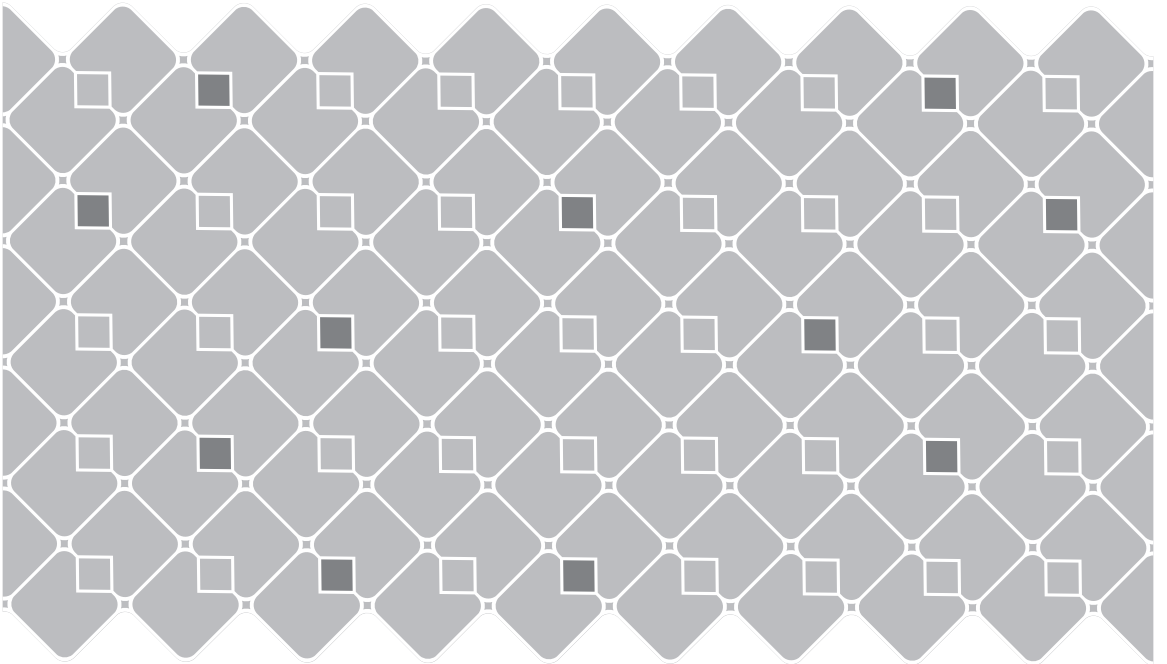
VMware ACE Administrator's Manual

VMware ACE 2.0



vmware®

VMware ACE Administrator's Manual
Revision: 20071019
Item: ACE-ENG-Q207-008

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About This Book

This manual, the *VMware ACE Administrator's Manual,* provides information about installing and using Workstation ACE Edition.

Revision History

This manual is revised with each release of the product or when necessary. A revised version can contain minor or major changes. Table 1 summarizes the significant changes in each version of this manual.

Table 1. Revision History

Revision	Description
20071019	Updated for ACE 2.0.2 release.
20070920	Updated for ACE 2.0.1 release.
20070507	GA release version.
20070423	First version of the Workstation ACE Edition documentation.

To view the most current version of the manual, see the VMware Web site:

http://www.vmware.com/support/pubs/ace_pubs.html

Intended Audience

This book is intended for anyone who needs to install, upgrade, or use Workstation ACE Edition. ACE 2 users typically include people who do software development and testing or work with multiple operating systems or computing environments: software

developers, QA engineers, trainers, salespeople who run demos, and anyone who wants to create virtual machines.

Document Feedback

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

docfeedback@vmware.com

Conventions

Table 2 illustrates the typographic conventions used in this manual.

Table 2. Conventions Used in This Manual

Style	Elements
Blue (online only)	Links, cross-references, and email addresses
Black boldface	User interface elements such as button names and menu items
`Monospace`	Commands, filenames, directories, and paths
`Monospace bold`	User input
Italic	Document titles, glossary terms, and occasional emphasis
<Name>	Variable and parameter names

Technical Support and Education Resources

The following sections describe the technical support resources available to you.

Self-Service Support

Use the VMware Technology Network (VMTN) for self-help tools and technical information:

- Product information – http://www.vmware.com/products/
- Technology information – http://www.vmware.com/communities/content/
- Documentation – http://www.vmware.com/support/pubs
- VMTN Knowledge Base – http://kb.vmware.com
- Discussion forums – http://www.vmware.com/community
- User groups – http://www.vmware.com/communities/content/vmug/

For more information about the VMware Technology Network, go to http://www.vmware.com/community/index.jspa.

