM Agent, VDM Client, and VDM Connection Server. This appendix describes the VDM GPO settings.

This Appendix covers these GPO types:

- “Computer Configuration” on page 77
- “VDM User Configuration for VDM Client” on page 80

Computer Configuration

VDM provides GPO administration templates to control computer configuration settings for VDM Agent, VDM Client, and VDM Connection Server.

VDM Agent Configuration

Use the following GPOs to configure VDM Agent settings:

- Log Configuration (number of days to keep logs) – Set this value to control the number of days for which log files are kept on the system. If no value is set, the default applies and log files will only be kept for seven days.
- Agent Configuration
 - AllowDirectRDP – If this value is enabled; it will be possible to connect directly to the virtual machine using any RDP client, other than just via the VDM Connection Server. The default value of this is false.

- **AllowSingleSignon** – Enable this value to allow single sign-on. In this case, users will only need to enter their credentials when connecting to the VDM Connection Server, otherwise they will need to login again when the remote connection is made. The default value of this is true.
- **VdmConnectionTicketTimeout** – Time in seconds for which the VDM connection ticket is valid. A VDM connection ticket is used by VDM clients when connecting to VDM Agent and is used for verification and single sign-on purposes. For security reasons, these tickets are only valid within the specified time period. If this value is not set, a default of 120 seconds applies.
- **Connect Using DNS Name** – If enabled, the VDM Server uses the DNS name of the machine to connect to, rather than its IP address. This is often used in a NAT/Firewall situation when the VDM client or VDM Server cannot use the virtual desktop IP address directly. The default value of this is true.
- **Enable extended logging** – Enable this value to include trace and debug events in the VDM log files.
- **Disk threshold for log and events in MegaBytes** – Set this value to control the maximum disk space for logs and events. If no value is set, a default of 200 (Megabytes) applies. When this value is reached, event logging will stop.

VDM Client Configuration

Use the following GPOs to configure VDM Client settings:

- **Log Configuration (Number of days to keep logs)** – Set this value to control the number of days for which log files are kept on the system. If no value is set, the default applies and log files will only be kept for seven days.
- **Scripting Definitions**
 - **VDM Server URL** – Set this value to specify the default VDM Server URL.
 - **VDM logon UserName** – Set this value to specify the default logon name.
 - **VDM logon DomainName** – Set this value to specify the default domain name.
 - **VDM Logon Password** – Set this value to specify the default password.
 - **DesktopName to select** – Set this value to specify the default desktop to select.
 - **DesktopLayout (when fully scripted only)** – Select from fullscreen, multimonitor or window.
 - **Suppress error messages (when fully scripted only)** – Set to enabled to suppress error messages.

- Security Settings (These are options that can be set with WinInet.dll and are used when connecting to the VDM Server using HTTPS).
 - Ignore incorrect SSL certificate common name (host name field) – Set this to enabled or disabled.
 - Ignore bad SSL certificate data received from the server – Set this to enabled or disabled.
 - Ignore unknown certificate authority problems – Set this to enabled or disabled.
 - Ignore certificate revocation problems – Set this to enabled or disabled.
 - Ignore incorrect usage problems – Set this to enabled or disabled.
- Enable extended logging – Enable this value to include trace and debug events in the VDM log files.
- Disk threshold for log and events in MegaBytes – Set this value to control the maximum disk space for logs and events. If no value is set, a default of 200 applies. When this value is reached, event logging will stop.

For more information about these security settings, refer to the Microsoft WinInet documentation on the Microsoft Website.

VDM Server Configuration

Use the following GPOs to configure VDM Server settings:

- Log Configuration (number of days to keep logs) – Set this value to control the number of days for which log files are kept on the system. If no value is set, the default applies and log files will only be kept for seven days.
- Enable extended logging – Enable this value to include trace and debug events in the VDM log files
- Disk threshold for log and events in MegaBytes – Set this value to control the maximum disk space threshold for logs and events. If no value is set, a default of 200 applies. When this value is reached, event logging will stop.

VDM User Configuration for VDM Client

Use the following user configuration GPOs to configure VDM client settings for end users:

- Scripting Definitions
 - VDM Server URL – Set this value to specify the default VDM Server URL.
 - VDM logon UserName – Set this value to specify the default logon name.
 - VDM logon DomainName – Set this value to specify the default domain name.
 - VDM Logon Password – Set this value to specify the default password.
 - DesktopName to select – Set this value to specify the default desktop.
 - DesktopLayout (when fully scripted only) – Select from fullscreen, multimonitor or window.
 - Suppress error messages (when fully scripted only) – Set to enabled to suppress error messages.
- RDP Settings (Refer to Microsoft documentation for a full description of the RDP Settings).
 - Color Depth – For 24 bit Windows XP, ensure that the Limit Maximum Color Depth policy in Computer Configuration/Administrative Templates/Windows Components/Terminal Services is set to Enabled at 24 bit.
 - Desktop Background
 - Show contents of window while dragging
 - Menu and animation
 - Themes
 - Cursor shadow
 - Font smoothing
 - Desktop composition

- Audio redirection
 - Redirect to client – MS RDP redirection played on client, default if not configured
 - Play in VM (needed for VoIP USB support) – Play in VM needs a shared USB audio device
 - Disable Audio – no audio
- Redirect drives
- Redirect printers
- Redirect serial ports
- Redirect smart cards
- Redirect clipboard
- Redirect supported plug and play devices
- Bitmap caching
- Shadow bitmaps
- Cache persistence active
- Windows key combinations
- Bitmap cache file size in Kb for 8bpp bitmaps
- Bitmap cache file size in Mb for 8bpp bitmaps
- Bitmap cache file size in Mb for 16bpp bitmaps
- Bitmap cache file size in Mb for 24bpp bitmaps
- Bitmap cache file size in Mb for 32bpp bitmaps
- Enable the shade – Set this to enabled or disabled
- Pin the Shade – Set this to enabled or disabled
- Don't check monitor alignment on spanning – Set this to enabled or disabled
- Enable multi-media acceleration – Set this to enabled or disabled

Refer to Microsoft documentation for a full description of the RDP Settings.

