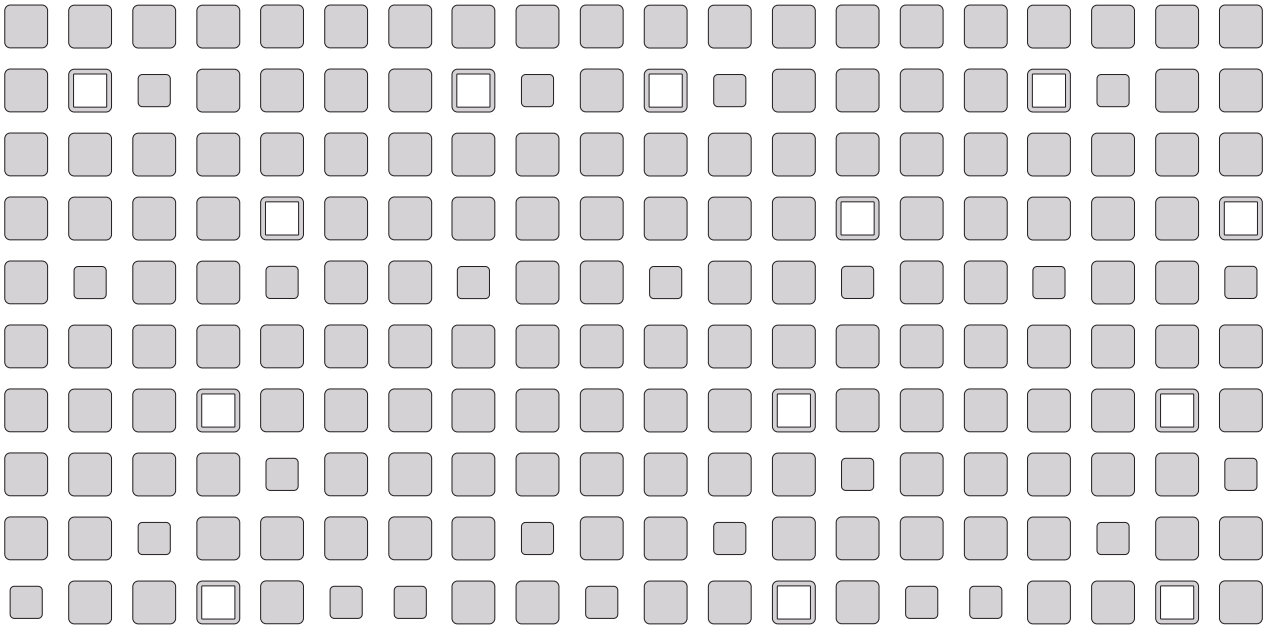
VMware ACE™

The Assured Computing Environment for the Enterprise

Administrator's Manual



vmware®

VMware, Inc.

3145 Porter Drive
Palo Alto, CA 94304
www.vmware.com

Please note that you will always 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.

Revision 20060308 Version: 1.0 Item: ACE-ENG-Q304-008

Table of Contents

Introduction and System Requirements 9
About VMware ACE 10
Ensure Safe Access to Enterprise Resources 10
Secure Data on Enterprise PCs 10
Standardize and Secure PC Environments 10
Key Features of VMware ACE 11
The VMware ACE Software 11
Host System Requirements for VMware ACE Manager 12
Host System Requirements for End Users 14
Virtual Machine Specifications 16
Supported Guest Operating Systems 18
Technical Support Resources 20
Documentation on the Web 20
VMware Knowledge Base 20
VMware User Community 20
Reporting Problems 20

Learning the Basics of VMware ACE Manager 23
Setting Up Your Administrative Workstation 24
Creating Packages to Distribute to Users 26
Basic Steps 26
Keeping Users Up-to-Date 27
Troubleshooting Users' Problems 28

Installing and Configuring VMware ACE Manager 29
Installing VMware ACE Manager 30
Installing on a Computer with a Different VMware Product 30
Installation Steps 30
Installing VMware ACE Manager Silently 33
Uninstalling VMware ACE Manager 35
Setting Preferences for VMware ACE Manager 36
Using Shared Folders in VMware ACE Manager 40

Creating Projects 43
Creating a Project 44
Using the New Project Wizard 44

Making Project Settings 46
Checklist: Creating a Project 49
Adding a Virtual Machine to a Project 51
Adding an Existing Virtual Machine 51
Adding a New Virtual Machine 53
Checklist: Adding a Virtual Machine 63

Setting Policies and Customizing VMware ACE 69
Setting Policies for a Project 71
Using the Policy Editor 71
Setting Policies for VMware ACE 74
Hot Fix Policy 74
Administrator Access Policy 75
Troubleshooting Policies 76
Easy Printer Setup Policies 77
VMware ACE Window Policies 78
User Preferences Policies 79
Setting Policies for Virtual Machines 81
Setting Authentication Policies 81
Setting Expiration Policies 83
Setting Copy Protection Policies 84
Setting Device Connection Policies 85
Setting Network Quarantine Policies 85
Configuring the Virtual Machines and Installing Software 111
Reviewing the Configuration of a Virtual Machine 111
Installing an Operating System and Applications in the Virtual Machine 112
Customizing the VMware ACE Interface 123
Creating and Specifying the Skin File 123
Customizing the VMware ACE Icons 123
Customizing the Title Bar Text 124
Customizing the Removable Device Display 124
Shortcut Key Values 126
Sample Skin File 128
Running the Completed Virtual Machine 129
Checking the Configuration before Creating a Package 129

Creating Packages to Deploy to Users 131
Creating a Package 132
Contents of the Package 136

Deploying and Maintaining Packages 137
Deploying Packages 138
Installing a Package Silently 139
Updating Virtual Machines 141
Distributing Software Updates 141
Creating Update Packages 141
Updating Network Quarantine Versions 142
Using nq-set to Update Network Quarantine Versions 146
Deploying Update Packages 149
Responding to Hot Fix Requests 150
Using Administrator Access on the End User's Computer 152

Installing and Running VMware ACE 153
Installing a VMware ACE Package 154
Running VMware ACE 156
Starting VMware ACE 156
Quitting VMware ACE 157
Enlarging VMware ACE to Fill the Screen 159
Understanding VMware ACE Status Indicators 159
Controlling Devices Attached to VMware ACE 160
Setting VMware ACE Preferences 161
Printing from VMware ACE 162
Uninstalling VMware ACE 162
Troubleshooting Problems 163

Using Virtual Disks 167
Configuring Hard Disk Storage in a Virtual Machine 168
Virtual Disk Basics 168
File Locations 169
Defragmenting and Shrinking Virtual Disks 171
Adding Drives to a Virtual Machine 173
Adding Virtual Disks to a Virtual Machine 173
Adding DVD or CD Drives to a Virtual Machine 174
Adding Floppy Drives to a Virtual Machine 176
Connecting a CD-ROM or Floppy Drive to an Image File 177

Disk Performance in Windows NT Guests on Multiprocessor Hosts ____ 178
Improving Performance ____ 178

Preserving the State of a Virtual Machine ____ 179
Using Suspend and Resume ____ 180
Using the Snapshot ____ 182
What Is Captured by the Snapshot? ____ 182
Removing the Snapshot ____ 183
Ways of Using the Snapshot ____ 183
The Snapshot and the Virtual Machine's Hard Disks ____ 184
The Snapshot and Other Activity in the Virtual Machine ____ 184

Networking Virtual Machines ____ 187
Components of the Virtual Network ____ 189
Common Networking Configurations ____ 191
Bridged Networking ____ 191
Network Address Translation (NAT) ____ 192
Host-Only Networking ____ 193
Changing the Networking Configuration ____ 195
Adding and Modifying Virtual Network Adapters ____ 195
Understanding NAT ____ 196
Using NAT ____ 196
The Host Computer and the NAT Network ____ 196
DHCP on the NAT Network ____ 196
DNS on the NAT Network ____ 197
External Access from the NAT Network ____ 197
Considerations for Using NAT ____ 198
Using NAT with NetLogon ____ 198

Configuring Video and Sound ____ 201
Setting Screen Color Depth in a Virtual Machine ____ 202
Changing Screen Color Depth on the Host ____ 202
Changing Screen Color Depth in the Virtual Machine ____ 202
Configuring Sound ____ 204
Installing Sound Drivers in Windows 9x and Windows NT Guest Operating Systems ____ 204

Connecting Devices to Virtual Machines ____ 205
Using Parallel Ports ____ 207
Parallel Ports ____ 207

Installation in Guest Operating Systems 207
Special Notes for the Iomega Zip Drive 208
Using Serial Ports 209
Using a Serial Port on the Host Computer 209
Using a File on the Host Computer 209
Connecting an Application on the Host to a Virtual Machine 210
Connecting Two Virtual Machines 211
Special Configuration Options for Advanced Users 212
Using USB Devices in a Virtual Machine 214
Notes on USB Support in VMware ACE 214
Enabling and Disabling the USB Controller 214
Connecting USB Devices 214
Using USB with a Windows Host 215
Replacing USB 2.0 Drivers on a Windows 2000 Host 215
Installing USB Devices as a Non-Administrator 216
Who Has Control over a USB Device? 216
Disconnecting USB Devices from a Virtual Machine 217
Human Interface Devices 217

Understanding Policies 219
Taking Advantage of Policies 220
Encryption and Authentication Policies 222
Encrypting a Virtual Machine's Files 222
Determining the Authentication Policy 222
Expiration Policies 224
Copy Protection Policies 225
VMware ACE Policies 226
Troubleshooting Policies 226
VMware ACE Window Policies 227
Easy Printer Setup Policies 227
User Preferences Policies 228
Administrator Access Policy 229
Network Quarantine Policies 230
Selecting the Type of Network Quarantine 230
Specifying Access to Networks and Machines 232
Allowing Access for Printer, DHCP, DNS and ICMP Traffic 232
Storing Access Lists for Network Quarantine 233

Using Advanced Network Quarantine 234
Defining Zones 235
Defining Host Policies 237
Defining Guest Policies 240
Writing Plug-In Policy Scripts 244
Authentication Plug-Ins 245
Renewal Plug-Ins 246
Device Connection Plug-Ins 247
Network Quarantine Plug-Ins 248
Sample Scripts 250

Glossary 259

Index 263

CHAPTER 1

Introduction and System Requirements

Welcome to VMware ACE. This section covers the following topics:

- About VMware ACE on page 10
- Host System Requirements for VMware ACE Manager on page 12
- Host System Requirements for End Users on page 14
- Virtual Machine Specifications on page 16
- Supported Guest Operating Systems on page 18
- Technical Support Resources on page 20

About VMware ACE

VMware ACE is an enterprise solution for IT desktop managers who want to rapidly provision standardized and secure PC environments throughout the extended enterprise. VMware ACE installs easily, improving the manageability, security and cost-effectiveness of any industry-standard PC.

VMware ACE enables IT desktop managers to apply enterprise IT policies to a virtual machine containing an operating system, enterprise applications and data to create an isolated PC environment known as an assured computing environment.

Through Virtual Rights Management technology, VMware ACE enables IT desktop managers to control assured computing environment lifecycles, secure enterprise information on PCs and ensure compliance with IT policies.

Unlike other products, VMware ACE is a hardware-independent solution that can be provisioned to any PC and works either connected or disconnected from the enterprise network.

VMware ACE is used across the enterprise to

- Ensure safe access to enterprise resources from remote and guest PCs
- Secure data on enterprise PCs
- Standardize and secure PC environments

Ensure Safe Access to Enterprise Resources

Reduce the threat from unmanaged and unsecured PCs used by telecommuters, partners and offshore workers to access enterprise resources. VMware ACE enables safe access to enterprise resources from assured computing environments — isolated PC environments that run on top of existing PCs. The assured computing environment contains an operating system, enterprise applications and preconfigured security settings.

Secure Data on Enterprise PCs

Secure enterprise information in assured computing environments on any PC throughout the extended enterprise. With Virtual Rights Management, built-in copy protection controls and automatic encryption, VMware ACE helps prevent theft, tampering and unauthorized copying of applications, data, system settings and files.

Standardize and Secure PC Environments

Self-policing and hardware-independent, VMware ACE improves the manageability, security and cost-effectiveness of PCs. Avoid building and supporting hardware-

specific images for PCs. Ensure compliance with IT policies while maintaining end user freedom.

Key Features of VMware ACE

Manageability

- Design once, deploy anywhere. Create standardized hardware-independent PC environments and deploy them to any PC throughout the extended enterprise.
- Virtual Rights Management interface. Control VMware ACE lifecycle, security settings, network settings, system configuration and user interface capabilities.

Security

- Rules-based network access. Identify and quarantine unauthorized or out-of-date VMware ACE environments. Enable access to the network once the VMware ACE environment complies with IT policies.
- Tamper-resistant computing environment. Protect the entire VMware ACE environment, including data and system configuration, with seamless encryption.
- Copy protected computing environment. Prevent end users from copying enterprise information.

Usability

- Customizable interface. Customize the behavior and look and feel for end users.
- Flexible computing environment. End users can revert to a previous state within seconds and can work online or when disconnected from the enterprise network.

The VMware ACE Software

As an administrator, you install VMware ACE Manager and use it to create virtual machines and package them for distribution to your end users. It allows you to set policies to ensure that your end users have a computing environment that meets your organization's security requirements.

VMware ACE Manager creates packages that include VMware ACE, the application your end users use to run the virtual machine. VMware ACE is simple to use and automatically runs the virtual machine you have configured.

Host System Requirements for VMware ACE Manager

What do you need to get the most out of VMware ACE Manager? Take the following list of requirements as a starting point. Remember that the virtual machines running under VMware ACE Manager are like physical computers in many ways — and, like physical computers, they generally perform better if they have faster processors and more memory.

PC Hardware

- Standard PC
- 500MHz or faster compatible x86 processor (recommended; 400MHz minimum)

  Compatible processors include

  - Intel®: Celeron®, Pentium® II, Pentium III, Pentium 4, Pentium M (including computers with Centrino™ mobile technology), Xeon™ (including "Prestonia")
  - AMD™: Athlon™, Athlon MP, Athlon XP, Duron™, Opteron™

  For additional information, including notes on processors that are not compatible, see the VMware knowledge base at *www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=967*.
- Multiprocessor systems supported
- Experimental support for AMD64 Opteron, Athlon 64 and Intel IA-32e CPU

Memory

- Enough memory to run the host operating system, plus memory required for each guest operating system and for applications on the host and guest; see your guest operating system and application documentation for their memory requirements
- 256MB recommended, 128MB minimum

Display

- 16-bit display adapter recommended; 8-bit display adapter required

Disk Drives

- 150MB free space required for basic installation
- At least 1GB free disk space recommended for each guest operating system and the application software used with it; if you use a default setup, the actual disk

space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer

- Additional disk space for building packages; temporary files require about as much space as those of the virtual machine included in the package
- IDE or SCSI hard drives, CD-ROM and DVD-ROM drives supported

Local Area Networking (Optional)

- Any Ethernet controller supported by the host operating system
- Non-Ethernet networks supported using built-in network address translation (NAT)

Windows Host Operating Systems

- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
- Windows XP Professional and Windows XP Home Edition with Service Pack 1 or 2
- Windows 2000 Professional Service Pack 3 or 4, Windows 2000 Server Service Pack 3 or 4, Windows 2000 Advanced Server Service Pack 3 or 4

Internet Explorer 4.0 or higher is required for the Help system.

Host System Requirements for End Users

What systems do your end users need to get the most out of VMware ACE? Take the following list of requirements as a starting point. Remember that the virtual machines running under VMware ACE are like physical computers in many ways — and, like physical computers, they generally perform better if they have faster processors and more memory.

PC Hardware

- Standard PC
- 500MHz or faster compatible x86 processor (recommended; 400MHz minimum)

  Compatible processors include

  - Intel®: Celeron®, Pentium® II, Pentium III, Pentium 4, Pentium M (including computers with Centrino™ mobile technology), Xeon™ (including "Prestonia")
  - AMD™: Athlon™, Athlon MP, Athlon XP, Duron™, Opteron™

  For additional information, including notes on processors that are not compatible, see the VMware knowledge base at *www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=967*.
- Multiprocessor systems supported
- Experimental support for AMD64 Opteron, Athlon 64 or Intel IA-32e CPU

Memory

- Enough memory to run the host operating system, plus memory required for the guest operating system and for applications on the host and guest; see your guest operating system and application documentation for their memory requirements
- 256MB recommended, 128MB minimum

Display

- 16-bit display adapter recommended; greater than 8-bit display adapter required

Disk Drives

- 80MB free space required for basic installation
- At least 1GB free disk space recommended for the guest operating system and the application software used with it; if you use a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer

- IDE or SCSI hard drives, CD-ROM and DVD-ROM drives supported

Local Area Networking (Optional)

- Any Ethernet controller supported by the host operating system
- Non-Ethernet networks supported using built-in network address translation (NAT)

Windows Host Operating Systems

- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
- Windows XP Professional and Windows XP Home Edition with Service Pack 1 or 2
- Windows 2000 Professional Service Pack 3 or 4, Windows 2000 Server Service Pack 3 or 4, Windows 2000 Advanced Server Service Pack 3 or 4

Internet Explorer 4.0 or higher is required for the Help system.

Virtual Machine Specifications

Each virtual machine created with VMware ACE Manager provides a platform that includes the following devices that your guest operating system can see.

Processor

- Same processor as that on host computer

  Note: A 64-bit processor runs in 32-bit legacy mode inside the virtual machine.

- Single processor per virtual machine on symmetric multiprocessor systems

Chip Set

- Intel 440BX-based motherboard with NS338 SIO chip and 82093AA IOAPIC

BIOS

- PhoenixBIOS™ 4.0 Release 6 with VESA BIOS

Memory

- Up to 3600MB, depending on host memory
- Maximum of 4GB total available for all virtual machines

Graphics

- VGA and SVGA support

IDE Drives

- Up to four devices — disks, CD-ROM or DVD-ROM (DVD drives can be used to read data DVD-ROM discs; DVD video is not supported)
- IDE virtual disks up to 128GB
- CD-ROM can be a physical device or an ISO image file

SCSI Devices

- Up to seven devices
- SCSI virtual disks up to 256GB
- LSI Logic® LSI53C1030 Ultra320 SCSI I/O controller
- Mylex® (BusLogic) BT-958 compatible host bus adapter (requires add-on driver from VMware for Windows XP and Windows Server 2003)

Floppy Drives

- Up to two 1.44MB floppy devices
- Physical drives or floppy image files

Serial (COM) Ports

- Up to four serial (COM) ports
- Output to serial ports, Windows or Linux files, or named pipes

Parallel (LPT) Ports

- Up to two bidirectional parallel (LPT) ports
- Output to parallel ports or host operating system files

USB ports

- Two-port USB 1.1 UHCI controller
- Supports devices including USB printers, scanners, PDAs, hard disk drives, memory card readers and still digital cameras

Keyboard

- 104-key Windows 95/98 enhanced

Mouse and Drawing Tablets

- PS/2 mouse
- Serial tablets supported

Ethernet Card

- Up to three virtual Ethernet cards
- AMD PCnet-PCI II compatible

Sound

- Sound output and input
- Emulates Creative Labs Sound Blaster AudioPCI (MIDI input, game controllers and joysticks not supported)

Virtual Networking

- Virtual networking supports most Ethernet-based protocols, including TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell NetWare and Network File System
- Built-in NAT supports client software using TCP/IP, FTP, DNS, HTTP and Telnet

Supported Guest Operating Systems

The operating systems listed here have been tested in VMware ACE virtual machines and are officially supported. For notes on installing the most common guest operating systems, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

Operating systems that are not listed are not supported for use in a VMware ACE virtual machine. For the most recent list of supported guest operating systems, see the support section of the VMware Web site, *www.vmware.com/support/*.

Microsoft Windows

- Windows, code-named Longhorn, beta (experimental)
- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
- Windows XP Professional and Windows XP Home Edition with Service Pack 1 or 2 (listed versions also supported with no service pack)
- Windows 2000 Professional Service Pack 1, 2, 3 or 4 (also supported with no service pack); Windows 2000 Server Service Pack 1, 2, 3 or 4 (also supported with no service pack); Windows 2000 Advanced Server Service Pack 3 or 4
- Windows NT® Workstation 4.0 Service Pack 6a, Windows NT Server 4.0 Service Pack 6a, Windows NT 4.0 Terminal Server Edition Service Pack 6
- Windows Me
- Windows 98 (including all Customer Service Packs) and Windows 98 SE
- Windows 95 (including Service Pack 1 and all OSR releases)
- Windows for Workgroups 3.11
- Windows 3.1

Microsoft MS-DOS

- MS-DOS 6.x

Linux

- Mandrake Linux 8.2, 9.0
- Red Hat Linux 7.0, 7.1, 7.2, 7.3, 8.0, 9.0
- Red Hat Enterprise Linux 2.1, 3.0
- Red Hat Linux Advanced Server 2.1
- SuSE Linux 7.3, 8.0, 8.1, 8.2, 9.0, 9.1

- SLES 7, 7 patch 2, 8
- Turbolinux Server 7.0, Enterprise Server 8, Workstation 8

Novell NetWare

- NetWare 5.1, 6, 6.5

FreeBSD

- FreeBSD 4.0–4.6.2, 4.8, 5.0

  Note: If you use SCSI virtual disks larger than 2GB with FreeBSD 4.0–4.3, there are known problems, and the guest operating system does not boot. To work around this issue, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

Solaris

- Solaris x86 Platform Edition 9 (experimental), 10 beta (experimental)

Technical Support Resources

Documentation on the Web

Full documentation for VMware ACE, including the latest updates to this manual, can be found on the VMware Web site at *www.vmware.com/support/*.

VMware Knowledge Base

You can find troubleshooting notes and tips for advanced users in the knowledge base on the VMware Web site at *www.vmware.com/kb*.

VMware User Community

Community Discussion Forums

The VMware community discussions forums are a set of moderated discussion forums hosted on the VMware Web site and open to all VMware users. In the forums, you can share your experiences in using VMware products, raise technical questions or issues and benefit from the expertise and advice of other VMware users.

To join in the forum discussions, go to *www.vmware.com/community/*.

Newsgroups

The VMware newsgroups are primarily forums for users to help each other. You are encouraged to read and post issues, work-arounds and fixes. While VMware personnel may read and post to the newsgroups, they are not a channel for official support. The VMware NNTP news server is at *news.vmware.com*.

For more information on the newsgroups and community forums, see *www.vmware.com/vcommunity*.

Reporting Problems

If you have problems while running VMware ACE, please report them to the VMware support team.

These guidelines describe the information we need from you to diagnose problems.

If a virtual machine exits abnormally or crashes, please run the support script to collect the appropriate log files and system information. Follow the steps below.

1. Open a command prompt.
2. Change to the VMware ACE Manager program directory.
   ```
   C:
   cd \Program Files\VMware\VMware ACE Manager
   ```

If you did not install the program in the default directory, use the appropriate drive letter and substitute the appropriate path in the `cd` command above.

3. Run the support script.
   `cscript vm-support.vbs`
4. After the script runs, it displays the name of the directory where it has stored its output. Use a file compression utility such as WinZip or PKZIP to zip that directory and include the zip file with your support request.

If you are reporting a problem you encountered while installing VMware ACE, it is also helpful to have your installation log file. The file is `VMInst.log`. It is saved in your temp folder. The default location is `C:\Documents and Settings\<username>\Local Settings\Temp`. The `Local Settings` folder is hidden by default. To see its contents, open **My Computer**, choose **Tools** > **Folder Options**, click the **View** tab and select **Show Hidden Files and Folders**.

Be sure to register your serial number. You may then report your problems by submitting a support request at *www.vmware.com/requestsupport*.

CHAPTER 2

Learning the Basics of VMware ACE Manager

The following sections provide an overview of how to use VMware ACE Manager to create and deploy virtual machines for your end users.

- Setting Up Your Administrative Workstation on page 24
- Creating Packages to Distribute to Users on page 26
  - Basic Steps on page 26
  - Keeping Users Up-to-Date on page 27
  - Troubleshooting Users' Problems on page 28

Setting Up Your Administrative Workstation

As an administrator, you need to install the VMware ACE Manager software on your workstation, referred to in this manual as your host computer. You can then run the VMware ACE Manager, your tool for creating and managing the virtual machines you distribute to your end users.

For details on how to install the VMware ACE Manager software, see Installing and Configuring VMware ACE Manager on page 29.

If your company already has a library of standard virtual machines, you need network access to that library from your host computer.

If you are creating new virtual machines, you need access to installers for the guest operating systems and application software you plan to install in the virtual machines.

You can install operating systems from CD, from ISO image files on a local drive or on the network, or from a PXE server. If you need to connect to an ISO file on a network drive, you use the networking capabilities of your host computer to make that connection.

You can install application software from CDs or from installers on a local drive or on the network. If you need to connect to an installer on the network, you use the networking capabilities of the virtual machine to make that connection. For details on networking in a virtual machine, see Networking Virtual Machines on page 187. If you need to use an installer on a local drive, you can use the virtual machine's networking capabilities or use shared folders in the virtual machine to gain access to the installer. For details on using shared folders, see Using Shared Folders in VMware ACE Manager on page 40.

You need to provide adequate disk space for three types of files:

- **Project files** — The files that define projects take up relatively little disk space. The default location for these files is `C:\Documents and Settings\<username>\My Documents\My Projects`. To change the default location, go to **Edit** > **Preferences** > **Workspace**. When you create a new project, you may specify a location for that project's files that is different from the default.
- **Virtual machine files** — The files for each virtual machine can be quite large, sometimes as large as several gigabytes. The default location for these files is `C:\Documents and Settings\<username>\My Documents\My`

`Virtual Machines`. To change the default location, go to **Edit** > **Preferences** > **Workspace**. When you create a new virtual machine, you can specify a location for that virtual machine's files that is different from the default.

- **Package files** — The package files created by VMware ACE Manager may be quite large. The default location for the package files is a folder named `Package` inside the project's folder. When you create a package, you can change the location for the package's files.

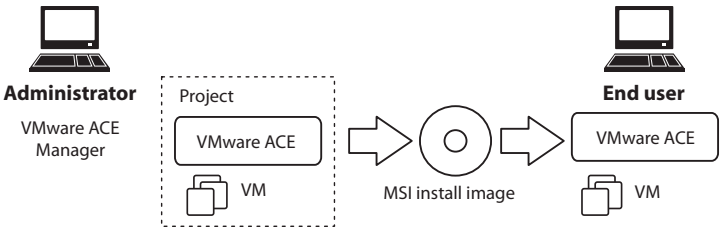
  In addition, VMware ACE Manager needs a substantial amount of temporary working space when it creates a package. The total is about twice the combined sizes of all the components of the package. The wizard displays information about the amount of space needed and the locations where the space is needed. If you do not have enough free space, the wizard displays an error message. You may move or delete files on the target drives to make room for the wizard's working files.

Creating Packages to Distribute to Users

Using the VMware ACE Manager, you create projects that include

- One or more virtual machines
- An application to run the virtual machines
- A set of policies to control the capabilities of the virtual machines

You then create packages, based on the projects, to distribute to your users.



When you create a package, you include VMware ACE and one or more virtual machines from the project. VMware ACE is the easy-to-use application that runs the virtual machines. For more information on VMware ACE, see Installing and Running VMware ACE on page 153.

Basic Steps

At the most basic level, you need to take the following steps to create and deploy virtual machines:

1. Create a project. Give the project a name that makes it easy to identify. For more information on creating projects, see Creating a Project on page 44. For a handy checklist, see Checklist: Creating a Project on page 49.
2. Add one or more virtual machines to the project. You can add existing virtual machines, create new virtual machines or both. For more information on adding virtual machines, see Adding a Virtual Machine to a Project on page 51. For a handy checklist, see Checklist: Adding a Virtual Machine on page 63.
3. Set policies for the virtual machines. You use policies to control what your users can do with their virtual machines — for example, what network access they have from the virtual machines and what devices on their host computers they may use in the virtual machines. For basic information on setting policies, see Setting Policies and Customizing VMware ACE on page 69. For a detailed discussion of policies, see Understanding Policies on page 219.

4. Install guest operating systems, VMware Tools and other software in the virtual machines. For information on installing VMware Tools, see Installing an Operating System and Applications in the Virtual Machine on page 112. For notes on installing particular guest operating systems, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.
5. Create packages to deploy to your users. The VMware ACE Manager guides you through the process and, for large packages, prepares the package so it spans multiple CDs or DVDs. For more information, see Creating Packages to Deploy to Users on page 131.
6. Give the packages to your users. You may distribute the packages on CD or DVD, or you may make them available on a network. The package includes an installer that installs the full package — VMware ACE and the virtual machines, along with the policies that control their use. For more information, see Deploying and Maintaining Packages on page 137.

Keeping Users Up-to-Date

VMware ACE Manager gives you tools you can use to ensure that your end users are running up-to-date virtual machines.

You may need to provide updates to users' packages. You may need to update the guest operating system or provide an update to a program running inside the virtual machine. Or you may need to update either the virtual machine itself or policies set for the package — or add a new virtual machine to the package. There are two basic approaches to updates.

- Deliver updates to the guest operating system or to programs running inside the virtual machine as you would with any other software updates — for example, using a patch management system.
- Provide a new package — to replace the virtual machine, to distribute an additional virtual machine or to change the policies applied to the VMware ACE application or the virtual machine. If you replace an existing virtual machine by supplying a new package, your end users lose any data or custom settings stored in that virtual machine.

If your users connect to your network, you can set network quarantine policies so out-of-date virtual machines have restricted access or no access to the network. You may, for example, give users with out-of-date virtual machines access only to the server where an update is available.

For information on these topics, see Deploying and Maintaining Packages on page 137.

Troubleshooting Users' Problems

Your users may need help with lost passwords, expired virtual machines or copy-protected virtual machines that they have moved to a different location. You can use the hot fix feature to respond to these problems.

For information on using the hot fix feature, see Hot Fix Policy on page 74 and Responding to Hot Fix Requests on page 150.

You may find it useful to modify the configuration of a virtual machine on an end user's computer. You may do so if you have enabled administrator access for VMware ACE in that package. For information, see Administrator Access Policy on page 75.

CHAPTER 3

Installing and Configuring VMware ACE Manager

The following sections guide you through installing VMware ACE Manager on your administrative workstation:

- Installing VMware ACE Manager on page 30
  - Installing on a Computer with a Different VMware Product on page 30
  - Installation Steps on page 30
  - Installing VMware ACE Manager Silently on page 33
  - Uninstalling VMware ACE Manager on page 35
- Setting Preferences for VMware ACE Manager
- Using Shared Folders in VMware ACE Manager on page 40

Installing VMware ACE Manager

Before you begin installing VMware ACE Manager, be sure you have

- A computer and host operating system that meet the system requirements for running VMware ACE Manager. See Host System Requirements for VMware ACE Manager on page 12.
- The VMware ACE Manager installation software. If you bought the packaged distribution of VMware ACE Manager, the installation software is on the CD in your package. If you bought the electronic distribution, the installation software is in the file you downloaded.
- Your VMware ACE Manager serial number. The serial number is included in the VMware ACE Manager package or in the email message confirming your electronic distribution order.

Installing on a Computer with a Different VMware Product

VMware ACE Manager cannot be installed on a computer with VMware Workstation or VMware GSX Server installed. If you have one of these products installed on the computer where you plan to install VMware ACE Manager, use the Add/Remove Programs control panel to remove the existing product, then install VMware ACE Manager.

You may install VMware ACE Manager on a computer that has VMware Remote Console or VMware VirtualCenter installed.

Installation Steps

1. Log on to your Microsoft Windows host as the Administrator user or as a user who is a member of the Windows Administrators group.

   Note: On a Windows XP or Windows Server 2003 host computer, you must be logged on as a local administrator (that is, not logged on to the domain) in order to install VMware ACE Manager.

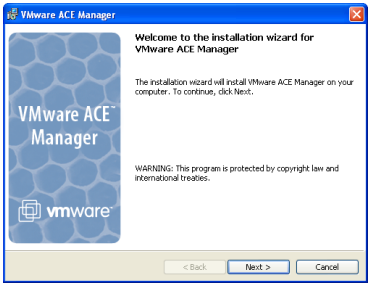
   Note: Although you must be logged on as an administrator to install VMware ACE Manager, a user with normal user privileges can run the program after it is installed. Keep in mind that you need one license for each user.

2. If you are installing from a CD, from the **Start** menu, choose **Run** and enter `D:\setup.exe`, where `D:` is the drive letter for your CD-ROM drive.

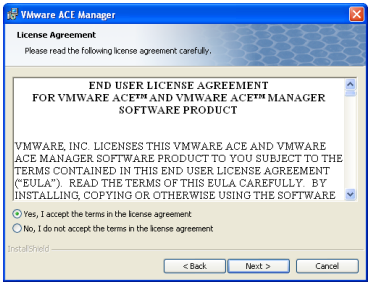
   If you are installing from a downloaded file, from the **Start** menu, choose **Run**, browse to the directory where you saved the downloaded installer file and run

the installer. (The filename is similar to `VMware-ACE-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers.)

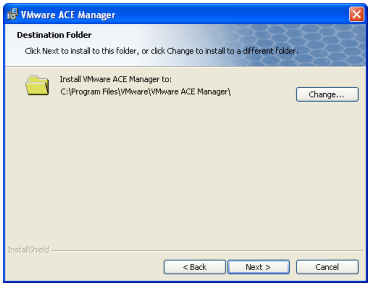
3. The Welcome dialog box appears.



Click **Next**.



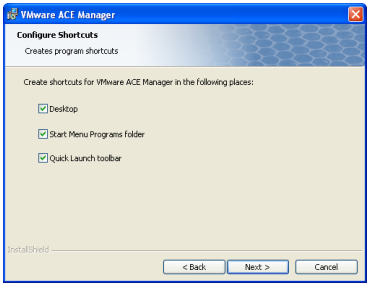
4. Acknowledge the end user license agreement (EULA). Select the **Yes, I accept the terms in the license agreement** option, then click **Next**.



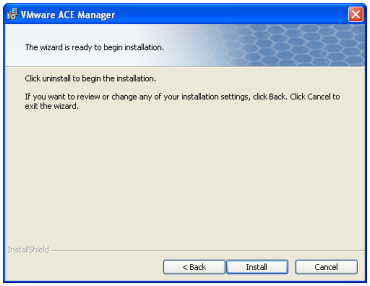
5. Choose the directory in which to install VMware ACE Manager. To install it in a directory other than the default, click **Change** and browse to your directory of choice. You must install VMware ACE Manager on a local drive, not on a network

drive. If the directory you specify does not exist, the installer creates it for you. Click **Next**.

Note: Windows and the Microsoft Installer limit the length of a path to a folder on a local drive to 255 characters. If the path to the VMware ACE Manager program folder exceeds this limit, an error message appears. You must select or enter a shorter path.



6. Select which shortcuts you want the installer to create.
7. The installer has gathered the necessary information and is ready to begin installing the software.

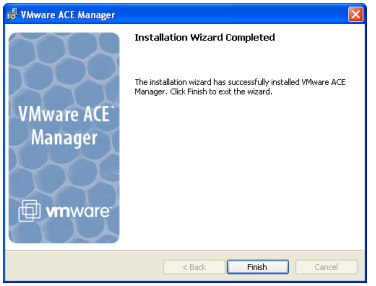


If you want to change any settings or information you provided, now is the time to make those changes. Click **Back** until you reach the dialog box containing the information you want to change.

If you do not need to make any changes, click **Install**. The installer begins copying files to your computer.

8. If the installer detects that the CD-ROM autorun feature is enabled, you see a message that gives you the option to disable this feature. Disabling it prevents undesirable interactions with the virtual machines you install on this system.

9. If you wish, enter your name, company name and serial number, then click **Next**. The serial number is on the registration card in your package. The user and company information you enter here is then made available in the About box (**Help** > **About VMware ACE Manager**). If you skip this step, you are prompted to enter your serial number the first time you run VMware ACE Manager.



10. Click **Finish**. The VMware ACE Manager software is installed.
11. You may see a prompt suggesting that you reboot your PC. If you do, reboot to allow VMware ACE Manager to complete the installation correctly.

Installing VMware ACE Manager Silently

If you are installing VMware ACE Manager on a number of Windows host computers, you may want to use the silent installation features of the Microsoft Windows Installer.

Before installing VMware ACE Manager silently, you must ensure that the host computer has version 2.0 or higher of the MSI runtime engine. This version of the installer is available in versions of Windows beginning with Windows XP and is available separately from Microsoft for versions of Windows beginning with Windows NT 4.0.

The following steps outline the procedures for a silent installation. For additional details on using the Microsoft Windows Installer, see the Microsoft Web site.

1. Silently extract the administrative installation image from the VMware ACE Manager installer:

   `setup.exe /a /s /v"/qn TARGETDIR=<InstallTempPath>"`

   `setup.exe` is the name of the installer on the CD distribution. If you are using a downloaded installer, the filename is similar to `VMwareACE-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers.

<InstallTempPath> is the full path to the folder where you want to store the administrative installation image.

2. Run a silent installation using msiexec and the administrative installation image you extracted in the previous step:

```
msiexec -i "<InstallTempPath>\VMware ACE.msi"
[INSTALLDIR="<PathToProgramDirectory>"] ADDLOCAL=ALL
[REMOVE=<featurename,featurename>] /qn
```

Enter the command on one line. If you want to install VMware ACE Manager in a location other than the default, change the path that follows INSTALLDIR= to specify the desired location.

You may use the optional REMOVE= property to skip installation of certain features. The REMOVE= property can take one or more of the following values:

Value	Description
Authd	The VMware authorization service
Network	Networking components including the virtual bridge and the host adapters for host only networking and NAT networking; do not remove if you want to use NAT or DHCP
DHCP	The virtual DHCP server
NAT	The virtual NAT device

If you specify more than one value, use a comma to separate the values. For example, REMOVE=Authd,NAT.

Note: If you specify REMOVE=Network, the installer skips installation of certain networking components, including NAT and DHCP. There is no need to specify DHCP or NAT separately.

You may customize the installation further by adding any of the following installation properties to the command using the format PROPERTY="value". A value of 1 means true; a value of 0 means false. If you use the serial number property, enter the serial number, complete with hyphens (xxxxx-xxxxx-xxxxx-xxxxx).

Property	Effect of the Property	Default
DESKTOP_SHORTCUT	Installs a shortcut on the desktop	1
DISABLE_AUTORUN	Disables CD autorun on the host	1
REMOVE_LICENSE	(Uninstall only) Removes all stored licenses at uninstall	0

Property	Effect of the Property	Default
SERIALNUMBER	Automatically enters the serial number	

For information on installing a VMware ACE package silently on an end user's computer, see Installing a Package Silently on page 139.

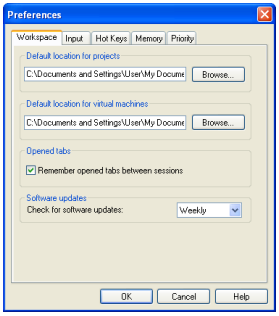
Uninstalling VMware ACE Manager

To uninstall VMware ACE Manager, use the Add/Remove Programs control panel. Select the entry for VMware ACE Manager, then click **Remove**. Follow the onscreen instructions.

Setting Preferences for VMware ACE Manager

The Preferences dialog box allows you to change a number of settings that apply to VMware ACE Manager itself, no matter what virtual machine you are running. The settings on the Workspace, Input and Hot Keys tabs apply to the user currently logged on to the host computer. They do not affect settings made by any other user on the computer. The settings on the Memory tab apply no matter what virtual machine is running or who is logged on to the host computer. The settings on the Priority tab apply to all virtual machines for the user currently logged on to the host computer. They do not affect settings made by any other user on the computer.

To make changes to these settings, choose **Edit** > **Preferences**.



Workspace — The Workspace tab lets you change the directory in which newly created projects and virtual machines are stored.

The project directory VMware ACE Manager uses by default is displayed under Default location for projects. To set a different directory, type in the path or click **Browse** to navigate to the directory you want to use. Workstation creates a directory for each new project under the directory you specify here.

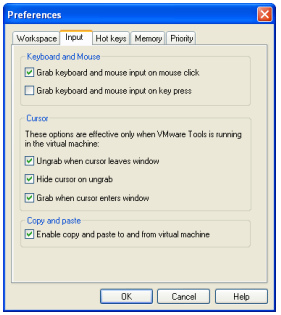
The virtual machine directory VMware ACE Manager uses by default is displayed under Default location for virtual machines. To set a different directory, type in the path or click **Browse** to navigate to the directory you want to use. Workstation creates a directory for each new virtual machine under the directory you specify here.

If you select the **Remember opened tabs between sessions** check box, you see a tab for each opened project and virtual machine the next time you start VMware ACE

Manager. A virtual machine is considered opened if both of the following conditions are true:

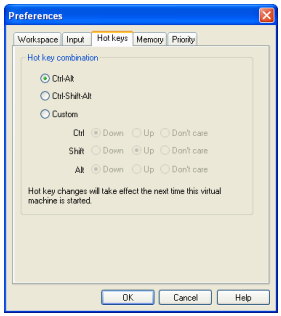
- The virtual machine was left open.
- The virtual machine was powered on and off, or powered on and suspended.

Use the **Check for software updates** drop-down list to determine how often VMware ACE Manager checks to see if new versions of the product are available. You can choose daily, weekly or monthly automatic checks, or choose **Never** to turn off automatic checking. You can check manually at any time by choosing **Help** > **Check for Updates on the Web.**



Input — The Input tab lets you adjust the way that the virtual machine captures control of keyboard and mouse.

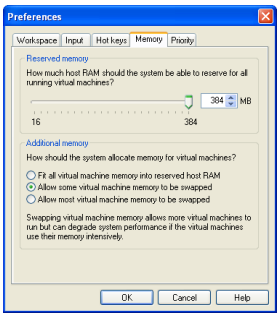
Note: The **Grab when cursor enters window** option allows you to move the mouse pointer back into the virtual machine window easily if you have been working in the virtual machine, then temporarily moved the mouse pointer outside the virtual machine window. The mouse pointer is grabbed only when VMware ACE Manager has focus (is the active application). Also, if you release the mouse pointer by pressing a hot-key combination — Ctrl-Alt by default — you must click inside the virtual machine window to make VMware ACE Manager grab the mouse pointer again.