Online and Telephone Support

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

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

Support Offerings

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

VMware Education Services

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

Introduction and System Requirements

1

Welcome to VMware ACE 2. This section covers the following topics:

About VMware ACE 2

VMware ACE 2 is a software solution that delivers enhanced management, security, and usability to standard desktop virtualization products. Using ACE 2, an organization can rapidly provision a standardized, secure PC environment—an ACE—to any device in the extended enterprise, regardless of whether it is managed by the ACE administrator. An ACE is a policy-protected virtual machine containing an operating system, applications, and data. Through virtual rights management technology, ACE 2 enables desktop administrators to control ACE lifecycles, protect data, and ensure compliance with IT policies including software lifecycle management and access to data and applications.

Unlike other desktop virtualization products, ACE 2 is a hardware-independent solution that can be provisioned to any PC and works either connected or disconnected from the enterprise network.

ACE 2 is used across an organization to:

- Ensure secure, controlled access to enterprise resources from a standardized PC environment called an ACE
- Provide a simplified end-user interface designed specifically for nontechnical users
- Provide policy-based controls including access, network, and device rights

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. ACE 2 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.

Simplified End-User Interface

Secure, then deploy 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, ACE 2 helps prevent theft, tampering and unauthorized copying of applications, data, system settings and files. It delivers these features in a user interface designed specifically for end-users who do not require the more complex interfaces found in other desktop virtualization products.

Standardize and Secure PC Environments

Self-policing and hardware-independent, ACE 2 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 user freedom. Provide policy-based controls including access, network, and device rights.

Key Features of ACE 2

The following sections describe the key features of ACE 2.

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 ACE 2 lifecycle, security settings, network settings, system configuration and user interface capabilities.
- Instance tracking. Through the user interface, view and manage the activation, expiration, and other policies of instances managed with the new policy server, ACE 2 Management Server.

Security

- Rules-based network access. Identify and quarantine unauthorized or out-of-date ACE instances. Enable access to the network once the ACE instance complies with IT policies.
- Tamper-resistant computing environment. Protect the entire ACE instance and package, including data and system configuration, with seamless encryption.
- Copy-protected computing environment. Prevent users from copying enterprise information.
- Roles-based secure SSL communications between ACE 2 Management Server and client.
- Resource signing. Specify that ACE Resource files be protected from all tampering.

Usability

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

ACE Option Pack for Workstation 6

Many of the administrator features and controls of ACE 2 are built into Workstation 6. To expose these ACE 2 features, users of Workstation 6 must acquire the ACE Option Pack.

The ACE Option Pack is a license enablement that turns an existing copy of Workstation 6 into Workstation 6 ACE Edition. There are no new software downloads required.

As an ACE administrator you install Workstation 6 software and then the ACE Option Pack license key. After entering the ACE Option Pack license key and restarting your copy of Workstation, you will immediately note that the title bar reads Workstation ACE Edition and you will now see additional menu items and commands in Workstation 6.

Workstation ACE Edition is a superset of Workstation 6 functionality. All Workstation 6 features remain available to you. In addition to all core Workstation 6 features, with Workstation ACE Edition you can now create ACE instances.

Workstation ACE Edition creates a policy-protected virtual machine (an ACE instance) as well as a virtual runtime environment (VMware Player) that is licensed and enabled to securely run ACE instances.

Key Concepts of ACE 2

The following are components of ACE 2:

- ACE master – A virtual machine template created by the ACE administrator. The master can be configured with various policies and devices and package settings and then used as the basis for creating any number of packages to be sent to ACE users.
- ACE instance – The virtual machine that ACE administrators create, associate to virtual rights management (VRM) policies, and then package for deployment to users. In short form, an ACE instance is an ACE.

The following are new features of ACE 2:

- ACE 2 Management Server

  The ACE 2 Management Server enables you to manage ACE instances, to dynamically publish policy changes for those instances, and to test and deploy packages more easily. It adds new integration with your Active Directory setups and provides secure Active Directory/LDAP integration, with role-based secure SSL communication.

  There are two ways administrators can interact with the ACE 2 Management Server: directly from Workstation ACE Edition's Instance View or through browser-based access to the ACE 2 Management Server Help Desk application.

  The Instance View allows an administrator to view and control all managed ACE instances. An advanced search function allows you to locate instances in the

database quickly. You can customize the Instance View by adding searchable custom fields.

The web-based ACE 2 Management Server Help Desk Application is designed to deliver a reduced set of administrative functionality through role-based access from any browser. See "Using the VMware Help Desk Web Application" on page 237 for more information.

The server uses the Apache 2.0 web server. The ACE 2 Management Server supports the use of external RDBMSs including Oracle 10g, Microsoft SQL Server 2000 or higher, and Postgres 7.4 or higher. In addition, it ships with an embedded SQLite database.