Glossary

A **Active Directory**

A Microsoft directory service that stores information about the network operating system and provides services. Active Directory configures and manages users and groups and enables administrators to set security policies, control resources, and deploy programs across an enterprise.

ADAM (Active Directory Application Mode)

An LDAP implementation based on Active Directory.

active session

A live connection from a client or Web Access user to a virtual desktop. An established connection to a virtual desktop that has not timed out.

administrator user interface

The Web-based administrator user interface used to perform configuration and management tasks in VDM. Also known as the VDM Administrator.

B **broker**

Also known as a connection broker. The VDM Connection Server is a type of connection broker.

C **connection broker**

A server that allows connections between remote users and virtual desktops and provides authentication and session management. The VDM Connection Server is a type of connection broker.

D **datastore**

Virtual representations of combinations of underlying physical storage resources in the datacenter. A datastore is the storage location (for example, a physical disk, a RAID, or a SAN) for virtual machine files.

desktop

See “virtual desktop.”

desktop virtual machine

See “virtual desktop.”

desktop pool

A pool of virtual machines that an administrator designates for users or groups of users. *See also “persistent desktop pool,” “non-persistent desktop pool.”*

DMZ (demilitarized zone)

A logical or physical subnetwork that connects internal servers to a larger, untrusted network (usually the Internet) and provides an additional layer of security and gives administrators more control over who can access network resources.

DNS (Domain Name System)

An Internet data query service that translates host names into IP addresses. Also called “Domain Name Server” or “Domain Name Service.”

F **FQDN (fully qualified domain name)**

The name of a host, including both the host name and the domain name. For example, the FQDN of a host named `esx1` in the domain `vmware.com` is `esx1.vmware.com`.

G **guest**

See “guest operating system.”

guest operating system

An operating system that runs inside a virtual machine.

H **high availability**

A system design approach that ensures a degree of operational continuity.

L **load balancing**

A technique used for distributing processes across servers so that the traffic load is spread more evenly and servers do not become overloaded.

- N** **non-persistent desktop pool**
A desktop pool in which users are not assigned to a specific desktop. When users log off or are timed out of a desktop, their desktops are returned to the pool and made available to other users. Users cannot save data or files to their desktops when using a non-persistent pool.
- P** **persistent desktop pool**
A desktop pool in which users are assigned to a specific desktop. Users log on to the same desktop every time and their data is preserved when they log off. Users can save data and files to their desktops when using a persistent pool.
- R** **RDP (remote desktop protocol)**
A multichannel protocol that allows a user to connect to a computer remotely.
- RSA SecurID**
A product from RSA that provides strong, two-factor authentication using a password and an authenticator.
- S** **security server**
A VDM Connection Server deployment that adds a layer of security between the Internet and the internal network.
- T** **thin client**
A device that allows a user to access virtual desktops but requires little memory or disk drive space. Application software, data, and CPU power resides on a network computer and not on the client device.
- V** **virtual desktop**
A desktop operating system that runs on a virtual machine. A virtual desktop is indistinguishable from any other computer running the same operating system.

Index

A

active sessions **53**

C

client command-line parameters **69**

configuration

 end-to-end **35**

 individual desktop **35**

 one-time **14, 33**

 pooled desktop **36**

customization specification **29**

D

desktop virtual machines

 preparing **11, 28**

desktops

 connecting to **45**

 connecting using the VDM
 Client **17, 45**

 connecting using VDM Web
 Access **18, 46, 47**

 entitling **45**

DMZ

 firewall ports **67**

E

events **56**

 viewing **56**

G

global configuration settings **54**

 direct connection to virtual
 desktop **54**

 reauthenticate after network
 interruption **55**

 require SSL for client
 connections **54**

 session timeout **54**

 usb redirection **54**

global settings

 configuring **55**

GPO

 computer configuration **77**

 user configuration for VDM client **80**

 VDM agent configuration **77**

 VDM client configuration **78**

 VDM server configuration **79**

H

high availability **32**

I

installation

 DMZ **65**

 multiserver **32**

 single server **13, 30, 31**

 VMware Agent **12, 28**

 VMware Tools **11, 28**

installing SSL certificates **58**

L

load balancing **62**

 DNS requirements **64**

 non-DMZ deployment **63**

M

MMR **23**

P

pooled desktop
configuration **39**

R

RSA SecurID **56**
enabling **57**

S

searching
desktops **52**
entitled users and groups
52
security server default TCP ports **67**
SSL certificate
creating the certificate signing
request **59**
importing **61**
installing **58**
using **61**

T

template, desktop virtual machine **29**
templates, creating **29**
troubleshooting **72**

U

upgrading VDM **25**

V

VDM
upgrading **25**
VDM Administrator
Configuration page **51**
Events page **52**
Inventory page **49**

user interface **52**

VDM agent
with multiple NICs **30**
VDM configuration data
exporting **69**
importing **69**
VDM Connection Server
disabling **34**
enabling **34**
installing **30**
SSL certificate **30, 58**
VDM diagnostic information **70**
VDM objects
deleting a desktop from a VDM
server **58**
deleting a virtual machine from a
VDM desktop **58**
removing a VirtualCenter server
from a VDM server **57**
VDM support tool **71**
VirtualCenter
assigning roles **38**
reading customization specifications
role **38**
template **29**
VDM administrator role **37**
VDM permissions **37**
VirtualCenter roles
assigning **39**