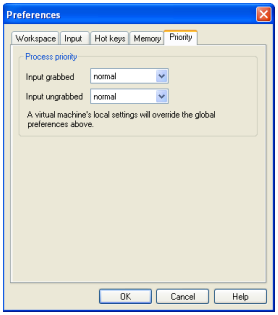
Hot keys — The Hot Key tab lets you change the key combination that determines whether certain combinations of keys are passed to the guest operating system or intercepted by VMware ACE Manager.

Note: Because Ctrl-Alt is the key combination used to tell VMware ACE Manager to release (ungrab) mouse and keyboard input, combinations that include Ctrl-Alt are not passed to the guest operating system. If you need to use such a combination — for example, use Ctrl-Alt-<Fkey> to switch between Linux workspaces in a virtual machine — press Ctrl-Alt-Space, release Space without releasing Ctrl and Alt, then press the third key of the key combination you want to send to the guest.

Using this dialog box, you can also construct your own custom hot-key combination.



Memory usage— The Memory tab lets you adjust the amount of physical RAM that can be used by all running virtual machines. It also lets you adjust how much virtual machine memory may be swapped to disk, allowing you to run more or larger virtual machines if you are willing to accept slower performance.



Process priorities — The Priority tab lets you determine the priority that the Windows process scheduler gives to your virtual machines when mouse and keyboard input are going to a particular virtual machine and when input is not going to that virtual machine.

You can adjust these settings to improve overall system performance based on the relative priority of work you are doing in various virtual machines and on the host computer.

To change the settings for a particular virtual machine, and override the global settings, open the virtual machine you want to adjust, choose **VM** > **Settings**, click the **Options** tab, select **Advanced**, then select the settings you want for that virtual machine fromthe drop-down lists under **Process priorities**.

Using Shared Folders in VMware ACE Manager

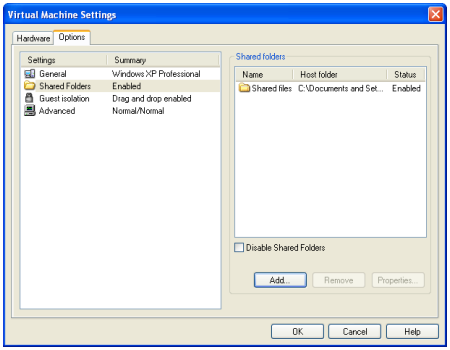
With shared folders, you can easily share files among virtual machines and the host computer. To use shared folders, you must have the current version of VMware Tools installed in the guest operating system and you must use the virtual machine settings editor to specify which directories are to be shared.

You can use shared folders with virtual machines running the following guest operating systems:

- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT 4.0
- Linux with a kernel version of 2.4 or higher

Note: The shared folder feature works as expected only if the folder you specify exists on the end users' computers. This may mean that you or your end users need to take special steps to create the target folder on the host computer. As a result, you should consider this an advanced feature in VMware ACE.

To set up one or more shared folders for a virtual machine, be sure the virtual machine is open in VMware ACE Manager and click its tab to make it the active virtual machine. Go to **VM** > **Settings** > **Options** and click **Shared folders**.



You can add one or more directories to the list. Those directories may be on the host computer or they may be network directories accessible from the host computer.

In a Windows virtual machine, shared folders appear in My Network Places (Network Neighborhood in a Windows NT virtual machine) under VMware Shared Folders. For example, if you specify the name `Test files` for one of your shared folders, you can navigate to it by opening **My Network Places** > **VMware Shared Folders** > **.host** > **Shared Folders** > **Test files**.

You can also go directly to the folder using the UNC path `\\.host\Shared Folders\Test files`.

You can map a shared folder to a drive letter just as you would with a network share.

Note: To see shared folders displayed in this way, you must update VMware Tools in the virtual machine to the current version. If your guest operating system has the version of VMware Tools that shipped with VMware Workstation 4.0, shared folders appear as folders on a designated drive letter.

In a Linux virtual machine, shared folders appear under `/mnt/hgfs`. So the shared folder in this example would appear as `/mnt/hgfs/Test files`.

To add a new shared folder to the list, click **Add**. On a Windows host, a wizard guides you through the process. On a Linux host, a dialog box appears. Enter the required information, then click **OK**.

Provide the following information:

- The path on the host to the directory you want to share. Type in the full path or browse to the directory.

  Note: If you plan to deploy a virtual machine that uses shared folders, be sure to specify a path that exists on your end users' computers. If the path does not exist, end users see an error message when they try to browse to the folder.

- The name for the directory. This is the name that appears inside the virtual machine.
- Whether the shared folder is enabled. You may want to add a folder to the list without enabling it immediately. You can then enable the folder at any time by clicking its name in this list, clicking **Properties** and enabling the folder in the Properties dialog box.
- Access options for the shared folder. You can give the current virtual machine read-only access, or read-write access. Access to files in the shared folder is also governed by permission settings on the host computer. For example, if you are running VMware ACE as a user named User, the virtual machine can read and write files in the shared folder only if User has permission to read and write them.

- Expiration options for the shared folder. You can specify that the folder is always enabled or that it is enabled only during the current working session. If you select **Disable after this session**, the shared folder is disabled when you suspend or power off the virtual machine.

To change the settings for a shared folder on the list, click the folder's name to highlight it, then click **Properties**. The Properties dialog box appears.

Change any settings you wish, then click **OK**.

Note: You can use shared folders to share any type of file. However, Windows shortcuts and Linux symbolic links do not work correctly if you try to use them via shared folders.

Caution: Do not open a file in a shared folder from more than one application at a time. For example, you should not open the same file using an application on the host operating system and another application in the guest operating system. In some circumstances, doing so could cause data corruption in the file.

CHAPTER 4

Creating Projects

The following sections guide you through the steps needed to create a project and add virtual machines to the project:

- Creating a Project on page 44
- Checklist: Creating a Project on page 49
- Adding a Virtual Machine to a Project on page 51
  - Adding an Existing Virtual Machine on page 51
  - Adding a New Virtual Machine on page 53
- Checklist: Adding a Virtual Machine on page 63

Creating a Project

A project contains one or more virtual machines and an application used to run those virtual machines. A wizard guides you through the steps you must take to create a project.

After you create the project, add one or more virtual machines to the project and set policies for the virtual machines and for the application. You can move directly from the New Project Wizard to the New Virtual Machine Wizard or launch the New Virtual Machine Wizard later by clicking **Add virtual machine to project** on the project summary display. You can move directly from the New Virtual Machine Wizard to the policy editor or launch the policy editor later by clicking **Edit policies** on any summary display.

Note: Be sure that all project and virual machine files are stored in a location that is backed up regularly. You must have access to the original project and virtual machine files when you create a package to send updates to your end users.

See Checklist: Creating a Project on page 49 for a worksheet you can use to gather the information you need when you create a new project.

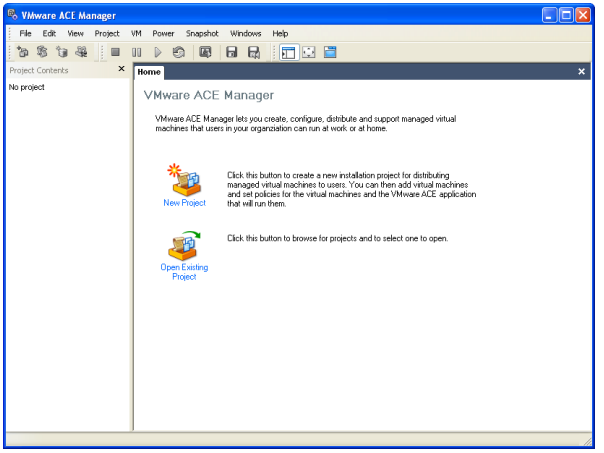
Using the New Project Wizard

To create a project, take the following steps:

1. Start VMware ACE Manager.

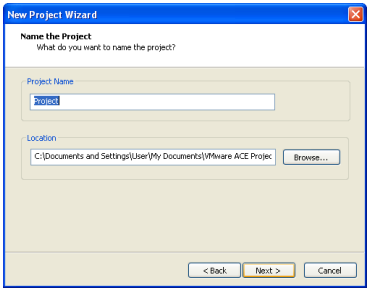
   The first time you run VMware ACE Manager, you are prompted to enter your serial number. The serial number is on the registration card in your package. If you wish, you may also enter your name and your company name. The user and

company information you enter here is made available in the About box (**Help** > **About VMware ACE Manager**).



Click the New Project icon to start the New Project Wizard.

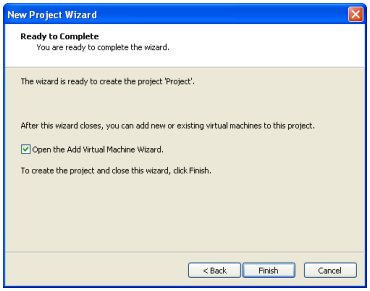
2. Click **Next** to enter the wizard. The Name the Project panel appears.



Enter a name for the project in the **Project Name** field. The name should be unique and should make it easy for you to identify the project.

The **Location** field shows the path to the folder where VMware ACE Manager stores the project file, which contains information about the contents of the project. You may accept the default location, type in a new location or click **Browse** to navigate to a new location.

3. Click **Next**. The Ready to Complete panel appears



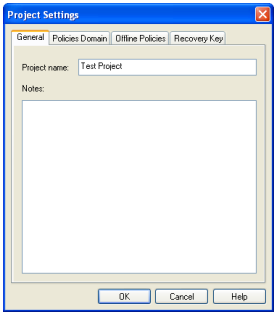
Select **Open the Add Virtual Machine Wizard** if you want to go directly to the Add Virtual Machine Wizard and add a virtual machine to the project.

Deselect **Open the Add Virtual Machine Wizard** if you do not want to add a virtual machine to the project at this time.

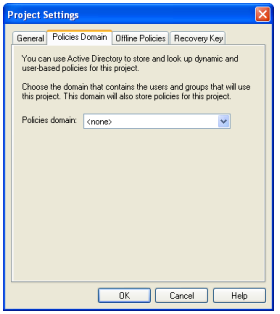
Click **Finish** to complete the New Project Wizard.

Making Project Settings

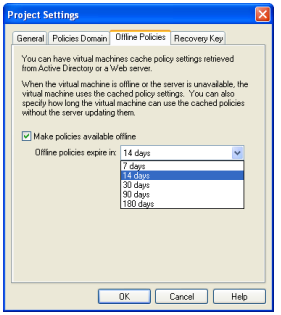
To specify general settings for the project, choose **Project** > **Settings**. The Project Settings dialog box appears.



On the General tab, you may update the project name and add or modify the project description.



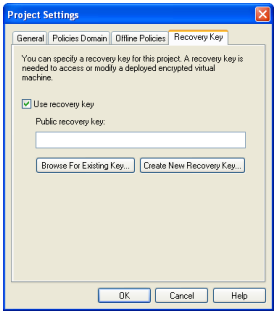
On the Policies Domain tab, you may choose an Active Directory domain to use for storing policies for the project.



On the Offline Policies tab, you may specify whether virtual machines in this project are allowed to cache policy settings. If you use Active Directory or a Web server to store policies, offline policies allow your end users to continue working even when they are unable to connect to the server where the policies are stored — for example, when they are working offline. Use the drop-down list to specify how long the cached policies remain valid.

If you enable offline policies, information is cached for the following policies:

- Authentication — the key
- Expiration — the expiration date
- Devices — the list of allowed users
- Network quarantine — all settings

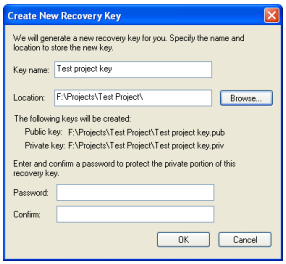


On the Recovery Key tab, you may specify the public key to be used for access to encrypted virtual machines. If you specify password protection for a virtual machine and want to be able to reset the password for a deployed virtual machine, you must specify a recovery key before you create the package that includes the virtual machine.

Select **Use recovery key** to configure a recovery key.

To use an existing PEM-format key pair, click **Browse for Existing Key** to navigate to the public key of the pair you want to use.

To create a new PEM-format key pair, click **Create New Recovery Key**. The Create New Recovery Key dialog box appears.



Enter a name and location for the key pair. Enter and confirm the password to protect the private key. Then click **OK** to generate the keys. It takes several seconds to generate the keys. When the keys are generated and saved, the Create New Recovery Key dialog box disappears and the newly generated public key is listed in the field on the Recovery Key tab.

Note: You must know the password for the private key and the location of the private key file in order to reset an end user's password.

Checklist: Creating a Project

You may find it helpful to photocopy this checklist and use it to collect the information you should have available when you create a new project.

What's the name for this project?

_____

What's the path to the location where you plan to store this project?

_____

Be sure you have enough free space at that location to store the files.

What virtual machines do you plan to include in the project?

☐ Existing virtual machines. Make a note of the path to the configuration (`.vmx`) file for each virtual machine you plan to include.

_____

_____

_____

_____

☐ New virtual machines. You may find it helpful to complete a checklist for each virtual machine you plan to create. See Checklist: Adding a Virtual Machine on page 63.

Will this project use network quarantine, with information stored in an Active Directory server?

☐ No.

☐ Yes. Use the following Active Directory domain:

_____

Will this project include password-protected virtual machines and need a recovery key?

☐ No.

☐ Yes. Use an existing key pair. Make a note of the path to the private key of the existing key pair.

_____

☐ Yes. Create a new key pair. Make a note of the location where you plan to store the new key pair. Follow your organization's procedure for storing the password

that protects the new private key.You need the password that protects the private key in order to reset an end user's password.

Adding a Virtual Machine to a Project

In VMware ACE Manager, you create a project first, then create a virtual machine within the project. You cannot create a new virtual machine outside the context of a project.

Once a virtual machine exists, you may add it to as many projects as you wish.

You may also add virtual machines created with certain other VMware products. Virtual machines created with the following products may be used in VMware ACE Manager projects:

- VMware Workstation 4.x
- VMware GSX Server 3.x

See Checklist: Adding a Virtual Machine on page 63 for a worksheet you can use to gather the information you need when you create a new virtual machine.

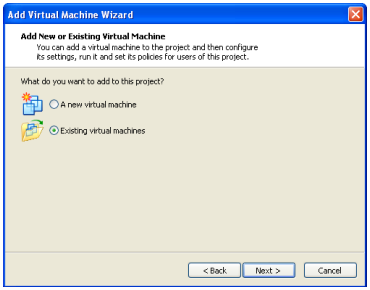
Caution: You should not change the name of a virtual machine in a project after you have created and distributed a package that includes the virtual machine. VMware ACE uses the name of a virtual machine to determine certain important settings, especially the name of the folder where the virtual machine is installed on the end user's computer. If you change the name of a virtual machine after you have distributed a package to end users, then create an update package using the new virtual machine name, the package installer attempts to install the update into a folder with a name based on the new virtual machine name. The update does not work properly, because the update is not installed into the folder used for the earlier install.

You may continue directly from the New Project Wizard to the Add Virtual Machine Wizard. Or you may start the Add Virtual Machine Wizard from the project summary display. To start the wizard from the project summary display, click **Add**.

Adding an Existing Virtual Machine

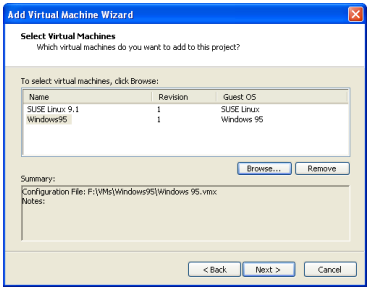
When the Add Virtual Machine Wizard starts, take the following steps to add an existing virtual machine to the project:

1. Click **Next** to enter the wizard. The Add New or Existing Virtual Machine panel appears.



Select **Existing virtual machines** and click **Next**.

2. The Select Virtual Machines panel appears.



Click **Browse** and navigate to the configuration (`.vmx`) file for the virtual machine you want to add to the project.

You may add one or more virtual machines to the project.

To remove a virtual machine from the list in this panel, choose the virtual machine's name in the list, then click **Remove**.

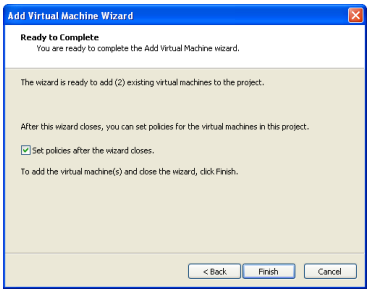
The new hardware wizard checks the virtual machine and warns you if any of its configuration settings make it inappropriate for use in VMware ACE. The following settings generate warnings:

- Generic SCSI device present
- Physical disks attached
- Virtual Ethernet adapters using custom networking
- Nondefault power settings — for example, power on after opening the virtual machine, enter full screen mode after powering on or close after powering off

- Nondefault working directory; the default is no directory specified, which means the virtual machine directory is used as the working directory
- Locked snapshot present

If the wizard warns you about any of these settings, you must open the virtual machine in the application used to create it and make the appropriate changes. You may then add the virtual machine to the project.

3. The Ready to Complete panel appears.



Select **Set policies after the wizard closes** if you want to go directly to the policy editor and set policies for the virtual machines in the project.

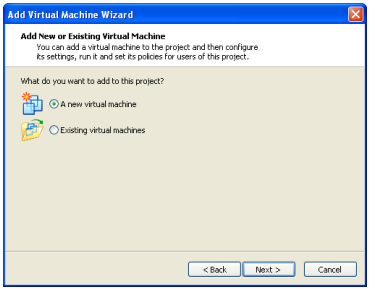
Deselect **Set policies after the wizard closes** if you do not want to set policies for the virtual machines at this time.

Click **Finish** to complete the Add Virtual Machine Wizard.

Adding a New Virtual Machine

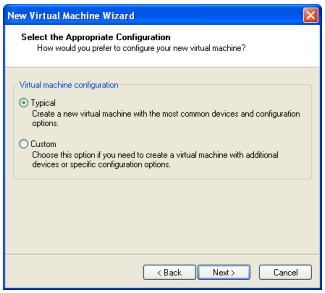
When the Add Virtual Machine Wizard starts, take the following steps to add a new virtual machine to the project:

1. Click **Next** to enter the wizard. The Add New or Existing Virtual Machine panel appears.



Select **A new virtual machine** and click **Next**.

2. The New Virtual Machine Wizard starts. Click **Next** to create a new virtual machine with the wizard.



Select the method you want to use for configuring your virtual machine.

If you select **Typical**, the wizard prompts you to specify or accept defaults for

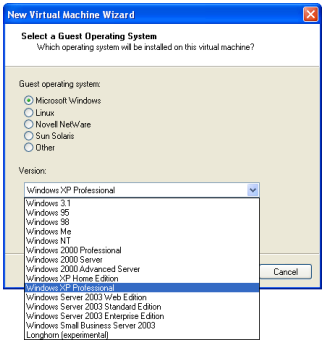
- The guest operating system
- The virtual machine name and the location of the virtual machine's files
- The network connection type
- Disk size
- Allocation of space for the disk
- Splitting the disk into 2GB files

Select **Custom** if you want to

- Store your virtual disk's files in a particular location
- Use an IDE virtual disk for a guest operating system that would otherwise have a SCSI virtual disk created by default

  By default, the new virtual machine uses an IDE disk for Windows 95, Windows 98, Windows Me, Windows XP, Windows Server 2003, NetWare and FreeBSD guests. The default for other guest operating systems is a SCSI disk.
- Use a physical disk rather than a virtual disk (this option is not appropriate for a virtual machine you plan to distribute as part of a project)
- Set memory options that are different from the defaults

3. Select a guest operating system.



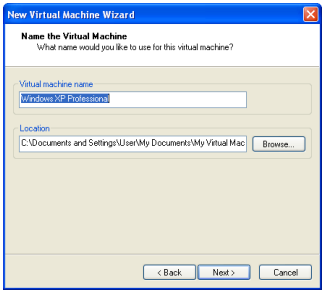
This panel asks which operating system you plan to install in the virtual machine. Select both an operating system and a version.

The Add Virtual Machine Wizard uses this information to select appropriate default values, such as the amount of memory needed. The wizard also uses this information when it names associated virtual machine files.

If the operating system you plan to use is not listed, select **Other** for both guest operating system and version.

The remaining steps assume you plan to install a Windows XP Professional guest operating system. You can find detailed installation notes for this and other guest operating systems in the *VMware Guest Operating System Installation Guide*, available on the VMware Web site or from the Help menu.

4. Select a name and folder for the virtual machine.



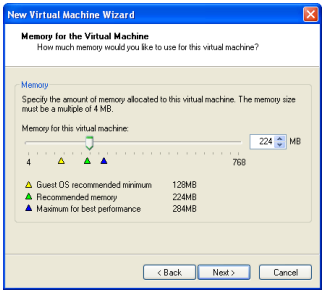
The name specified here is used as the name of the folder where the files associated with this virtual machine are stored.

Each virtual machine should have its own folder. All associated files, such as the configuration file and the disk file, are placed in this folder.

The default folder for this Windows XP Professional virtual machine is `C:\Documents and Settings\<username>\My Documents\My Virtual Machines\Windows XP Professional`.

5. If you selected **Typical** as your configuration path, skip to step 6.

   If you selected **Custom** as your configuration path, you may adjust the memory settings or accept the defaults.

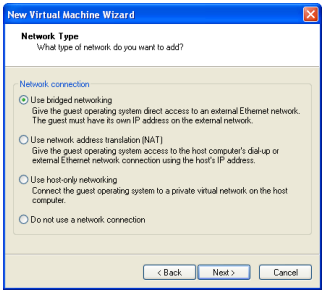


   When choosing the virtual machine memory settings, you need to consider the amount of memory required by the guest operating system and applications. You also need to consider the amount of RAM installed on your end users' computers and the amount of RAM required by the host operating system. Do not set the virtual machine memory below the amount recommended for the guest operating system. If you set virtual machine memory higher than that minimum, you should not set it so high that the host operating system cannot run comfortably. For common configurations, set the virtual machine memory no higher than half the amount of RAM you expect to find on end users' host computers.

   Note: You cannot allocate more than 2GB of memory to a virtual machine if the virtual machine's files are stored on a file system such as FAT32 that does not support files greater than 2GB.

   Click **Next** to continue.

6. Configure the networking capabilities of the virtual machine.



If the package is to be installed on a host computer that is on a network and a separate IP address is available for the virtual machine (or it can get one automatically from a DHCP server), select **Use bridged networking**. This setting is most likely to be appropriate if the package is to be installed on a computer connected to an office network.

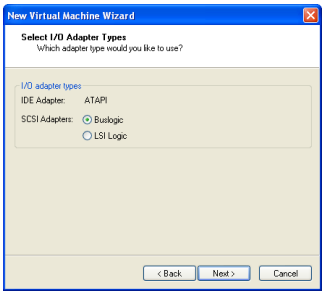
If the package is to be installed where no separate IP address is available for the virtual machine but the virtual machine must be able to connect to the Internet, select **Use network address translation (NAT)**. NAT also allows the end user to share files between the virtual machine and the host operating system.

For more details about VMware ACE networking options, see Networking Virtual Machines on page 187.

7. If you selected **Typical** as your configuration path, skip to step 11.

   If you selected **Custom** as your configuration path, continue with the steps below to configure a disk for the virtual machine.

8. Select the type of SCSI adapter you want to use with the virtual machine.



An IDE adapter and a SCSI adapter are installed in the virtual machine. You do not need to make any configuration choices for the IDE adapter. You can choose

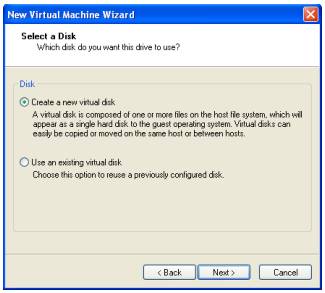
a BusLogic or an LSI Logic SCSI adapter. The default for your guest operating system is already selected. All guests except Windows Server 2003, Red Hat Enterprise Linux 3 and NetWare default to the BusLogic adapter.

The LSI Logic adapter has improved performance and works better with generic SCSI devices.

The choice of which SCSI adapter to use is separate from the choice to make the virtual disk an IDE or SCSI disk.

Older guest operating systems do not include a driver for the LSI Logic adapter. If you choose to use the LSI Logic adapter in an operating system that does not have a driver for it, you must download the driver from the LSI Logic Web site. See the *VMware Guest Operating System Installation Guide* for details about the driver and the guest operating system you plan to install in this virtual machine.

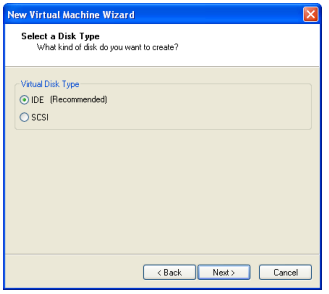
9. Select the disk you want to use with the virtual machine.



Select **Create a new virtual disk**.

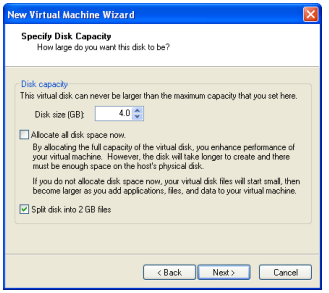
Virtual disks are appropriate for any virtual machines distributed in a package. By default, virtual disks start as small files on the host computer's hard drive, then expand as needed — up to the size you specify in a later step. That step also allows you to allocate all the disk space when the virtual disk is created, if you wish.

10. Select whether to create an IDE or SCSI disk.



The wizard recommends the best choice based on the guest operating system you selected. All Linux distributions you can select in the wizard use SCSI virtual disks by default, as do Windows NT, Windows 2000, Windows Server 2003 and Longhorn. All Windows operating systems except Windows NT, Windows 2000, Windows Server 2003 and Longhorn use IDE virtual disks by default; NetWare, FreeBSD, MS-DOS and other guests default to IDE virtual disks.

11. Specify the capacity of the virtual disk.



Enter the size of the virtual disk that you wish to create.

If you wish, select **Allocate all disk space now**.

Allocating all the space at the time you create the virtual disk gives somewhat better performance, but it requires as much disk space as the size you specify for the virtual disk.

If you do not select this option, the virtual disk's files start small and grow as needed, but they can never grow larger than the size you set here.

You can set a size between 0.1GB and 256GB for a SCSI virtual disk or 128GB for an IDE virtual disk. The default is 4GB.

You may also specify whether you want the virtual disk created as one large file or split into a set of 2GB files. You should split your virtual disk if it may be stored on a FAT32 file system.

Note: Because the Microsoft installer cannot install files larger than about 4.3GB, you should also split the virtual disk if the disk is larger than 4GB. You may wish to split the virtual disk even if it is smaller than 4GB. If you plan to distribute the VMware ACE package on CD or DVD, the package installs more quickly if you split the files. For the fastest package installation, be sure that the files that make up the virtual disks are smaller than 4GB and smaller than the media used to distribute the package. Thus you get best results if you split the virtual disk files and distribute the package on DVD.

Make the Virtual Disk Big Enough

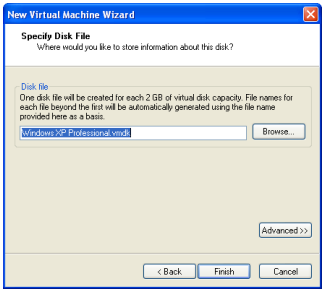
The virtual disk should be large enough to hold the guest operating system and all of the software that you intend to install, with room for data and growth.

You may prefer to increase total disk space by adding virtual disks to the virtual machine. You can install additional virtual disks using the virtual machine settings editor (**VM** > **Settings**). You must add any additional virtual disks after completing this wizard but before you create the package for distribution to your end users.

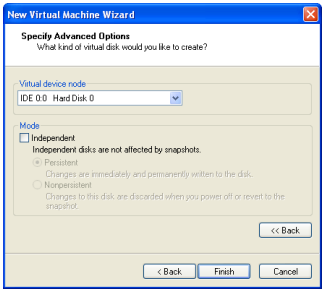
Consider this example: You need about 500MB of actual free space on the file system containing the virtual disk to install Windows Me and popular applications such as Microsoft Office inside the virtual machine. You can set up a single virtual disk to hold these files. Or you can split them up — installing the operating system on the first virtual disk and using a second virtual disk for applications or data files.

12. If you selected **Typical** as your configuration path, click **Finish** and the wizard sets up the files needed for the virtual machine.

    If you selected **Custom** as you configuration path, continue with the next step, specifying the location of the virtual disk's files.



    If you want to specify which device node should be used by your SCSI or IDE virtual disk, click **Advanced**.



    On the Specify Advanced Options panel, you can also specify a disk mode. This is useful in certain special-purpose configurations in which you want to exclude disks from the snapshot.

    Normal disks are included in the snapshot. In most cases, you should use normal disks, leaving **Independent** unchecked.

    Independent disks are not included in the snapshot.

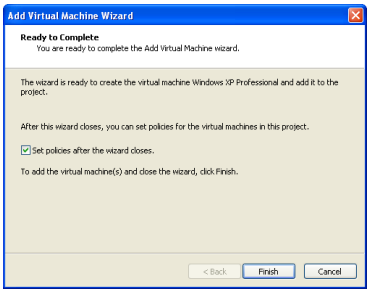
    Caution: The independent disk option should be used only by advanced users who need it for special-purpose configurations.

You have the following options for an independent disk:

- **Persistent** — changes are immediately and permanently written to the disk.
- **Nonpersistent** — changes to the disk are discarded when you power off the virtual machine.

When you have set the filename and location you want to use and have made any selections you want to make on the advanced settings panel, click **Finish**.

13. When you click **Finish,** the wizard sets up the files needed for your virtual machine.
14. The Ready to Complete panel appears.



Select **Set policies after the wizard closes** if you want to go directly to the policy editor and set policies for the virtual machines in the project.

Deselect **Set policies after the wizard closes** if you do not want to set policies for the virtual machines at this time.

Click **Finish** to complete the Add Virtual Machine Wizard.

Checklist: Adding a Virtual Machine

You may find it helpful to photocopy this checklist and use it to collect the information you should have available when you add virtual machines to a project.

Do you plan to add an existing virtual machine or create a new one?

☐ Existing

What is the path to the configuration (`.vmx`) file for this virtual machine?

_____

If you plan to add an existing virtual machine, stop here.

☐ New

If you plan to create a new virtual machine, continue with the other items on this checklist.

What guest operating system do you plan to install in the new virtual machine?

_____

If you plan to install from installation CDs, be sure to have the CDs available.

If you plan to use a PXE installation server, be sure to enable networking when you create the virtual machine.

If you plan to install from ISO image files on the network, what is the path to the ISO files?

_____

Note: Be sure to install VMware Tools in the virtual machine after you finish installing the guest operating system.

What applications do you plan to install in the virtual machine?

If you plan to install from installation CDs, be sure to have the CDs available.

If you plan to install from files on the network, be sure to enable networking when you create the virtual machine and note the paths to the installers below.

_____

_____

_____

_____

_____

_____

Do you need to run Sysprep in the virtual machine?

If you plan to run Sysprep from a CD, be sure to have the CD available.

If you plan to run Sysprep from the network, be sure to enable networking when you create the virtual machine and note the path to Sysprep below.

_____

Do you want to take the typical or custom path through the New Virtual Machine Wizard?

☐ Typical

The typical path lets you specify

- The guest operating system
- The virtual machine name and the location of the virtual machine's files
- The network connection type
- Disk size
- Allocation of space for the disk
- Splitting the disk into 2GB files

☐ Custom

The custom path lets you specify

- The guest operating system
- The virtual machine name and the location of the virtual machine's files
- The network connection type
- A location for the virtual disk files that is different from the location for the other virtual machine files
- The use of an IDE virtual disk for a guest operating system that would have a SCSI virtual disk by default
- The use of memory options different from the default

What's the name for this virtual machine?

_____

What's the path to the location where you plan to store this virtual machine?

_____

Be sure you have enough free space at that location to store the files. If you are following the custom path, you have an option at a later stage in the wizard to specify a separate location for the virtual disk files.

Custom path only: How much memory should the virtual machine use?

☐ Default set by the wizard

☐ Custom setting of _____ MB

What kind of networking do you want to use in this virtual machine?

☐ Bridged

If the virtual machine will run on a host computer that is on a network and a separate IP address will be available for the virtual machine (or the virtual machine can get one automatically from a DHCP server), use bridged networking. This choice may be appropriate if the virtual machine will run on a corporate network.

☐ NAT

If the virtual machine will need to share an IP address with the host computer, use network address translation (NAT). This choice may be the best one if the virtual machine will run on a home computer.

☐ None

Custom path only: What type of virtual SCSI adapter do you want to use in the virtual machine? The default for your guest operating system is selected by the wizard. The LSI Logic adapter has improved performance, but some guest operating systems do not have drivers for this adapter.

☐ Default set by the wizard

☐ BusLogic

☐ LSI Logic

Custom path only: What kind of disk do you want to use in the virtual machine?

☐ New virtual disk

This is the best selection in most cases.

☐ Existing virtual disk

If you want to reuse an existing virtual disk, select this option. You may want to select this option if you are creating a virtual machine with the same operating system and applications as one you created before but you want to apply different policies. In most cases, if you want to reuse an existing virtual disk, it is better to add the existing virtual machine to the project.

Custom path only: What disk type do you want to use? The wizard recommends a selection based on the guest operating system.

☐ Default set by the wizard

☐ IDE

☐ SCSI

How big should the virtual disk be?

☐ Default (4GB)

☐ Custom size of _____ GB

You can set a size between 0.1GB and 256GB for a SCSI virtual disk or 128GB for an IDE virtual disk. The default is 4GB.

What other selections should be made on the panel for configuring the virtual disk?

☐ Allocate all disk space

Allocating all the space at the time you create the virtual disk gives somewhat better performance, but it requires as much disk space as the size you specify for the virtual disk. It makes the distribution package for your project larger — possibly much larger. However, it ensures that your users have enough disk space set aside for the virtual machine and do not run out of space unexpectedly.

☐ Split disk into 2GB files

You should split the virtual disk if it may be stored on a FAT32 file system.

Note: Because the Microsoft installer cannot install files larger than about 4.3GB, you should also split the virtual disk if the disk is larger than 4GB.

Custom path only: Where do you want to store the virtual disk's files?

By default, the virtual disk files are stored in the same directory as the virtual machine's other files — for example, the configuration file. If you plan to store the virtual disk files in a different location, note the path below.

_____

Custom path only: Do you need to specify a particular IDE or SCSI device node to be used by the virtual disk?

In most cases, you should accept the default. If you need to specify the device node, make a note of it below.

_____

CHAPTER 5

Setting Policies and Customizing VMware ACE

The following sections guide you through the steps to set policies for a project, prepare your virtual machine, customize the VMware ACE interface and run the virtual machine in the VMware ACE interface:

- Setting Policies for a Project on page 71
- Setting Policies for VMware ACE on page 74
- Setting Policies for Virtual Machines on page 81
  - Setting Authentication Policies on page 81
  - Setting Expiration Policies on page 83
  - Setting Copy Protection Policies on page 84
  - Setting Device Connection Policies on page 85
  - Setting Network Quarantine Policies on page 85
- Configuring the Virtual Machines and Installing Software on page 111
  - Reviewing the Configuration of a Virtual Machine on page 111

- Installing an Operating System and Applications in the Virtual Machine on page 112
- Customizing the VMware ACE Interface on page 123
- Running the Completed Virtual Machine on page 129
  - Checking the Configuration before Creating a Package on page 129

Setting Policies for a Project

Policies give you control over many aspects of the virtual machines you distribute to your end users. You can, for example

- Permit the virtual machine to be used only by certain users and groups defined in your Active Directory domains.
- Specify which network resources your users may access from the virtual machine.
- Permit users to connect and disconnect certain removable devices configured for the virtual machine.
- Control the lifetime of the virtual machine.

For many policy categories, you can write your own plug-ins to determine what permissions and restrictions to apply.

For additional information on policies, see Understanding Policies on page 219.

Using the Policy Editor

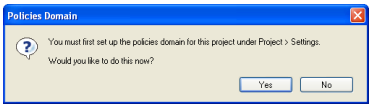
You set policies using the policy editor. You may continue directly from the Add Virtual Machine Wizard to the policy editor. Or you may start the policy editor from any summary display. To start the policy editor from the project summary display, select the name of a virtual machine, then click **Policies**.

You may set default policies for all virtual machines, policies that apply to a particular virtual machine and policies that apply to VMware ACE, the application included in the project.

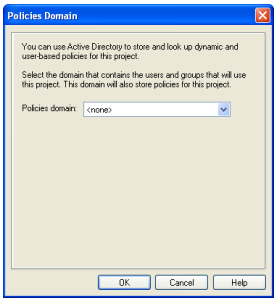
Before you can set policies based on users and groups in your Active Directory service, you must choose an Active Directory domain. You must also choose an Active Directory domain if you want to use the Active Directory service to store dynamic network quarantine settings.

Note: If you store policies on your Active Directory server, you must be sure end users' host computers have been added to the domain where the policies are stored, and end users must log on to that domain so VMware ACE has access to the policies. Similarly if you set policies based on users and groups in your Active Directory domain, end users' host computers must log on to a domain where those users and groups are defined.

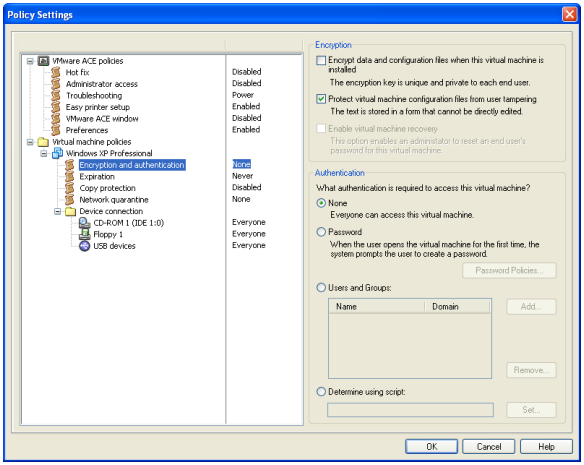
If you attempt to make a policy setting that requires an Active Directory domain and you have not yet specified the domain, a dialog box notifies you that you need to set up the domain.



Click **Yes** to open a second dialog box that allows you to specify the policies domain. If you click **No**, you can specify the domain at any time in the project settings editor (**Project** > **Settings**).



Choose the appropriate domain name from the **Policies domain** drop-down list.



The list of settings available in the right pane of the policy editor depends on the category you select in the left pane. For several categories, the settings are similar to those in the following list:

- **None** — No restrictions are imposed.
- **Password** — Users must log on with a password.
- **Users and groups** — Specified users or members of specified groups defined in your Active Directory service have permission to take the action. Click **Add** to add a user or group to the list. To remove a name from the list, select the name of a user or group in the list, then click **Remove**.
- **Determine using script** — Use your own custom plug-in to determine what settings are applied. Click **Set** to open a dialog box that lets you locate the plug-in script file and specify the command line for running the script. You may also specify a timeout interval in case the script does not run to completion.

  Scripts used in a project must be in the `Project Resources` folder under the project folder. They must be in the main `Project Resources` folder, not in a subdirectory under that folder. If the scripts need any additional resource files, place those files in the main `Project Resources` folder, too.

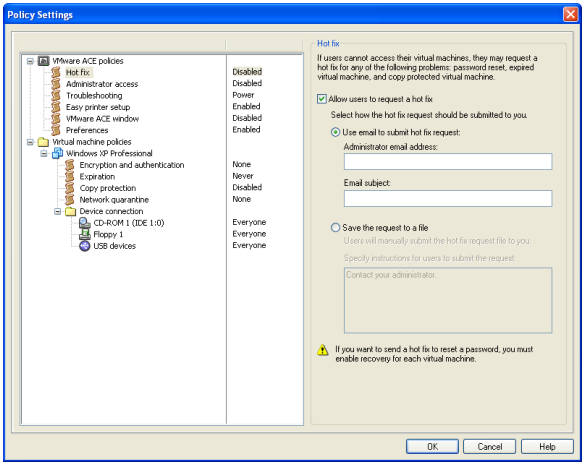
  For details on how to create plug-in scripts, see Writing Plug-In Policy Scripts on page 244.

Setting Policies for VMware ACE

To set policies for VMware ACE, click the + sign beside **VMware ACE policies** to show the categories of settings, then edit the settings as described below.

Hot Fix Policy

Select **Hot fix** to specify that users are allowed to request hot fixes for specific problems.



If you enable the hot fix feature, end users can easily request help to resolve the following problems:

- Lost or forgotten password

  Note: If you want to be able to use a hot fix to reset an end user's password for encrypted virtual machines, you must enable recovery for each virtual machine. For details, see Setting Authentication Policies on page 81.

- Expired VMware ACE environment
- Copy protected VMware ACE environment run from a new location

It is also easy for you to respond to their requests.

To enable the hot fix feature, select **Allow users to request a hot fix**.

The hot fix request is a file that the end user must submit to an administrator for action. After enabling the hot fix feature, you must select the preferred way for the end user to submit the hot fix request. Choose one of the following:

- **Use email to submit hot fix request** — The Hot Fix Request Wizard on the end user's computer attempts to use a MAPI email client on the host operating system to send the hot fix request as an attachment to an email message. The message uses the email address and subject line that you specify here.
- **Save the request to a file** — The end user saves the script, then must submit it to an administrator manually.

  The end user sees any submission instructions you enter in the field labeled **Specify instructions for users to submit the request**.

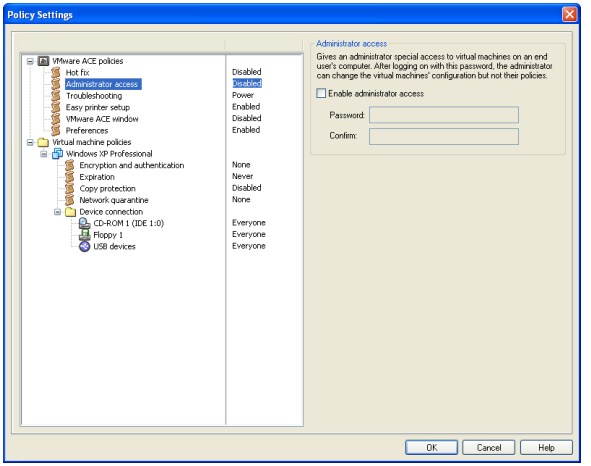
If you choose email and the automatic submission fails, the Hot Fix Request Wizard gives the end user an opportunity to save the hot fix request as a file. The end user must then send the file to an administrator manually.