See "ACE 2 Management Server" on page 31 for system requirements for the ACE 2 Management Server, and see Chapter 4, "Installing and Configuring the ACE 2 Management Server," on page 53 for information about installing and configuring the ACE 2 Management Server.

- ACE 2 Management Server Appliance

  ACE 2 Management Server is now available as a production virtual appliance. The appliance is a self-contained, pre-installed, pre-configured ACE 2 Management Server packaged in a virtual machine. Using this appliance is the fastest way to get an ACE 2 Management Server running in your environment. The ACE 2 Management Server appliance is eligible for all the same VMware support options offered with other ACE 2 Management Server installation configurations.

- Pocket ACE

  Pocket ACE allows an administrator to bundle and deploy an ACE onto a USB portable media device, including USB flash drives, Apple iPod mobile digital devices, and portable hard drives. Pocket ACE is designed to be run directly from the USB portable media device and can be run with the VMware Player that is bundled with the software.

- Virtual Printer

  VMware ACE allows you to configure your ACE instances to use printers that are configured on their host operating systems.

- Linux Systems Available as Host Systems for ACE User Machines

  You can create a single package that can be installed on either a Windows or Linux host operating system.

- Instance Customization

  The instance customization feature automates Microsoft Sysprep deployment tools actions and streamlines the process of customizing instances after they have been deployed to user machines. This feature makes it easier for you to deploy and customize a single package for many users.

- Remote Domain Join

  The remote domain join feature, which you set up through the instance customization pages in the package settings editor, allows you to automate the join of a remote ACE instance through your own VPN client/server setup to the domain that you specify.

- Modular ACE Components

  ACE 2 allows greater flexibility and mobility for ACE distributions and instances. You can install Workstation ACE Edition and ACE packages on the same machine. You can install multiple ACE instances on a single user machine. You can easily move the instances within the same system. And you can move one particular type of ACE instance from host computer to host computer; see Chapter 10, "Pocket ACE," on page 207. You, or the user, can delete single or multiple ACE instances while leaving other ACE instances on the same machine intact.

- Updated Policy and Package Settings

  Enhancements to the policies and package settings you can apply and the ways in which you can update policies make it easier for you to secure and manage your ACE deployments. All policies are dynamic. Updated policies and package settings include:

  - Network access – These policies give you fine-grained and flexible control over the network access you provide to users of your ACE instances. Using a packet filtering firewall, the network access feature of ACE 2 lets you specify exactly which machines or subnets an ACE instance or its host system may access. This means that you can, for example, configure the instance so it is allowed to connect only to your VPN server, which then controls access to other resources. You can also customize the network access settings to filter on the basis of network addresses, traffic direction, protocol, and ports.

  - Access control – The new activation policy (one of the access control policies, along with authentication) allows you to determine who can activate an ACE instance after the ACE package has been installed, giving you finer control over your ACE instances.

  - Policy update frequency – This policy allows you to specify how long the managed ACE instances created from a specific ACE master can be used

without having the instances contact the ACE 2 Management Server for policy updates.

- Removable devices – This policy allow you to control whether users can connect and disconnect removable devices from their ACE instances.
- USB devices – This policy allows you to specify in detail which USB devices and device classes can be accessed by ACE instances created from a specific ACE master.
- Copy protection, for both standalone and managed instances – This policy lets you ensure that an ACE instance can run only from the location where it was originally installed. For managed instances, this policy allows you to specify whether users can move or copy an instance without getting approval from an administrator.
- Snapshots – This policy allows you to specify whether a user can control their own snapshot and/or control the reimage snapshot. These controls are independent of one another.
- Host-guest data script – This policy allows you to specify a script that will run on the host operating system after the ACE instance is powered on. This script can be used to pass information about the host to the guest operating system.
- Administrator mode – This policy allows you to configure virtual machine settings (on Windows host systems only) directly on the users' machines and to use snapshot commands that have not been enabled for the user. Its password setting also provides you with access to the vmware-acetool command-line troubleshooting program on standalone ACE instances.
- Runtime preferences – This policy allows you to configure settings for runtime. You can specify various settings that your users can access on their machines when running ACE instances.
- Hot fix – This policy allows you to activate the hot fix feature for standalone ACE instances. You can use the hot fix policy to specify that users can request hot fixes for specific problems, such as lost or forgotten passwords or expired instances.
- Resource signing – This policy allows you to specify that ACE Resource files be protected from all tampering.
- Custom EULA package setting – This package setting allows you to provide a custom EULA (end-user license agreement) that appears when an ACE instance is activated. You can use this feature to display a custom

license-agreement message that the user must see and accept before the instance can be run for the first time.

- Package lifetime package setting – This package setting allows you to specify a time period during which an ACE package can be installed.