For details on responding to hot fix requests, see Responding to Hot Fix Requests on page 150.

For details on how the end user interacts with the Hot Fix Request Wizard, see Requesting a Hot Fix on page 163.

Administrator Access Policy

Select **Administrator access** to set an administrator password so you can run the virtual machine in a special troubleshooting application on the end user's computer and make changes to the virtual machine's configuration.

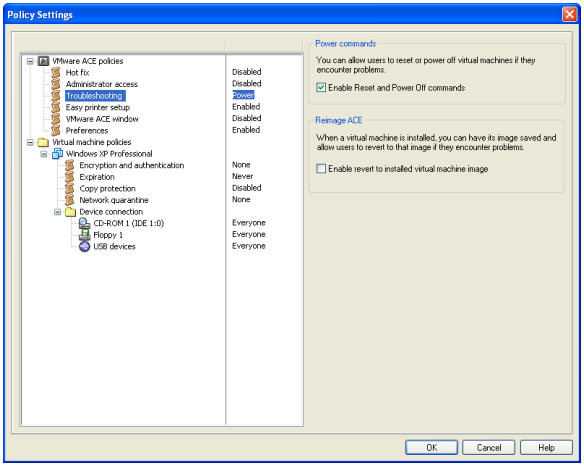


Select **Enable administrator access** if you want to enable this function, then enter and confirm the password to be used for administrator access on the end user's

computer. For more information, see Using Administrator Access on the End User's Computer on page 152.

Troubleshooting Policies

Select **Troubleshooting** to specify which items appear under Troubleshooting on the VMware ACE menu.



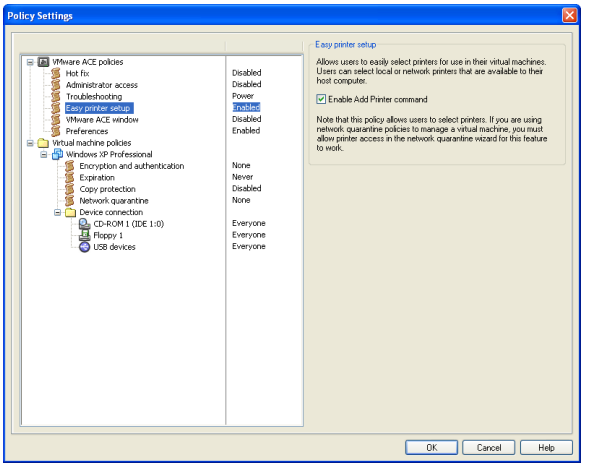
Under Power commands, you may select **Enable Reset and Power Off commands**. If you enable these commands, the end user may power off or reset the virtual machine from the menu in VMware ACE (**VMware ACE** > **Troubleshoot** > **Reset** or **VMware ACE** > **Troubleshoot** > **Power Off and Exit**).

Under Reimage ACE, you may select **Enable revert to installed virtual machine image**. If you enable this feature, VMware ACE captures an image of the virtual machine at the time it is installed on the end user's machine. The end user may then revert to this original state by choosing **VMware ACE** > **Troubleshoot** > **Revert to the Installed <vmname> Environment**, where <vmname> is the name of the virtual machine.

Note: If the virtual machine uses password authentication, reverting to the installed environment returns the virtual machine to its state after the initial password was selected. If you enable this feature, you should also consider implementing hot fixes so you can respond easily if end users revert and have forgotten their original passwords.

Easy Printer Setup Policies

Select **Easy printer setup** to specify whether to give end users access to a command that simplifies printer setup for a Windows virtual machine.



Select **Enable Add Printer command** to provide an Add Printer item on the VMware ACE menu. End users can use this menu item to set up a printer available on the host for use in the virtual machine.

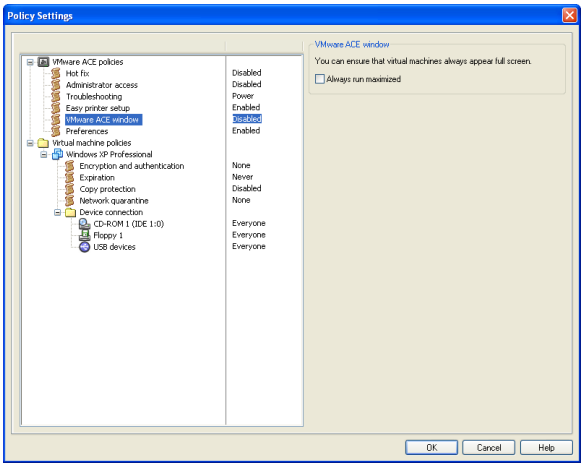
Easy printer setup relies on network printer sharing. If you set network quarantine policies and want to enable easy printer setup, you must also enable printer access on the Traffic panel of the Network Quarantine Wizard. For details, see Setting Network Quarantine Policies on page 85.

Some special steps may be necessary if your end users need to connect network printers to their virtual machines. For details, see Easy Printer Setup Policies on page 227.

Note: Printer sharing is not supported in Windows Server 2003 Web Edition. As a result, the easy printer setup feature does not work on a host computer running Windows Server 2003 Web Edition.

VMware ACE Window Policies

Select **VMware ACE Window** to specify the appearance of VMware ACE on the end user's computer.

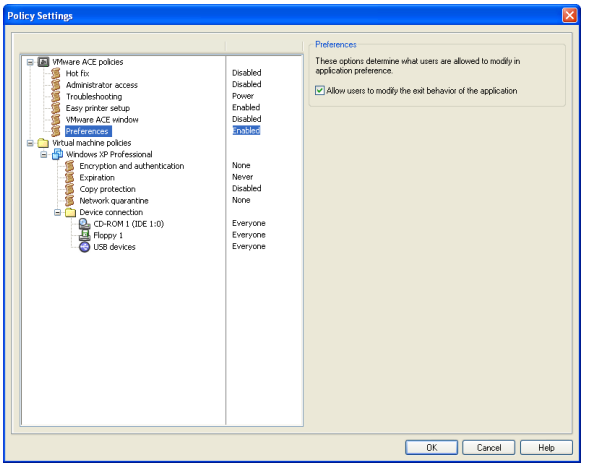


Under VMware ACE Window, you may select **Always run maximized**. If you select this policy, VMware ACE fills the full screen when it starts, hiding the host operating system. You may find this useful, for example, to avoid user confusion about the differences between the two environments.

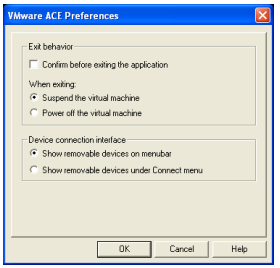
Note: The end user can minimize the VMware ACE display and return to the host operating system by clicking the minimize button on the toolbar. If the mouse pointer is not available, pressing Ctrl-Alt minimizes the display.

User Preferences Policies

Select **Preferences** to specify what settings are available to end users in the VMware ACE Preferences dialog box (**VMware ACE** > **Preferences**).



You may select **Allow users to modify the exit behavior of the application**. If you do, the exit behavior settings are available in the Preferences dialog box, as shown below.



The exit behavior preferences allow the end user to specify the following:

- **Confirm before exiting the application** — When the end user gives the command to exit VMware ACE, either from the menu or by clicking the X in the upper right corner of the window or toolbar, a dialog box appears. The end user may confirm the intention to exit VMware ACE or click **Cancel** to continue working.
- **Suspend the virtual machine** when exiting — This is the default behavior. VMware ACE suspends the virtual machine and closes. The next time the end

user runs the virtual machine, it resumes operation from the point at which it was suspended.

- **Power off the virtual machine** when exiting — VMware ACE powers off the virtual machine. The next time the end user launches VMware ACE, the virtual machine starts from a powered off state and the guest operating system boots.

Setting Policies for Virtual Machines

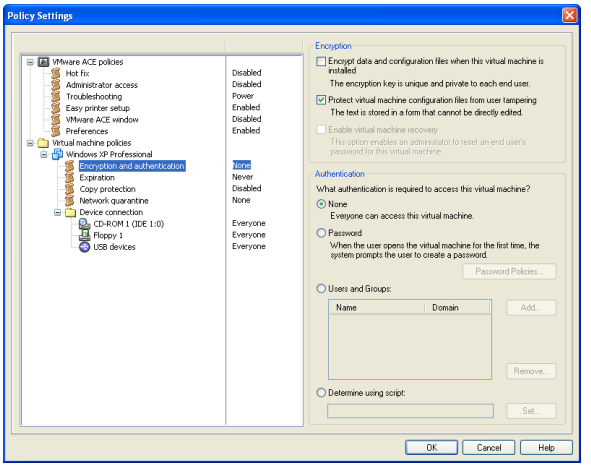
In the policy editor, you can edit policies for each virtual machine in the project.

To set policies for an individual virtual machine in your project, click the + sign beside the name of the virtual machine. The list of policy categories appears below the virtual machine name and you may edit the settings as described in the following sections:

- Setting Authentication Policies on page 81
- Setting Expiration Policies on page 83
- Setting Copy Protection Policies on page 84
- Setting Device Connection Policies on page 85
- Setting Network Quarantine Policies on page 85

Setting Authentication Policies

Select **Encryption and authentication** from the Policy list to specify whether the virtual machine's data is to be encrypted and who has access to this virtual machine.



Encrypted Virtual Machine

To protect the contents of the virtual machine, you can specify that the package installer encrypts the virtual machine when it is installed. To do so, select **Encrypt data and configuration files when this virtual machine is installed**. Each installation of the virtual machine is encrypted differently.

You must specify an authentication method if you want the installer to encrypt the virtual machines. If you select **Encrypt data and configuration files when this virtual machine is installed**, you cannot select **None** as the authentication method.

If you encrypt the virtual machine, its configuration files are automatically protected against viewing and tampering. Even if you do not encrypt the virtual machine, you may select **Protect virtual machine configuration files from user tampering**.

If you encrypt the virtual machine, also select **Enable virtual machine recovery** if you want to be able to use a hot fix to reset the end user's password.

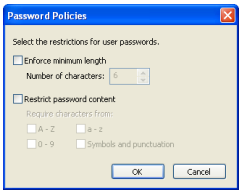
No Authentication Requirements

If you select **None**, there are no restrictions on access to this virtual machine.

Password Authentication

If you select **Password**, the virtual machine is password protected and does not run until the user enters the correct password. Each user must set a password the first time that user's installation of this virtual machine is opened.

Click **Password Policies** to specify requirements for user passwords.



To require that passwords be at least a certain length, select **Minimum Password Length**, then enter the number of characters required.

To require a mix of characters, select **Restrict Password Contents**, then select the types of characters required. You may require that the password include one or more of the following:

- Capital letters
- Lowercase letters
- Numerals
- Symbols and punctuation

Make the selections you want, then click **OK**.

Active Directory Authentication

Select **Users and groups** to enable access by individuals or groups defined in an Active Directory domain.

If you attempt to make a policy setting that requires an Active Directory domain and you have not yet specified the domain, a dialog box notifies you that you need to set up the domain. Click **Yes** to open a second dialog box that allows you to specify the policies domain. If you click **No**, you can specify the domain at any time in the project settings editor (**Project** > **Settings**). Select **Policies Domain** and check to be sure you have chosen the correct domain.

Click **Add** to add users or groups to the approved list. The Add Users or Groups dialog box allows you to select users or groups defined for the currently selected domain.

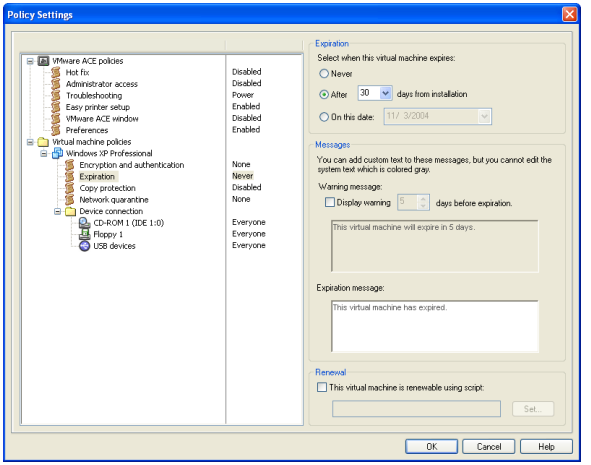
To remove a user or group from the approved list, select a name, then click **Remove**.

Script-Based Authentication

Select **Determine using script** if you want to use your own custom plug-in to determine who can use the virtual machine. Click **Set** to open a dialog box that lets you locate the plug-in script file and specify the command line for running the script. You may also specify a timeout interval in case the script does not run to completion. For details on how to create plug-in scripts, see Writing Plug-In Policy Scripts on page 244.

Setting Expiration Policies

Select **Expiration** from the Policy list to set an expiration date for the virtual machine. When a virtual machine expires, the files remain on the end user's computer, but the virtual machine cannot be used.



You may select one of the following options for expiration:

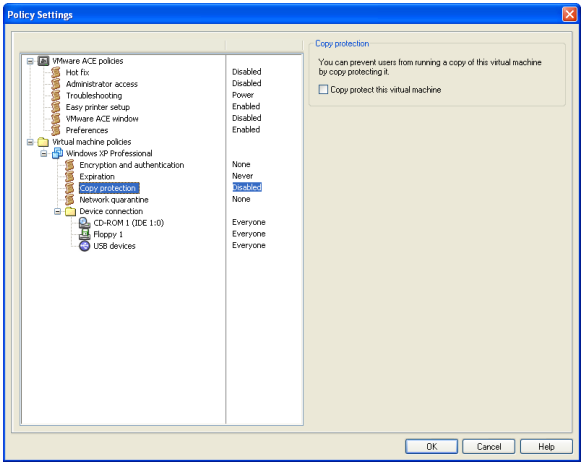
- **Never** — The virtual machine does not expire.
- **After x days from installation** — The virtual machine runs for the specified number of days after the package is installed, then cannot be used.
- **On this date** — The virtual machine runs until and on the specified date. It cannot be used after the specified date.

If the virtual machine is set to expire, you may also specify a script used to renew the virtual machine. Click **Set** to open a dialog box that lets you locate the plug-in script file and specify the command line for running the script. You may also specify a timeout interval in case the script does not run to completion. For details on creating scripts, see Writing Plug-In Policy Scripts on page 244.

You may customize the expiration message, enable a warning message, set the time when the warning message first appears and customize the text of the warning message.

Setting Copy Protection Policies

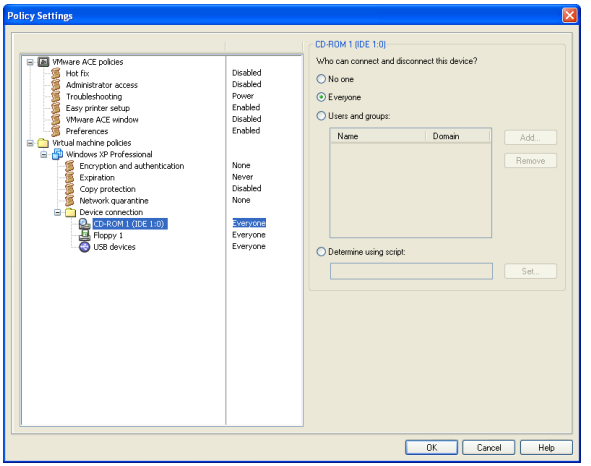
Select **Copy protection** from the Policy list to ensure that virtual machines can run only from the location where they are originally installed.



Select **Copy protect this virtual machine** to restrict the virtual machine so it can run only from the location where it is installed by the package installer. If you select this restriction and the virtual machine is copied or moved to a new location, it cannot run from that new location.

Setting Device Connection Policies

Click the + sign to open the **Device connection** folder, then select a device to specify who is allowed to connect and disconnect that device. The list for a specific virtual machine shows only the devices actually configured for that virtual machine. To add devices, use the virtual machine settings editor (**VM** > **Settings**).



You may select one of the following options for each device:

- **No one** — End users may not connect and disconnect the device.
- **Everyone** — All end users may connect and disconnect the device.
- **Users and groups** — Specified users or members of specified groups defined in your Active Directory service have permission to connect and disconnect the device. Click **Add** to add a user or group to the list. To remove a name from the list, select the name of a user or group in the list, then click **Remove**.
- **Determine using script** — Use your own custom plug-in to determine what settings are applied. Click **Set** to open a dialog box that lets you locate the plug-in script file and specify the command line for running the script. You may also specify a timeout interval in case the script does not run to completion. For more information, see Device Connection Plug-Ins on page 247.

Setting Network Quarantine Policies

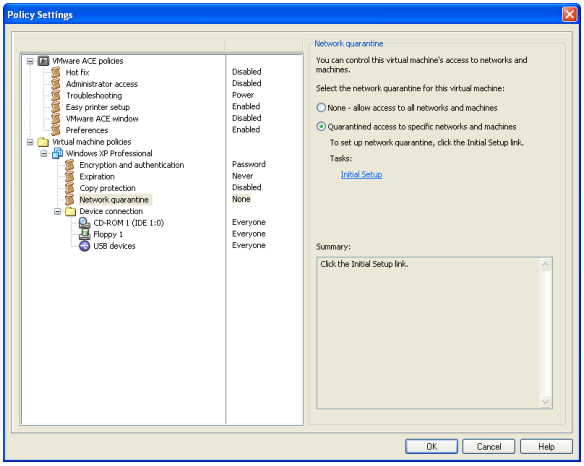
Network quarantine policies give you flexible control over user access to network resources. For example, you can

- Allow users to access only specified machines or subnets.

- Require that users have up-to-date virtual machines in order to access network resources.
- Temporarily block virtual machine access to network resources to control a virus outbreak.

For more information, see Network Quarantine Policies on page 230.

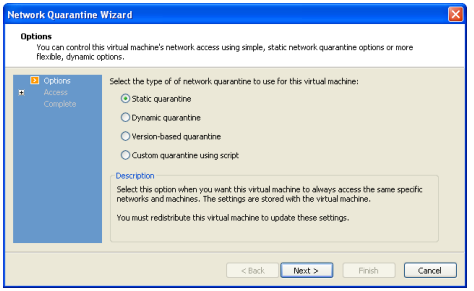
Select **Network quarantine** to control whether the virtual machine has normal network access or restricted access on the basis of rules you specify.



To allow unrestricted network access, select **None – access to all networks and machines**.

To specify network quarantine settings, select **Quarantined access to specific networks and machines**, then click **Initial Setup** to set quarantine policies. The wizard guides you through the settings. You may rerun the wizard at any time to change the settings.

When you click **Initial Setup**, the Network Quarantine Options panel appears.



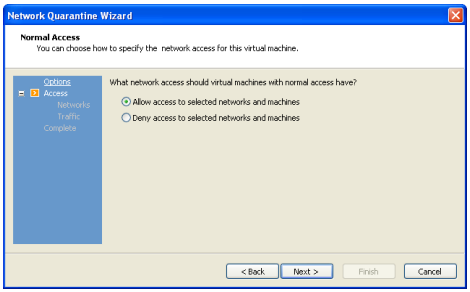
Select the type of network quarantine you want to apply to the virtual machine, then click **Next** to continue through the wizard.

- **Static quarantine** — You specify a single list of approved networks and machines or of networks and machines that are off-limits. The list is stored with the virtual machine and distributed as part of the package. If you need to make any changes in the future, you must update the package and distribute the update to your users. If you select this option, see Static Quarantine on page 88 for the next steps in the wizard.
- **Dynamic quarantine** — You specify a single list of approved or disapproved networks and machines. The list is stored on a server. The virtual machine checks the server frequently and retrieves the list. If you need to make any changes in the future, you update the list stored on the server. If you select this option, see Dynamic Quarantine on page 90 for the next steps in the wizard.
- **Version-based quarantine** — You specify two lists of approved or disapproved networks and machines. One list is used for up-to-date virtual machines. The other list is used for out-of-date virtual machines. The lists are stored on a server. The virtual machine checks the server frequently and retrieves the lists. VMware ACE uses the list of approved or disapproved networks and machines that is appropriate for the virtual machine's version. If you need to make any changes to the lists or the network quarantine version in the future, you do so by updating the information stored on the server. If you select this option, see Version-Based Quarantine on page 95 for the next steps in the wizard.
- **Custom quarantine using script** — You specify two lists of approved or disapproved networks and machines. You also specify a script that runs to determine which list the virtual machine should use. If you select this option, see Custom Quarantine Using a Script on page 102 for the next steps in the wizard.

For guidelines on how to write custom quarantine scripts, see Writing Plug-In Policy Scripts on page 244.

Static Quarantine

1. The Access panel appears.

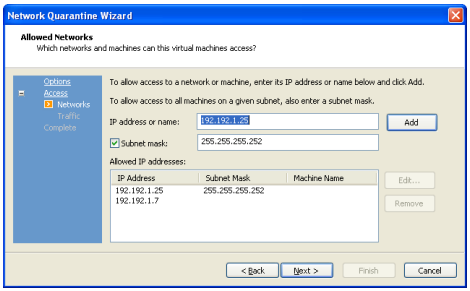


Select the way you want to specify network access.

- **Allow access to selected networks and machines** — Specify a whitelist of networks and machines with which the virtual machine may communicate.
- **Deny access to selected networks and machines** — Specify a blacklist of networks and machines with which the virtual machine is not allowed to communicate.

You may set up either a whitelist or a blacklist but not both.

2. The Networks and Machines panel appears.



Enter the IP address or the fully qualified host name for each network or machine that this virtual machine may access, then click **Add**.

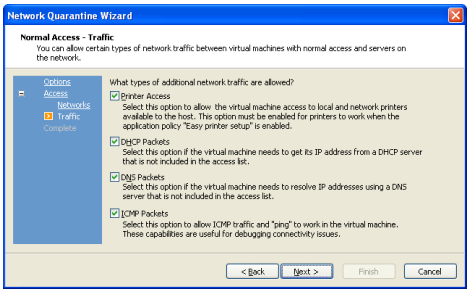
If you enter a host name, the wizard resolves the name and displays both the host name and the IP address in the list.

To specify a single machine, you may also enter its IP address.

To specify a subnet, enter the starting IP address for the subnet, select **Subnet mask** and enter the mask in the corresponding field in dotted quad format.

When the list is complete, click **Next**.

3. If you specified networks and machines that are allowed, the Network Traffic panel appears. If you specified networks and machines that are denied, skip to the next step.

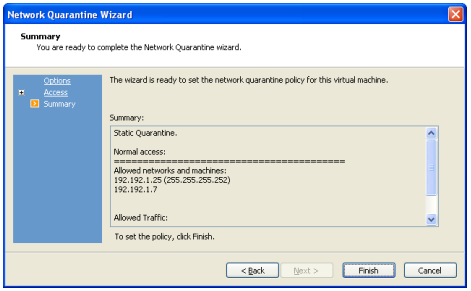


Using this panel, you may set up exceptions to allow certain types of network traffic that would otherwise be blocked by the rules you set on the Networks and Machines panel. This is useful, for example, if virtual machine users are restricted to a particular subnet but the DNS server on your network is not on that subnet.

- **Printer access** — Select this option to be sure a Windows virtual machine can use local and network printers available on the host. Be sure to select this option if you configure the virtual machine to allow easy printer setup. Easy printer setup uses network sharing to connect the virtual machine to a printer configured on the host computer.
- **DHCP packets** — Select this option if the virtual machine needs to get its IP address from a DHCP server that is not included in the access list.
- **DNS packets** — Select this option if the virtual machine needs to resolve IP addresses using a DNS server that is not included in the access list.
- **ICMP packets** — Select this option if you need support for the ping command — for example, to check network connectivity to and from the virtual machine.

Click **Next**.

4. The Summary panel appears.



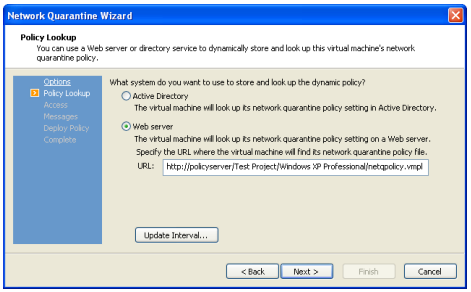
This panel displays a summary of the settings you have made using the wizard. Review the settings to be sure they are correct.

To modify settings, click **Back** until you reach the appropriate panel to make the needed change.

If all settings are correct, click **Finish**. The wizard closes and returns you to the policy editor.

Dynamic Quarantine

1. The Policy Lookup panel appears.



Select the type of server you want to use to store the list of approved networks and machines. VMware ACE checks the list on this server to determine what network access is approved for the virtual machine.

- **Active Directory** — Select this option if you plan to store the network quarantine policy on your Active Directory server. The wizard adds this information to your Active Directory server for you.

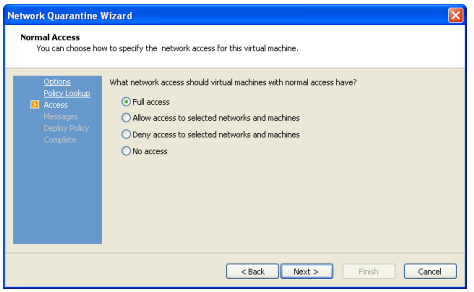
  Note: In order to use the directory service option, you must choose an Active Directory domain in the project settings editor. If you select **Active Directory** and have not yet chosen an Active Directory domain, the wizard opens a

dialog box that gives you the option of setting the domain at this time. Click **Yes** to open the Policies Domain dialog box.

- **Web server** — Select this option if you plan to store the network quarantine list on a Web server. Enter the URL of the file where you plan to store the list. Be sure to include the filename in the URL. The wizard creates this file for you at the end of the process.

Click **Update Interval** to specify how often VMware ACE should check for changes to the network quarantine policies. You may choose an interval from 5 minutes to 1 day. The default is 5 minutes.

2. The Normal Access panel appears.

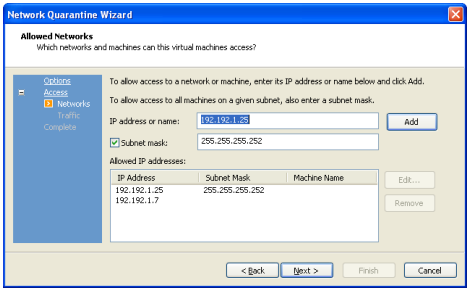


Select the way you want to specify network access.

- **Full access** — No restrictions are imposed.
- **Allow access to selected networks and machines** — Specify a whitelist of networks and machines with which the virtual machine may communicate.
- **Deny access to selected networks and machines** — Specify a blacklist of networks and machines with which the virtual machine is not allowed to communicate.
- **No access** — Block all network access.

You may set up either a whitelist or a blacklist but not both.

3. The Networks and Machines panel appears.



Enter the IP address or the fully qualified host name for each network or machine that should be on the whitelist or blacklist, then click **Add**.

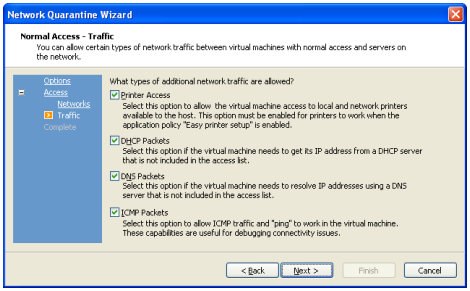
If you enter a host name, the wizard resolves the name and displays both the host name and the IP address in the list.

To specify a single machine, you may also enter its IP address.

To specify a subnet, enter the starting IP address for the subnet, select **Subnet mask** and enter the mask in the corresponding field in dotted quad format.

When the list is complete, click **Next**.

4. If you specified networks and machines that are allowed, the Network Traffic panel appears. If you specified networks and machines that are denied, skip to the next step.

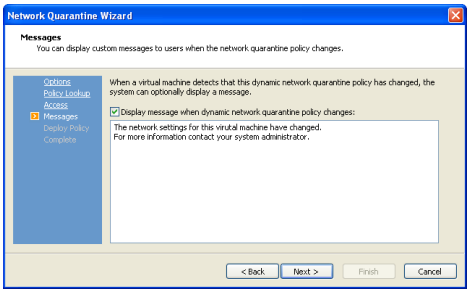


Using this panel, you may set up exceptions to allow certain types of network traffic that would otherwise be blocked by the rules you set on the Networks and Machines panel. This is useful, for example, if virtual machine users are restricted to a particular subnet but the DNS server on your network is not on that subnet.

- **Printer access** — Select this option to be sure a Windows virtual machine can use local and network printers available on the host. Be sure to select this option if you configure the virtual machine to allow easy printer setup. Easy printer setup uses network sharing to connect the virtual machine to a printer configured on the host computer.
- **DHCP packets** — Select this option if the virtual machine needs to get its IP address from a DHCP server that is not included in the access list.
- **DNS packets** — Select this option if the virtual machine needs to resolve IP addresses using a DNS server that is not included in the access list.
- **ICMP packets** — Select this option if you need support for the ping command — for example, to check network connectivity to and from the virtual machine.

Click **Next**.

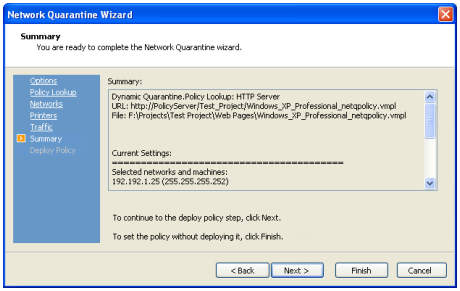
5. The Messages panel appears.



If you select **Display message when dynamic quarantine policy changes**, enter the message you want end users to see when the network quarantine policy changes.

Click **Next** to continue.

6. The Summary panel appears.

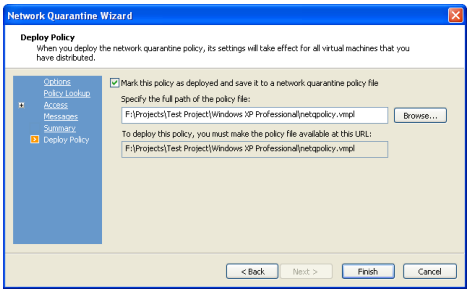


This panel displays a summary of the settings you have made using the wizard. Review the settings to be sure they are correct.

To modify settings, go to the appropriate panel to make the needed change.

To continue to the Deploy Policy panel, click Next. To set the policy without deploying it, click **Finish**.

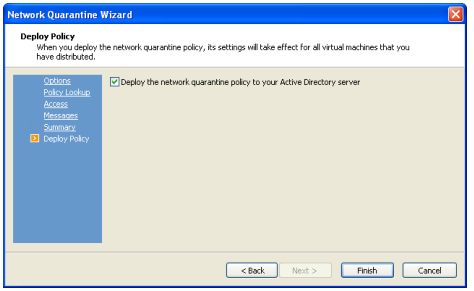
7. If you selected **Web server**, the Deploy Policy panel that appears looks like this.



Select **Mark this policy as deployed and save it to a network quarantine policy file** to capture your policy changes. You may type the path and filename for the policy file or click **Browse** to navigate to the location where you want to save the file. Be sure to copy the updated policy file to the URL shown in this panel. The new policies take effect as soon as you make the file available on the Web server.

Click **Finish** to save the policy file.

If you selected **Active Directory**, the Deploy Policy panel that appears looks like this.



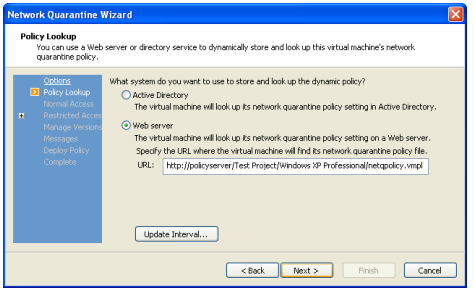
Select **Deploy the network quarantine policy to your Active Directory server**.

When you click **Finish**, the wizard deploys the new policies, which take effect immediately.

Version-Based Quarantine

Network access restrictions are based on the virtual machine's version number. The virtual machine's version number can be checked against a directory server or a Web server that you specify. If the virtual machine's version number matches criteria you specify, it is granted normal access to the network, based on rules you set. If the virtual machine's version number does not match the criteria you specify, it is granted only restricted access, based on a second set of rules.

1. The Policy Lookup panel appears.



Select the type of server you want to use to store the list of approved networks and machines. VMware ACE checks the list on this server to determine what network access is approved for the virtual machine.

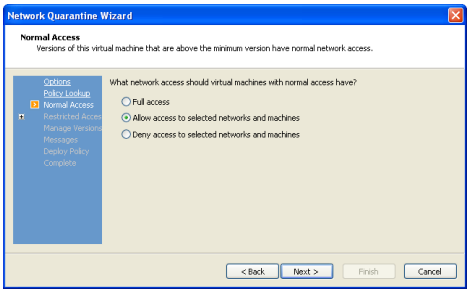
- **Active Directory** — Select this option if you plan to store the network quarantine policy on your Active Directory server. The wizard adds this information to your Active Directory server for you.

  Note: In order to use the directory service option, you must choose an Active Directory domain in the project settings editor. If you select **Active Directory** and have not yet chosen an Active Directory domain, the wizard opens a dialog box that gives you the option of setting the domain at this time. Click **Yes** to open the Policies Domain dialog box.

- **Web server** — Select this option if you plan to store the network quarantine list on a Web server. Enter the URL of the file where you plan to store the list. Be sure to include the filename in the URL. The wizard creates this file for you at the end of the process.

Click **Update Interval** to specify how often VMware ACE should check for changes to the network quarantine policies. You may choose an interval from 5 minutes to 1 day. The default is 5 minutes.

2. The Normal Access panel appears.

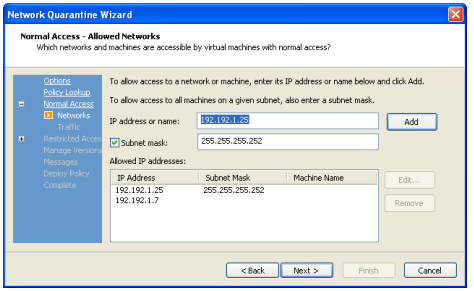


Select the way you want to specify network access.

- **Full access** — No restrictions are imposed.
- **Allow access to selected networks and machines** — Specify a whitelist of networks and machines with which the virtual machine may communicate.
- **Deny access to selected networks and machines** — Specify a blacklist of networks and machines with which the virtual machine is not allowed to communicate.

You may set up either a whitelist or a blacklist but not both.

3. If you are specifying a whitelist or blacklist, the Networks and Machines panel appears.



Enter the IP address or the fully qualified host name for each network or machine that should be on the whitelist or blacklist if this virtual machine qualifies for normal access, then click **Add**.

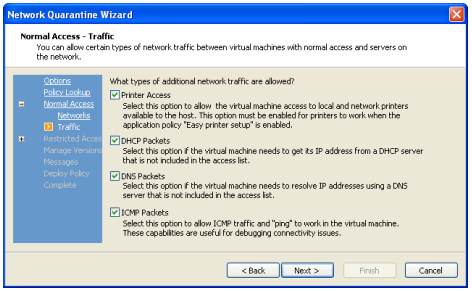
If you enter a host name, the wizard resolves the name and displays both the host name and the IP address in the list.

To specify a single machine, you may also enter its IP address.

To specify a subnet, enter the starting IP address for the subnet, select **Subnet mask** and enter the mask in the corresponding field in dotted quad format.

When the list is complete, click **Next**.

4. If you specified networks and machines that are allowed, the Network Traffic panel appears. If you specified networks and machines that are denied, skip to the next step.



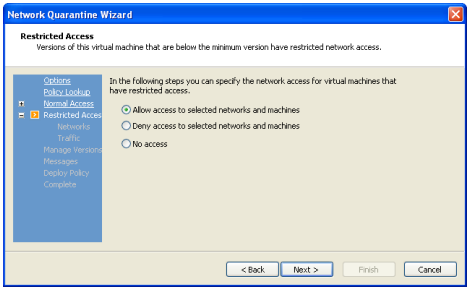
Using this panel, you may set up exceptions to allow certain types of network traffic that would otherwise be blocked by the rules you set on the Networks and Machines panel. This is useful, for example, if virtual machine users are restricted to a particular subnet but the DNS server on your network is not on

that subnet. At this time, you are making these settings for the virtual machine if it qualifies for normal access.

- **Printer access** — Select this option to be sure a Windows virtual machine can use local and network printers available on the host. Be sure to select this option if you configure the virtual machine to allow easy printer setup. Easy printer setup uses network sharing to connect the virtual machine to a printer configured on the host computer.
- **DHCP packets** — Select this option if the virtual machine needs to get its IP address from a DHCP server that is not included in the access list.
- **DNS packets** — Select this option if the virtual machine needs to resolve IP addresses using a DNS server that is not included in the access list.
- **ICMP packets** — Select this option if you need support for the ping command — for example, to check network connectivity to and from the virtual machine.

Click **Next**.

5. The Restricted Access panel appears.



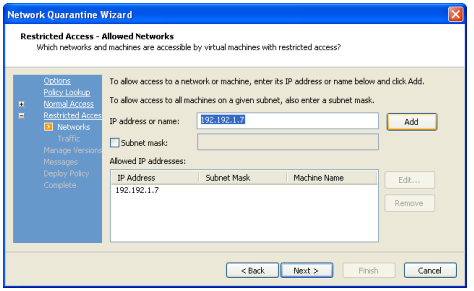
Select the way you want to specify network access.

- **Allow access to selected networks and machines** — Specify a whitelist of networks and machines with which the virtual machine may communicate.
- **Deny access to selected networks and machines** — Specify a blacklist of networks and machines with which the virtual machine is not allowed to communicate.
- **No access** — Block all network access.

You may set up either a whitelist or a blacklist but not both.

Click **Next** to continue.

6. The Networks and Machines panel appears again.



Enter the IP address or the fully qualified host name for each network or machine that this virtual machine may access if it does not qualify for normal access, then click **Add**.

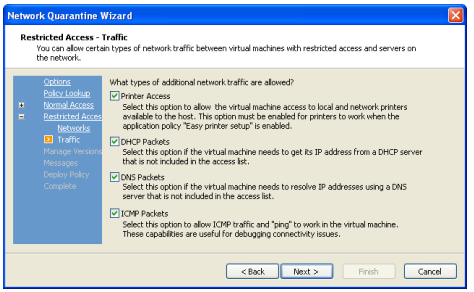
If you enter a host name, the wizard resolves the name and displays both the host name and the IP address in the list.

To specify a single machine, you may also enter its IP address.

To specify a subnet, enter the starting IP address for the subnet, select **Subnet mask** and enter the mask in the corresponding field in dotted quad format.

When the list is complete, click **Next**.

7. If you specified networks and machines that are allowed, the Network Traffic panel appears. If you specified networks and machines that are denied, skip to the next step.



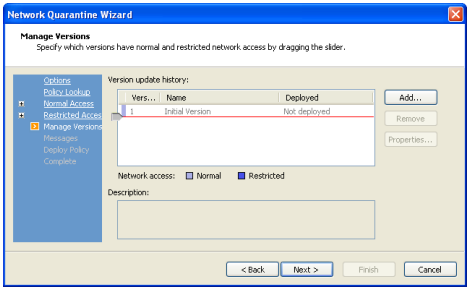
Using this panel, you may set up exceptions to allow certain types of network traffic that would otherwise be blocked by the rules you set on the Networks and Machines panel. This is useful, for example, if virtual machine users are restricted to a particular subnet but the DNS server on your network is not on

that subnet. At this time, you are making these settings for the virtual machine if it does not qualify for normal access.

- **Printer access** — Select this option to be sure a Windows virtual machine can use local and network printers available on the host. Be sure to select this option if you configure the virtual machine to allow easy printer setup. Easy printer setup uses network sharing to connect the virtual machine to a printer configured on the host computer.
- **DHCP packets** — Select this option if the virtual machine needs to get its IP address from a DHCP server that is not included in the access list.
- **DNS packets** — Select this option if the virtual machine needs to resolve IP addresses using a DNS server that is not included in the access list.
- **ICMP packets** — Select this option if you need support for the ping command — for example, to check network connectivity to and from the virtual machine.

Click **Next**.

8. The Manage Versions panel appears.



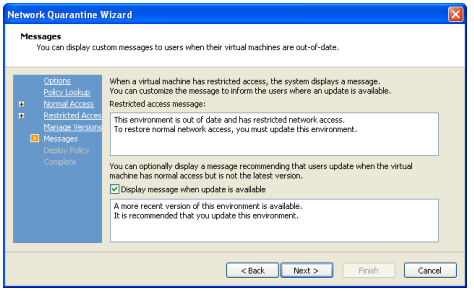
To change the name for the initial version of the virtual machine or add a description, choose the version in the list and click **Properties**.

The initial version is shown with normal access, but the name is dimmed because the virtual machine has not yet been deployed.

If you update the virtual machine at some later time, you may return to this panel to specify which versions have normal access and which versions have restricted access.

Click **Next** to continue.

9. The Messages panel appears.

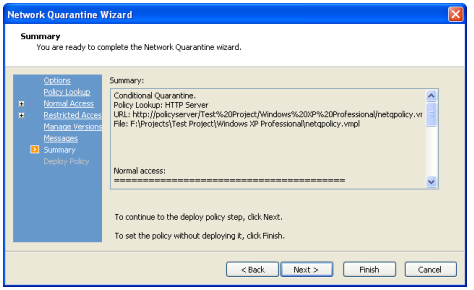


You may enter a custom message that end users see when the virtual machine has restricted access.

If you select **Display message when update is available**, enter the message you want end users to see when the virtual machine has normal access but a more recent version is available.

Click **Next** to continue.

10. The Summary panel appears.

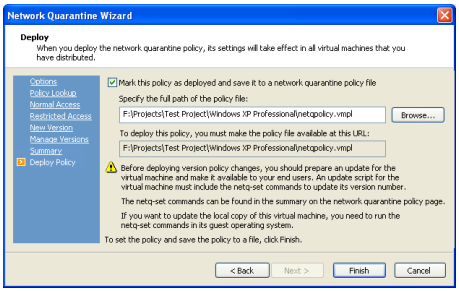


This panel displays a summary of the settings you have made using the wizard. Review the settings to be sure they are correct.

To modify settings, go to the appropriate panel to make the needed change.

To continue to the Deploy Policy panel, click Next. To set the policy without deploying it, click **Finish**.

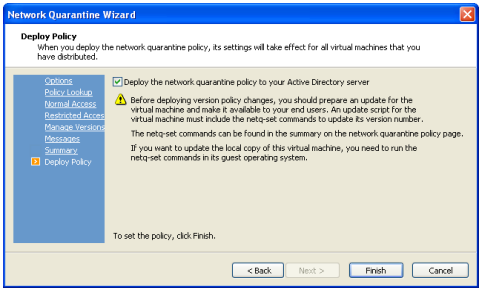
11. If you selected **Web server**, the Deploy Policy panel that appears looks like this.



Select **Mark this policy as deployed and save it to a network quarantine policy file** to capture your policy changes. You may type the path and filename for the policy file or click **Browse** to navigate to the location where you want to save the file. Be sure to copy the updated policy file to the URL shown in this panel. The new policies take effect as soon as you make the file available on the Web server.

Click **Finish** to save the policy file.

If you selected **Active Directory**, the Deploy Policy panel that appears looks like this.



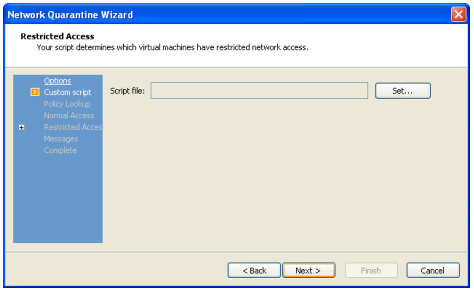
Select **Deploy the network quarantine policy to your Active Directory server**.

When you click **Finish**, the wizard deploys the new policies, which take effect immediately.

Custom Quarantine Using a Script

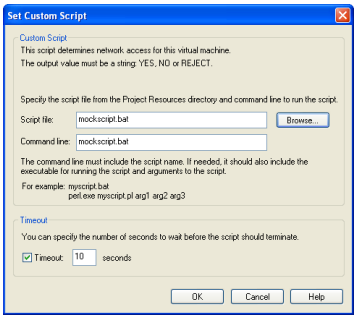
Network access restrictions are based on your custom plug-in script, which determines whether the virtual machine has normal or restricted network access. For details on writing plug-ins, see Writing Plug-In Policy Scripts on page 244.

1. The Custom Quarantine Script panel appears.



   Click **Set** to specify the plug-in script you want to use.

2. The Set Custom Script dialog box appears.



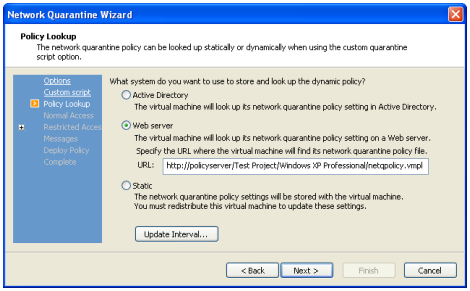
   Enter the path to the script file you want to use or click **Browse** to navigate to the file. The script should be in the `Project Resources` folder under the project folder for the current project.

   Make any necessary changes to the command line shown in the **Command line** field.

   If you wish, you may specify a timeout interval. If the script has not completed by the end of that interval, VMware ACE terminates the script.

   Click **OK**, then click **Next**.

3. The Policy Lookup panel appears.



Select the type of server you want to use to store the network quarantine policy. VMware ACE checks the list on this server to determine what network access is approved for the virtual machine.

- **Active Directory** — Select this option if you plan to store the network quarantine policy on your Active Directory server. The wizard adds this information to your Active Directory server for you.

  Note: In order to use the directory service option, you must choose an Active Directory domain in the project settings editor. If you select **Active Directory** and have not yet chosen an Active Directory domain, the wizard opens a dialog box that gives you the option of setting the domain at this time. Click **Yes** to open the Policies Domain dialog box.

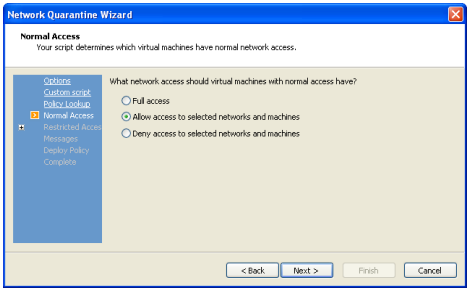
- **Web server** — Select this option if you plan to store the network quarantine list on a Web server. Enter the URL of the file where you plan to store the list. Be sure to include the filename in the URL. The wizard creates this file for you at the end of the process.

- **Static** — Select this option if you want the network quarantine policy settings stored with the virtual machine. If you need to make any changes in the future, you must update the package and distribute the update to your users.

Click **Update Interval** to specify how often VMware ACE should check for changes to the network quarantine policies. You may choose an interval from 5 minutes to 1 day. The default is 5 minutes.

Click **Next** to continue.

4. The Normal Access panel appears.

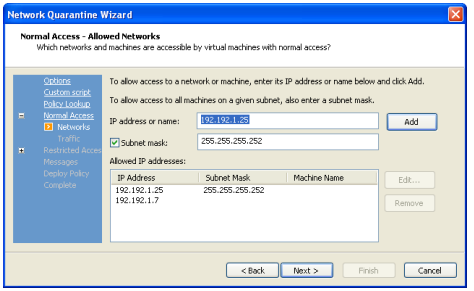


Select the way you want to specify network access.

- **Full access** — No restrictions are imposed.
- **Allow access to selected networks and machines** — Specify a whitelist of networks and machines with which the virtual machine may communicate.
- **Deny access to selected networks and machines** — Specify a blacklist of networks and machines with which the virtual machine is not allowed to communicate.

You may set up either a whitelist or a blacklist but not both.

5. The Networks and Machines panel appears.



Enter the IP address or the fully qualified host name for each network or machine that this virtual machine may access if it qualifies for normal access, then click **Add**.

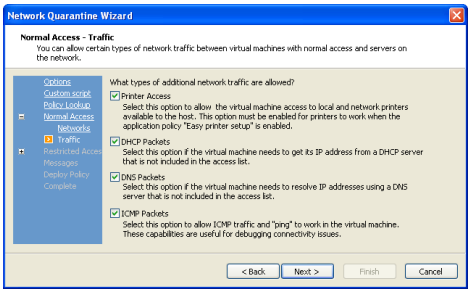
If you enter a host name, the wizard resolves the name and displays both the host name and the IP address in the list.

To specify a single machine, you may also enter its IP address.

To specify a subnet, enter the starting IP address for the subnet, select **Subnet mask** and enter the mask in the corresponding field in dotted quad format.

When the list is complete, click **Next**.

6. If you specified networks and machines that are allowed, the Network Traffic panel appears. If you specified networks and machines that are denied, skip to the next step.

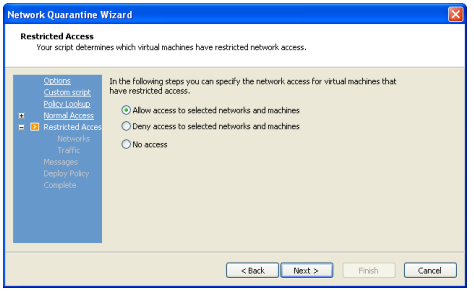


Using this panel, you may set up exceptions to allow certain types of network traffic that would otherwise be blocked by the rules you set on the Networks and Machines panel. This is useful, for example, if virtual machine users are restricted to a particular subnet but the DNS server on your network is not on that subnet. At this time, you are making these settings for the virtual machine if it qualifies for normal access.

- **Printer access** — Select this option to be sure a Windows virtual machine can use local and network printers available on the host. Be sure to select this option if you configure the virtual machine to allow easy printer setup. Easy printer setup uses network sharing to connect the virtual machine to a printer configured on the host computer.
- **DHCP packets** — Select this option if the virtual machine needs to get its IP address from a DHCP server that is not included in the access list.
- **DNS packets** — Select this option if the virtual machine needs to resolve IP addresses using a DNS server that is not included in the access list.
- **ICMP packets** — Select this option if you need support for the ping command — for example, to check network connectivity to and from the virtual machine.

Click **Next**.

7. The Restricted Access panel appears.



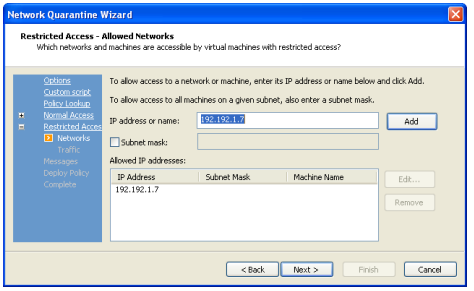
Select the way you want to specify network access.

- **Allow access to selected networks and machines** — Specify a whitelist of networks and machines with which the virtual machine may communicate.
- **Deny access to selected networks and machines** — Specify a blacklist of networks and machines with which the virtual machine is not allowed to communicate.
- **No access** — Block all network access.

You may set up either a whitelist or a blacklist but not both.

Click **Next** to continue.

8. The Networks and Machines panel appears again.



Enter the IP address or the fully qualified host name for each network or machine that this virtual machine may access if it does not qualify for normal access, then click **Add**.

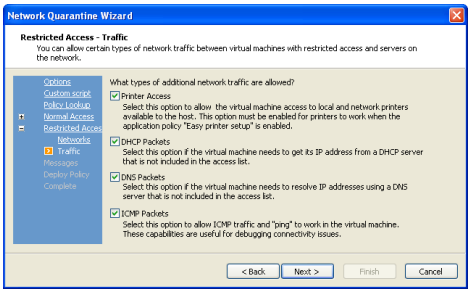
If you enter a host name, the wizard resolves the name and displays both the host name and the IP address in the list.

To specify a single machine, you may also enter its IP address.

To specify a subnet, enter the starting IP address for the subnet, select **Subnet mask** and enter the mask in the corresponding field in dotted quad format.

When the list is complete, click **Next**.

9. If you specified networks and machines that are allowed, the Network Traffic panel appears. If you specified networks and machines that are denied, skip to the next step.

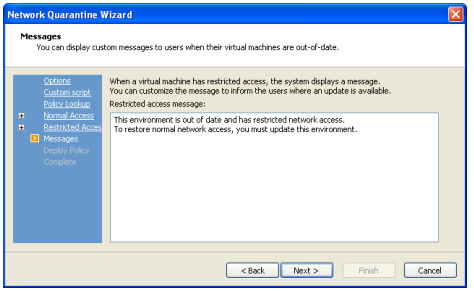


Using this panel, you may set up exceptions to allow certain types of network traffic that would otherwise be blocked by the rules you set on the Networks and Machines panel. This is useful, for example, if virtual machine users are restricted to a particular subnet but the DNS server on your network is not on that subnet. At this time, you are making these settings for the virtual machine if it does not qualify for normal access.

- **Printer access** — Select this option to be sure a Windows virtual machine can use local and network printers available on the host. Be sure to select this option if you configure the virtual machine to allow easy printer setup. Easy printer setup uses network sharing to connect the virtual machine to a printer configured on the host computer.
- **DHCP packets** — Select this option if the virtual machine needs to get its IP address from a DHCP server that is not included in the access list.
- **DNS packets** — Select this option if the virtual machine needs to resolve IP addresses using a DNS server that is not included in the access list.
- **ICMP packets** — Select this option if you need support for the ping command — for example, to check network connectivity to and from the virtual machine.

Click **Next**.

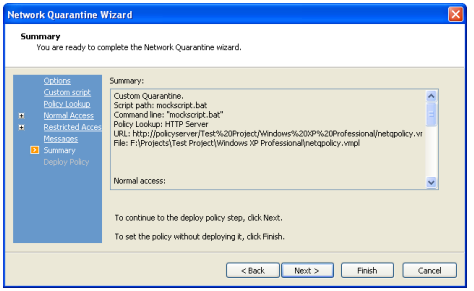
10. The Messages panel appears.



Enter the message you want end users to see when this virtual machine has restricted access.

Click **Next** to continue.

11. The Summary panel appears.

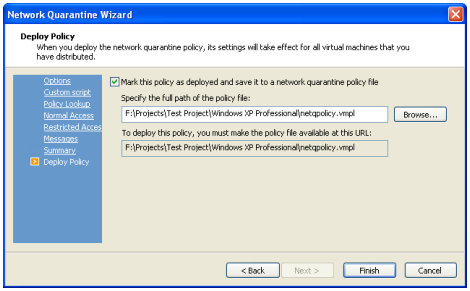


This panel displays a summary of the settings you have made using the wizard. Review the settings to be sure they are correct.

To modify settings, go to the appropriate panel to make the needed change.

To continue to the Deploy Policy panel, click Next. To set the policy without deploying it, click **Finish**.

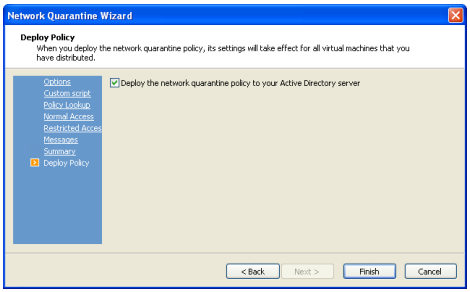
12. If you selected **Web server**, the Deploy Policy panel that appears looks like this.



Select **Mark this policy as deployed and save it to a network quarantine policy file** to capture your policy changes. You may type the path and filename for the policy file or click **Browse** to navigate to the location where you want to save the file. Be sure to copy the updated policy file to the URL shown in this panel. The new policies take effect as soon as you make the file available on the Web server.

Click **Finish** to save the policy file.

If you selected **Active Directory**, the Deploy Policy panel that appears looks like this.



Select **Deploy the network quarantine policy to your Active Directory server**.

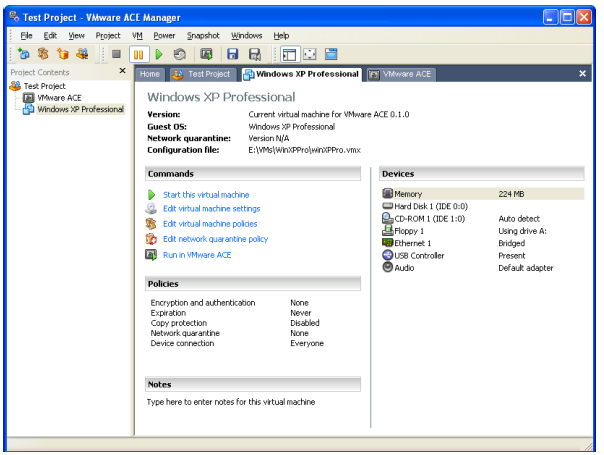
When you click **Finish**, the wizard deploys the new policies, which take effect immediately.

Configuring the Virtual Machines and Installing Software

To finish preparing your project, review the configuration of all virtual machines and be sure that the appropriate operating system and software are installed in each virtual machine.

Reviewing the Configuration of a Virtual Machine

Select a virtual machine in the project list. The display shows the virtual machine overview.



Devices

The Devices list provides an overview of the devices configured for this virtual machine and the basic settings for each device. The list includes the virtual machine's memory and such virtual devices as hard disks, CD-ROM drives, floppy disks, Ethernet adapters, USB controllers and audio devices.

To change the settings for an existing device, double-click the name of the device, then change the settings as needed.

To add a device click **Edit virtual machine settings** in the Commands list, click **Add**, then follow the instructions provided by the wizard.

Note: In this release, you may experience problems if you configure a virtual machine to use hardware such as a floppy disk or a CD-ROM drive but the host computer does not have corresponding hardware. Be sure the computers on which

you plan to run this virtual machine have the physical devices needed to support those virtual devices — for example, CD-ROM drives, floppy disks, Ethernet adapters, USB controllers and audio devices.

Policies

The Policies list provides an overview of the policies set for this virtual machine.

To change the policies for the virtual machine, click **Edit virtual machine policies** in the Commands list, then change the settings as needed.

Notes

To add notes about this virtual machine, click inside the notes field and type. The notes are saved with the virtual machine configuration.

Installing an Operating System and Applications in the Virtual Machine

Before deploying virtual machines to your end users, be sure they have the necessary operating system and software installed.

If you created a new virtual machine and added it to the project, you must install a guest operating system in the virtual machine. The steps in this section describe how to install a Windows XP guest operating system from an installation CD. For notes on installing all supported guest operating systems, see the *Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

If you added an existing virtual machine, it may already have a guest operating system installed. Be sure the guest operating system has the appropriate updates.

If you are deploying a Windows virtual machine to multiple users, you must set up Sysprep in the guest operating system just as you would on a physical computer you intended to clone for a large deployment. Sysprep prepares the operating system for deployment by installing special software that reconfigures the operating system on the next boot.

Installing a Guest Operating System

A new virtual machine is like a physical computer with a blank hard disk. Before you can use it, you need to partition and format the virtual disk, and install an operating system. The operating system's installation program may handle the partitioning and formatting steps for you.

Installing a guest operating system inside your VMware ACE virtual machine is essentially the same as installing it on a physical computer. The basic steps for a typical operating system are:

1. Start VMware ACE.
2. Insert the installation CD-ROM or floppy disk for your guest operating system.

   Note: In some host configurations, the virtual machine is not able to boot from the installation CD-ROM. You can work around that problem by creating an ISO image file from the installation CD-ROM. Use the Virtual Machine Control Panel to connect the virtual machine's CD drive to the ISO image file, then power on the virtual machine.
3. Power on your virtual machine by clicking the **Power On** button.
4. Follow the instructions provided by the operating system vendor.

Installing Windows XP

The next section provides notes on installing a Windows XP guest operating system.

1. Insert the Windows XP CD in the CD-ROM drive.

   Note: If you plan to use a PXE server to install the guest operating system over a network connection, you do not need the operating system installation media. When you power on the virtual machine in the next step, the virtual machine detects the PXE server.
2. Power on the virtual machine to start installing Windows XP.
3. Follow the Windows XP installation steps as you would for a physical computer.
4. Install VMware Tools in the guest operating system.

   Note: Be sure to install VMware Tools in the guest operating system. A number of key features in VMware ACE are provided by the VMware Tools package.

The installers for VMware Tools for Windows, Linux, FreeBSD and NetWare guest operating systems are built into VMware ACE Manager as ISO image files.

VMware Tools for Windows supports Windows 95, Windows 98, Windows Me, Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003 and Longhorn guest operating systems.

Installing VMware Tools in a Windows Guest Operating System

The detailed steps for installing VMware Tools depend on the version of Windows you are running. The steps that follow show how to install VMware Tools in a Windows XP guest. Some steps that are automated in newer versions of Windows must be performed manually in Windows 9x and Windows NT.

Note: If you are running VMware ACE Manager on a Windows host and your virtual machine has only one CD-ROM drive, the CD-ROM drive must be configured as an IDE or SCSI CD-ROM drive. It cannot be configured as a generic SCSI device.

1. Power on the virtual machine.
2. When the guest operating system starts, prepare your virtual machine to install VMware Tools.

   Choose **VM** > **Install VMware Tools**.

The remaining steps take place inside the virtual machine.

Note: You must log on to a Windows NT, Windows 2000, Windows XP, Windows Server 2003 or Longhorn guest operating system as an administrator in order to install VMware Tools. Any user can install VMware Tools in a Windows 95, Windows 98 or Windows Me guest operating system.

3. If you have autorun enabled in your guest operating system (the default setting for Windows operating systems), a dialog box appears after a few seconds. It asks if you want to install VMware Tools. Click **Yes** to launch the InstallShield wizard.

   If autorun is not enabled, the dialog box does not appear automatically. If it doesn't appear, run the VMware Tools installer. Click **Start** > **Run** and enter `D:\setup\setup.exe` where `D:` is your first virtual CD-ROM drive.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The VMware ACE software contains an ISO image that looks like a CD-ROM to your guest operating system and even appears as a CD-ROM in Windows Explorer. This image contains all the files needed to install VMware Tools in your guest operating system. When you finish installing VMware Tools, this image file no longer appears in your CD-ROM drive.

4. Follow the onscreen instructions.

   Note: At some stages in the installation process, you may see Digital Signature Not Found dialog boxes. You can safely ignore the messages and click the button to continue installing these drivers.

5. On Windows Server 2003, Windows Me, Windows 98 SE and Windows 98 guests, the SVGA driver is installed automatically and the guest operating system uses it after it reboots. With Windows 2000 and Windows XP guests, you do not have to reboot to use the new driver.

Installing VMware Tools in a Linux Guest Operating System

1. Power on the virtual machine.
2. After the guest operating system has started, prepare your virtual machine to install VMware Tools.

   Choose **VM** > **Install VMware Tools**.

The remaining steps take place inside the virtual machine.

3. You may install VMware Tools in text mode or from a terminal in an X window session.
4. As root (`su -`), mount the VMware Tools virtual CD-ROM image, change to a working directory (for example, `/tmp`), uncompress the installer, then unmount the CD-ROM image.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The VMware ACE software contains an ISO image that looks like a CD-ROM to your guest operating system. This image contains all the files needed to install VMware Tools in your guest operating system.

   Note: Some Linux distributions use different device names or organize the `/dev` directory differently. If your CD-ROM drive is not `/dev/cdrom`, modify the following commands to reflect the conventions used by your distribution.

   ```
   mount /dev/cdrom /mnt
   cd /tmp
   tar zxf /mnt/vmware-linux-tools.tar.gz
   umount /mnt
   ```

5. Run the VMware Tools installer.

   ```
   cd vmware-tools-distrib
   ./vmware-install.pl
   ```

   Respond to the questions the installer displays on the panel. Be sure to respond yes when the installer offers to run the configuration program.

6. Log off of the root account.

   ```
   exit
   ```

7. Start X and your graphical environment if they are not already running.

   Note: If this is the first time you have installed VMware Tools in this virtual machine, you must restart X to activate graphics and mouse features in the VMware Tools package.

8. In an X terminal, launch the VMware Tools application in the background.

   ```
   vmware-toolbox &
   ```

   Note: You may run VMware Tools as root or as a normal user. To shrink virtual disks, you must run VMware Tools as root (`su -`).

Starting VMware Tools Automatically in a Linux Guest Operating System

You may find it helpful to configure your guest operating system so VMware Tools starts when you start your X server. The steps for doing so vary depending on your Linux distribution and your desktop environment. Check your operating system documentation for the appropriate steps to take.

For example, in a Red Hat Linux 7.1 guest using GNOME, follow these steps.

1. Open the Startup Programs panel in the GNOME Control Center.

   Main Menu (click the foot icon in the lower left corner of the screen) > **Programs** > **Settings** > **Session** > **Startup Programs**

2. Click **Add**.
3. In the **Startup Command** field, enter `vmware-toolbox`.
4. Click **OK**, click **OK** again, then close the GNOME Control Center.

The next time you start X, VMware Tools starts automatically.

Installing VMware Tools in a FreeBSD Guest Operating System

1. Power on the virtual machine.
2. Prepare your virtual machine to install VMware Tools.

   Choose **VM** > **Install VMware Tools**.

The remaining steps take place inside the virtual machine, not on the host computer.

3. You may install VMware Tools in text mode or from a terminal in an X window session.
4. As root (`su -`), mount the VMware Tools virtual CD-ROM image, change to a working directory (for example, `/tmp`), uncompress the installer, then unmount the CD-ROM image.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The VMware ACE software contains an ISO image that looks like a CD-ROM to your guest operating system. This image contains all the files needed to install VMware Tools in your guest operating system.

   ```
   mount /cdrom
   cd /tmp
   tar zxf /cdrom/vmware-freebsd-tools.tar.gz
   umount /cdrom
   ```

5. Run the VMware Tools installer.

```
cd vmware-tools-distrib
./vmware-install.pl
```

6. Log off of the root account.

   ```
   exit
   ```

7. Start X and your graphical environment if they are not already running.

   Note: If this is the first time you have installed VMware Tools in this virtual machine, you must restart X to activate graphics and mouse features in the VMware Tools package.

8. In an X terminal, launch the VMware Tools application in the background.

   ```
   vmware-toolbox &
   ```

   Note: You may run VMware Tools as root or as a normal user. To shrink virtual disks, you must run VMware Tools as root (`su -`).

Note: In a FreeBSD 4.5 guest operating system, sometimes VMware Tools does not start after you install VMware Tools, reboot the guest operating system or start VMware Tools on the command line in the guest. An error message appears:

```
Shared object 'libc.so.3' not found.
```

The required library was not installed. This does not happen with full installations of FreeBSD 4.5, but does occur for minimal installations. To fix the problem of the missing library, take the following steps:

1. Insert and mount the FreeBSD 4.5 installation CD or access the ISO image file.
2. Change directories and run the installation script.

   ```
   cd /cdrom/compat3x
   ./install.sh
   ```

Installing VMware Tools in a NetWare Guest Operating System

1. Power on the virtual machine.
2. Prepare your virtual machine to install VMware Tools.

   Choose VM > Install VMware Tools.

The remaining steps take place inside the virtual machine.

3. Load the CD-ROM driver so the CD-ROM device mounts the ISO image as a volume. Do one of the following.
   - In the system console for a NetWare 6.5 virtual machine, type

     ```
     LOAD CDDVD
     ```

   - In the system console for a NetWare 6.0 or NetWare 5.1 virtual machine, type

```
LOAD CD9660.NSS
```

4. When the driver finishes loading, you can begin installing VMware Tools. In the system console, type

   ```
   vmwtools:\setup.ncf
   ```

   When the installation finishes, the message `VMware Tools for NetWare are now running` appears in the Logger screen (NetWare 6.5 and NetWare 6.0 guests) or the Console screen (NetWare 5.1 guests).

5. Restart the guest operating system. In the system console, type

   ```
   restart server
   ```

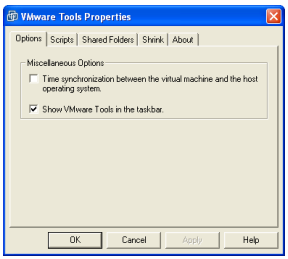
Configuring VMware Tools

This section shows the options available in a Windows XP guest operating system. Similar configuration options are available in VMware Tools for other guest operating systems.

When VMware Tools is running, an icon with the VMware boxes logo appears in the guest operating system's system tray by default. If you prefer to hide this icon, change the setting on the Options tab.

To open the VMware Tools control panel, double-click the VMware Tools icon in the system tray.

If the VMware Tools icon does not appear in the system tray, go to **Start** > **Control Panel**. Locate the VMware Tools icon and double-click it.



The Options tab shows the Miscellaneous Options.

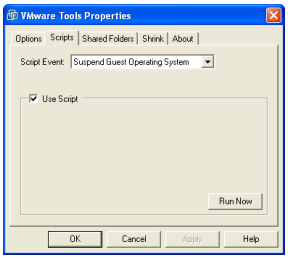
- Time synchronization between the virtual machine and the host operating system

  Note: You can synchronize the time in the guest operating system with the time on the host operating system only when you set the clock in the guest operating system to a time earlier than the time set on the host.

Under some circumstances, the virtual machine may synchronize time with the host even though this item is not selected. If you want to disable time synchronization completely, open the virtual machine's configuration file (`.vmx`) in a text editor and set the following options to `FALSE`.

```
tools.syncTime
tools.synchronize.restore
time.synchronize.resume.disk
time.synchronize.continue
time.synchronize.shrink
```

- Show VMware Tools in the taskbar



The Scripts tab (available only in Windows guests) lets you enable, disable and run scripts that are associated with the Suspend, Resume, Power On and Power Off buttons.

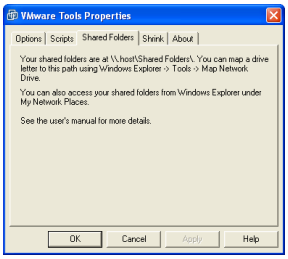
If the virtual machine is configured to use DHCP, the script that is executed when suspending a virtual machine releases the IP address of the virtual machine. The script that is executed when resuming a virtual machine renews the IP address of the virtual machine.

To run one of these scripts at some other time, select the script you want from the drop-down menu, then click **Run Now**.

To disable all scripts, deselect **Use Scripts**.

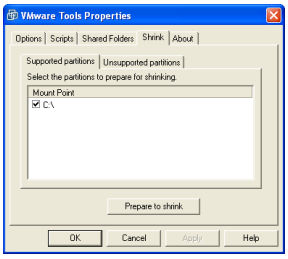
Note: Scripts cannot be run in Windows 95, NetWare or FreeBSD guest operating systems.

Note: Scripts in Windows NT and Windows Me guest operating systems do not release and renew the IP address.



The Shared Folders tab provides information on where to find your shared folders.

For more information on shared folders, see Using Shared Folders in VMware ACE Manager on page 40.



The Shrink tab gives you access to the controls you need if you wish to reclaim unused space in a virtual disk.

In some configurations, it is not possible to shrink virtual disks. If your virtual machine uses such a configuration, the Shrink tab displays information explaining why you cannot shrink your virtual disks.

Using the System Console to Configure VMware Tools in a NetWare Guest Operating System

You can configure certain virtual machine options such as time synchronization, CPU idling and device configuration with VMware Tools in a NetWare virtual machine using the system console. The VMware Tools command line program is called `vmwtool`. To see the options associated with this command, at the system console, type

```
vmwtool help
```

Each command in the following table must be entered into the system console after the VMware Tools command `vmwtool`. Use the following format:
`vmwtool <command>`

`vmwtool` **Command**	**Definition**
`help`	Displays a summary of VMware Tools commands and options in a NetWare guest.
`partitonlist`	Displays a list of all disk partitions in the virtual disk and whether or not a partition can be shrunk.
`shrink <partition>`	Shrinks the listed partitions. If no partitions are specified, then all partitions in the virtual disk are shrunk. The status of the shrink process appears at the bottom of the system console.
`devicelist`	Lists each removable device in the virtual machine, its device ID and whether the device is enabled or disabled. Removable devices include the virtual network adapter, CD-ROM and floppy drives.
`disabledevice <device name>`	Disables the specified device or devices in the virtual machine. If no device is specified, then all removable devices in the virtual machine are disabled.
`enabledevice <device name>`	Enables the specified device or devices in the virtual machine. If no device is specified, then all removable devices in the virtual machine are enabled.
`synctime [on|off]`	Lets you turn on or off synchronization of time in the guest operating system with time on the host operating system. By default, time synchronization is turned off. Use this command without any options to view the current time synchronization status. You can synchronize the time in the guest operating system with time on the host operating system only when the time in the guest operating system is earlier than the time set in the host.
`idle [on|off]`	Lets you turn on or off the CPU idler. By default, the idler is turned on. The CPU idler program is included in VMware Tools for NetWare guests. The idler program is needed because NetWare servers do not idle the CPU when the operating system is idle. As a result, a virtual machine takes CPU time from the host regardless of whether the NetWare server software is idle or busy.

Installing Application Software

If you plan to distribute application software in the virtual machine, be sure the correct software is installed.

You may install application software in the virtual machine just as you would on a physical computer — using a CD or an installer file on a network server, for example.

If you are installing from a file on the network, you may need to change the networking configuration of the virtual machine or network settings of the guest operating system in order to navigate to the installer file. If you need to make such changes, be sure to reconfigure the settings as needed after you finish installing the application software.

Customizing the VMware ACE Interface

You may customize several aspects of the VMware ACE user interface, including the text that appears in the title bar and the way removable devices are represented in the interface.

You save these customizations in a text file and identify that text file, called the skin file, by adding a line to the `preferences.ini` file in the project folder.

Creating and Specifying the Skin File

Each line in the skin file has the following form:

```
parameter = "value"
```

To comment out a line in the skin file, begin the line with the # sign.

The parameters, acceptable values and defaults are listed in tables in this section.

Save the skin file with any filename you wish. Save the skin file in the `Project Resources` folder under the project folder for the project to which it applies.

1. Use a text editor to open the `preferences.ini` file in the project folder and add the following line:

   ```
   vmplayer.skin = "<filename>"
   ```

   If the skin file is not in the project folder, specify the full path to the file.

2. Save `preferences.ini`.

Customizing the VMware ACE Icons

VMware ACE has separate large and small application icons. The large icon is used in the application switching interface (visible when you press Alt-Tab). The size of the large icon is usually 32x32 pixels, but VMware ACE uses whatever size is specified in the system preference for icon size. The small (16x16) icon is used in the VMware ACE title bar and on the Windows taskbar button for VMware ACE.

The icons used for these purposes must be in `.ico` format and are specified by the following options in the skin file:

```
player.iconSmall = "<filename>"
player.iconLarge = "<filename>"
```

One `.ico` file can contain multiple icons of different sizes. You can specify the same `.ico` file for `player.iconSmall` and `player.iconLarge`. VMware ACE extracts the icon of the appropriate size for each use.

Customizing the Title Bar Text

You may specify what text appears in the VMware ACE title bar. You may also specify the font and font size used to display the text.

The text displayed in the title bar consists of three sections — a prefix, the virtual machine name and a suffix. The parameters listed here allow you to set any prefix and suffix, or to omit the prefix, the suffix or both. They also allow you to include or omit the virtual machine name.

If you leave the defaults for all values, the title bar displays only the virtual machine name at 32 points in the font MS Shell Dlg.

Parameter	Type	Default	Controls
`player.title.prefix`	string	""	Title bar prefix
`player.title.useVMName`	boolean (TRUE or FALSE)	TRUE	Is virtual machine name displayed?
`player.title.suffix`	string	""	Title bar suffix
`player.title.font.face`	string	"MS Shell Dlg"	Name of font (font must be on end user's computer)
`player.title.font.size`	integer	32	Point size for the text

Customizing the Removable Device Display

Removable devices are shown in the VMware ACE interface either by buttons on a toolbar or by menu items on a Connect menu. You can specify the type of display. You can also specify text, icon or a combination of the two and specify custom icons.

If you use custom icons, copy the icon files to the `Project Resources` folder under the project folder for the project in which they are used.

Settings you make in the skin file override any settings the end user may make in the VMware ACE preferences dialog box.

Use the following parameter to control whether devices are shown as toolbar items.

Parameter		
Type	**Default**	**Controls**
`player.deviceBar.toplevel`		
boolean	FALSE	Use TRUE for a toolbar, FALSE for a menu

You may customize the display for each removable device configured in the virtual machine. The following device names are used for the removable devices you can control with these parameters:

- floppy0, floppy1
- serial0, serial1, serial2, serial3
- parallel0, parallel1, parallel2
- ide0:0, ide0:1, ide1:0, ide1:1 (IDE CD-ROM or hard drives)
- scsi0:0-scsi0:7 (SCSI CD-ROM or hard drives)

Substitute the appropriate device name for `<deviceName>` in the parameters in the following table:

Parameter		
Type	**Default**	**Controls**
`player.deviceBar.<deviceName>.buttonStyle`		
string (text, icon, texticon)		Appearance of toolbar button or menu item
`player.deviceBar.<deviceName>.buttonText`		
string	User-friendly device name	Text that appears on the toolbar button or menu item when device is connected
`player.deviceBar.<deviceName>.buttonTextDisconnected`		
string (optional)	Normal button text	Text that appears on the toolbar button or menu item when device is disconnected
`player.deviceBar.<deviceName>.tooltip`		
string	""	Text that appears in the tooltip when device is connected
`player.deviceBar.<deviceName>.tooltipDisconnected`		
string (optional)	Normal tooltip	Text that appears in the tooltip when device is disconnected
`player.deviceBar.<deviceName>.icon`		

Parameter		
Type	**Default**	**Controls**
filename	Icon representing this type of device	Custom icon file when device is connected; copy icon file to the `Project Resources` folder under the project folder
`player.deviceBar.<deviceName>iconDisconnected`		
filename (optional)	Normal icon	Custom icon file when device is disconnected
`player.deviceBar.<deviceName>.shortcutKey`		
keySpec		Shortcut key combination to toggle device between connected and disconnected

For details on the values for keySpec, see the section below.

Shortcut Key Values

The shortcut key entries described in this section require you to enter a virtual key code as part of the value for an option. Virtual key codes are entered in hexadecimal format — as a hexadecimal number preceded by 0x. For example, to use the virtual key code of 5A as a value, type `0x5A`.

Microsoft provides a reference list of virtual key codes on the MSDN Web site. At the time this manual was written, the reference list was at *msdn.microsoft.com/library/en-us/winui/WinUI/WindowsUserInterface/UserInput/VirtualKeyCodes.asp*.

The hot key entries also include modifier keys. The modifier keys are Ctrl, Alt and Shift, or a combination of those keys.

Modifier key	Value
No modifier	0x0
Alt	0x1
Ctrl	0x2
Shift	0x4
Ctrl-Alt	0x3
Alt-Shift	0x5
Ctrl-Shift	0x6
Ctrl-Alt-Shift	0x7

When listing a key plus a modifier, type the virtual key code for the key followed by a comma, then type the value for the modifier key or keys. For example, the value entry for Ctrl-Shift-F1 is `0x70,0x6`.

Note: Keep the following limitations in mind when defining shortcut keys:

- Do not use the Pause key with the Ctrl key. You may use the Pause key with other modifier keys.
- If you use F12, you must use one or more modifier keys. You cannot use F12 alone.
- You cannot use combinations that include only the Shift, Ctrl and Alt keys. These keys may be used only as modifiers in combination with some other key.

Sample Skin File

```
player.title.prefix = "Our Company <<"
player.title.suffix = ">> Environment"
# player.title.useVMName = FALSE

# player.deviceBar.toplevel = TRUE
player.deviceBar.floppy0.buttonStyle = "icon"
player.deviceBar.floppy0.buttonText = "First Floppy Drive"
player.deviceBar.floppy0.shortcutKey = "0x30,0x7"
player.deviceBar.floppy0.icon = "custom-floppy.ico"
player.deviceBar.floppy0.tooltip = "Click to disconnect"
player.deviceBar.floppy0.tooltipDisconnected = "Click to connect"
# player.deviceBar.ide1:0.buttonStyle = "icon"
```

Running the Completed Virtual Machine

Before you create a package for deployment, you may wish to run the virtual machines in your project.

There are two ways to run a virtual machine from VMware ACE Manager. You can power on the virtual machine directly in the VMware ACE Manager interface. Or you can click **Run in VMware ACE** to view a virtual machine as your end users will see it, running in the VMware ACE interface.

When you run the virtual machine in the VMware ACE interface from within VMware ACE Manager, authentication policies are not applied.

Click **Run in VMware ACE** on the VMware ACE Manager display for the virtual machine. This launches the VMware ACE interface and runs the virtual machine in it.

For a more thorough test of the virtual machine as your end users will see it, you should create a package and install it on another computer.

Note: You can run any virtual machine directly in VMware ACE Manager to be sure the guest operating system and applications perform as expected. However, a virtual machine running in VMware ACE Manager does not respect any policies that restrict its functionality.

Checking the Configuration before Creating a Package

When you run a virtual machine in the VMware ACE interface, the virtual machine is affected by any changes you make while you are running it. In addition, when you quit the VMware ACE interface, the virtual machine is suspended, not shut down and powered off.

If a virtual machine is suspended on one host computer, it cannot be resumed reliably on a host computer with different hardware.

Use the VMware ACE Manager to check the virtual machine's configuration and to be sure that the virtual machine is powered off, not just suspended, before you create a package including the virtual machine.

CHAPTER 6

Creating Packages to Deploy to Users

The following sections guide you through the process of creating a package to deploy to your end users:

- Creating a Package on page 132
- Contents of the Package on page 136

Creating a Package

After you have created a project and applied policies to the virtual machines in the project, you create packages to deploy those virtual machines to end users. A package includes an installer and the additional files needed to install a virtual machine and the VMware ACE application that runs the virtual machine.

You may deploy a package over a network or on DVD or CD. If you deploy the package on discs, the first disc of the set includes the autorun files needed to start the installer automatically when the user inserts the disc in the host computer's drive.

A wizard guides you through the process of creating a package.

To create a package, take the following steps:

1. Start VMware ACE Manager and open the project you want to use as the basis for the package.
2. To assure that the package is as compact as possible, defragment and shrink the virtual disks before you create the package. Take the following actions, in the order listed:
   a. Run a disk defragmentation utility inside the virtual machine to defragment each virtual disk.
   b. Use the VMware Tools control panel to shrink each virtual disk. In a Windows guest, double-click the VMware Tools icon in the system tray. In a Linux or FreeBSD guest, run `vmware-toolbox`. Click the **Shrink** tab. Select the virtual disks you want to shrink, then click **Prepare to Shrink**.

      Shrinking disks may take considerable time.
3. Be sure that the virtual machine in the package is configured as you want it, then be sure it is shut down and powered off.

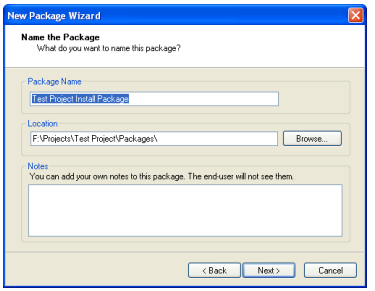
   Note, for example, that if you previewed the virtual machine in the VMware ACE interface, the virtual machine is affected by any changes you made while you were previewing it. In addition, when you quit the VMware ACE interface, the virtual machine is suspended, not shut down and powered off.

   If a virtual machine is suspended on one host computer, it cannot be resumed reliably on a host computer with different hardware. As a result, you must be sure that a virtual machine is powered off, not just suspended, when you create a package including that virtual machine.

   Also be sure that there is no snapshot for the virtual machine. If a snapshot exists, remove it (**Snapshot** > **Remove Snapshot**) before creating the package.

Note: Be sure the version of VMware Tools provided with VMware ACE is installed in the guest operating system. A number of key features in VMware ACE are provided by the VMware Tools package.

4. Under Commands, click **Create package for distribution to end users**. This starts the New Package Wizard.
5. Click **Next** to enter the wizard. The Name the Package panel appears.



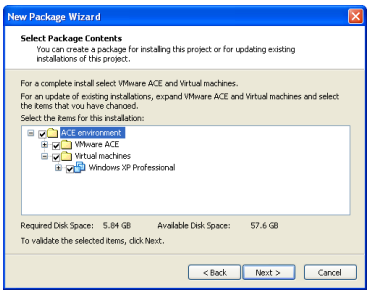
Enter a name for the package in the **Package name** field.

The **Location** field displays the path to the default location for storing the package's files. To change the location, type a new path into the field or click **Browse** and navigate to the new location.

Use the **Notes** field to enter any background information you want to store with the package. Your end users do not see this information.

Click **Next**.

6. The Select Package Contents panel appears. It shows the application and all virtual machines available in the project.

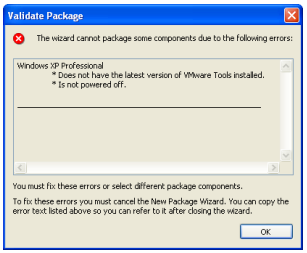


You can include VMware ACE and the virtual machines by selecting **ACE environment**.

To include only some of the items, click the + signs to expand the tree, then select only those items you want to include.

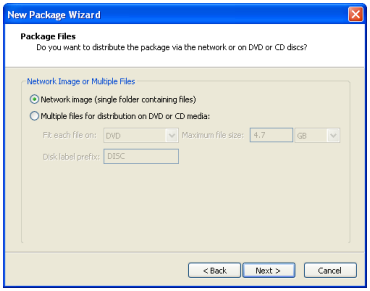
Click **Next**.

7. The wizard checks the items you want to include. If it finds any problems, the Validate Package panel appears.



Click **OK**, cancel the wizard, correct the problems, then start the wizard again.

8. The Package Files panel appears.



For network distribution, select **Network image**.

If you plan to distribute the package on CD or DVD, select **Multiple folders for creating distribution DVDs or CDs**.

When you select the multiple files option, you must choose the type of media you plan to use. If you choose **DVD** or **CD**, the default media size for a standard disc is shown. If you choose **Custom**, you may set the maximum file size for the media you plan to use.

When the package wizard creates the package, it divides the package into sets of files small enough to fit on the media you choose in this step.

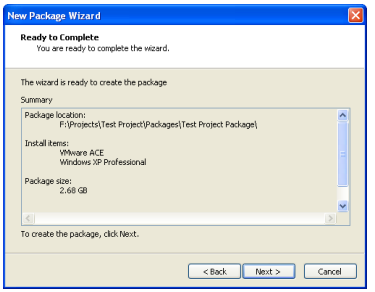
The default disc label prefix is shown. You may change it if you wish. When files are created for each disc, they are saved into folders named with this prefix plus a number, beginning with 1.

Note: When you use multiple discs, be sure that the disc label you enter in your disc burning software for each disc is the same as the name of the folder the wizard creates to hold that disc's contents (for example, DISC1, DISC2).

Note: When the package wizard creates a package, it needs a substantial amount of working space for temporary files. The total is about twice the combined sizes of all the components of the package. The wizard displays information about the amount of space needed and the locations where the space is needed. If you do not have enough free space, the wizard displays an error message. You may move or delete files on the target drives to make room for the wizard's working files.

Click **Next**.

9. The Ready to Complete panel appears.



Review the summary information. If you need to make changes, click **Back**. If the information is correct, click **Next**.

A progress bar appears while the wizard is creating the package files. It may take quite some time to complete this step, especially for packages that include large virtual machines or multiple virtual machines.

The wizard notifies you when the package is complete and tells you how many files are included in the package.

10. If you created a single file for network distribution, the file is now ready to copy to the appropriate location on a network.

    If you created one or more files for distribution on CD or DVD, the files are now ready to burn to disc. Use disc-burning software of your choice to create the discs.

    Note: Be sure that the disc label you enter in your disc-burning software for each disc is the same as the name of the folder the wizard creates to hold that disc's contents.

Contents of the Package

The following files and folders are in a package:

- `autorun.inf` — This file, included in packages for distribution on removable media, automatically starts the package installation process when the host operating system scans the first CD or DVD in the installation set.
- `setup.exe` — Use this file to start the package installation process if the installer is not launched automatically by an `autorun.inf` file.
- `instmsiw.exe` — This is the redistributable installer for the MSI 2.0 runtime.
- `<ProjectName>.msi` — This is the installer for the package.
- `VMware ACE.msi` — This is the installer for the VMware ACE application. It is installed automatically by `<ProjectName>.msi`.
- The package contains a folder for the virtual machine and a folder named Package that contains additional files needed for the package.

CHAPTER 7

Deploying and Maintaining Packages

The following section describes the key tasks involved in deploying and maintaining VMware ACE packages:

- Deploying Packages on page 138
- Installing a Package Silently on page 139
- Updating Virtual Machines on page 141
  - Distributing Software Updates on page 141
  - Creating Update Packages on page 141
  - Updating Network Quarantine Versions on page 142
  - Using nq-set to Update Network Quarantine Versions on page 146
- Deploying Update Packages on page 149
- Responding to Hot Fix Requests on page 150
- Using Administrator Access on the End User's Computer on page 152

Deploying Packages

The first time you deploy a new package, the process is quite straightforward.

If you use CDs or DVDs to deploy the package, be sure the discs are clearly labeled so your users can insert them in the proper order. The `setup.exe` file is on the first disc in the set. For installation instructions, see Installing a VMware ACE Package on page 154.

If you deploy the package over a network, be sure your end users know where to find the installer. For installation instructions, see Installing a VMware ACE Package on page 154.

Note: End users may install packages from only one project on a host computer at any one time. A user who wants to install a package created from a different project must first uninstall the existing package, then install the new one.

You may want to give your end users copies of Running VMware ACE on page 156, which covers the most commonly used features of VMware ACE.

Installing a Package Silently

If you are installing a VMware ACE package on a number of Windows host computers, you may want to use the silent installation features of the Microsoft Windows Installer.

Before installing a VMware ACE package silently, you must ensure that the host computers have version 2.0 or higher of the MSI runtime engine. This version of the installer is available in versions of Windows beginning with Windows XP. The installer for the runtime is also included in the VMware ACE package as `instmsiw.exe`.

To install the runtime silently from the VMware ACE package, issue the following command:

```
instmsiw.exe /Q
```

This section outlines what you need to do to install a VMware ACE package silently. For additional details on using the Microsoft Windows Installer, see the Microsoft Web site.

To perform a silent installation using default settings, issue the following command:

```
msiexec -i package.msi /qn
```

This command installs the package and application (if included) into the default locations and creates a shortcut for each virtual machine on the desktop. The default location for the VMware ACE application is `<ProgramFiles>\VMware\VMware ACE`. The default location for the virtual machine files is `<CommonAppData>\VMware\VMware ACE\<project_name>`.

You can customize the basic package installation command to specify one or more of the following:

- Installation directory for the virtual machine
- Installation directory for the VMware ACE application
- Installation without a desktop icon

The following example command illustrates the options and their usage:

```
msiexec -i package.msi DESKTOP_SHORTCUTS=0
INSTALLDIR="G:\packages"
APP_PROPERTIES="INSTALLDIR=""D:\My Apps\VMware ACE""" /qn
```

Enter the command on one line.

Option	Description
`DESKTOP_SHORTCUTS`	When set to 0, skips installation of virtual machine shortcuts on the desktop. The default is 1.

Option	Description
INSTALLDIR	(Sets the root installation directory for the VMware ACE application
APP_PROPERTIES	Passes information to the application installer; useful for setting the application directory for the VMware ACE application

You can also install an upgrade silently. An upgrade is always installed in the same directory or directories as the previous package.

Updating Virtual Machines

From time to time, you may need to update your end users' virtual machines. In general, there are two ways of providing updates.

- You may need to update the guest operating system or provide an update to a program running in the guest operating system.
- You may need to update either the virtual machine itself or policies applied to the virtual machine or add a new virtual machine to the package.

Distributing Software Updates

If you simply need to update the operating system or other software running inside the virtual machine, in most cases you should use the same mechanisms you use to distribute software updates to physical computers.

The advantage of distributing updates in this way is that end users' data stored in their virtual machines is not affected by the update.

If you are using virtual machine versions to ensure that your end users are running up-to-date virtual machines, see Using nq-set to Update Network Quarantine Versions on page 146 for information on how to update the version number when the user updates software in the virtual machine.

If you plan to distribute additional copies of the virtual machine, you should also use `nq-set` to update the version number in your local copy of the virtual machine and create an updated package for future distribution.

Creating Update Packages

If you need to provide a completely new virtual machine to your end users — either as a replacement to an existing virtual machine or in addition to any existing virtual machines — or if you need to change the policies applied to the virtual machine, you can create an update package for your users to install. You create the update package using the same project you did to create the original package.

Note: If your users replace an existing virtual machine by installing the update package, everything in the virtual machine is replaced. This means any user data and settings stored in the original virtual machine are lost.

In general, when you create an update package, you follow the same steps you do to create a new package.

1. Using VMware ACE Manager, make any needed changes to the virtual machines. For example, you may want to update software installed in the virtual machines

or change the policies applied to the virtual machines. For details, see Creating Projects on page 43.

You can update most polices by distributing a package that contains the new policies. However, you should note the following exceptions:

- Reimage virtual machine — You may change this setting at any time, but the change affects only virtual machines that are installed or reinstalled after you make the change. If you distribute a package that contains only policies, changes to this policy have no effect on virtual machines that are already installed. The end user sees no error message, but the updated policy is not applied.
- Encryption and authentication — You may change these settings at any time, but the change can be applied only if you include the virtual machine in the package. You should not distribute a policy-only package that includes changes to encryption and authentication policies. Package installation will fail for the affected virtual machine.
- Recovery key (**Project** > **Settings**) — Recovery key changes are not supported in upgrades to existing projects.

2. If you are using virtual machine versions for network quarantine, be sure to set the correct version number when you apply network quarantine policies to the virtual machine. For details, see Updating Network Quarantine Versions on page 142.
3. Create the package as described in Creating Packages to Deploy to Users on page 131.

Note: All packages installed on an end user's computer must come from the same VMware ACE Manager project.

Updating Network Quarantine Versions

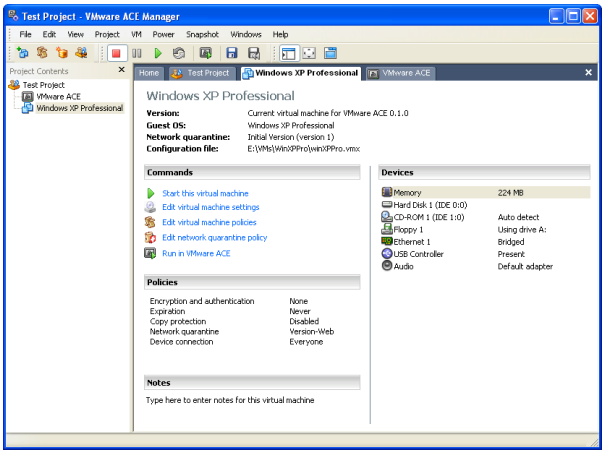
If you are using network quarantine versions to control virtual machine access to your network, be sure to update the version numbers when you make changes to the virtual machine.

Changing the version is a two-part process.

- Use the policy editor to update the version and store the new settings on the Web server or Active Directory server where you store policy settings.
- Run the `nq-set` command in your copy of the virtual machine so the correct version number is included when you create new packages. For details, see Using nq-set to Update Network Quarantine Versions on page 146.

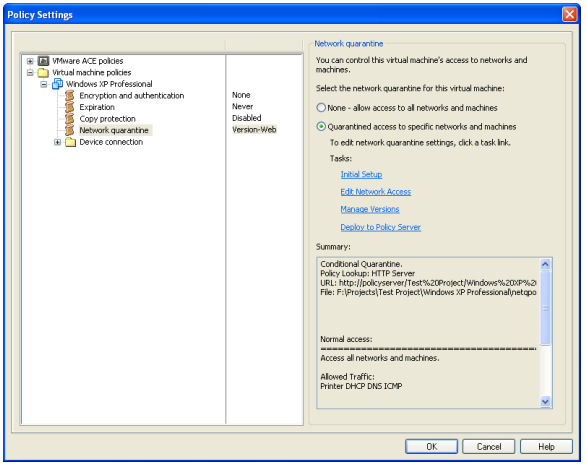
Take the following steps to update the network quarantine version:

1. Start VMware ACE Manager, open the project and click the name of the virtual machine in the project contents list to show the virtual machine summary.



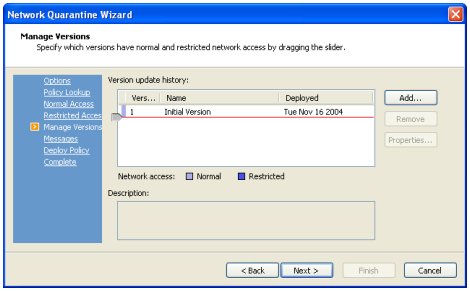
In the Commands section, click **Edit network quarantine policy**.

2. The policy editor opens.



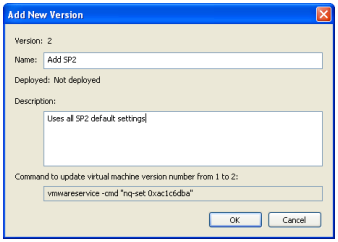
Click the **Manage Versions** link.

3. The Manage Versions panel appears.



To add a new version to the list, click **Add**.

4. The Add New Version dialog box appears.

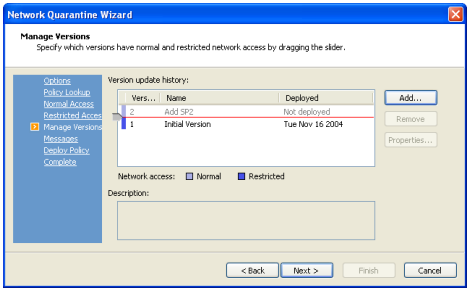


You can change the name for the new version of the virtual machine and add a description if you wish.

The dialog box displays the `nq-set` command needed to update the version number for the virtual machine. You may copy the command from the dialog box and paste it into a text file for later use. You must run this command in your local copy of the virtual machine. And if you are distributing your update using a patch management system or by sending end users an updater that they must run, this command must also be part of the update script run in the end users' guest operating systems. For details on the `nq-set` command, see Using nq-set to Update Network Quarantine Versions on page 146.

Click **OK** to continue.

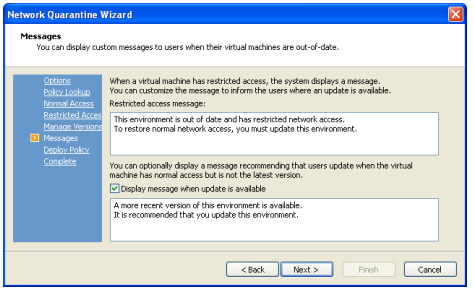
5. The Manage Version panel now shows the new version in the list.



Click and drag the slider at the left of the versions list to specify which versions have normal access and which versions have restricted access. Versions above the red line have normal access, as defined in your network quarantine policies. Versions below the red line have restricted access.

Click **Next** to continue.

6. The Messages panel appears.



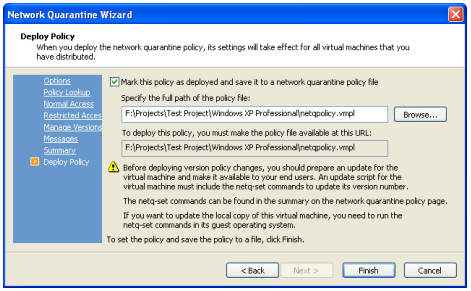
You may enter a custom message that end users see when the virtual machine has restricted access.

If you select **Display message when update is available**, enter the message you want end users to see when the the virtual machine has normal access but a more recent version is available.

Click **Next** to continue.

7. The Ready to Complete panel appears. If the information in the summary is correct, click **Next** to continue. Otherwise, use the navigation links on the left to go to the panels where you want to make changes.

8. The Deploy Policy panel appears.



The options available on the panel depend on the type of network quarantine you are using and whether you are storing your policies on an Active Directory server or on a Web server. Make the appropriate selections, then click **Finish**.

You have completed the process for updating the network quarantine version stored on your Web server or Active Directory server.

Using nq-set to Update Network Quarantine Versions

When you perform software updates inside the virtual machine, use the `nq-set` command to update the network quarantine version for the virtual machine. The version number is used to determine which network quarantine policies to apply to the virtual machine if you are using either version-based network quarantine or custom network quarantine.

The `nq-set` command must be run from within the guest operating system. It is available in the guest operating system after you install the version of VMware Tools provided with VMware ACE Manager.

Note: In this release, you must run the `nq-set` command in the guest operating system while the virtual machine is running in preview mode or while it is running in VMware ACE on the end user's computer. It does not take effect if you simply run the virtual machine by powering it on within VMware ACE Manager.

Windows guest: The command is

```
C:\Program Files\vmware\vmware tools\vmwareservice -cmd
"nq-set [-n] [new descriptor]"
```

Enter the entire command on a single line.

Linux guest: The command is

```
/usr/sbin/vmware-guestd --cmd "nq-set [-n] [new
descriptor]"
```

Enter the entire command on a single line.

In the commands above, `-n` is an optional flag that instructs the host to verify the validity of the new descriptor but not save it.

Return Values
The exit value of the command is 0 if the descriptor is valid, or 1 if it is invalid.

Sample Usage
If you want to check whether descriptor 0x7B4C2902 is valid, use the optional `-n` flag, as shown in the following command:

```
/usr/sbin/vmware-guestd --cmd "nq-set -n 0x7B4C2902"
```

An exit value of 0 means that the descriptor is valid

To set the descriptor to the value 0xFA542D3F, use the following command:

```
/usr/sbin/vmware-guestd --cmd "nq-set 0xFA542D3F"
```

An exit value of 0 means that the descriptor is valid and has been saved.

Custom network quarantine applications can save arbitrary strings by using the `nq-set` command. For example, assume that you want to save the following string:

```
"os=winxp-sp2,ie=6.0,virusdefs=4.0,office=2003-sp1"
```

You may do so using the following command:

```
/usr/sbin/vmware-guestd --cmd "nq-set os=winxp-
sp2,ie=6.0,virusdefs=4.0,office=2003-sp1"
```

Enter the entire command on a single line.

An exit value of 0 means that the descriptor is valid and has been saved.

Using nq-set with Version-Based Network Quarantine
Each version update defined in the Network Quarantine Wizard has a network quarantine descriptor associated with it. The Network Quarantine Wizard also displays the command you need to run in the guest operating system to update the descriptor. To view that command, go to the Manage Versions panel in the Network Quarantine Wizard, choose the version you want to check, then click **Properties**. The command is shown in the field at the bottom of the screen.

You must update the network quarantine descriptor after you apply an update to the guest. Updates must be applied in the order that they were defined.

Note: Your patching mechanism should check whether the `nq-set` command will succeed before it applies any updates to prevent the user from applying patches out of order and causing the guest patch level to be out of sync with the network

quarantine identifier. You can verify whether a `nq-set` command would succeed by passing the `-n` flag to the command.

Using nq-set with Custom Network Quarantine

The network quarantine descriptor can store an arbitrary string that describes the patch level of the guest operating system and other software. Your custom plug-in script should verify that arbitrary string, then decide whether to grant the virtual machine normal network access or restricted network access.

For details on writing network quarantine plug-ins, see Network Quarantine Plug-Ins on page 248.

Deploying Update Packages

You deploy update packages the same way you deploy original packages.

If you use CDs or DVDs to deploy the package, be sure the discs are clearly labeled so your users can insert them in the proper order. The `setup.exe` file is on the first disc in the set. For installation instructions, see Installing a VMware ACE Package on page 154.

If you deploy the package over a network, be sure your end users know where to find the installer. For installation instructions, see Installing a VMware ACE Package on page 154.

Responding to Hot Fix Requests

If you have enabled the hot fix feature, end users can easily request help to resolve the following problems:

- Lost or forgotten password
- Expired VMware ACE environment
- Copy protected VMware ACE environment run from a new location

The end user runs the Hot Fix Request Wizard, which generates a hot fix request file. The end user may submit this file to you as an email attachment or in some other way.

To respond to the hot fix request, take the following steps:

1. Save the file to a location you can reach easily from the computer where you are running VMware ACE Manager.
2. From the VMware ACE Manager menu, choose **File** > **Open Hot Fix Request**.

   VMware ACE Manager opens the project that produced the end user's package and opens a hot fix tab within the project. If VMware ACE Manager cannot find the project, it displays the name of the project and allows you to navigate to the project (`.vmprj`) file.
3. The hot fix tab displays the end user's name and email address, the problem that led to the hot fix request and any additional note the end user entered.

   Click **Approve this hot fix request** to open a dialog box where you can make the appropriate settings to approve the request. Click **Deny this hot fix request** to deny the request.
4. Enter the appropriate information in the dialog box.
   - Lost or forgotten password — Browse to the location of the private recovery key used for the project. Enter the recovery key password. Enter and confirm a temporary password for the user. You must communicate this temporary password to the user separately.
   - Expired VMware ACE environment — Set the new expiration information for the virtual machine. You may extend use by a specified number of days or set a new expiration date.
   - Copy-protected VMware ACE environment run from a new location — The dialog box displays the path to the location from which the end user wants to run the virtual machine.

- Denied request — The dialog box provides a field in which you can enter a message to the end user.

5. Select the method for sending the response. Then click **OK**.

   If you selected **Automatically email to user**, the hot fix is sent automatically when you click **OK**. If you saved a hot fix file, you must locate that file and send it to the end user.

6. If you saved a file to send manually, send the hot fix (`.vmhf`) file to the end user.
7. The display on the hot fix tab shows the status of the hot fix request — approved or denied — and the date on which you took action.

The end user applies the hot fix by double-clicking the hot fix file.

Using Administrator Access on the End User's Computer

For some troubleshooting tasks, you may find it useful to work at the end user's computer with the ability to modify the configuration of the virtual machine. This might be helpful, for example, if an end user has an unusually configured host computer and you need to make changes in the way the virtual machine's devices are mapped to the host hardware.

The administrator access policy allows you to run the virtual machine in an enhanced interface that looks similar to VMware ACE Manager and gives you access to the virtual machine's configuration settings.

If administrator access is enabled, you can launch the troubleshooting application with the following command:

```
vmware -k "<path>\<vmname>.vmx"
```

Include the full path to the virtual machine's configuration file.

Enter the administrator password in the password dialog box. You may then make any needed changes in the virtual machine settings editor (**VM** > **Settings**).

For information on enabling the administrator access policy, see Administrator Access Policy on page 75.

CHAPTER 8

Installing and Running VMware ACE

The following sections describe how to install packages and use VMware ACE:

- Installing a VMware ACE Package on page 154
- Running VMware ACE on page 156
  - Starting VMware ACE on page 156
  - Quitting VMware ACE on page 157
  - Enlarging VMware ACE to Fill the Screen on page 159
  - Understanding VMware ACE Status Indicators on page 159
  - Controlling Devices Attached to VMware ACE on page 160
  - Setting VMware ACE Preferences on page 161
  - Printing from VMware ACE on page 162
  - Uninstalling VMware ACE on page 162
  - Troubleshooting Problems on page 163

Installing a VMware ACE Package

You may install a VMware ACE package from a location on the network or from one or more CDs or DVDs. In either case, take the following steps:

1. Log on to your Microsoft Windows host as the Administrator user or as a user who is a member of the Windows Administrators group.

   Caution: Do not install VMware ACE on a Windows NT Server 4.0 system that is configured as a primary or backup domain controller.

   Note: On a Windows XP or Windows Server 2003 host computer, you must be logged in as a local administrator (that is, not logged in to the domain) in order to install VMware ACE.

   Note: Although you must be logged in as an administrator to install VMware ACE, a user with normal user privileges can run the program after it is installed.

2. If installing from CDs or DVDs, insert the first disc into the computer's drive. If installing from the network, navigate to the location of the installer.
3. Find the `setup.exe` file and double-click to start the installer.
4. Follow the instructions in the installation wizard.

   The installer installs the VMware ACE application in `<ProgramFiles>\VMware\VMware ACE`.

   The installer asks where you want to place the virtual machine files. The default location is `<CommonAppData>\VMware\VMware ACE\<project_name>`. If you want to place the files in a different location, you may enter the path to the new location or click **Browse** and navigate to the new location. Be sure the location you specify has enough space to hold the virtual machine files. If it does not, the installer prompts you to specify a different location.

5. If the installer detects that the CD-ROM autorun feature is enabled, you see a message that gives you the option to disable this feature. Disabling it prevents undesirable interactions with the virtual machines you install on this system.
6. Click **Finish** to complete the installation. The wizard closes and a VMware ACE icon is visible on the desktop.

Your system administrator may provide a VMware ACE package designed to update a package you installed earlier. The installation steps for the update package are the same as those for the original package.

All packages installed on your computer must come from the same source (known to your system administrator as a VMware ACE Manager project). Among other things, this means that you cannot install packages provided by more than one organization on the same computer.

Running VMware ACE

This section provides an overview of the most used features of VMware ACE. You may not see all these features in the VMware ACE installed on your computer. Certain features are available only if the administrator who created the package included them.

Starting VMware ACE

To start VMware ACE, double-click its icon on the desktop or launch it from the Start menu.

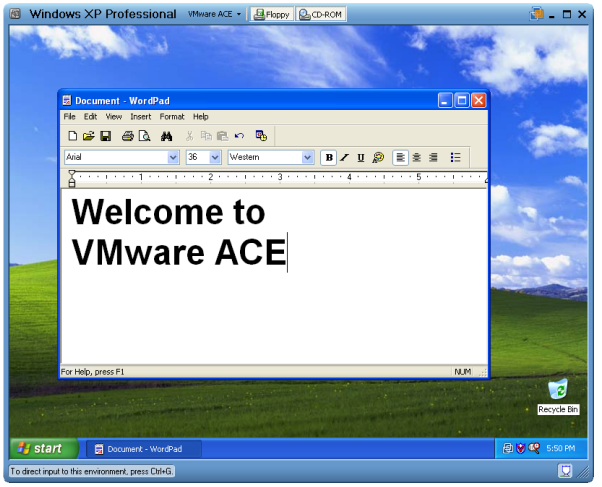
If the administrator has configured the virtual machine so a password is required, a password dialog box appears.

The first time the VMware ACE environment runs, the dialog box requires you to select and confirm a password. Your administrator may require that you include numbers or punctuation marks, or that you mix capital and lower case letters. The dialog box shows what requirements your administrator has set.

On subsequent uses, the dialog box requires you to enter the password you set when you first ran the VMware ACE environment. To change the password later, open the **VMware ACE** menu on the toolbar at the top of the VMware ACE screen and choose **Change Password**.

VMware ACE starts.

If the operating system inside your VMware ACE environment asks you to press Ctrl-Alt-Del to log on, press Ctrl-Alt-Ins instead.



Click inside the VMware ACE window to begin using the guest operating system and the applications installed in the VMware ACE environment. In general, you use the operating system and applications just as you would if they were running directly on a physical computer.

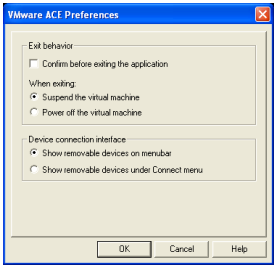
Quitting VMware ACE

Be sure to quit VMware ACE before you shut down the host computer — the computer where VMware ACE is running.

To quit VMware ACE, click the exit button on the VMware ACE window or toolbar — the X in the upper-right corner.

The VMware ACE environment shuts down and the window closes. When you next start the VMware ACE environment, it restarts with applications running and files open much as they would be on a laptop computer after you suspended and resumed operation.

If your system administrator has enabled the appropriate controls, you may change the exit behavior in the Preferences dialog box (**VMware ACE** > **Preferences**).

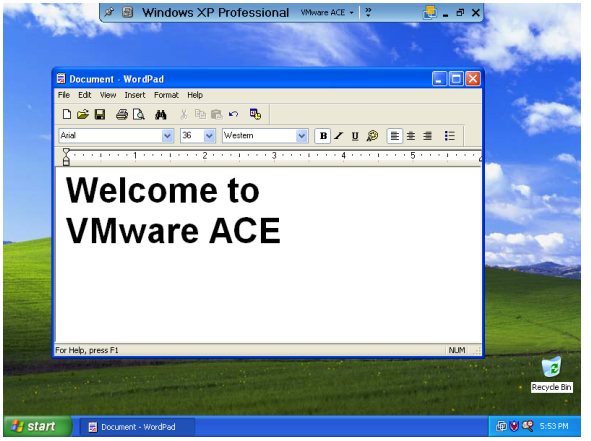


You may specify the following:

- **Confirm before exiting the application** — When you give the command to exit VMware ACE, either from the menu or by clicking the X in the upper right corner of the window or toolbar, a dialog box appears. You may confirm the intention to exit VMware ACE or click **Cancel** to continue working.
- **Suspend the virtual machine** when exiting — This is the default behavior. VMware ACE suspends the virtual machine and closes. The next time you run the VMware ACE environment, it resumes operation from the point where it was suspended.
- **Power off the virtual machine** when exiting — VMware ACE powers off the virtual machine. The next time you launch the VMware ACE environment, it starts from a powered off state and the guest operating system boots.

Enlarging VMware ACE to Fill the Screen

Click the maximize button on the VMware ACE window to run your VMware ACE environment in full screen mode. The desktop expands to fill the full screen, leaving a small toolbar visible at the top of the screen.



After a few seconds with no use, the toolbar hides. To make it visible again, move the mouse pointer to the top edge of the screen.

To pin the toolbar so it is always visible, click the pushpin on the toolbar. To release the toolbar so it can hide again, click the pushpin a second time.

To reduce the VMware ACE display so it is running in a window again, click the restore button on the toolbar. To return to a window if the mouse pointer is not available, press Ctrl-Alt.

Note: If your system administrator has configured VMware ACE to run only in full screen mode, you cannot run it in a window. If you click the minimize button on the toolbar or press Ctrl-Alt, the VMware ACE environment is minimized and you see the host operating system.

Understanding VMware ACE Status Indicators

Your VMware ACE environment has several indicators to keep you aware of its status. In window mode, these indicators appear at the top and bottom of the VMware ACE window. In full screen mode, the status indicators appear on the toolbar at the top of your screen.

The activity indicator shows that your VMware ACE environment is running. It is represented by the VMware logo of three interlocking squares. This indicator appears

near the upper right corner of the VMware ACE window or near the right end of the toolbar. While your VMware ACE environment is running, the activity indicator is animated.

The status icon tray is at the bottom right of the VMware ACE window or immediately left of the activity indicator on the toolbar. The status icon tray may display one or both of the following icons:

- The network quarantine indicator is a shield-shaped icon. If your VMware ACE environment uses network quarantine features, this icon appears. Hold your mouse pointer over the icon to see whether some or all of the network traffic is being blocked.

  Click the network quarantine status icon to open the Network Quarantine Info dialog box, which displays a detailed summary of your VMware ACE environment's network quarantine status.

- The updates available icon appears as an arrow pointing up. If this icon appears in your status icon tray, there are updates available for your VMware ACE environment. A yellow arrow indicates a recommended update. A red arrow indicates a required update.

  Click the updates available icon to open the Update Available dialog box, which displays details about the available update.

If your VMware ACE environment uses advanced network quarantine features, a host quarantine icon appears in the system tray of your computer's Windows operating system. The icon features a VMware logo connected to a network cable. Hold your mouse pointer over the icon for a brief description of host quarantine status. Click the icon to open the Host Quarantine Info dialog box, which displays a detailed summary of the host quarantine status.

Controlling Devices Attached to VMware ACE

Your administrator may have configured VMware ACE to give the VMware ACE environment access to some of the devices attached to your host computer, such as the floppy disk drive, the CD or DVD drive and the Ethernet adapter. Depending on the preferences you set (see Setting VMware ACE Preferences on page 161) icons for those devices may appear in the toolbar or the devices may be listed under a Connect menu.

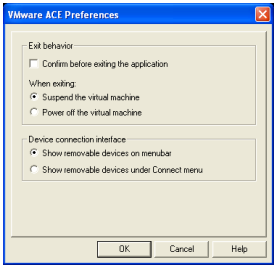
To disconnect and reconnect the devices shown on the toolbar, click a device's icon to toggle it off and on. A device with a depressed icon is connected. If the device appears level with the toolbar, it is disconnected.

To disconnect and reconnect the devices from the Connect menu, click the name of a device to toggle it off and on. A check beside the name of a device indicates that it is connected. If there is no check mark, the device is disconnected.

Note: Only one machine — either the host computer or the VMware ACE environment — may use floppy disk drives and USB devices at any one time. This means that if your VMware ACE environment is configured to use the device, and if you want to use that device directly on your host computer, you must first be sure it is disconnected from the VMware ACE environment. The Ethernet adapter may be shared by the host computer and the VMware ACE environment.

Setting VMware ACE Preferences

You can set preferences that control the behavior of VMware ACE. The options available to you depend on choices made by your system administrator. To change the preferences, choose **VMware ACE** > **Preferences**. The VMware ACE Preferences dialog box appears.



If your system administrator has made them available, you may set the preferences described below.

The exit behavior preferences allow you to specify the following:

- **Confirm before exiting the application** — When you give the command to exit VMware ACE, either from the menu or by clicking the X in the upper right corner of the window or toolbar, a dialog box appears. You may confirm the intention to exit VMware ACE or click **Cancel** to continue working.
- **Suspend the virtual machine** when exiting — This is the default behavior. VMware ACE suspends the virtual machine and closes. The next time you launch VMware ACE, the VMware ACE environment resumes operation from the point where it was suspended.

- **Power off the virtual machine** when exiting — VMware ACE powers off the virtual machine. The next time you launch VMware ACE, the virtual machine starts from a powered off state and the guest operating system boots.

The device connection interface preferences let you specify how you connect and disconnect devices such as floppy disk drives, CD or DVD drives, Ethernet adapters and sound devices available for use in VMware ACE. You may select one of the following:

- **Show removable devices on toolbar** — To disconnect and reconnect the devices shown on the toolbar, click a device's icon to toggle it off and on. A device with a depressed icon is connected. If the device appears level with the toolbar, it is disconnected.
- **Show removable devices under Connect menu** — To disconnect and reconnect the devices from the Connect menu, click the name of a device to toggle it off and on. A check beside the name of a device indicates that it is connected. If there is no check mark, the device is disconnected.

Printing from VMware ACE

To print from your VMware ACE environment, you may use any printer accessible from VMware ACE. If your system administrator enabled a streamlined printer setup feature, there is a special choice on the VMware ACE menu to make it easier for you to configure a printer that is connected to your host computer. Choose **Add Printer** to view a list of printers that are already configured on your host computer. You may select one or more of these computers to be configured for your VMware ACE environment.

You may also need to install printer drivers in the VMware ACE environment. Install the drivers the same way you would on the host computer. Be sure you have the correct drivers for the operating system running in your VMware ACE environment.

In some cases, network printers cannot be configured using the Add Printer menu choice. If you are unable to add a network printer in this way, you may still add it from within the VMware ACE environment, using the operating system's features for adding printers. Or you may contact your system administrator for assistance.

Uninstalling VMware ACE

To uninstall VMware ACE, use the Add/Remove Programs control panel. The entry for VMware ACE uses the name assigned by your system administrator when the VMware

ACE package was created. Select that entry, then click **Remove**. Follow the onscreen instructions.

Troubleshooting Problems

If you encounter problems while running your VMware ACE environment, contact your system administrator for assistance.

Requesting a Hot Fix

When certain problems occur, VMware ACE provides a simplified method for contacting your system administrator — a wizard that lets you request a hot fix for your problem.

If your system administrator has enabled the hot fix mechanism, you can use it to resolve the following problems:

- Lost or forgotten password
- Expired VMware ACE environment
- Copy-protected VMware ACE environment run from a new location

The hot fix request automatically includes the nature of the problem. The Hot Fix Request Wizard allows you to include an additional message to your system administrator, if you wish. The wizard also asks for your name and email address so your system administrator can send you the hot fix or contact you for additional information.

Your system administrator may have configured your VMware ACE environment to submit the hot fix request automatically. If not, or if the automatic submission fails, you may save the hot fix request in a file and submit that file to your administrator. Be sure to note the path to the file shown in the final panel of the Hot Fix Request Wizard. Also note any submission instructions the administrator provides. The wizard displays those instructions in the panel that allows you to save the hot fix request file.

If your system administrator approves your hot fix request, you receive the hot fix in the form of a file. Save the hot fix to the desktop of your host computer or to some other convenient location. Double-click the hot fix to apply it.

Lost or Forgotten Password — If your system administrator configured VMware ACE so a password is required, you may try three times to enter your password correctly. If the password you enter is rejected, check the Caps Lock indicator to be sure it is not on and be careful to enter capital and lowercase letters exactly as you did when you set up the password.

If you have lost or forgotten your password, click the **Hot Fix Request** button in the password dialog box. This starts the Hot Fix Request Wizard.

If your system administrator approves your hot fix request, the administrator gives you a new temporary password. After applying the hot fix, use that temporary password to run your VMware ACE environment. You should then choose **VMware ACE** > **Change Password** to set a password of your choice.

Expired VMware ACE Environment — If your system administrator configured your VMware ACE environment to run for a limited time, you receive an error message if you try to run the VMware ACE environment after it has expired. To request an extension of the time you are authorized to run the VMware ACE environment, click the **Hot Fix Request** button in the error dialog box. This starts the Hot Fix Request Wizard.

Copy Protected VMware ACE Environment Run from a New Location — If your system administrator has applied copy protection to your VMware ACE environment, it runs only from the location where it is installed by the VMware ACE package installer. If you try to run it from a different location — for example, if you have copied it to a different directory — you receive an error message. To request authorization to run the VMware ACE environment from the new location, click the **Hot Fix Request** button in the error dialog box. This starts the Hot Fix Request Wizard.

Resetting and Powering Off

In the course of troubleshooting a problem, your system administrator may ask you to reset or power off your VMware ACE environment. These commands are on the VMware ACE menu. Choose **VMware ACE** > **Troubleshoot** > **Reset** or **VMware ACE** > **Troubleshoot** > **Power Off and Exit**.

The reset command affects your VMware ACE environment the same way a reset button affects a physical computer. Giving the reset command is like turning the power off, then immediately turning it on again.

The power off command affects your VMware ACE environment the same way a turning off the power affects a physical computer. Giving the power off command is like turning the power off and leaving it off. In addition, the VMware ACE environment closes. The next time you run your VMware ACE environment, you see a VMware startup screen for a few moments before the operating system in your VMware ACE environment begins to run.

Reverting to the Original Installed VMware ACE Environment

If you encounter serious problems with your VMware ACE environment, your system administrator may tell you to use a menu choice to revert to the original state of your environment.

If you do revert to the original state, you lose all changes made to your VMware ACE environment since you installed it — including any data you have saved in the environment, any new software you have installed and any configuration changes. Thus in most cases you should not take this action unless your system administrator recommends it.

To revert to the original installed VMware ACE environment, choose **VMware ACE** > **Troubleshooting** > **Revert to the Installed <name> Environment**, where <name> is the name of the VMware ACE environment.

This menu item is available only if your system administrator has enabled it.

CHAPTER 9

Using Virtual Disks

The following sections provide information on configuring your virtual machine's hard disk storage so it best meets your needs:

- Configuring Hard Disk Storage in a Virtual Machine on page 168
  - Virtual Disk Basics on page 168
  - File Locations on page 169
  - Defragmenting and Shrinking Virtual Disks on page 171
- Adding Drives to a Virtual Machine on page 173
  - Adding Virtual Disks to a Virtual Machine on page 173
  - Adding DVD or CD Drives to a Virtual Machine on page 174
  - Adding Floppy Drives to a Virtual Machine on page 176
- Disk Performance in Windows NT Guests on Multiprocessor Hosts on page 178

Configuring Hard Disk Storage in a Virtual Machine

Like a physical computer, a VMware ACE virtual machine stores its operating system, programs and data files on one or more hard disks.

The New Virtual Machine Wizard creates a virtual machine with one disk drive. You can use the virtual machine settings editor (**VM** > **Settings**) to add more disk drives to your virtual machine, to remove disk drives from your virtual machine or to change certain settings for the existing disk drives.

This section describes the choices you can make in setting up hard disk storage for your virtual machine.

Virtual Disk Basics

In the most common configurations, VMware ACE creates virtual hard disks, which are made up of files that are typically stored on your host computer's hard disk.

A virtual disk is a file or set of files that appears as a physical disk drive to a guest operating system. While you are working in VMware ACE Manager, the files can be on the host machine or on a remote computer. When an end user installs a package, the virtual disk files are always stored locally.

When you configure a virtual machine with a virtual disk, you can install a new operating system onto the virtual disk without repartitioning a physical disk or rebooting the host.

IDE virtual disks can be as large as 128GB. SCSI virtual disks can be as large as 256GB. Depending on the size of the virtual disk and the host operating system, VMware ACE creates one or more files to hold each virtual disk.

By default, the actual files used by the virtual disk start out small and grow to their maximum size as needed. The main advantage of this approach is the smaller file size. Smaller files require less storage space and result in a more compact package for distribution to your end users. They also are easier to move if you want to move the virtual machine to a new location. However, it takes longer to write data to a disk configured in this way.

Virtual disks can be set up as IDE disks for any guest operating system. They can be set up as SCSI disks for any guest operating system that has a driver for the LSI Logic or BusLogic SCSI adapter available in a VMware ACE virtual machine. You determine which SCSI adapter to use at the time you create the virtual machine.

Note: To use SCSI disks in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP or Server 2003.

A virtual disk of either type can be stored on either type of physical hard disk. That is, the files that make up an IDE virtual disk can be stored on either an IDE hard disk or a SCSI hard disk. So can the files that make up a SCSI virtual disk. They can also be stored on other types of fast-access storage media, such as DVD-ROM or CD-ROM discs.

File Locations

Disk Files

The virtual machine settings editor (**VM** > **Settings**) allows you to choose the disk files for a virtual machine.

You may want to choose a file other than the one created by the New Virtual Machine Wizard if you are using a virtual disk that you created in a different location or if you are moving the automatically created disk files to a new location.

The disk files for a virtual disk store the information that you write to a virtual machine's hard disk — the operating system, the program files and the data files. The virtual disk files have a `.vmdk` extension.

A virtual disk is made up of one or more `.vmdk` files.

On Windows hosts, each virtual disk is contained in one file by default. You may, as an option, configure the virtual disk to use a set of files limited to 2GB per file. Use this option if you or your end users may place the virtual disk on a file system that does not support files larger than 2GB. This is also the preferred option for virtual machines that may be installed on a FAT32 file system.

You must set this option at the time the virtual disk is created.

If you are setting up a new virtual machine, in the New Virtual Machine Wizard follow the **Custom** path. In the panel that allows you to specify the virtual disk's capacity, select **Split disk into 2GB files**.

If you are adding a virtual disk to an existing virtual machine, follow the steps in the Add Hardware Wizard. In the panel that allows you to specify the virtual disk's capacity, select **Split disk into 2GB files**.

When a disk is split into multiple files, larger virtual disks have more `.vmdk` files.

The first `.vmdk` file for each disk is small and contains pointers to the other files that make up the virtual disk. The other `.vmdk` files contain data stored by your virtual machine and use a small amount of space for virtual machine overhead.

If you chose to allocate space for the virtual disk in advance, the file sizes are fixed, and most of the files are 2GB. As mentioned above, the first file is small. The last file in the series may also be smaller than 2GB.

If you did not allocate the space in advance, the `.vmdk` files grow as data is added, to a maximum of 2GB each — except for the first file in the set, which remains small.

The virtual machine settings editor shows the name of the first file in the set — the one that contains pointers to the other files in the set. The other files used for that disk are automatically given names based on the first file's name.

For example, a Windows XP Professional virtual machine using the default configuration, with files that grow as needed, stores the disk in files named `Windows XP Professional.vmdk`, `Windows XP Professional-s001.vmdk`, `Windows XP Professional-s002.vmdk` and so on.

Lock Files

A running virtual machine creates lock files to prevent consistency problems on virtual disks. If the virtual machine did not use locks, multiple virtual machines might read and write to the disk, causing data corruption.

Lock files are always created in the same directory as the `.vmdk` file.

The locking methods used by VMware software on Windows and Linux hosts are different, so files shared between programs running on the two platforms are not fully protected. If you use a common file repository that provides files to users of VMware products on both Windows and Linux hosts, be sure that each virtual machine is run by only one user at a time.

When a virtual machine is powered off, it removes the lock files it created. If it cannot remove the lock, a stale lock file is left protecting the `.vmdk` file. For example, if the host machine crashes before the virtual machine has a chance to remove its lock file, a stale lock remains.

If a stale lock file remains when the virtual machine is started again, the virtual machine tries to remove the stale lock. To make sure that no virtual machine could be using the lock file, the virtual machine checks the lock file to see if

1. The lock was created on the same host where the virtual machine is running.
2. The process that created the lock is not running.

If those two conditions are true, the virtual machine can safely remove the stale lock. If either of those conditions is not true, a dialog box appears, warning you that the virtual machine cannot be powered on. If you are sure it is safe to do so, you may delete the lock files manually. When created by VMware products on Windows hosts, the filenames of the lock files end in `.lck`.

Defragmenting and Shrinking Virtual Disks

If you have a virtual disk that grows as data is added, you can defragment and shrink it as described in this section.

To defragment the virtual disks attached to a virtual machine, power off the virtual machine, then go to the virtual machine settings editor (**VM** > **Settings**).

Select the virtual disk you want to defragment, then click **Defragment**.

Defragmenting disks may take considerable time.

Note: The defragmentation process requires free working space on the host computer's disk. If your virtual disk is contained in a single file, for example, you need free space equal to the size of the virtual disk file. Other virtual disk configurations require less free space.

When a virtual machine is powered on, you can shrink its virtual disks from the VMware Tools control panel. You cannot shrink virtual disks if a snapshot exists. To remove the snapshot if one exists, choose **Snapshot** > **Remove Snapshot**.

1. To launch the control panel in a Windows guest, double-click the VMware Tools icon in the system tray or choose **Start** > **Settings** > **Control Panel**, then double-click **VMware Tools**.

   To launch the control panel in a Linux or FreeBSD guest, become root (`su -`), then run `vmware-toolbox`.

2. Click the **Shrink** tab.
3. Select the virtual disks you want to shrink, then click **Prepare to Shrink**.

The shrink tool reclaims unused space in the virtual disk. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive.

Shrinking disks may take considerable time.

In some configurations, it is not possible to shrink virtual disks. If your virtual machine uses such a configuration, the Shrink tab displays information explaining why you cannot shrink your virtual disks.

For best disk performance, you can take the following three actions, in the order listed:

1. Run a disk defragmentation utility inside the virtual machine.
2. Use the VMware ACE defragmentation tool. Go to **VM** > **Settings**, click the listing for the virtual disk you want to defragment, then click **Defragment**.
3. Run a disk defragmentation utility on the host computer.

Adding Drives to a Virtual Machine

VMware ACE virtual machines can use up to four IDE devices and up to seven SCSI devices. Any of these devices can be a virtual hard disk or DVD or CD-ROM drive. A virtual machine can read data from a DVD-ROM disc. VMware ACE does not support playing DVD movies in a virtual machine.

Adding Virtual Disks to a Virtual Machine

Virtual disks are stored as files on the host computer or on a network file server. While you are working in VMware ACE Manager, the files can be on the host machine or on a remote computer. When an end user installs a package, the virtual disk files are always stored locally. It does not matter whether the physical disk that holds the files is IDE or SCSI. A virtual IDE drive can be stored on an IDE drive or on a SCSI drive. So can a virtual SCSI drive.

Use the virtual machine settings editor (**VM** > **Settings**) to add a new virtual disk to your virtual machine. The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the VMware ACE Manager toolbar.

Note: If you have a Windows NT 4.0 guest with a SCSI virtual disk, you cannot add both an additional SCSI disk and an IDE disk to the configuration.

1. Open the virtual machine settings editor (**VM** > **Settings**) and click **Add**. The Add Hardware Wizard guides you through the steps to create your virtual disk.
2. Click **Hard Disk**, then click **Next**.
3. Select **Create a New Virtual Disk**, then click **Next**.
4. Choose whether you want the virtual disk to be an IDE disk or a SCSI disk.
5. Set the capacity for the new virtual disk.

   If you wish, select **Allocate all disk space now**.

   Allocating all the space at the time you create the virtual disk gives somewhat better performance, but it requires as much disk space as the size you specify for the virtual disk.

   If you do not select this option, the virtual disk's files start small and grow as needed, but they can never grow larger than the size you set here.

   You can set a size between 2GB and 256GB for a SCSI virtual disk or 128GB for an IDE virtual disk. The default is 4GB.

You may also specify whether you want the virtual disk created as one large file or split into a set of 2GB files. You should split your virtual disk if it may be stored on a FAT32 file system.

6. Accept the default filename and location for the virtual disk file or change it, if you want to use a different name or location. To find a different folder, click **Browse**.

   If you want to specify a device node for your virtual disk, click **Advanced**.

   On the advanced settings panel, you can also specify a disk mode. This is useful in certain special-purpose configurations in which you want to exclude disks from the snapshot. For more information on the snapshot feature, see Using the Snapshot on page 182.

   Normal disks are included in the snapshot. In most cases, this is the setting you want — with **Independent** deselected.

   Independent disks are not included in the snapshot. If you select **Independent**, you have the following options:

   - **Persistent** — Changes are immediately and permanently written to the disk.
   - **Nonpersistent** — Changes to the disk are discarded when you power off or revert to the snapshot.

   When you have set the filename and location you want to use and have made any selections you want to make on the advanced settings panel, click **Finish**.

7. The wizard creates the new virtual disk. It appears to your guest operating system as a new, blank hard disk. Use the guest operating system's tools to partition and format the new drive for use.

Adding DVD or CD Drives to a Virtual Machine

You can add one or more DVD or CD drives to your virtual machine. You can connect the virtual machine's drive to a physical drive on the host machine or to an ISO image file.

If the virtual machine's drive is connected to an ISO image, that ISO image is included in the package for distribution to end users.

You can configure the virtual DVD or CD drive as either IDE or SCSI, no matter what kind of physical drive you connect it to. In other words, if your host computer has an IDE CD drive, you can set up the virtual machine's drive as either SCSI or IDE and connect it to the host's drive. The same is true if the host's physical drive is a SCSI drive.

Adding a DVD or CD Drive

1. Open the virtual machine settings editor (**VM** > **Settings**) and click **Add** to start the Add Hardware Wizard.
2. Click **DVD/CD-ROM Drive**, then click **Next**.
3. Select **Use physical drive** if you want to connect the virtual machine's drive to a physical drive on the host computer. Select **Use ISO Image** if you want to connect the virtual machine's drive to an ISO image file.
4. Do one of the following:
   - If you selected **Use physical drive**, choose **Auto detect**.

     Note: If you specify a particular physical drive, a CD drive must exist at the specified drive letter on end users' computers.

     If you do not want the CD drive connected when the virtual machine starts, deselect **Connect at power on**.

     Click **Advanced** if you want to specify the device node the drive should use in the virtual machine.

     On the advanced settings panel you may also select **Legacy emulation**. This is necessary only if you have had problems using normal mode. The legacy emulation mode does not support all the capabilities of normal mode. For example, if you are using legacy emulation mode, you cannot record CDs, you cannot read multisession CDs, you cannot extract digital audio from a CD and you cannot read or write DVDs. For details, see Legacy Emulation for DVD and CD Drives on page 176.

     After you have made any desired changes in these settings, click **Finish**.
   - If you selected **Use ISO Image**, enter the path and filename for the image file or click **Browse** to navigate to the file.

     If you do not want the CD drive connected when the virtual machine starts, deselect **Connect at power on**.

     Click **Advanced** if you want to specify the device node the drive should use in the virtual machine.

     After you have made any desired changes in these settings, click **Finish**.
5. The drive is set up initially so it appears to the guest operating system as an IDE drive. If you want it to appear to the guest operating system as a SCSI drive, click the drive's entry in the virtual machine settings editor and make that change in the settings panel on the right.

Legacy Emulation for DVD and CD Drives

The virtual machine settings editor (**VM** > **Settings**) provides a **Legacy emulation** option for DVD and CD drives attached to the virtual machine.

If you encounter problems using your DVD or CD drive, try selecting **Legacy emulation**.

Note that in legacy emulation mode, you can read from data discs in the DVD or CD drive, but some other functions are not available.

When **Legacy emulation** is deselected, the guest operating system communicates directly with the drive. This direct communication enables capabilities that are not possible in legacy emulation mode, such as using CD and DVD writers to burn discs, reading multisession CDs, performing digital audio extraction and viewing video.

However, in some cases, the DVD or CD drive may not work correctly when the guest operating system is communicating directly with the drive. In addition, certain drives and their drivers do not work correctly in raw mode. Selecting **Legacy emulation** is a way to work around these problems.

Adding Floppy Drives to a Virtual Machine

You can add floppy drives to your virtual machine, to a total of two floppy drives. A virtual floppy drive can connect to a physical floppy drive on the host computer, to an existing floppy image file or to a blank floppy image file.

If the virtual machine's drive is connected to a floppy image, that floppy image is included in the package for distribution to end users.

Adding a Floppy Drive

1. Open the virtual machine settings editor (**VM** > **Settings**) and click **Add** to start the Add Hardware Wizard.
2. Click **Floppy Drive**, then click **Next**.
3. Select what you want to connect to — a physical floppy drive on the host computer, an existing floppy image file or a new floppy image file. Click **Next**.
4. If you selected **Use a physical floppy drive**, choose **A:** from the drop-down list, then click **Finish**.

   Note: If you set the floppy drive to be connected at power on, be sure all your end users have floppy disk drives configured as drive A: on their host computers.

   If you selected **Use a floppy image**, type the path and filename for the floppy image file you want to use or click **Browse** to navigate to the file. Click **Finish**.

If you selected **Create a blank floppy image**, use the default path and filename or type in a new one. To navigate to a location, click **Browse**. When the field contains the path and filename you want to use for the new floppy image file, click **Finish**.

Note: By default, only one floppy drive is enabled in the virtual machine's BIOS. If you are adding a second floppy drive to the virtual machine, click inside the virtual machine window and press F2 as the virtual machine boots to enter the BIOS setup utility. On the main panel, choose **Legacy Diskette B:** and use the plus (+) and minus (-) keys on the numerical keypad to select the type of floppy drive you want to use. Then press F10 to save your changes and close the BIOS setup utility.

Connecting a CD-ROM or Floppy Drive to an Image File

You can use the virtual machine settings editor to connect an existing virtual CD-ROM or floppy drive to an image file.

You can connect a virtual CD-ROM drive to an ISO image file.

Connecting to an ISO Image File

1. Open the virtual machine settings editor (**VM** > **Settings**) and select the DVD/CD-ROM drive you want to connect to the image file.
2. Select **Use ISO Image** and enter the path and filename for the image file or click **Browse** to navigate to the file.
3. Click **OK** to save the configuration and close the virtual machine settings editor.

Connecting to a Floppy Image File

1. Open the virtual machine settings editor (**VM** > **Settings**) and select the floppy drive you want to connect to an image file.
2. Type the path and filename for the floppy image file you want to use or click **Browse** to navigate to the file.

   If you want to create a new image file, click **Create**. Use the default filename and folder or change them as you wish.
3. Click **Finish**.

Disk Performance in Windows NT Guests on Multiprocessor Hosts

Some users have seen slower than expected disk input and output performance when running Windows NT guest operating systems. They see the problem in a virtual machine using IDE virtual disks on a multiprocessor host computer. The I/O issue is especially noticeable when the virtual machine is booting.

Note: Performance in Windows NT guest operating systems may also be affected by disk fragmentation on the host computer.

Improving Performance

You may increase performance by enabling DMA (direct memory access) on the virtual hard disk's IDE channel in the virtual machine.

If you have a virtual disk and a DVD/CD-ROM attached as master and slave to the primary IDE controller (channel 0) and you want to enable DMA, power off the virtual machine and use the virtual machine settings editor (**VM** > **Settings**) to move the DVD/CD-ROM drive to the secondary IDE controller (channel 1) at IDE 1:0.

You can enable the DMA feature after you finish installing Windows NT. You must install Service Pack 6a. Download `DMACHECK.EXE` from the Microsoft Web site (*support.microsoft.com/support/kb/articles/Q191/7/74.ASP*) and run it.

Click the **Enabled** option for the IDE controller and channel configured for the virtual disk. Typically, this is channel 0 only, unless you have the virtual machine configured with multiple virtual disks and no virtual DVD/CD-ROM drive.

As noted above, you should not enable DMA on an IDE channel with a virtual DVD/CD-ROM drive attached.

CHAPTER 10

Preserving the State of a Virtual Machine

VMware ACE offers two ways to preserve the state of a virtual machine. The following sections describe these features and help you understand which is appropriate in particular situations:

- Using Suspend and Resume on page 180
- Using the Snapshot on page 182
  - What Is Captured by the Snapshot? on page 182
  - Removing the Snapshot on page 183
  - Ways of Using the Snapshot on page 183
  - The Snapshot and the Virtual Machine's Hard Disks on page 184
  - The Snapshot and Other Activity in the Virtual Machine on page 184

Using Suspend and Resume

The suspend and resume feature is available to you when you are running a virtual machine in VMware ACE Manager.

You should not include a suspended virtual machine in a package for distribution to end users.

The suspend and resume feature is most useful when you want to save the current state of your virtual machine, then pick up work later with the virtual machine in the same state it was when you stopped.

Once you resume and do additional work in the virtual machine, there is no way to return to the state the virtual machine was in at the time you suspended.

To preserve the state of the virtual machine so you can return to the same state repeatedly, take a snapshot. For details, see Using the Snapshot on page 182.

The speed of the suspend and resume operations depends on how much data has changed while the virtual machine has been running. In general, the first suspend operation takes a bit longer than later suspend operations do.

When you suspend a virtual machine, a file with a `.vmss` extension is created. This file contains the entire state of the virtual machine. When you resume the virtual machine, its state is restored from the `.vmss` file.

To suspend a virtual machine:

1. If your virtual machine is running in full screen mode, return to window mode by pressing the Ctrl-Alt key combination.
2. Click **Suspend** on the VMware ACE toolbar.
3. When VMware ACE has completed the suspend operation, it is safe to exit VMware ACE.

   File > **Exit**

To resume a virtual machine that you have suspended:

1. Start VMware ACE and choose a virtual machine you have suspended.
2. Click **Resume** on the VMware ACE toolbar.

   Note that any applications you were running at the time you suspended the virtual machine are running and the content is the same as it was when you suspended the virtual machine.

On your end users' computers, VMware ACE suspends the virtual machine when the user clicks the exit button on the VMware ACE window or toolbar — the X in the

upper-right corner. The virtual machine is resumed automatically when the end user launches VMware ACE again.

Using the Snapshot

The snapshot feature is available to you when you are running a virtual machine in VMware ACE Manager.

You may not include a virtual machine with a snapshot in a package for distribution to end users.

The snapshot feature is most useful when you want to preserve the state of the virtual machine so you can return to the same state repeatedly. You may, for example, want to take a snapshot before you begin testing an update to software in the virtual machine. If testing is successful, you can remove the snapshot, thus integrating the changes you made into the base virtual machine. If there are problems during testing, you can revert to the snapshot, thus discarding the changes made since you took the snapshot.

To simply save the current state of your virtual machine, then pick up work later with the virtual machine in the same state it was when you stopped, suspend the virtual machine. For details, see Using Suspend and Resume on page 180.

You can take a snapshot while a virtual machine is powered on, powered off or suspended. (If you are suspending a virtual machine, wait until the suspend operation has finished before taking the snapshot.) A snapshot preserves the virtual machine just as it was when you took the snapshot — the state of the data on all the virtual machine's disks and whether the virtual machine was powered on, powered off or suspended. You can then revert to that snapshot at any time.

When you revert to a snapshot, you discard all changes made to the virtual machine since you took the snapshot.

Use the **Snapshot** and **Revert** buttons on the Workstation toolbar to take a snapshot and revert to it later.

You can take a new snapshot at almost any time. When you take a new snapshot, you replace the previous snapshot. You can have only one active snapshot at a time.

What Is Captured by the Snapshot?

The snapshot captures the entire state of the virtual machine at the time you take the snapshot. This includes:

- The state of all the virtual machine's disks.
- The contents of the virtual machine's memory.
- The virtual machine settings.

When you revert to the snapshot, you return all these items to the state they were in at the time you took the snapshot.

Removing the Snapshot

You can remove the snapshot any time the virtual machine is powered off. Removing the snapshot does not destroy any data in the virtual machine. You keep all changes made since you took the snapshot. For example, changes made to data stored on the virtual hard disk are written to the virtual disk files. You then permanently accumulate additional changes as you run the virtual machine. You cannot revert to a previous state because the snapshot no longer exists.

To remove the snapshot, shut down and power off the virtual machine. Then, on the VMware ACE menu, choose **Snapshot** > **Remove Snapshot**.

Ways of Using the Snapshot

The following examples illustrate the most common ways you can use the snapshot. These examples apply only when you are running the snapshot in VMware ACE Manager.

No Snapshot

If you do not take a snapshot, your virtual machine runs the same way a physical computer does. All changes you make while you are working with a virtual machine are saved and you cannot return to an earlier state.

If you do not need to use the snapshot feature, it is best to run your virtual machine with no snapshot. This provides best performance. To be sure a virtual machine has no snapshot, choose **Snapshot** > **Remove Snapshot**. You can then disable the snapshot functionality for the virtual machine. Choose **VM** > **Settings** > **Options** > **Snapshot** and select **Disable snapshots**.

Making Risky Changes

If you plan to make risky changes in a virtual machine (for example, testing new software or examining a virus), take a snapshot before you begin to make those changes. If you encounter a problem, click **Revert** to return the virtual machine to its state at the time you took the snapshot.

If the first action you take causes no problems and you want to protect the virtual machine in its new state, you can take a new snapshot. You can have only one snapshot at a given time. When you take the new snapshot, you replace your previous snapshot. You do not lose any data. For example, changes made to data stored on the virtual hard disk are written to the virtual disk files.

Starting a Virtual Machine Repeatedly in the Same State

You can configure the virtual machine to revert to the snapshot any time it is powered off. To do so, choose **VM** > **Settings** > **Options** > **Snapshot**. Under **When powering off**, select **Revert to the snapshot**. If you want the virtual machine to be suspended when you launch it, suspend the virtual machine before taking the snapshot. Similarly, if you want the virtual machine to be powered on or powered off when you launch it, be sure it is powered on or powered off when you take the snapshot.

The Snapshot and the Virtual Machine's Hard Disks

When a snapshot exists and the virtual machine saves data to disk, that data is written to a set of redo-log files. These files have `.REDO` as part of the filename and are stored in the virtual machine's working directory.

Newly saved data continues to accumulate in the redo-log files until you take an action that affects the snapshot.

- Remove the snapshot — When you remove the snapshot, the changes accumulated in the redo-log files are written permanently to the base disks, either the virtual disk files or the physical disks, depending on your virtual machine's hard disk configuration.
- Revert to the snapshot — When you revert to the snapshot, the contents of the redo-log files are discarded. Any additional changes once again accumulate in the redo-log files.
- Take a snapshot — If you take a snapshot when the virtual machine already has a snapshot, changes stored in the redo-log files are written permanently to the base disk. Then any subsequent changes once again accumulate in the redo-log files.

The Snapshot and Other Activity in the Virtual Machine

When you take a snapshot, be aware of other activity going on in the virtual machine and the likely impact of reverting to the snapshot. In general, it is best to take the snapshot when no applications in the virtual machine are communicating with other computers.

The potential for problems is greatest if the virtual machine is communicating with another computer, especially in a production environment.

Consider a case in which you take a snapshot while the virtual machine is downloading a file from a server on the network. After you take the snapshot, the virtual machine continues downloading the file, communicating its progress to the

server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Or consider a case in which you take a snapshot while an application in the virtual machine is sending a transaction to a database on a separate machine. If you revert to the snapshot — especially if you revert after the transaction starts but before it has been committed — the database is likely to be confused.

CHAPTER 11

Networking Virtual Machines

VMware ACE provides virtual networking components that let you create a wide range of configurations.

If you select the **Typical** setup path in the New Virtual Machine Wizard when you create a virtual machine, the wizard sets up bridged networking for the virtual machine. You can choose any of the common configurations — bridged networking, network address translation (NAT) or host-only networking — by selecting the **Custom** setup path. The wizard then connects the virtual machine to the appropriate virtual network.

On a Windows host, the software needed for all networking configurations is installed when you install VMware ACE.

The first topics in this section give you a quick look at the virtual networking components that VMware ACE provides and show how you can use them with your virtual machine. The rest of the section provides more detail on some networking capabilities.

In the virtual machines you create for your end users, you are most likely to use NAT or bridged networking with an IP address provided by a DHCP server.

This section covers the following topics:

- Components of the Virtual Network on page 189
- Common Networking Configurations on page 191
  - Bridged Networking on page 191
  - Network Address Translation (NAT) on page 192
  - Host-Only Networking on page 193
- Changing the Networking Configuration on page 195
  - Adding and Modifying Virtual Network Adapters on page 195
- Understanding NAT on page 196
  - Using NAT on page 196
  - The Host Computer and the NAT Network on page 196
  - DHCP on the NAT Network on page 196
  - DNS on the NAT Network on page 197
  - External Access from the NAT Network on page 197
  - Considerations for Using NAT on page 198
  - Using NAT with NetLogon on page 198

Components of the Virtual Network

Virtual switch — Like a physical switch, a virtual switch lets you connect other networking components together. Virtual switches are created as needed by the VMware ACE software, up to a total of nine switches. You can connect one or more virtual machines to a switch.

A few of the switches and the networks associated with them are, by default, used for special named configurations. The bridged network normally uses VMnet0. The NAT network uses VMnet8 by default. The other available networks are simply named VMnet2, VMnet3, VMnet4, and so on.

You connect a virtual machine to a switch by selecting the virtual network adapter you want to connect in the virtual machine settings editor, then configuring it to use the desired virtual network.

Bridge — The bridge lets you connect your virtual machine to the LAN used by your host computer. It connects the virtual network adapter in your virtual machine to the physical Ethernet adapter in your host computer.

The bridge is installed during VMware ACE installation. It is set up automatically when you create a new virtual machine using bridged networking.

Host virtual adapter — The host virtual adapter is a virtual Ethernet adapter that appears to your host operating system as a VMware Virtual Ethernet Adapter. It allows you to communicate between your host computer and the virtual machines on that host computer. The host virtual adapter is used in NAT configurations.

The host virtual adapter is not connected to any external network.

The software that creates the host virtual adapter is installed when you install VMware ACE. A host virtual adapter is then created automatically when you boot the host computer.

You can set up additional host virtual adapters as needed.

NAT device — The NAT (network address translation) device allows you to connect your virtual machines to an external network when you have only one IP network address on the physical network and that address is used by the host computer. You can, for example, use NAT to connect your virtual machines to the Internet through a dial-up connection on the host computer or through the host computer's Ethernet adapter or wireless Ethernet adapter. NAT is also useful when you need to connect to a non-Ethernet network, such as Token Ring or ATM.

The NAT device is set up automatically when you install VMware ACE.

DHCP server — The DHCP (dynamic host configuration protocol) server provides IP network addresses to virtual machines in configurations that are not bridged to an external network — for example, NAT configurations.

Packet filter — A packet filter supports the network quarantine feature of VMware ACE, making it possible for you to specify exactly which machines or subnets a virtual machine may access.

Network adapter — One virtual network adapter is set up for your virtual machine when you create it with the New Virtual Machine Wizard using any type of networking. It appears to the guest operating system as an AMD PCNET PCI adapter.

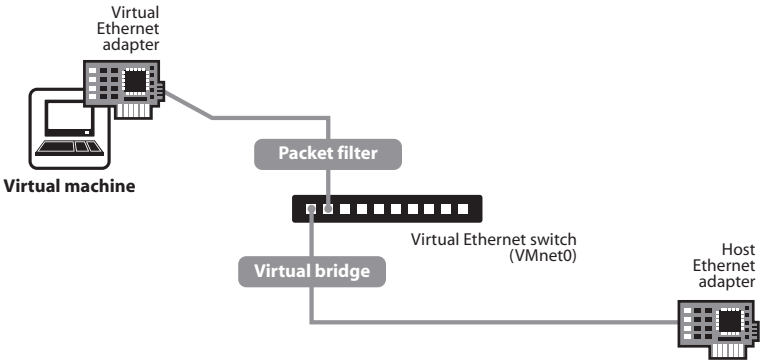
You can create and configure up to three virtual network adapters in each virtual machine using the virtual machine settings editor.

Common Networking Configurations

The following sections illustrate the networking configurations that are set up for you automatically when you choose the standard networking options in the New Virtual Machine Wizard or virtual machine settings editor.

Only one virtual machine is shown in each example, but multiple virtual machines can be connected to the same virtual Ethernet switch.

Bridged Networking



Bridged networking connects a virtual machine to a network using the host computer's Ethernet adapter.

Bridged networking is set up automatically if you select **Use bridged networking** in the New Virtual Machine Wizard or if you select the **Typical** setup path.

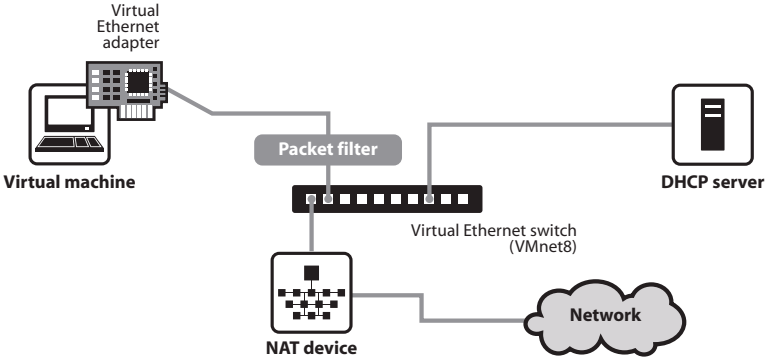
If your host computer is on an Ethernet network, this is often the easiest way to give your virtual machine access to that network. On a Windows host, you can use bridged networking to connect to either a wired or a wireless network. Bridged networking is often the best choice for virtual machines that will connect to an organization's internal network.

If you use bridged networking, your virtual machine needs to have its own identity on the network. For example, on a TCP/IP network, the virtual machine needs its own IP address. Your network administrator can tell you whether IP addresses are available for your virtual machine and what networking settings you should use in the guest operating system. Generally, your guest operating system may acquire an IP address and other network details automatically from a DHCP server, or you may need to set the IP address and other details manually in the guest operating system. NAT is often the best choice for virtual machines that will be deployed to remote locations.

If you use bridged networking, the virtual machine is a full participant in the network. It has access to other machines on the network and can be contacted by other machines on the network as if it were a physical computer on the network.

If you make some other selection in the New Virtual Machine Wizard and later decide you want to use bridged networking, you can make that change in the virtual machine settings editor (**VM** > **Settings**). For details, see Changing the Networking Configuration on page 195.

Network Address Translation (NAT)



NAT gives a virtual machine access to network resources using the host computer's IP address.

A network address translation connection is set up automatically if you follow the **Custom** path in the New Virtual Machine Wizard and select **Use network address translation**.

If you want to connect to the Internet or other TCP/IP network using the host computer's dial-up networking or broadband connection and you are not able to give your virtual machine an IP address on the external network, NAT is often the easiest way to give your virtual machine access to that network.

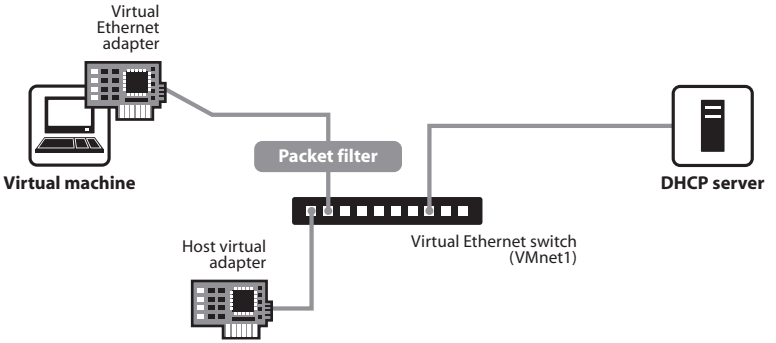
NAT also allows you to connect to a TCP/IP network using a Token Ring adapter on the host computer.

If you use NAT, your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination.

If you select NAT, the virtual machine can use many standard TCP/IP protocols to connect to other machines on the external network. For example, you can use HTTP to browse Web sites, FTP to transfer files and Telnet to log on to other computers. In the default configuration, computers on the external network cannot initiate connections to the virtual machine. That means, for example, that the default configuration does not let you use the virtual machine as a Web server to send Web pages to computers on the external network.

If you make some other selection in the New Virtual Machine Wizard and later decide you want to use NAT, you can make that change in the virtual machine settings editor (**VM** > **Settings**). For details, see Changing the Networking Configuration on page 195.

Host-Only Networking



Host-only networking creates a network that is completely contained within the host computer.

A host-only network is set up automatically if you select **Use Host-Only Networking** in the New Virtual Machine Wizard.

Host-only networking provides a network connection between the virtual machine and the host computer, using a virtual Ethernet adapter that is visible to the host operating system. This approach can be useful if you need to set up an isolated virtual network.

If you use host-only networking, your virtual machine and the host virtual adapter are connected to a private TCP/IP network. Addresses on this network are provided by the VMware DHCP server.

If you make some other selection in the New Virtual Machine Wizard and later decide you want to use host-only networking, you can make that change in the virtual machine settings editor (**VM** > **Settings**). For details, see Changing the Networking Configuration on page 195.

Routing and Connection Sharing

If you install the proper routing or proxy software on your host computer, you can establish a connection between the host virtual Ethernet adapter and a physical network adapter on the host computer. This allows you, for example, to connect the virtual machine to a Token Ring or other non-Ethernet network.

On a Windows 2000, Windows XP or Windows Server 2003 host computer, you can use host-only networking in combination with the Internet connection sharing feature in Windows to allow a virtual machine to use the host's dial-up networking adapter or other connection to the Internet. See your Windows documentation for details on configuring Internet connection sharing.

Changing the Networking Configuration

Using the virtual machine settings editor (**VM** > **Settings**), you can add virtual Ethernet adapters to your virtual machine and change the configuration of existing adapters.

Adding and Modifying Virtual Network Adapters

To add a new virtual Ethernet adapter, follow these steps.

1. Select the virtual machine to which you want to add the adapter and be sure it is powered off.
2. Open the virtual machine settings editor (**VM** > **Settings**).
3. Click **Add**.
4. The Add Hardware Wizard starts. Select **Network Adapter**. Click **Next**.
5. Select the network type you want to use — **Bridged**, **NAT** or **Host-only**.
6. Click **Finish**. The new adapter is added.
7. Click **OK** to save your configuration and close the virtual machine settings editor.

To change the configuration of an existing virtual network adapter, follow these steps.

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Select the adapter you want to modify.
3. Select the network type you want to use — **Bridged**, **NAT** or **Host-only**.
4. Click **OK** to save your changes and close the virtual machine settings editor.
5. Be sure the guest operating system is configured to use an appropriate IP address on the new network. If the guest is using DHCP, release and renew the lease. If the IP address is set statically, be sure the guest has an address on the correct virtual network.

Understanding NAT

Network address translation — or NAT — provides a simple way for virtual machines to use most client applications over almost any type of network connection available to the host. The only requirement is that the network connection must support TCP/IP.

NAT is useful when you have a limited supply of IP addresses or are connected to the network through a non-Ethernet network adapter. NAT works by translating addresses of virtual machines in a private VMnet network to that of the host machine. When a virtual machine sends a request to access a network resource, it appears to the network resource as if the request came from the host machine.

NAT uses the host's own network resources to connect to the external network. Thus, any TCP/IP network resource to which the host has access should be available through the NAT connection.

The chief advantage of NAT is that it provides a transparent, easily configured way for virtual machines to gain access to network resources.

Using NAT

The NAT device is connected to the VMnet8 virtual switch. Virtual machines connected to the NAT network also use the VMnet8 virtual switch.

The NAT device waits for packets coming from virtual machines on the VMnet8 virtual network. When a packet arrives, the NAT device translates the address of the virtual machine to that of the host before forwarding the packet to the external network. When data arrives from the external network for the virtual machine on the private network, the NAT device receives the data, replaces the network address with that of the virtual machine and forwards the data to the virtual machine on the virtual network. This translation occurs automatically and requires minimal configuration on the guest and the host.

The Host Computer and the NAT Network

The host computer has a host virtual adapter on the NAT network (identical to the host virtual adapter on the host-only network). This adapter allows the host and the virtual machines to communicate with each other for such purposes as file sharing. The NAT device never forwards traffic from the host virtual adapter.

DHCP on the NAT Network

In order to make networking configuration easy, a DHCP server is automatically installed when you install VMware ACE. Virtual machines running on the network with

the NAT device can dynamically obtain their IP addresses by sending out DHCP requests. The DHCP server on the NAT network, which is also used in host-only networking configurations, dynamically allocates IP addresses in the range of <net>.128 through <net>.254, where <net> is the network number assigned to your NAT network. VMware ACE always uses a Class C address for NAT networks. IP addresses <net>.3 through <net>.127 can be used for static IP addresses. IP address <net>.1 is reserved for the host adapter; <net>.2 is reserved for the NAT device.

In addition to the IP address, the DHCP server on the NAT network also sends out additional configuration information that enables the virtual machine to operate automatically. This information includes the default gateway and the DNS server. In the DHCP response, the NAT device instructs the virtual machine to use the IP address <net>.2 as the default gateway and DNS server. This causes all IP packets destined for the external network and DNS requests to be forwarded to the NAT device.

DNS on the NAT Network

The NAT device acts as a DNS server for the virtual machines on the NAT network. Actually, the NAT device is a DNS proxy and merely forwards DNS requests from the virtual machines to a DNS server that is known by the host. Responses come back to the NAT device, which then forwards them to the virtual machines.

If they get their configuration information from DHCP, the virtual machines on the NAT network automatically use the NAT device as the DNS server. However, the virtual machines can be statically configured to use another DNS server.

The virtual machines in the private NAT network are not, themselves, accessible via DNS. If you want the virtual machines running on the NAT network to access each other by DNS names, you must set up a private DNS server connected to the NAT network.

External Access from the NAT Network

In general, any protocol using TCP or UDP can be used automatically by a virtual machine on the NAT network so long as the virtual machine initiates the network connection. This is true for most client applications such as Web browsing, Telnet, passive-mode FTP and downloading streaming video. Additional protocol support has been built into the NAT device to allow FTP and ICMP echo (ping) to work completely transparently through the NAT.

On the external network to which the host is connected, any virtual machine on the NAT network appears to be the host itself, because its network traffic uses the host's IP address. It is able to send and receive data using TCP/IP to any machine that is accessible from the host.

Before any such communication can occur, the NAT device must set up a mapping between the virtual machine's address on the private NAT network and the host's network address on the external network.

When a virtual machine initiates a network connection with another network resource, this mapping is created automatically. The operation is perfectly transparent to the user of the virtual machine on the NAT network. No additional work needs to be done to let the virtual machine access the external network.

The same cannot be said for network connections that are initiated from the external network to a virtual machine on the NAT network.

When a machine on the external network attempts to initiate a connection with a virtual machine on the NAT network, it cannot reach the virtual machine because the NAT device does not forward the request. Network connections that are initiated from outside the NAT network are not transparent.

File sharing of the type used by Windows operating systems and Samba is possible among computers on the NAT network — including virtual machines and the host computer. If you are using WINS servers on your network, a virtual machine using NAT networking can access shared files and folders on the host that are known by the WINS server so long as those shared files and folders are in the same workgroup or domain.

Considerations for Using NAT

Because NAT requires that every packet sent and received from virtual machines is in the NAT network, there is an unavoidable performance penalty. Our experiments show that the penalty is minor for dial-up and DSL connections and performance is adequate for most VMware ACE uses.

NAT is not perfectly transparent. It does not normally allow connections to be initiated from outside the network, although you can set up server connections by manually configuring the NAT device. The practical result is that some TCP and UDP protocols that require a connection be initiated from the server machine — some peer to peer applications, for example — do not work automatically, and some may not work at all.

A standard NAT configuration provides basic-level firewall protection because the NAT device can initiate connections from the private NAT network, but devices on the external network cannot normally initiate connections to the private NAT network.

Using NAT with NetLogon

When using NAT networking in a virtual machine with a Windows guest operating system running on a Windows host, you can use NetLogon to log on to a Windows

domain from the virtual machine. You can then access file shares known by the WINS server in the domain.

To use NetLogon, you need to know how WINS servers and Windows domain controllers work. This section explains how to set up the virtual machine to use NetLogon. The setup process is similar to the way you set up a physical computer on one LAN that is using a domain controller on another LAN.

In order to log on to a Windows domain outside the virtual NAT network, the virtual machine needs access to a WINS server for that domain. There are two ways you can connect the virtual machine to a WINS server.

- You can connect to the WINS server provided by the DHCP server used on the NAT network. This approach works only if the WINS server is already set up on the host.
- To connect from the virtual machine to a WINS server not set up on the host, you can manually enter the IP address of the WINS server.

Using NAT to Connect to an Existing WINS Server Already Set Up on the Host

In order to use this method, a WINS server in the same workgroup or domain must be set up on the host. These steps use Windows 2000, Windows XP or Windows Server 2003 as a guide. The process is similar for Windows NT, Windows Me and Windows 9x guests.

1. In the virtual machine, right-click **My Network Places** and select **Properties**.
2. In the Network Connections window, right-click the virtual network adapter and select **Properties**.
3. In the Properties dialog box, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. In the TCP/IP Properties dialog box, click **Advanced**.
5. Click the **WINS** tab, then under **NetBIOS setting**, select **Use NetBIOS setting from DHCP Server**.
6. Click **OK** twice, then click **Close**.

Manually Entering the IP Address of a WINS Server

Use this method to connect to a WINS server in the same workgroup or domain that is not already set up on the host.

1. In the virtual machine, right-click **My Network Places** and select **Properties**.
2. In the Network Connections window, right-click the virtual network adapter and select **Properties**.

3. In the Properties dialog box, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. In the TCP/IP Properties dialog box, click **Advanced**.
5. Click the **WINS** tab, then click **Add**.
6. In the TCP/IP WINS Server dialog box, enter the IP address for the WINS server in the **WINS server** field, then click **OK**. The IP address of the WINS server appears in the WINS addresses list on the WINS tab.

   Repeat steps 5 and 6 for each WINS server to which you want to connect from this virtual machine.
7. Click **OK** twice, then click **Close**.

Now that the virtual machine has an IP address for a WINS server, you use NetLogon in the virtual machine to log on to a domain and access shares in that domain.

For example, if the WINS server covers a domain with a domain controller, it is possible to access that domain controller from the virtual machine and add the virtual machine to the domain. You need to know the user ID and password of the Administrator on the domain controller.

Note: Your access is limited to shares of virtual machines that are on the same NAT network or are bridged on the same domain.

CHAPTER 12

Configuring Video and Sound

The following sections provide information on configuring the video display and sound for VMware ACE.

- Setting Screen Color Depth in a Virtual Machine on page 202
  - Changing Screen Color Depth on the Host on page 202
  - Changing Screen Color Depth in the Virtual Machine on page 202
- Configuring Sound on page 204
  - Installing Sound Drivers in Windows 9x and Windows NT Guest Operating Systems on page 204

Setting Screen Color Depth in a Virtual Machine

The number of screen colors available in the guest operating system depends on the screen color setting of the host operating system.

Virtual machines support

- 16-color (VGA) mode
- 8-bit pseudocolor
- 16 bits per pixel (16 significant bits per pixel)
- 32 bits per pixel (24 significant bits per pixel)

If the host is in 15-bit color mode, the guest operating system's color setting controls offer 15-bit mode in place of 16-bit mode.

If the host is in 24-bit color mode, the guest operating system's color setting controls offer 24-bit mode in place of 32-bit mode.

If you run a guest operating system set for a greater number of colors than your host operating system is using, you can encounter various problems. In some cases, for example, the colors in the guest are not correct. In others, the guest operating system is not able to use a graphical interface.

If you encounter problems, you can either increase the number of colors available on the host or decrease the number of colors used in the guest.

For best performance, use the same number of colors in the guest and on the host.

Changing Screen Color Depth on the Host

If you choose to change the color settings on your host operating system, you should first shut down the guest operating system, power off the virtual machine and close VMware ACE Manager or VMware ACE.

Follow standard procedures for changing the color settings on your host operating system, then restart VMware ACE Manager or VMware ACE and the virtual machine.

Changing Screen Color Depth in the Virtual Machine

If you choose to change the color settings in the guest operating system, the approach depends on the combination of host and guest you are using.

Follow the normal process for changing screen colors in your guest operating system. In a Windows guest, the Display Properties control panel offers only those settings that are supported.

In a Linux or FreeBSD guest, you must change the color depth before you start the X server or restart the X server after making the changes.

Configuring Sound

VMware ACE provides a sound device compatible with the Sound Blaster AudioPCI and supports sound in Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows Server 2003 and Linux guest operating systems. The VMware ACE sound device is enabled by default.

Sound support includes PCM (pulse code modulation) output and input. For example, you can play `.wav` files, MP3 audio and Real Media audio. MIDI output from Windows guests is supported through the Windows software synthesizer. MIDI input is not supported, and no MIDI support is available for Linux guests.

Windows 2000, Windows XP and most recent Linux distributions automatically detect the sound device and install appropriate drivers for it.

Installing Sound Drivers in Windows 9x and Windows NT Guest Operating Systems

Windows 95, Windows 98, Windows 98SE and Windows NT 4.0 do not have drivers for the Sound Blaster AudioPCI adapter. To use sound in these guest operating systems, you must download the driver from the Creative Labs Web site (*www.creative.com*) and install it in the guest operating system.

Creative Labs has a number of Web sites serving various regions of the world. The adapter name varies, depending on the region, but usually includes AudioPCI.

CHAPTER 13

Connecting Devices to Virtual Machines

The following sections describe how to use various devices with a virtual machine:

- Using Parallel Ports on page 207
  - Parallel Ports on page 207
  - Installation in Guest Operating Systems on page 207
  - Special Notes for the Iomega Zip Drive on page 208
- Using Serial Ports on page 209
  - Using a Serial Port on the Host Computer on page 209
  - Using a File on the Host Computer on page 209
  - Connecting an Application on the Host to a Virtual Machine on page 210
  - Connecting Two Virtual Machines on page 211
  - Special Configuration Options for Advanced Users on page 212
- Using USB Devices in a Virtual Machine on page 214
  - Notes on USB Support in VMware ACE on page 214
  - Enabling and Disabling the USB Controller on page 214

- Connecting USB Devices on page 214
- Using USB with a Windows Host on page 215
- Replacing USB 2.0 Drivers on a Windows 2000 Host on page 215
- Installing USB Devices as a Non-Administrator on page 216
- Who Has Control over a USB Device? on page 216
- Disconnecting USB Devices from a Virtual Machine on page 217
- Human Interface Devices on page 217

Using Parallel Ports

VMware ACE supports a partial emulation of bidirectional PS/2-style ports.

Parallel Ports

Parallel ports are used by a variety of devices, including printers, scanners, dongles and disk drives.

VMware ACE emulates the most commonly used functions of PS/2 hardware. However, interrupts requested by a device connected to the physical port are not passed to the virtual machine. Also, the guest operating system cannot use DMA (direct memory access) to move data to or from the port. For this reason, some devices that attach to the parallel port may not work correctly.

Installation in Guest Operating Systems

If the virtual machine is configured with a parallel port, most guest operating systems automatically detect it at installation time and install the required drivers. Some operating systems, including Linux, Windows NT and Windows 2000, automatically detect the ports at boot time. Others, like Windows 95 and Windows 98, do not.

To add a parallel port to the virtual machine's configuration, take these steps in VMware ACE Manager with the virtual machine powered off.

1. Open the virtual machine settings editor.

   VM > Settings

2. Click **Add** to start the New Hardware Wizard.
3. Select **Parallel Port**, then click **Next**.
4. Make the appropriate selection to use a physical parallel port or connect the virtual parallel port to a file.
5. If you selected **Use physical port**, use the drop-down list to choose the port that will be used on the end user's host machine.

   If you selected **Use output file**, enter the path and filename or browse to the location of the file.
6. Under **Device status**, the default setting is **Connect at power on**. Clear the check box if you want to deselect this setting.
7. Click **Finish**.

In a Windows 95 or Windows 98 guest, after you add the port, run the guest operating system's Add New Hardware Wizard (**Start** > **Settings** > **Control Panel** > **Add New Hardware**) and let Windows detect the new device.

Special Notes for the Iomega Zip Drive

On Windows 95 or Windows 98, use of older drivers for the Iomega Zip drive may cause the guest operating system to lock up intermittently at boot time or during installation of the guest operating system. The newest Iomega drivers work reliably in our tests. They are available at *www.iomega.com/software/index.html*.

Using Serial Ports

A VMware ACE virtual machine can use up to four virtual serial ports. The virtual serial ports can be configured in several ways.

- You can connect a virtual serial port to a physical serial port on the host computer.
- You can connect a virtual serial port to a file on the host computer.
- You can make a direct connection between two virtual machines or between a virtual machine and an application running on the host computer.

You can also select whether to connect the virtual serial port when you power on the virtual machine.

Using a Serial Port on the Host Computer

You can set up the virtual serial port in a virtual machine to use a physical serial port on the host computer. This is useful, for example, if you want to use a modem or a hand-held device in your virtual machine.

To install a virtual serial port that connects to a physical serial port on the host computer, take the following steps:

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.
4. Select **Use physical serial port on the host**, then click **Next**.
5. Choose the port on the host computer that you want to use for this serial connection. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 212.
6. Click **Finish**, then click **OK** to close the virtual machine settings editor.
7. Power on the virtual machine.

Using a File on the Host Computer

You can set up the virtual serial port in a virtual machine to send its output to a file on the host computer. This is useful, for example, if you want to capture the data a

program running in the virtual machine sends to the virtual serial port or if you need a quick way to transfer a file from the guest to the host.

To install a virtual serial port that connects to a file on the host computer, take the following steps:

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.
4. Select **Output to file**, then click **Next**.
5. Browse to the file on the host computer that you want to use to store the output of the virtual serial port. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 212.
6. Click **Finish**, then click **OK** to close the virtual machine settings editor.
7. Power on the virtual machine.

Connecting an Application on the Host to a Virtual Machine

You can set up the virtual serial port in a virtual machine to connect to an application on the host computer. This is useful, for example, if you want to use an application on the host to capture debugging information sent from the virtual machine's serial port.

To install a direct serial connection between an application on the host and a virtual machine, take the following steps:

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.
4. Select **Output to named pipe**, then click **Next**.
5. Use the default pipe name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`.
6. Select **This end is the server** or **This end is the client**. In general, select **This end is the server** if you plan to start this end of the connection first.
7. Select **The other end is an application**.

8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 212.
9. Click **Finish**, then click **OK** to close the virtual machine settings editor.
10. On your host computer, configure the application that communicates with the virtual machine to use the same pipe name.
11. Power on the virtual machine.

Connecting Two Virtual Machines

You can set up the virtual serial ports in two virtual machines to connect to each other. This is useful, for example, if you want to use an application in one virtual machine to capture debugging information sent from the other virtual machine's serial port.

To install a direct serial connection between two virtual machines (a server and a client), take the following steps:

In the server virtual machine

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.
4. Select **Output to named pipe**, then click **Next**.
5. Use the default pipe name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`.
6. Select **This end is the server**.
7. Select **The other end is a virtual machine**.
8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 212.

9. Click **Finish**, then click **OK** to close the virtual machine settings editor.

In the client virtual machine

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.
4. Select **Use named pipe**.
5. Use the default name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`. The pipe name must be the same on both the server and the client.
6. Select **This end is the client**.
7. Select **The other end is a virtual machine**.
8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 212.
9. Click **Finish**, then click **OK** to close the virtual machine settings editor.

Special Configuration Options for Advanced Users

Two special configuration options are available for serial connections between a virtual machine and the host or between two virtual machines. These options are of interest primarily to developers who are using debugging tools that communicate over a serial connection.

Improving CPU Performance when Debugging

The first option must be set in the virtual machine settings editor. This option is useful when the serial port is being used by the guest operating system in polled mode as opposed to interrupt mode. Polled mode causes the virtual machine to consume a disproportionate share of CPU time. This makes the host and other guests run sluggishly.

To restore performance for applications on the host, in the virtual machine settings editor, select the virtual serial port, and check the **Yield CPU on poll** check box. This configuration option forces the affected virtual machine to yield processor time if the only task it is trying to do is poll the virtual serial port.

Changing the Input Speed of the Serial Connection

To use the second option, power off the virtual machine and close the VMware ACE Manager window, then use a text editor to add the following line to your virtual machine's configuration file:

```
serial<n>.pipe.charTimePercent = <x>
```

This option is useful if you want to squeeze every possible bit of speed from your serial connection over a pipe to the virtual machine. In principle, there is no limit on the output speed — the speed at which the virtual machine sends data through the virtual serial port. In practice, the output speed depends on how fast the application at the other end of the pipe reads data coming into it.

`<n>` is the number of the serial port, starting from `0`. So the first serial port is `serial0`.

`<x>` is any positive integer. It specifies the time taken to transmit a character, expressed as a percentage of the default speed set for the serial port in the guest operating system. For example, a setting of `200` forces the port to take twice as long per character, or send data at half the default speed. A setting of `50` forces the port to take only half as long per character, or send data at twice the default speed.

You should first use the guest operating system to configure the serial port for the highest setting supported by the application you are running in the virtual machine.

Once the serial port speed is set appropriately in the guest operating system, experiment with this setting. Start with a value of `100` and gradually decrease it until you find the highest speed at which your connection works reliably.

Using USB Devices in a Virtual Machine

VMware ACE provides a two-port USB 1.1 controller. You can use up to two USB devices in your virtual machine if both your host operating system and your guest operating system support USB. If your host computer supports USB 2.0 devices, you can use those devices in the virtual machine.

Although your host operating system must support USB, you do not need to install device-specific drivers for your USB devices in the host operating system if you want to use those devices only in the virtual machine.

On a Windows 2000 host computer with USB 2.0 support, be sure you are using the Microsoft USB 2.0 driver for the USB controller. Third-party USB 2.0 drivers, such as those provided by some motherboard manufacturers, are not supported. For notes on replacing the third-party drivers, see Replacing USB 2.0 Drivers on a Windows 2000 Host on page 215.

Notes on USB Support in VMware ACE

We have tested a variety of USB devices with this release. In general, if the guest operating system has appropriate drivers, you should be able to use PDAs, printers, storage (disk) devices, scanners, MP3 players, digital cameras and memory card readers.

Modems and certain streaming data devices, such as speakers and Web cams, do not work properly.

Enabling and Disabling the USB Controller

The virtual machine's USB ports are enabled by default. If you will not use USB devices in a virtual machine, you can disable its USB controller using the virtual machine settings editor.

Connecting USB Devices

When a virtual machine is running, its window is the active window and a USB device is plugged into the host computer, the device automatically connects to the guest instead of the host. This autoconnect feature can be disabled in the USB Controller panel of the virtual machine settings editor (**VM** > **Settings**). If all of the virtual machine's USB ports are already occupied when it is trying to connect automatically to a new device, a dialog box gives you a choice: you can either disconnect one of the existing USB devices to free its port or ignore the new device, allowing the device to connect to the host.

Choose **VM** > **Removable Devices** to connect specific USB devices to your virtual machine. You can connect up to two USB devices at a time. If the physical USB devices are connected to the host computer through a hub, the virtual machine sees only the USB devices, not the hub.

There is a menu item for each of the USB ports. Move the mouse over one of these items to see a cascading menu of devices that are plugged into your host computer and available for use. To connect a device to the virtual machine, click its name.

If a device is already connected to that port, click the name of a new device to release the first device and connect the new one.

To release a connected device, click **None** on the cascading menu for the port to which it is connected.

If you physically plug a new device into the host computer and the autoconnect feature does not connect it to a virtual machine, the device is initially connected to the host. Its name is also added to the **VM** > **Removable Devices** menu so you can connect it to the virtual machine manually.

Using USB with a Windows Host

Windows 2000, Windows XP and Windows Server 2003 hosts: When a particular USB device is connected to a virtual machine for the first time, the host detects it as a new device named VMware USB Device and installs the appropriate VMware driver.

Windows XP and Windows Server 2003 hosts: User confirmation is required in the Found New Hardware Wizard. Select the default action — **Install the software automatically**. Once the software is installed, the guest operating system detects the USB device and searches for a suitable driver.

When you are synchronizing a PDA, such as a Palm handheld or Handspring Visor, to a virtual machine for the first time, the total time required to load the VMware USB device driver on the host and the PDA driver in the guest may exceed the device's connection timeout value. This causes the device to disconnect itself from the computer before the guest can synchronize with it. If this occurs, let the guest finish installing the PDA driver, dismiss any connection error warnings, then try synchronizing the PDA again. The second attempt should succeed.

Replacing USB 2.0 Drivers on a Windows 2000 Host

To use VMware ACE on a Windows 2000 host that has USB 2.0 ports, you must use the Microsoft USB 2.0 drivers for the USB controller in the host operating system. If your host operating system is using a third-party driver — a driver supplied by your motherboard vendor, for example — you must replace it.

Take the following steps to check the provider of your driver:

1. Go to the Device Manager. Right-click **My Computer**, choose **Properties**, click the **Hardware** tab, then click **Device Manager**.
2. Expand the listing for Universal Serial Bus controllers.
3. Right-click the listing for the controller and choose **Properties**.
4. Click the **Driver** tab. If the driver provider shown on that page is Microsoft, you have the correct driver already.

If the driver provider is not Microsoft, download the latest USB driver for your host operating system from the Microsoft Web site and follow the Microsoft instructions to install it. Details are available in Microsoft knowledge base article 319973.

Installing USB Devices as a Non-Administrator

Any user on a Windows host can connect USB devices for use in a virtual machine. You do not need administrative privileges on the host to connect a USB device to a virtual machine.

Note: A USB device must be installed on the host before it can be used in a virtual machine.

Who Has Control over a USB Device?

Only one computer — host or guest — can have control of a USB device at any one time.

Device Control on a Windows Host

When you connect a device to a virtual machine, it is "unplugged" from the host or from the virtual machine that previously had control of the device. When you disconnect a device from a virtual machine, it is "plugged in" to the host.

Caution: On Windows 2000, Windows XP and Windows Server 2003 hosts, you need to take a special step to disconnect USB network and storage devices from the host. There is a system tray icon called Eject Hardware on Windows 2000 and Safely Remove Hardware on Windows XP and Windows Server 2003. Use this icon to disconnect the device from the host before connecting it to a virtual machine.

Note: On Windows 2000, Windows XP and Windows Server 2003 hosts, when you connect a USB network or storage device in a virtual machine, you may see a message on your host that says the device can be removed safely. This is normal behavior, and you can simply dismiss the dialog box. However, do not remove the device from your physical computer. VMware ACE automatically transfers control of the device to the virtual machine.

Under some circumstances, if a USB storage device is in use on the host (for example, one or more files stored on the device are open on the host), an error appears in the virtual machine when you try to connect to the device. You must let the host complete its operation or close any application connected to the device on the host, then connect to the device in the virtual machine again.

Disconnecting USB Devices from a Virtual Machine

Before unplugging a USB device or using the **VM** > **Removable Devices** menu to disconnect it from a virtual machine, be sure it is in a safe state.

You should follow the procedures the device manufacturer specifies for unplugging the device from a physical computer. This is true whether you are physically unplugging it, moving it from host to virtual machine or moving it from virtual machine to host.

This is particularly important with data storage devices (a Zip drive, for example). If you move a data storage device too soon after saving a file and the operating system has not actually written the data to the disk, you can lose data.

Human Interface Devices

USB human interface devices, such as the keyboard and mouse, are not handled though the virtual machine's USB controller. Instead, they appear in the virtual machine as a standard PS/2 keyboard and mouse, even though they are plugged into USB ports on the host.

CHAPTER 14

Understanding Policies

Policies are at the heart of managed virtual machines. They give you control over many aspects of your end users' experience. The following sections provide background information on how to determine which policy settings are appropriate for your environment and how to create your own plug-ins to apply custom policies.

- Taking Advantage of Policies on page 220
- Encryption and Authentication Policies on page 222
- Expiration Policies on page 224
- Copy Protection Policies on page 225
- VMware ACE Policies on page 226
- Network Quarantine Policies on page 230
- Using Advanced Network Quarantine on page 234
- Writing Plug-In Policy Scripts on page 244

Taking Advantage of Policies

With policies, you can specify what controls your end users see when they launch VMware ACE, how long they may run a particular virtual machine, what parts of your organization's network they are allowed to use from the virtual machine and many other capabilities of the VMware ACE application and the virtual machine it runs for the end user.

You set policies with the policy editor. You can run the policy editor immediately after you create a new virtual machine or launch it later from the project or virtual machine summary display in VMware ACE Manager. For details on how to use the policy editor, see Setting Policies for a Project on page 71.

You can change some or all of the policies for a VMware ACE virtual machine at any time by editing the policies, then creating and distributing a new package that contains only the policies.

For some policies, you can effectively make changes at any time, without deploying a new package to your end users. The following examples describe some of the things you can do:

- **Authentication:** If you authenticate users based on users and groups in your Active Directory service, you can change the access list for a virtual machine at any time. VMware ACE Manager stores the changes in your Active Directory service, and all installations of that virtual machine will respect the new access list the next time end users launch them. For more information, see Encryption and Authentication Policies on page 222.
- **Network quarantine:** With most of the network quarantine options, you can change network access at any time. Use dynamic quarantine, conditional quarantine or custom quarantine and specify that the access list governing network access is stored on a Web server or in your Active Directory service. You can then modify the access list at any time, using VMware ACE Manager, and the affected virtual machines will respect the new network quarantine conditions the next time they connect to the network. For more information, see Network Quarantine Policies on page 230.

The policies you set for a project are stored in a policy (`.vmpl`) file with a filename corresponding to that of the virtual machine's configuration (`.vmx`) file. The policy file is stored in the directory that stores the project files. Policies can be changed by anyone running VMware ACE Manager who has permission to modify the file.

Note: If you store policies on your Active Directory server, you must be sure end users' host computers have been added to the domain where the policies are stored

and end users must log on to that domain so VMware ACE has access to the policies. Similarly if you set policies based on users and groups in your Active Directory domain, end users' host computers must log on to a domain where those users and groups are defined.

If you store policies on your Active Directory server, they are stored in a container called VMware directly under the top hierarchy of the domain controller container. By default, this container is not visible in the MMC console. To view the container, in Manage Active Directory Users and Computers, enable advanced features (**View** > **Advanced Features**).

Encryption and Authentication Policies

Encryption policies control how a virtual machine's files are stored. Authentication policies control who is allowed to use the virtual machine.

Encrypting a Virtual Machine's Files

If you specify that the virtual machine should be encrypted, the VMware ACE installer encrypts the virtual machine's files, including the configuration file and the virtual disk files, when it installs VMware ACE on the end user's computer. The encryption key is different on each computer.

Encryption is especially useful for virtual machines that may be used on portable computers and may contain sensitive information. By encrypting the virtual machine, you protect the data files even if the computer is lost or stolen.

The end user of the virtual machine does not have to think about the encryption. The end user must use some method of authentication to run VMware ACE, which then handles the details of encrypting and decrypting the files as needed.

Determining the Authentication Policy

VMware ACE provides several methods for authenticating users. If you select an authentication method, VMware ACE will not run until the user is authenticated.

No Authentication

If you select **None** in the policy editor, no authentication is required to launch VMware ACE and run the virtual machine.

This setting is appropriate only if the virtual machine has no access to sensitive information and should be widely available. For example, this setting might be appropriate for distributing virtual machines containing demonstrations you want to make available without restrictions.

Note: If you want to encrypt the virtual machine, you must require some form of authentication.

Password Authentication

If you select password authentication, each end user must set a password the first time VMware ACE runs and enter that password each time VMware ACE runs.

Password authentication may be appropriate in various circumstances — especially if end users need to run VMware ACE when they are not connected to your organization's network.

If end users forget their passwords, they can create hot fix requests and send them to a designated administrator. The administrator can reset the password using VMware ACE Manager and provide the hot fix to the end user. The end user double-clicks the hot fix file to apply it, then runs VMware ACE and sets a new password. For more information on hot fixes, see Responding to Hot Fix Requests on page 150.

Authentication for Active Directory Users and Groups

If you select authentication based on Active Directory users and groups, VMware ACE ensures that the user currently logged on to the host computer is authorized to run the virtual machine. If not, VMware ACE does not start.

Authentication for users and groups is appropriate only if end users are logged on to an Active Directory domain, generally on a LAN.

If you select this means of authentication, you can change the list of authorized users for any virtual machine at any time. To do so, run VMware ACE Manager, open the appropriate project and use the policy editor to change the list of authorized users. VMware ACE Manager saves the updated list to your Active Directory service.

Authentication Determined by a Plug-In Script

To apply your own tests for authentication, you may write a custom plug-in, using any scripting language that can run on the end user's host computer. For more information, see Writing Plug-In Policy Scripts on page 244.

Expiration Policies

You can use expiration policies to limit the lifetime of a virtual machine. You may find this useful, for example, if you need to provide a computing environment for a contractor and want to be sure it can be used only for the duration of the contract. Setting a virtual machine to expire can also be useful if you want to provide a time-limited demonstration to potential customers.

In the policy editor, you may select one of the following options for expiration:

- **Never** — The virtual machine does not expire.
- **After x days from installation** — The virtual machine runs for the specified number of days after the package is installed, then cannot be used. Consider this option for such uses as time-limited demonstrations.
- **On this date** — The virtual machine runs until and on the specified date. It cannot be used after the specified date. Consider this option for such uses as computing environments for contractors.

You can extend the life of an expired virtual machine in three ways.

- You can create your own plug-in — a renewal script you specify in the policy editor. That script is distributed with the VMware ACE package. For example, you can design the plug-in to query a server on your network and, based on the results of that query, do one of the following:
  - Make no change.
  - Renew the virtual machine for a specified number of days.
  - Renew the virtual machine until a specific date.
  - Set the virtual machine so it never expires.
  - Expire the virtual machine.

  For more information on creating your own plug-in, see Writing Plug-In Policy Scripts on page 244.
- You can use the policy editor to change the expiration date, then create a new VMware ACE package containing only the updated policies. When your end users install the new package, they get the new expiration date.
- If an end user sends you a hot fix request asking for an extension, you can send a hot fix with a different expiration setting.

Copy Protection Policies

Copy protection policies let you ensure that a virtual machine can run only from the location where the VMware ACE installer placed it.

To apply this copy protection, select **Copy protect this virtual machine** as the copy protection policy in the policy editor.

If you copy protect a virtual machine, it is still possible for the virtual machine's files to be moved or copied. However, the copy-protected virtual machine cannot run from the new location.

VMware ACE Policies

VMware ACE policies apply to the VMware ACE application itself. These policies allow you to give end users more or less control over certain VMware ACE functions. There is also a policy that gives you privileged access to the virtual machine on the end user's computer so you can change configuration settings.

Troubleshooting Policies

The troubleshooting policies determine whether certain options appear on the VMware ACE menu.

- Under Power commands, you may select **Enable Reset and Power Off commands**. If you enable these commands, the end user may power off or reset the virtual machine from the menu in VMware ACE (**VMware ACE** > **Troubleshoot** > **Reset** or **VMware ACE** > **Troubleshoot** > **Power Off and Exit**). The effect of the reset command available from the menu is similar to that of the hardware reset button on a physical computer.

  If you do not enable these menu commands, the end user normally shuts down the virtual machine by clicking the exit button on the VMware ACE window or toolbar — the X in the upper-right corner. In this case, VMware ACE suspends the virtual machine, rather than powering it off.

  Also, if you do not enable these menu commands, the end user still has access to the guest operating system's shutdown and restart commands. If the end user uses the guest operating system's shutdown command, VMware ACE closes after the operating system shuts down. The next time the end user starts VMware ACE, the virtual machine powers on and goes through a complete boot cycle.

- Under Revert to installed image, you may select **Enable revert to installed virtual machine image**. If you enable this feature, VMware ACE captures an image of the virtual machine at the time it is installed on the end user's machine. The end user may then revert to this original state by choosing **VMware ACE** > **Troubleshoot** > **Revert to the Installed <vmname> Environment**, where <vmname> is the name of the virtual machine.

  The virtual machine image is similar to a snapshot. It includes the state of the virtual machine's disks., the contents of the virtual machine's memory and the virtual machine settings.

  If an end user chooses **Revert to the Installed <vmname> Environment**, a warning message appears. It cautions that all changes to the virtual machine will

be lost and urges the user to take this action only if advised to do so by a system administrator.

Note: If the virtual machine uses password authentication, reverting to the installed environment returns the virtual machine to its state after the initial password was selected. If you enable this feature, you should also consider implementing hot fixes so you can respond easily if end users revert and have forgotten their original passwords.

VMware ACE Window Policies

Under VMware ACE Window, you may select **Always run maximized**. If you select this policy, VMware ACE fills the full screen when it starts and hides the host operating system. Thus the end user sees only one environment — the virtual machine or the host operating system — occupying the entire screen at any one time. You may find this useful, for example, to avoid user confusion about the differences between the two environments.

The end user can minimize the VMware ACE display and return to the host operating system by clicking the minimize button on the toolbar. If the mouse pointer is not available, pressing Ctrl-Alt minimizes the display.

Easy Printer Setup Policies

Under **Easy printer setup** you may select **Enable Add Printer command** to provide an Add Printer item on the VMware ACE menu. This menu choice makes it much easier for an end user to configure a local printer connected to the host computer so it can be used in a Windows guest operating system.

Easy printer setup displays a list of all printers configured on the host, both locally connected printers and network printers, and the end user may choose freely from that list. If the list includes network printers available to the host, special steps may be needed to use those printers from the guest operating system.

Network Printers Requiring Authentication

Users may need to log on to a print server or otherwise authenticate themselves before using a network printer. The following points describe how to deal with the most common cases:

- The guest operating system and the host operating system are configured as members of the same domain. Easy printer setup should work with no difficulties.

- You know in advance which printer the end user needs to use. If you configure the printer in the guest operating system before you create the package, the end user does not need to configure the printer.
- The printer requires authentication and is not yet set up in the guest operating system. Easy printer setup does not work. The end user must follow the normal steps to set up a network printer in the guest operating system.

Host and Guest Operating Systems with Different DNS Settings

If the host and guest operating systems have different DNS settings, easy printer setup may be unable to add a network printer that is configured on the host. This is particularly likely if the virtual machine is configured to use NAT networking, because in that case the host and guest operating systems are configured to be in different domains.

If host and guest are in different domains and the printer name that appears in the host operating system is not fully qualified with a domain name, easy printer setup may not be able to connect the printer to the guest operating system.

The easiest way to resolve this problem is to be sure the DNS settings for both host and guest use the same search path. In particular, it is important that the guest operating system's search path include the domain in which the printer is located.

User Preferences Policies

The user preferences policies allow you to specify what settings are available to end users in the VMware ACE Preferences dialog box.

Allow users to modify the exit behavior of the application — This option makes the exit behavior settings available in the VMware ACE Preferences dialog box. If these settings are available, the end user can control what happens when VMware ACE receives an exit command, either from the menu or from a click on the X in the upper right of the window or toolbar.

The exit behavior preferences allow the end user to specify the following:

- Confirm before exiting the application — When the end user gives the command to exit VMware ACE, a dialog box appears. The end user may confirm the intention to exit VMware ACE or click **Cancel** to continue working.

The end user may also control the state of the virtual machine when it exits.

- Suspend the virtual machine — This is the default behavior. VMware ACE suspends the virtual machine and closes. The next time the end user launches VMware ACE, the virtual machine resumes operation from the point where it was suspended.

- Power off the virtual machine — VMware ACE powers off the virtual machine. The next time the end user launches VMware ACE, the virtual machine starts from a powered off state and the guest operating system boots.

Administrator Access Policy

The administrator access policy allows you to set an administrator password so you can run the virtual machine in a special troubleshooting application on the end user's computer and make changes to the virtual machine's configuration. This can be useful for troubleshooting and correcting problems that may arise in a particular end user's setup.

If you enable administrator access, you can launch the troubleshooting application with the following command:

```
vmware -k <path>\<vmname>.vmx
```

Include the full path to the virtual machine's configuration file.

Enter the administrator password in the password dialog box. You may then make any needed changes in the virtual machine settings editor (VM > Settings).

Note: Administrator access is not available for encrypted virtual machines.

Network Quarantine Policies

Network quarantine policies give you fine-grained control over the network access you provide to users of your virtual machines.

Using a packet filtering firewall, the network quarantine feature of VMware ACE lets you specify exactly which machines or subnets a virtual machine may access. This means that you can, for example, configure the virtual machine so it is allowed to connect only to your VPN server, which then controls access to other resources.

Network quarantine rules can be dynamic. This means, for example, that you can quickly lock virtual machines out of all or part of your network to help combat the spread of a worm or virus without deploying updated packages.

You can also set different network quarantine policies for virtual machines based on a version you assign. This means you can, for example, give out-of-date virtual machines access to the server that provides a required patch or software update but not to other parts of your network.

You set and modify network quarantine policies with a wizard. Open the policy editor from the Commands list on the project or virtual machine details page, select **Network quarantine**, select **Quarantined access to specific networks and machines**, then click **Network Quarantine Wizard**.

The following sections provide background on some of the decisions you make as you set network quarantine policies for a virtual machine. For step-by-step instructions on using the Network Quarantine Wizard, see Setting Network Quarantine Policies on page 85.

Selecting the Type of Network Quarantine

The following four types of network quarantine are available:

- **Static quarantine** — You specify a single list of approved or disapproved networks and machines. The list is stored with the virtual machine and distributed as part of the package. If you need to make any changes in the future, you must create a package containing at least the policies for the affected virtual machine and distribute the update to your users.

  Static quarantine is somewhat simpler to configure and may be the most convenient choice if you do not plan to change the access list.

- **Dynamic quarantine** — You specify a single list of approved or disapproved networks and machines. The list is stored on a server. Each time the virtual machine runs, and at regular intervals while it is running, it checks the server

and retrieves the list. If you need to make any changes in the future, you update the list stored on the server.

Dynamic quarantine gives you the flexibility to modify the access list at any time you need to make changes. If you are using Active Directory and choose to store the access list in your Active Directory service, VMware ACE Manager stores your updates on the server for you. If you use a Web server to store the access list, VMware ACE Manager creates the file, which you must then copy to the specified location on the Web server.

- Version-based quarantine — You specify two lists of approved networks and machines. One list is used for virtual machines that have a network quarantine version approved for normal access. The other list is used for virtual machines with versions that do not qualify for normal access. The lists are stored on a server. Each time the virtual machine runs, and at frequent intervals while it is running, it contacts the server and provides its network quarantine version. Based on that version, the server provides the appropriate list of approved networks and machines. If you need to make any changes to the lists or the network quarantine version in the future, you do so by updating the information stored on the server.

  Like dynamic quarantine, version-based quarantine gives you the flexibility to modify the access lists at any time you need to make changes. In addition, version-based quarantine allows you to impose special restrictions on virtual machines that do not meet the current criteria for normal access — for example, allowing them to communicate only with an update server.

  If you are using Active Directory and choose to store the access lists in your Active Directory service, VMware ACE Manager stores your updates on the server for you. If you use a Web server to store the access lists, VMware ACE Manager creates the files, which you must then copy to the specified location on the Web server.

  Note: VMware Tools provides services that are essential for version-based quarantine. This means you cannot use version-based quarantine with guest operating systems such as MS-DOS and Windows 3.1

- Custom quarantine using script — You develop your own plug-in, using any scripting language that can run on the end user's machine, to apply the tests you need to apply and return results that indicate whether access should be restricted. Rules can be stored statically or dynamically. Custom quarantine is useful, for example, if you need to integrate your deployment with third-party

compliance detection software. For more information, see Writing Plug-In Policy Scripts on page 244.

Note: VMware Tools provides services that are essential for custom quarantine. This means you cannot use custom quarantine with guest operating systems such as MS-DOS and Windows 3.1

Specifying Access to Networks and Machines

You may allow a virtual machine unrestricted network access, or you may limit access to specified machines or parts of the network. Depending on your network configuration and the type of access you need to specify, you may use a whitelist or a blacklist. You must use one or the other consistently for any one virtual machine. You cannot mix whitelists and blacklists for one virtual machine.

You can specify access in the following ways:

- Allow or deny access to an individual machine using its IP address.
- Allow or deny access to an individual machine using its machine name; the Network Quarantine Wizard looks up the machine's IP address in DNS and inserts the address for you.
- Allow or deny access to a subnet; you enter the starting address, select **Subnet mask** and enter the subnet mask in the field.

You may enter as many items as you like in the list. You may use any mix of machine IP addresses, machine names and subnets.

In the Networks and Machines panel, you do not need to include network addresses needed for printers or for DHCP and DNS servers. You can allow network traffic for those purposes in separate panels.

Allowing Access for Printer, DHCP, DNS and ICMP Traffic

The Network Traffic panel allows you to create special-purpose exceptions to the restrictions configured on the Networks and Machines panel. You may specify that certain types of network traffic may go to and from machines and subnets outside the access list you created on the Networks and Machines panel. This is useful, for example, if virtual machine users are restricted to a particular subnet but the DNS server on your network is not on that subnet.

- **Printer access** — Select this option to be sure a Windows virtual machine can use local and network printers available on the host. Be sure to select this option if you configure the virtual machine to allow easy printer setup. Easy printer setup uses network sharing to connect the virtual machine to a printer configured on the host computer.

- **DHCP packets** — Select this option if the virtual machine needs to get its IP address from a DHCP server that is not included in the access list.
- **DNS packets** — Select this option if the virtual machine needs to resolve IP addresses using a DNS server that is not included in the access list.
- **ICMP packets** — Select this option if you need support for the ping command — for example, to check network connectivity to and from the virtual machine.

Storing Access Lists for Network Quarantine

If you use dynamic quarantine or version-based quarantine, you select the type of server you want to use to store the list of approved networks and machines. You may also use a server to store access lists if you are using custom quarantine based on a script. VMware ACE checks the list on this server to determine what network access is approved for the virtual machine. You have the following options:

- **Active Directory server** — Select this option if you plan to store the network quarantine list on your Active Directory server. The Network Quarantine Wizard adds this information to your Active Directory server for you.
- **Web server** — Select this option if you plan to store the network quarantine list on a Web server. The wizard creates the file for you. Depending on the choices you make on the Policy Lookup panel, the wizard copies the file to the Web server for you or prompts you to copy it.

To update a network quarantine list, open the appropriate virtual machine and run the Network Quarantine Wizard again. You may go directly to the Networks and Machines panel for normal access or restricted access. Make the necessary changes on one panel or both, then click **Finish**. If you store the network quarantine list on a Web server, copy the new file to the server. You do not need to send any updates directly to your end users.

Using Advanced Network Quarantine

Advanced network quarantine features allow you to control the host computer's access to the network. This is useful if you want to give the virtual machine access to the network but block or restrict host computer access.

You can apply different policies to the host computer based on the network to which the host is attached.

Advanced network quarantine features also allow you to apply different policies to the virtual machine based on the network to which the host is attached.

For example, a mobile worker using an unmanaged laptop computer may have VMware ACE installed and use the virtual machine, which you manage, to connect to a corporate VPN from remote locations. When the mobile worker comes to the corporate office, you may regard the unmanaged laptop computer as a security risk, because you do not know whether the host operating system is infected by viruses. Using advanced network quarantine, you can block the host operating system from the network but still allow the guest operating system running in VMware ACE to connect to the corporate VPN — or even allow the guest to have full network access.

Note: You can use advanced network quarantine features only if you select **Quarantined access to specific networks and machines** in the policy editor, then select **Static quarantine** in the Network Quarantine Wizard. You cannot use these features if you select **None** in the network quarantine pane of the policy editor, and you cannot use them with dynamic, version-based or custom network quarantine.

To take advantage of advanced network quarantine, you must use a text editor to make changes to one or more policy files.

Depending on the policies you want to establish, you must add some or all of the following:

- Zone descriptions — Define characteristics that clearly identify each network for which you want to set advanced network quarantine policies. These settings go in `app.vmpl` in the main folder for the project. For details, see Defining Zones on page 235.
- Host policies — For each zone you have defined, you may set policies to enable or restrict the host computer's network access when it is connected to that network zone. These settings go in `app.vmpl` in the main folder for the project. For details, see Defining Host Policies on page 237.
- Guest policies — For each zone you have defined, you may set policies to control the virtual machine's network access when the host computer is

connected to that network zone. These settings go in `<vmname>.vmpl` in the affected virtual machine's folder inside the project folder. For details, see Defining Guest Policies on page 240.

Defining Zones

Zone descriptions describe the characteristics of a network zone. VMware ACE examines the network or networks directly connected to network adapters on the host computer to see if there is a match for all the criteria in any of the zone definitions. If there is a match, the policies for that zone are enforced.

The characteristics you can define in the zone descriptions include such things as IP addresses for a subnet, IP addresses of certain key servers on the network, and DNS names for machines or networks.

Choose the characteristics you specify carefully.

There are trade-offs between using shorter and longer lists of parameters.

If you use a longer list, you minimize the chances of a "false-positive" or a misidentification. This can be important if you are providing a VMware ACE package to someone who connects a host computer to multiple networks at different times. If one of the other networks matches the characteristics you define in the zone definition, the host policies are applied — even if the host is not connected to your network.

In some cases, however, using a longer list may also increase the likelihood that an end user could circumvent the detection mechanism — for example, switching the host to use static IP instead of DHCP and configuring the host with only a subset of the characteristics defined for your zone (for example, only IP address, or IP address and DNS server information).

Another point to consider is that the addresses or names of certain servers may change over time. Such changes may also introduce detection issues.

Using a smaller set of information — for example, using only the IP address and netmask — in a zone description lessens the chance that the detection mechanism will fail to restrict a host or guest that should be restricted, but it also increases the chance that a false positive or misidentification can occur. Such false positives are especially likely if your network is using a common netblock, such as 10/8, 172.16/12 or 192.168/16, that is also used by other networks.

Exit VMware ACE Manager if it is running, then use a text editor to add the zone descriptions to `app.vmpl` in the main folder for the project.

Each zone description must start with the following:

```
zoneDescription.<zone_number>.present = "1"
zoneDescription.<zone_number>.key = "<zone_number>"
zoneDescription.<zone_number>.name = "<zone_name>"
```

The value of <zone_number> starts at zero and increments sequentially. The value of <zone_name> is a descriptive name of your choice. The first two zone descriptions might start with sections similar to the following:

```
zoneDescription.0.present = "1"
zoneDescription.0.key = "0"
zoneDescription.0.name = "Corporate HQ"

zoneDescription.1.present = "1"
zoneDescription.1.key = "1"
zoneDescription.1.name = "Eastern Region Office"
```

The value of key matches the number used as part of the parameter names in each group.

Each zone description must contain one or more of the following parameters describing the characteristics of the zone:

zoneDescription.<zone_number>.subnets = "<IP_address>/<subnet>"
This parameter specifies an IP address or subnet range that is used by the network. The value may be a comma-separated list of IP addresses and subnets. The value of <subnet>, if you include it, must be the number of bits in the netmask. Do not use any spaces in the comma-separated list. A network adapter matches this condition if it is using an IP address that lies within any of the specified ranges.

zoneDescription.<zone_number>.domainName = "<domain_name>"
This parameter specifies the domain name of the network — for example, mycompany.com. Only one entry may be used. You may not use a list of entries. The interpretation of this parameter is governed by the value of domainNameExactMatch (below).

zoneDescription.<zone_number>.domainNameExactMatch = "1"
This parameter modifies the domainName option (above). It specifies whether the domain name must exactly match <domain_name> or whether a match should be scored anytime the string contains <domain_name>. For example, if the value of this parameter is 1, then corp.mycompany.com is not considered a match for mycompany.com. If the value of this option is 0, then corp.mycompany.com is considered a match for mycompany.com. The default value is 0.

zoneDescription.<zone_number>.dhcpServers = "<IP_address>"
This parameter specifies one or more IP addresses for DHCP servers on the network,

using a comma-separated list with no spaces. A network adapter matches this condition if it is using at least one of these servers.

`zoneDescription.<zone_number>.gateways = "<IP_address>"`
This parameter specifies one or more IP addresses for default gateways on the network, using a comma-separated list with no spaces. A network adapter matches this condition if it is using at least one of these gateways.

`zoneDescription.<zone_number>.dnsServers = "<IP_address>"`
This parameter specifies one or more IP addresses for DNS servers on the network, using a comma-separated list with no spaces. A network adapter matches this condition if it is using at least one of these servers.

`zoneDescription.<zone_number>.minDnsServersToMatch = "<number>"`
This parameter modifies the `dnsServers` parameter (above). A network may have multiple DNS servers, and a host may be configured to use more than one DNS server. If the value of this option is greater than `1`, the host must be using the specified number of DNS servers on the list before a network adapter is considered to be on the defined network.

`zoneDescription.<zone_number>.winsServers = "<IP_address>"`
This parameter specifies one or more IP addresses for WINS servers on the network, using a comma-separated list with no spaces. A network adapter matches this condition if it is using at least one of these servers.

`zoneDescription.<zone_number>.minWinsServersToMatch = "<number>"`
This parameter modifies the `winsServers` parameter (above). A network may have multiple WINS servers, and a host may be configured to use more than one WINS server. If the value of this option is greater than `1`, the host must be using the specified number of WINS servers on the list before a network adapter is considered to be on the defined network.

Defining Host Policies

The host policies you can define for each zone may establish either whitelists — networks and machines to which connections are allowed — or blacklists — networks and machines to which connections are prohibited.

Note: Even when the host is otherwise blocked from all access to the network, it is allowed to communicate with DNS and DHCP servers so the zone detection mechanism can function properly.

Note: Any restrictions on the host's network access also restrict network access for a virtual machine using NAT networking, because the NAT connection is affected by all the policies you apply to the host. If you impose host quarantine rules, you may prefer

to use bridged networking. Or if you are using NAT networking, give the host access to the network resources required by the virtual machine. For example, you may want to allow the host — and thus the virtual machine — to connect to a VPN server. The VPN server then controls access to additional resources. In addition, if you have set authentication or device connection policies that require access to a particular server, you must allow host access to that server.

Caution: Host quarantine settings may conflict with settings in certain other software running on the host computer — for example, software firewalls. For information on configuring software on the host computer to avoid these conflicts, see *www.vmware.com/info?id=110*.

Exit VMware ACE Manager if it is running, then use a text editor to add the host policies to `app.vmpl` in the main folder for the project.

To enable the host quarantine feature you must add the following line to the file:

```
host.useZones = "1"
```

By default, the host is allowed full network access. The options to disable this default are described below. Every host zone policy must start with the following lines:

```
host.zone.<zone_number>.present = "1"
host.zone.<zone_number>.key = "<zone_number>"
host.zone.<zone_number>.descriptionName = "<zone_name>"
```

The value of `<zone_number>` starts at zero and increments sequentially. The first two host policy sections might start with sections similar to the following:

```
host.zone.0.present = "1"
host.zone.0.key = "0"
host.zone.0.descriptionName = "Eastern Regional Office"

host.zone.1.present = "1"
host.zone.1.key = "1"
host.zone.1.descriptionName = "Corporate HQ"
```

The value of `key` matches the zone number used as part of the parameter names in each group.

The value of `descriptionName` must match the name specified in the zone description you want to use. The number for `<zone_number>`, however, is independent of the zone numbers in the zone description. The value of the zone number in this section — the value of the `host.zone` parameter — determines the order in which VMware ACE searches the zones for a match. When it finds a match, it applies the policies defined for the zone with the same zone name and stops searching.

This approach allows you to specify the host zones in a different order from that in the list of zone descriptions.

Using the examples above, VMware ACE first searches for a match for the Eastern Regional Office zone description (`zone.description.1` criteria in the zone descriptions). If it finds a match, it applies the host quarantine policies defined for `host.zone.0`.

You may specify the following policies for each zone:

`host.zone.<zone_number>.blockIPv4 = "1"`
This policy specifies whether IPv4 network traffic should be blocked. If you add this policy with a value of `1`, IPv4 traffic is blocked. The policy defaults to `0`, which allows IPv4 traffic.

Note: The advanced network quarantine features have not been tested with IPv6. Use of these features in an IPv6 environment is not supported.

`host.zone.<zone_number>.exceptions.IPv4 = "<dns_name_or_IP>"`
This policy specifies a list of exceptions to the policy specified by the `blockIPv4` settings. You may mix DNS names and IP addresses in a comma-separated list. Do not use any spaces in the comma-separated list. For each item in the list, you may specify a subnet — for example, `/24` — if you wish. You may specify subnets for both IP addresses and DNS names. When you specify `blockIPv4 = "1"`, the list is a whitelist. When you specify `blockIPv4 = "0"`, the list is a blacklist.

```
host.zone.<zone_number>.restrictARP = "0"
host.zone.<zone_number>.restrictDHCP = "0"
host.zone.<zone_number>.restrictDNS = "0"
host.zone.<zone_number>.restrictICMP = "0"
```
These policies may appear in the policy file and are set to `0` by default. Do not change these defaults, which are required for the zone detection feature to work properly.

Defining Modified Default Host Policies

By default, the host computer has network access. This default and other defaults can be changed by specifying a default policy. To specify a modified set of default policies, use the same parameters that are described in this section, except substitute the prefix `host.default` for the prefix `host.zone.<zone_number>` shown in the descriptions above. You can specify new defaults for `blockIPv4` and `exceptions.IPv4`. You do not need to specify the parameters `present`, `key` or `descriptionName` when you set these defaults; do not use them with the `host.default` prefix.

Defining Guest Policies

If you want to enforce different network quarantine policies in the guest operating system based on the network zone to which the host computer is attached, you must use a text editor to make changes in the virtual machine's policy file — `<vmname>.vmpl` in the affected virtual machine's folder inside the project folder.

Take the following steps:

1. Before editing `<vmname>.vmpl`, launch the Network Quarantine Wizard from the policy editor and set the network quarantine policies you want to apply to the virtual machine when it is connected to zone 0. Be sure to select **Static quarantine**. For step-by-step instructions on using the Network Quarantine Wizard, see Setting Network Quarantine Policies on page 85.
2. Exit VMware ACE Manager, then open `<vmname>.vmpl` in your text editor.
3. To enable the zones feature for a virtual machine, find the line that begins with `guest.useZones` and change it to the following:

   ```
   guest.useZones = "1"
   ```

4. Add a set of lines for the zone, specified in a manner similar to that used to define host policies. For zone 0, add the following lines:

   ```
   guest.zone.0.present = "1"
   guest.zone.0.key = "0"
   guest.zone.0.descriptionName = "<zone_name>"
   ```

   The value of `descriptionName` must match the name specified in the zone description you want to use. The number for `<zone_number>`, however, is independent of the zone numbers in the zone description. The value of the zone number in this section — the value of the `guest.zone` parameter — determines the order in which VMware ACE searches the zones for a match. When it finds a match, it applies the guest quarantine policies defined for the zone with the same zone name and stops searching.

   This approach allows you to specify the guest zones in a different order from that in the list of zone descriptions.

5. Find the set of lines beginning with `quarantine.` and make a copy of the entire block of lines. These may include lines beginning with one or more of the following:

   ```
   quarantine.configurationBlock
   quarantine.networkSettings
   quarantine.webFile
   quarantine.httpRoot
   ```

```
quarantine.showUpdatesAvailMsg
quarantine.descriptor.Type
quarantine.descriptor.custom.script
```

Notice that `quarantine.configurationBlock` is followed by a very long string of parameters and settings. These are key quarantine settings; be careful not to modify those parameters and settings.

6. At the beginning of each line, add `guest.zone.<zone_number>.` Thus for zone 0, you change `quarantine.configurationBlock` to `guest.zone.0.quarantine.configurationBlock` and so on.
7. Save and close `<vmname>.vmpl`.
8. Start VMware ACE Manager, then launch the Network Quarantine Wizard from the policy editor and set the network quarantine policies you want to apply to the virtual machine when it is connected to zone 1.

   If you do not want to define policies for any additional zones, skip to step 12.
9. Repeat the steps you took for zone 0, except that the lines referring to the specific zone must use the number 1 in place of the number 0.

   This means the three lines you add to specify the zone are the following:

   ```
   guest.zone.1.present = "1"
   guest.zone.1.key = "1"
   guest.zone.1.descriptionName = "<zone_name>"
   ```

   Similarly, in the block of lines you copy, you change `quarantine.configurationBlock` to `guest.zone.1.quarantine.configurationBlock`, and so on.
10. Save and close `<vmname>.vmpl`.
11. Take the same steps for any other zones you want to define for this virtual machine. You may set policies for any or all of the zones defined in `app.vmpl`, but you may skip any zones for which you want to apply the default network quarantine policies.
12. Launch the Network Quarantine Wizard from the policy editor and set the default network quarantine policies for the virtual machine. The default policies are applied when the host is not in any of the zones you have configured.

Switching Network Connection Type Based on Zones

You may find it useful to configure the virtual machine's Ethernet adapter to use bridged networking in some zones and NAT in other zones. For zones in which you are using host quarantine to restrict the host's network access, it is generally simpler to

use bridged networking. For zones in which the host's network access is unrestricted, you may prefer to use NAT networking.

You can use advanced network quarantine policy options to specify the networking type for each zone. If you specify the network type for any zone, you should specify it for all zones.

Make the following changes after you have defined guest policies for all zones as described in Defining Guest Policies on page 240:

1. Use a text editor to open `<vmname>.vmpl` in the affected virtual machine's folder inside the project folder. Exit VMware ACE Manager, then open `<vmname>.vmpl` in your text editor.
2. Do one of the following:
   - To use the same settings in all zones, look for the following lines. If they exist, edit them appropriately. If they do not exist, add them to the policy file.

     ```
     quarantine.networkType.present = "1"
     quarantine.networkType.defaultNetwork = "<type>"
     ```

     The value of `<type>` may be `"bridged"` for bridged networking or `"nat"` for NAT networking.
   - To use different settings in different zones, add the following two lines for each zone.

     ```
     guest.zone.<zone_number>.quarantine.networkType.present = "1"
     guest.zone.<zone_number>.quarantine.networkType.defaultNetwork = "<type>"
     ```

     The value of <zone_number> must match the value defined in the line `guest.zone.<zone_number>.key = "<zone_number>"` and the value of `<type>` may be `"bridged"` for bridged networking or `"nat"` for NAT networking.

     You must have both lines in the section for each zone.

When the virtual machine powers on, or when it changes zones, all virtual Ethernet adapters configured for that virtual machine are changed to the specified network type.

Switching adapter types requires the guest operating system to renew any DHCP leases it may have held. On Windows guest operating systems, this can be forced by disconnecting the virtual adapters temporarily. For this reason, VMware ACE disconnects the adapters briefly each time the adapter changes from bridged to NAT or vice versa.

In most cases, the default value for this disconnection period is appropriate to force renewal of DHCP leases. If you experience difficulties when using the default setting or if you are using Linux guests, which do not respond to the temporary disconnection, you can take the following steps to disable or configure this disconnection period:

1. Use a text editor to open `<vmname>.vmpl` in the affected virtual machine's folder inside the project folder. Exit VMware ACE Manager, then open `<vmname>.vmpl` in your text editor.
2. Do one of the following:
   - To use the same settings in all zones, look for the following line. If it exists, edit it appropriately. If it does not exist, add it to the policy file.

     ```
     quarantine.networkType.disconnectTime = "<value>"
     ```

     The value of `<value>` may be `-1`, `0` or any positive integer. If the value is `-1`, the default disconnection time is used. If the value is `0`, the adapter is not disconnected. If the value is a positive integer, the adapter is disconnected for the specified number of seconds before it is reconnected.
   - To use different settings in different zones, add the following line for each zone.

     ```
     guest.zone.<zone_number>.quarantine.networkType.disconnectTime = "<value>"
     ```

     The value of <zone_number> must match the value defined in the line `guest.zone.<zone_number>.key = "<zone_number>"` and the value of `<value>` may be `-1`, `0` or any positive integer. If the value is `-1`, the default disconnection time is used. If the value is `0`, the adapter is not disconnected. If the value is a positive integer, the adapter is disconnected for the specified number of seconds before it is reconnected.

Writing Plug-In Policy Scripts

You may write your own plug-ins to control certain policies in VMware ACE. You may use any language that is supported on the end user's computer.

For security reasons, plug-ins must be deployed as part of a package and installed by the package installer. They cannot be deployed separately to end users' computers and cannot be modified by the end user.

Your plug-ins must write the appropriate values to StdOut. Output to StdOut maybe up to 4096 bytes long.

After creating a project, place any scripts you want to use for that project in the `Project Resources` folder under the project folder. They must be in the main `Project Resources` folder, not in a subdirectory under that folder. If the scripts need any additional resource files, place those files in the main `Project Resources` folder, too. Your script should reference those resources using relative paths.

Your plug-ins may also write messages to StdErr. Output to StdErr maybe up to 4096 bytes long. Any messages generated on StdErr are captured in the VMware ACE log file on the end user's machine at `<UserAppData>\VMware\VMware ACE\<package_name>\Virtual Machines\<VM_name>\vmware.log`.

The exit code of a script indicates whether the script succeeded or failed.

The following environment variables are set in the script execution environment:

Variable	Description
VMWARE_NQ_DESCRIPTOR	If custom network quarantine is in use, this variable holds the network quarantine descriptor that was last set by an update.
VMWARE_EXPIRE_TIME	This is the time at which this virtual machine will expire. If set to -1, it means never expire; if set to 0, it means expired.
VMWARE_PROJ_ID	The ID of the project to which this virtual machine belongs.
VMWARE_MVM_ID	The ID of this virtual machine. The virtual machine ID is unique within a project.

All plug-ins run each time the end user launches VMware ACE or resets the virtual machine. Some may run more often. For example, an expiration plug-in is run once each 24 hours, and you may specify the interval for running a network quarantine plug-in by setting an update interval in the Network Quarantine Wizard.

The sample scripts presented in Sample Scripts on page 250 are installed with VMware ACE Manager. The default location is `C:\Program Files\VMware\VMware ACE Manager\Samples`.

The following descriptions give the format for the output that your plug-ins must write to StdOut to control various policies.

Authentication Plug-Ins

The following table outlines the basic information you need to write authentication plug-ins.

Question	Explanation
When does this script execute?	This script executes when the virtual machine is opened.
What relevant environment variables are available to the script?	No authentication-specific environment variables are available, but VMWARE_PROJ_ID and VMWARE_MVM_ID give some context, indicating what virtual machine the user is trying to open.
What is the expected output?	The output of this script is hashed to create a key to encrypt and decrypt virtual machine files. The first time this script is run, the output is hashed to encrypt the virtual machine. When a virtual machine is decrypted, the script must return the same value. If the script returns a different value, the virtual machine is not decrypted and the user sees an error message. The script may return any value. To ensure best security, a value that includes only printable characters should be at least 32 bytes long. For binary data, the value should be at least 16 bytes long to ensure proper entropy.
What can I do with this script?	The script should do one of the following: • If the user is to be granted access to the virtual machine, generate the data used to create the key for this user and send it as output. The data should be unique for each user. • If the user is to be denied access to the virtual machine, the script should exit with a non-zero exit code. **Note:** This is a reference to the exit code, not the output value.
Where should the output of the script go?	The script should send its output to StdOut.

Question	Explanation
What should the exit code of the script be?	If access is granted, the exit code should be 0. If access is denied, the exit code should be nonzero. **Note:** This is a reference to the exit code, not the output value.

Renewal Plug-Ins

The following table outlines the basic information you need to write renewal plug-ins.

Questions	Explanation
When does this script execute?	This script executes every time the virtual machine is powered on or reset.
What relevant environment variables are available to the script?	VMWARE_EXPIRE_TIME It holds the current expiration time, expressed as seconds since Jan. 1, 1970 (UTC).
What is the expected output?	If the output of this script is greater than 32767, it is interpreted as a date, expressed as the number of seconds since Jan. 1, 1970 (UTC). Otherwise, it is interpreted as the number of days to allow the virtual machine to run, beginning on the current date.
What can I do with this script?	The script may do one of the following: • Set the virtual machine expired. If the output is a time that is in the past, the virtual machine is expired. Note that the value must be greater than 32767, otherwise the output is treated as a number of days and the virtual machine is allowed to run for the specified number of days, beginning on the current date. • Allow the virtual machine to run. If the output is a date in the future, expressed as a number of seconds since Jan. 1, 1970 (UTC), the virtual machine is renewed. Times are rounded up to midnight of the day specified. If the output is a value less than 32767, the virtual machine is allowed to run for the specified number of days, beginning on the current date. • Take no action. If the output is 0, nothing is changed. • Set the virtual machine so it never expires. Generate an output value of -1.
Where should the output of the script go?	Your script should send its output to StdOut.

Questions	Explanation
What should the exit code of the script be?	It should be 0. Any nonzero exit code voids any output to StdOut.

Note: Because the script runs each time the end user launches VMware ACE or resets the virtual machine, the current date is different each time the script runs. Take this changing reference point into account in your script.

Device Connection Plug-Ins

The following table outlines the basic information you need to write device connection plug-ins:

Question	Explanation
When does this script execute?	This script executes when the virtual machine is powered on.
What relevant environment variables are available to the script?	No specific environment variables are available. But you should set different scripts (scripts with different arguments) for each device. This enables each script to determine why it is being called.
What is the expected output?	The output of this script is a boolean. Output a value of TRUE if the user is allowed to change the connection status of the device or FALSE to deny the user the ability to change the connection status of the device.
What can I do with this script?	The script should determine if the current user is allowed to change the connection status of a device. • Send TRUE to StdOut to allow permission to change connection status. • Send FALSE to StdOut to deny permission to change connection status.
Where should the output of the script go?	The script should send its output to StdOut.
What should the exit code of the script be?	The script should always exit with a status of 0.

Network Quarantine Plug-Ins

The following table outlines the basic information you need to write network quarantine plug-ins.

Question	Explanation
When does this script execute?	This script executes at power on, at reset and when a virtual machine sends a network quarantine descriptor update.
What relevant environment variables are available to the script?	VMWARE_NQ_DESCRIPTOR contains the string last set by a guest update. To do a guest update, you run `nq-set` (a command provided by VMware Tools) in the guest operating system.
What is the expected output?	The output of the script may be one of the following, in all capital letters as shown: • YES — The current network quarantine descriptor is valid and should be given normal access. • NO — The current network quarantine descriptor is valid and should be given restricted access. • REJECT — The current network quarantine descriptor is invalid.
What can I do with this script?	The script should do both of the following: • Verify that the string contained in VMWARE_NQ_DESCRIPTOR is valid. • Evaluate the network quarantine descriptor and decide whether to give normal or restricted access to the virtual machine.
Where should the output of the script go?	The script should send its output to StdOut.
What should the exit code of the script be?	It should be 0. Any nonzero exit code voids any output to StdOut.

Updating Virtual Machine Versions with the nq-set Command

The comments in the sample network quarantine scripts provided with VMware ACE Manager mention the `nq-set` command. If you update the guest operating system or other software in the virtual machine after distributing it, be sure your updater runs the `nq-set` command inside the virtual machine to update the virtual machine's version descriptor appropriately.

If you do not run `nq-set`, VMware ACE cannot detect that the virtual machine has been updated.

For details on using `nq-set`, see Using nq-set to Update Network Quarantine Versions on page 146.

Sample Scripts

Sample Authentication Script

The following sample script is written in C. It is installed by VMware ACE Manager as `sampleAuth.c`. You may compile it with a C compiler if you want to run it.

```
/*
 *
 * VMware Sample Script
 *
 *
 * This is a sample authentication script for VMware ACE.
 *
 *
 * Input to script:
 *      None

 *
 * Returns:
 *      Exit code of 0 if successful (user is correctly authenticated)
 *     Exit code nonzero if an error occurred, or if authentication
 *     failed
 *
 *     Expected output:
 *     Seed data to hash to create key for encryption/authentication
 *     subsystem on stdout.
 *
 *
 * Notes:
 *      If the script returns success, its output will be hashed to
 *      create a key. Therefore it is important that the output of
 *      this script is unique for each user, and that there is enough
 *      data to make a meaningful key. (That is, at least 16 bytes.)
 *
 *
 * Notes about this sample:
 *      This script contains key data (hard-coded) for several users.
 *      The script assumes that the username is contained in an
 *      environment variable called TEST_USERNAME (a fictitious
 *     environment variable used in this sample).
 *
 *      It will then return the correct data for that user if one
 *      exists; otherwise it will return an error exit code (1).
 *
 *
 */
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

typedef struct {
   char *name;
   char *keydata;
} UserListType;

static UserListType userList[] = {
        {"charlie", "E1C4F612135B4D98A33B2C9BD595025D"},
        {"kathy", "C79AFFEF773D61225751C2566858DB08"},
        {"beth", "05B169B439B26AAB2EA4F755B7E3800C"},
        {"ernie", "8CE63D4AA2068BD8AFF2D1B05F3495A5"},
        {"bert", "172B1619B2EFBE0E4F381AA1C428F049"},
                NULL
};

int
main(int argc,
       char *argv[])
{

   char *username;
    int counter;
   int result = 1;

    /* Get the username from the env. var TEST_USERNAME */
   username = getenv("TEST_USERNAME");
   if (username == NULL) {
       /* No user specified, exit with an error */
      fprintf(stderr, "TEST_USERNAME not set\n");
      goto exit;
    }


    counter = 0;

   while (userList[counter].name != NULL) {
       if (strcmp(userList[counter].name, username) == 0) {
          /* Found the right user; print their key */
         printf("%s", userList[counter].keydata);
         result = 0;
         goto exit;
       }
```

```
        counter++;
        }

    /* No match found */
   fprintf(stderr, "User (%s) not found in list\n", username);

exit:
    return result;
}
```

Sample Renewal Script

The following sample script is written in VB Script. It is installed by VMware ACE Manager as `expire_on_fridays.vbs`.

```
'
' VMware Sample Script
'
' This is a sample expiration/renewal script for VMware ACE
'
' This script returns a UTC time (number of seconds since
' 1/1/1970) for use in determining product expiration. If
' the time returned is less than the current time, the
' product has expired, otherwise it has not. This script
' always marks the product as expired on Fridays, just
' because. Otherwise, it expires on Jan 1, 2010.
'
' This script must be run as follows:
' cscript -nologo expire_on_fridays.vbs

Dim StdOut
Dim StdErr

Set StdOut = WScript.StdOut
Set StdErr = WScript.StdErr

' Output to stderr is sent to the VMware log file. It
' does not, in itself, constitute an error in the script.
StdErr.WriteLine "Running expire_on_fridays.vbs"

If (DatePart("w", Now) = 6) Then

    ' It's a Friday. Game over.
     StdOut.Write DateDiff("s", "1/1/1970", Now) - 100
Else
```

```
    StdOut.Write DateDiff("s", "1/1/1970", "1/1/2010")
End If
```

Sample Device Connection Script

The following sample script is written in C. It is installed by VMware ACE Manager as `sampleDevice.c`. You may compile it with a C compiler if you want to run it.

```
/*
 * VMware Sample Script
 *
 * This is a sample device policy script for VMware ACE.

 * Notes about this sample:
 *
 *    This script will examine the contents of an environment variable
 *     and output YES if the variable is set, or NO if it isn't.
 *
 *    This script always exits successfully (exit code 0)
 *
 *      The environment variable is called TEST_DEVICE
 *
 * Input to script:
 *     This script does not depend on any environment variables set by
 *      VMware ACE
 *
 * Returns:
 *      Returns 0 for success
 *
 * Expected output:
 *      The script may output to stdout:
 *              'YES' - Allow the user to manage the device
 *              'NO' - Do not allow the user to manage the device
 */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int
main(int argc,
       char *argv[])
{
       char *env_var;

    /* Test for existence of TEST_DEVICE variable in environment: */
```

```
    env_var = getenv("TEST_DEVICE");
     if ((env_var == NULL) || (strlen(env_var) == 0)) {
         printf("NO");
     } else {
         printf("YES");
     }

     return 0;
}
```

Sample Network Quarantine Script 1

The following sample script is written in C. It is installed by VMware ACE Manager as `sampleQuarantine.c`. sYou may compile it with a C compiler if you want to run it.

```
/*
 * VMware Sample Script
 *
 * This is a sample network quarantine script for VMware ACE.
 *
 * Notes About this sample:
 *      The NQ Script does 2 things, (1) verifies that the string in
 *      VMWARE_NQ_DESCRIPTOR is valid, and (2) returns whether the
 *      guest operating system that this descriptor is from should be
 *           given normal access (YES), or should be given restricted
 *     access (NO)
 *
 *      For testing purposes a list of NQ_DESCRIPTORS is stored
 *      statically in this file, each with its corresponding result
 *      (YES/NO/REJECT); this sample script will match the value in
 *      VMWARE_NQ_DESCRIPTOR to a stored string and output its stored
 *      "up-to-date" state (YES/NO/REJECT).
 *      If there are no matches, then we output REJECT.
 *
 * Input to script:
 *      Script examines the environment variable VMWARE_NQ_DESCRIPTOR
 *
 * Returns:
 *      Returns 0 for success
 *
 * Expected output:
 *      The script may output to stdout:
 *          'YES'     - the descriptor is valid and up-to-date
 *           'NO'      - the descriptor is valid and not up-to-date
 *           'REJECT'  - the descriptor is not valid
```

```
 *
 * Setting the NQ descriptor:
 *      To set the NQ descriptor from the guest os you must run the
 *      following command (without the brackets around the new
 *     descriptor):
 *
 *      On a Linux guest:
 *      (Binary located at /src/sbin)
 *         vmware-guestd --cmd "nq-set [new descriptor]"
 *
 *      On a Windows guest:
 *      (Binary located at C:\Program Files\VMware\VMware Tools)
 *         vmwareservice -cmd "nq-set [new descriptor]"
 *
 * (without the brackets around the new descriptor)
 *
 */

#include <stdio.h>
#include <stdlib.h>
#include <string.h>

typedef struct {
     char *descriptor;
     char *uptodate;
} DescriptorListType;

static DescriptorListType descriptorList[] = {
     {"os=winxp-sp2,ie=6.0,virusdefs=4.0,office=2003-sp1", "YES"},
     {"os=winxp-sp1,ie=6.0,virusdefs=4.0,office=2003-sp1", "NO"},
     {"uptodate", "YES"},
     {"notuptodate", "NO"},
     {"rejectme", "REJECT"}
     NULL
};

int
main(int argc,
       char *argv[])
{
     char *descriptor;
     int counter;
     int result = 1;

/* Get the current descriptor from the env. var
   * VMWARE_NQ_DESCRIPTOR
    */
```

```
     descriptor = getenv("VMWARE_NQ_DESCRIPTOR");
     if (descriptor == NULL) {
     fprintf(stderr, "VMWARE_NQ_DESCRIPTOR not set\n");
     goto exit;
}

     result = 0;
     counter = 0;
     while (descriptorList[counter].descriptor != NULL) {
     if (strcmp(descriptorList[counter].descriptor, descriptor) == 0 {
               /* Found the right descriptor */
                printf("%s", descriptorList[counter].uptodate);
                goto exit;
          }
          counter++;
      }

      /* No match found */
      printf("REJECT");

exit:
      return result;
}
```

Sample Network Quarantine Script 2

The following sample script is written in Perl. It is installed by VMware ACE Manager as `sampleQuarantine.pl`. You need a Perl interpreter to run this script.

```
#
# VMware Sample Script
#
# This is a sample network quarantine script for VMware ACE.
#
# Notes About this sample:
#    The NQ Script does 2 things, (1) verifies that the string in
#    VMWARE_NQ_DESCRIPTOR is valid, and (2) returns wether the guest
#    operating system that this descriptor is from should be given
#    normal access (YES), or should be given restricted access (NO)
#
#     For testing purposes 2 lists of NQ_DESCRIPTORS are stored
#     statically in this file: an approved list and an unapproved
#     list. This sample script will match the value in
#     VMWARE_NQ_DESCRIPTOR to a stored string, and output YES if it
#     came from the approved list, NO if it came from the unapproved
#     list, and REJECT otherwise.
```

```
#
# Input to script:
#     Script examines the environment variable VMWARE_NQ_DESCRIPTOR
#
# Returns:
#    Returns 0 for success
#
# Expected output:
#    The script may output to stdout:
#        'YES'      - the descriptor is valid and up-to-date
#        'NO'        - the descriptor is valid and not up-to-date
#        'REJECT'   - the descriptor is not valid
#
# Setting the NQ descriptor:
#    To set the NQ descriptor from the guest os you must run the
#    following command:
#
#    On a Linux guest:
#    (Binary located at /src/sbin)
#        vmware-guestd --cmd "nq-set [new descriptor]"
#
#    On a Windows guest:
#    (Binary located at C:\Program Files\VMware\VMware Tools)
#         vmwareservice -cmd "nq-set [new descriptor]"
#
# (without the brackets around the new descriptor)
#

my @approved = (
    "os=winxp-sp2,ie=6.0,virusdefs=4.0,office=2003-sp1",
    "uptodate"
);

my @unapproved = (
    "os=winxp-sp1,ie=6.0,virusdefs=4.0,office=2003-sp1",
    "notuptodate"
);

sub find_match{
    foreach (@approved) {
        if (/^$_[0]$/i) {
            return "YES";
        }
    }

    foreach (@unapproved) {
```

```
        if (/^$_[0]$/i) {
            return "NO";
        }
    }

    return "REJECT";
}

my $nqEnvName = 'VMWARE_NQ_DESCRIPTOR';
my $nqVal = $ENV{$nqEnvName};

print &find_match($nqVal);
```

CHAPTER 15

Glossary

Bridged networking — A type of network connection between a virtual machine and the rest of the world. Under bridged networking, a virtual machine appears as an additional computer on the same physical Ethernet network as the host.
See also Host-only networking.

Configuration — See Virtual machine configuration file.

Full screen mode— A display mode in which the virtual machine's display fills the entire screen.

Guest operating system — An operating system that runs inside a virtual machine.
See also Host operating system.

Host computer — The physical computer on which the VMware ACE software is installed. It hosts the VMware ACE virtual machines.

Host-only networking — A type of network connection between a virtual machine and the host. Under host-only networking, a virtual machine is connected to the host on a private network, which normally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the

same network.
See also Bridged networking, Custom networking and Network address translation.

Host operating system — An operating system that runs on the host machine.
See also Guest operating system.

Hot fix — An installable file that resets a user's password, renews an expired virtual machine or allows a cop-protected virtual machine to run from a new location.

Network address translation (NAT) — A type of network connection that allows you to connect your virtual machines to an external network when you have only one IP network address, and that address is used by the host computer. If you use NAT, your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination.

Network quarantine — A set of controls, governed by policies, that ensure only up-to-date virtual machines have access to an organization's network and allow administrators to specify which machines or subnets a virtual machine may access.

New Virtual Machine Wizard — A point-and-click interface for convenient, easy creation of a virtual machine configuration. To launch it, choose File > New Virtual Machine. It prompts you for information, suggesting default values in most cases. It creates files that define the virtual machine.
See also Virtual machine settings editor.

Package — An installable bundle for distribution to end users. The package may include one virtual machine and an application used to run virtual machines.

Policy — A policy controls the capabilities of a virtual machine. Policies are set in the policy editor.

Project — A set of components for creating packages. You create and manage projects in the VMware ACE Manager. You may include some or all of the components of a project when you create a package.

Resume — Return a virtual machine to operation from its suspended state. When you resume a suspended virtual machine, all applications are in the same state they were when the virtual machine was suspended.
See also Suspend.

Shared folder — A shared folder is a folder on the host computer — or on a network drive accessible from the host computer — that can be used by both the

host computer and one or more virtual machines. It provides a simple way of sharing files between host and guest or among virtual machines. In a Windows virtual machine, shared folders appear in My Network Places (Network Neighborhood in a Windows NT virtual machine) under VMware Shared Folders. In a Linux virtual machine, shared folders appear under a specified mount point.

Snapshot — A snapshot preserves the virtual machine just as it was when you took the snapshot — the state of the data on all the virtual machine's disks and whether the virtual machine was powered on, powered off or suspended. VMware ACE Manager lets you take a snapshot of a virtual machine at any time and revert to that snapshot at any time. You can take a snapshot when a virtual machine is powered on, powered off or suspended.

Suspend — Save the current state of a running virtual machine. To return a suspended virtual machine to operation, use the resume feature.
See also Resume.

Virtual disk — A virtual disk is a file or set of files, usually on the host file system, that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. When you configure a virtual machine with a virtual disk, you can install a new operating system into the disk file without the need to repartition a physical disk or reboot the host.

Virtual machine — A virtualized x86 PC environment in which a guest operating system and associated application software can run.

Virtual machine configuration — The specification of what virtual devices (disks, memory size, etc.) are present in a virtual machine and how they are mapped to host files and devices.

Virtual machine configuration file — A file containing a virtual machine configuration. It is created by the New Virtual Machine Wizard. It is used by VMware ACE applications to identify and run a specific virtual machine.

Virtual machine settings editor — A point-and-click editor used to view and modify the settings of a virtual machine. You can launch it from the **VM** menu.
See also New Virtual Machine Wizard.

Virtual Network Editor — A point-and-click editor used to view and modify the networking settings for the virtual networks created by VMware ACE. You can launch it from the **Edit** menu.

VMware ACE — A simple application that allows an end user to run a virtual machine. The end user installs this client software by installing a package that includes the client.

VMware ACE Manager — The program used by the administrator to create and update projects, virtual machines and packages.

VMware Tools — A suite of utilities and drivers that enhances the performance and functionality of your guest operating system. Key features of VMware Tools include some or all of the following, depending on your guest operating system: an SVGA driver, a mouse driver, the VMware Tools control panel, and support for such features as shared folders, shrinking virtual disks, time synchronization with the host, VMware Tools scripts, and connecting and disconnecting devices while the virtual machine is running.

Index

File extensions

.lck 171

.REDO 184

.vmdk 169

.vmhf 151

.vmpl 220

.vmprj 150

.vmss 180

.wav 204

A

Access
  network quarantine 230, 234

Adapter
  host virtual 189
  virtual Ethernet 195

Add
  DVD or CD drive 174
  existing virtual machine to project 51
  floppy drive 176
  new virtual machine to project 53
  parallel port 207
  serial port 209
  virtual disk 173
  virtual Ethernet adapter 195
  virtual machine to project 51

Address
  IP in virtual machine 57
  network address translation 196

Administrator access
  using on end user's computer 152

Athlon 12, 14

Audio
  See Sound

AudioPCI 204

Authentication
  policies 81, 222

Autorun
  disable 32, 154

B

BIOS
  provided in virtual machine 16

Bridge 189

Bridged networking
  defined 259

BSD
  supported guest operating systems 19

BusLogic 16

C

CD
  adding drive to virtual machine 174
  CD-ROM image file 16

Celeron 12, 14

Centrino 12, 14

Checklist
  add virtual machine 63
  new project 49

Clock
  synchronize guest and host 118

Color
  screen colors in a virtual machine 202

Comm port
  See Serial connection, Serial port

Configuration
  virtual machine 261

Configure
  hot keys 38
  memory use 38
  parallel port 207
  preferences for VMware ACE Manager 36
  process priorities on Windows host 39
  screen colors 202
  serial port 209
  sound 204
  USB controller 214
  virtual Ethernet adapter 195
  virtual machine 111
  virtual network 191, 195

Connect
  devices with VMware ACE 160
  USB devices 214

Copy protection
policies 84, 225
requesting to run from a new location 164
CPU
host requirement 12, 14
provided in virtual machine 16
Create
floppy image file 177
named pipe 210, 211
new virtual machine 53
package 132
policies 71
policies for a virtual machine 81
policies for VMware ACE 74
project 44
Creative Labs 17, 204
Ctrl-Alt 38

D

Date
See Time
Decrease
See Shrink
Defragment
virtual disks 171
Deploy
new package 138
update package 149
updates 141
virtual machine 132
Devices
controlling with VMware ACE 160
disconnecting from USB controller 217
provided in virtual machine 16
USB 214
DHCP
DHCP server 190
on a virtual network with NAT 196
server on virtual network 192, 193
Direct memory access
See DMA
Disable
autorun 32, 154
scripts 119
shared folder 41
USB controller 214
Disconnect
devices with VMware ACE 160
USB devices 217
Disk
space required on host computer 12, 14
Disk files 169
Disks
adding virtual disks 173
available in virtual machine 16
defragmenting 171
file locations 169
See also Virtual disk
shrinking 171
virtual 261
virtual disk size in new virtual machine 54
Display
color depth 202
Distribute
new package 138
update package 149
updates 141
virtual machine 132
DMA
and disk performance 178
DNS 197
Driver
sound 204
Drives
See Disks
Duron 12, 14
DVD
adding drive to virtual machine 174

E

Enable
shared folder 41
USB controller 214
Encryption
policies 222
Ethernet
adding virtual adapter 195
virtual adapter 190
Expiration
policies 83, 224
requesting extension 164

F

Files
location of virtual disk files 54
redo log 184

Firewall 198

Floppy
add drive to virtual machine 176
drives in virtual machine 16
image file 16, 177

Forums 20

FreeBSD
supported guest operating systems 19
VMware Tools for 116

FTP 197

Full screen
mode defined 259
setting for VMware ACE 159

G

Grab
keyboard and mouse input 37

Graphics
See also Display
support in virtual machine 16, 202

Guest operating system
defined 259

H

Host computer
defined 259
restricting access to the network 234

Host operating system 260

Host quarantine 237

Host virtual adapter 189

Host-only networking
basic configuration 193
defined 259

Hot fix
defined 260
requesting 163
responding 150

Hot keys
configuring 38
for full screen switch mode 126

I

ICMP 197

IDE
drives in virtual machine 16

Image file
floppy 16, 177
ISO 16, 175, 177

Input
capturing from keyboard and mouse 37

Install
a VMware ACE package silently 139
on Windows host 30
operating system in virtual machine 112
package 154
software in virtual machine 112
VMware ACE 154
VMware ACE Manager silently 33

interface
customizing VMware ACE 123

Iomega
parallel port Zip drives 208

IP address
in virtual machine 57

ISO image file 16, 175, 177

K

Keyboard
sending input to virtual machine 37
USB 217

Knowledge base 20

L

Link
symbolic link does not work in shared folder 42

Linux
supported guest operating systems 18
VMware Tools for 114

Lock files 170

LSI Logic 16, 58

M

Memory
amount required on host 12, 14
available in virtual machine 16
setting for a virtual machine 56
swapping 38

MIDI 204
Mode
full screen 259
Modifier keys
for full screen switch mode 126
Mouse
sending input to virtual machine 37
USB 217
MP3 204
MS-DOS
supported guest operating systems 18
Mylex 16

N

Named pipe 210, 211
NAT
and DHCP 196
and DNS 197
and the host computer 196
defined 260
external access from a NAT network 197
on virtual network 192, 196
virtual device 189
when creating a virtual machine 57
NetLogon 198
NetWare
See Novell NetWare
Network
adding and modifying virtual Ethernet adapters 195
advanced quarantine 234
advanced quarantine policies for guest 240
bridge 189
bridged networking 259
changing the configuration 195
common configurations 191
components 189
DHCP server 190
host virtual adapter 189
host-only 193, 259
NAT 192, 196, 260
NAT as firewall 198
NAT device 189
quarantine policies for host computer 237
restricting host computer access 234
switch 189
Token Ring 192
virtual DHCP server 192, 193
virtual Ethernet adapter 190
Virtual Network Editor 261
virtual switch 189
zones for advanced quarantine 235
Network address translation
defined 260
See NAT
Network quarantine 85
defined 260
policies 230, 234
updating version 142
New Virtual Machine Wizard 168, 260
Newsgroups 20
NIC
See Ethernet
Novell NetWare
supported guest operating systems 19
VMware Tools for 117
nq-set 146

O

Operating system
guest 259
host 260
supported Windows host 13, 15
Opteron 12, 14

P

Package
creating 132
defined 260
deploy update 149
deploying 138
installing 154
updating 141
Parallel ports
and Iomega Zip drives 208
in a virtual machine 207
installing in virtual machines 207
Password
requesting 163
Pentium 12, 14

Ping 197
Pipe
named 210, 211
Plug-in
writing 244
Policies
advanced network quarantine for guest 240
authentication 81, 222
copy protection 84, 225
encryption 222
expiration 83, 224
network quarantine 85, 230, 234
network quarantine for host 237
overview 220
removable devices 85
setting 71
setting for a virtual machine 81
setting for VMware ACE 74
using scripts 244
VMware ACE application 226
Policy
defined 260
Power off
VMware ACE 164
Preferences
setting 36
VMware ACE 161
Printer
installing in VMware ACE 77, 89, 93, 98, 100, 106, 108, 162, 227
Priorities
for virtual machines on Windows host 39
Process scheduler 39
Processor
host requirement 12, 14
provided in virtual machine 16
Project
add virtual machine checklist 63
adding a new virtual machine 53
adding a virtual machine 51
adding an existing virtual machine 51
create 44
defined 260
new project checklist 49

Q

Quarantine
advanced 234
network, defined 260
Quit
VMware ACE 157

R

RAM
amount required on host 12, 14
available in virtual machine 16
Real Media 204
Reclaim
disk space 120, 121
Redo-log file 184
Registration 21
Removable devices 85
Remove
See also Uninstall
USB devices 217
VMware ACE 162
Reset
VMware ACE 164
Restore
virtual machine to state in snapshot 182
Resume
defined 260
virtual machine 180
Return
See Revert
Revert
to snapshot 182
Run
suspended virtual machine 180
virtual machine in VMware ACE interface 129
VMware ACE 156

S

Save
state of virtual machine 180, 182
Screen
colors 202
Script
writing 244

SCSI
devices in virtual machine 16
drivers 58
Security
policies 222, 225
Serial connection
between host application and virtual machine 210
between two virtual machines 211
to a serial port on the host 209
Serial port
installing and using 209
Server
DHCP 190, 196, 199
DNS 197
WINS 198
Set
policies 71
policies for a virtual machine 81
policies for VMware ACE 74
preferences in VMware ACE 161
Set up
custom interface for VMware ACE 123
hot keys 38
package 132, 154
parallel port 207, 209
preferences for VMware ACE Manager 36
process priorities on Windows host 39
project 44
rmemory use 38
screen colors 202
sound 204
USB controller 214
virtual machine configuration 111
virtual network 191, 195
VMware ACE 154
Settings editor
virtual machine 261
Shared folder
and Linux symbolic link 42
and Windows shortcut 42
defined 260
enable and disable 41
using in VMware ACE Manager 40
Shortcut
does not work in shared folder 42
Shrink
virtual disks 120, 121, 171
Silent
installation of a VMware ACE package 139
installation of VMware ACE Manager 33
Size
virtual disk 16, 59
Snapshot
defined 261
removing 183
virtual machine 182
ways of using 183
what is saved in 182
Software
installing in virtual machine 112
Sound
configuring 204
drivers for Windows 9x and Windows NT guest operating systems 204
support in guest 17
Sound Blaster 204
Start
suspended virtual machine 180
VMware ACE 156
Stop
VMware ACE 157
Suspend
defined 261
virtual machine 180
Swapping
memory 38
Switch
virtual network 189
workspaces in Linux guest 38

T

Telnet 197
Time
synchronize guest and host 118
Token Ring 192
Tools
VMware Tools 262

Troubleshooting
requesting a hot fix 163
responding to hot fix requests 150
using administrator access 152

U

UI
see Interface

Uninstall
on Windows host 35
See also Remove
VMware ACE 162

Unplug
USB devices 217

USB
connecting devices 214
control of devices by host and guest 216
devices in a virtual machine 214
disconnecting devices 217
enabling and disabling the controller 214
keyboard and mouse 217
on a Windows host 215
supported device types 214

V

Version
command to update in virtual machine 146
network quarantine 142
updating 142

Virtual disk
add to virtual machine 173
defined 261
location 54
See also Disks
size 16, 54, 59, 173

Virtual machine
adding to project 51, 53
configuring 111
defined 261
installing software 112
memory settings 56
resuming 180
running in VMware ACE interface 129
setting policies 81
suspending 180
updating 141
updating version 142
viewing in VMware ACE interface 129

Virtual machine settings editor
defined 261

Virtual Network Editor 261

Virtual switch 189

VMnet8 196

VMware ACE
application policies 226
customizing the user interface 123
defined 261
installing 154
installing silently 139
quitting 157
running 156
setting policies 74
setting preferences 161
starting 156
stopping 157
uninstall 162

VMware ACE Manager
defined 262
installing silently 33

VMware Tools
defined 262
for FreeBSD guests 116
for Linux guests 114
for NetWare guests 117
for Windows guests 113

W

Windows
installing on Windows host 30
supported guest operating systems 18
uninstalling on Windows host 35
VMware Tools for 113

Windows 95
sound driver 204

Windows 98
sound driver 204

Windows NT
sound driver 204

Wizard
new virtual machine 169, 260
shared folder 41

Workspaces
switching in Linux guest 38

X

Xeon 12, 14

Z

Zip drives
on a parallel port 208
Zones
network quarantine 234, 235