- Troubleshooting tools

  The vmware-acetool command-line program and the hot fix feature are available for use by administrators to fix users' common problems on standalone ACE instances. The Help Desk Web application and the Instance View can be used to fix those same sorts of problems for managed instances.

- Enhancements to Preview Mode

  Preview mode allows you to run the ACE instance as it will run on the user's machine as well as see the effects of changed policies as they will appear on the ACE user's machine without your having to package and install them. It also allows you to see many of the effects of your setup choices for an ACE package without having to expend the time and effort required for a full package deployment and installation.

- New ACE Integration with Workstation

  The VMware ACE product is now a superset of VMware Workstation, so you get all the advantages of both products in one easy-to-use interface. Workstation features such as multiple snapshots and full and linked clones are now available to you.

Hardware and Software Recommendations for This Release

The following sections describe hardware and software recommendations for this release.

Workstation ACE Edition (ACE Administrator)

What do you need to get the most out of Workstation ACE Edition? Use the following list of requirements as a starting point. An ACE is like a physical computer in many ways—and, like a physical computer, it generally performs better if it has a faster processor and more memory.

PC Hardware

- Standard PC

  1000MHz or faster compatible x86 and x86-64 architecture processor (recommended; 600MHz 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, AMD64 Opteron, Athlon 64

- Multiprocessor systems supported
- Experimental support for 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 memoryrequirements.
  - 512MB minimum, 1GB recommended

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 (32-bit)

- Windows Vista
- Windows XP Home Edition, SP1, SP2
  Windows XP Professional, SP1, SP2
  (Listed versions are also supported with no service pack.)
- Windows 2000 Server SP3, SP4
  Windows 2000 Professional, SP3, SP4
  Windows 2000 Advanced Server, SP3, SP4
- Windows Server 2003 Standard Edition, SP1, SP2
  Windows Server 2003 Web Edition, SP1, SP2
  Windows Server 2003 Small Business Edition, SP1, SP2
  Windows Server 2003 Enterprise Edition, SP1, SP2
  Windows Server 2003 R2
  (Listed versions are also supported with no service pack.)

Windows Host Operating Systems (64-Bit)

- Windows Vista
- Windows XP Professional x64 Edition
- Windows Server 2003 x64 Edition SP1, SP2
  Windows Server 2003 x64 Edition R2

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

VMware Player (End-User Client Devices)

The following sections describe VMware Player system requirements.

Hardware Requirements

- Processor speed – 400MHz or faster (500MHz or faster recommended)
- Memory – 256MB minimum. 512MB recommended. You must have enough memory to run the host operating system, plus the 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.
- Hard disk – At least 1GB free disk space for each guest operating system. For installation, VMware Player requires approximately 70MB.

Supported Host Operating Systems

VMware Player is available for both Windows and Linux host operating systems.

Windows Host Operating Systems (32-Bit)

Workstation supports the following Windows 32-bit host operating systems:

- Windows Vista Enterprise Edition
  Windows Vista Business Edition
  Windows Vista Home Basic and Premium Editions
  Windows Vista Ultimate Edition
- Windows Server 2003 Standard Edition, SP1, SP2
  Windows Server 2003 Web Edition, SP1, SP2
  Windows Server 2003 Small Business Edition, SP1, SP2
  Windows Server 2003 Enterprise Edition, SP1, SP2
  Windows Server 2003 R2
  (Listed versions are also supported with no service pack.)
- Windows XP Home Edition, SP1, SP2
  Windows XP Professional, SP1, SP2
  (Listed versions are also supported with no service pack.)
- Windows 2000 Server SP3, SP4
  Windows 2000 Professional, SP3, SP4
  Windows 2000 Advanced Server, SP3, SP4

Windows Host Operating Systems (64-Bit)

- Windows Vista Enterprise Edition
  Windows Vista Business Edition
  Windows Vista Home Basic and Premium Editions
  Windows Vista Ultimate Edition
- Windows Server 2003 x64 Edition SP1, SP2
  Windows Server 2003 x64 Edition R2
- Windows XP Professional x64 Edition

A Web browser is required for the Help system.

Linux Host Operating Systems (32-Bit)

Supported distributions and kernels are listed below. Workstation might not run on systems that do not meet these requirements.

NOTE As newer Linux kernels and distributions are released, VMware modifies and tests its products for stability and reliability on those host platforms. VMware makes every effort to add support for new kernels and distributions in a timely manner, but until a kernel or distribution is added to the list below, its use with VMware products is not supported. Look for newer prebuilt modules in the download area of the VMware Web site. Go to www.vmware.com/download/.

- Mandriva Linux 2006 and 2007
  Mandriva Corporate Desktop 4.0
  Mandriva Corporate Server 4.0
  Mandrake Linux 10.1
  Mandrake Linux 9.0 — stock 2.4.19

- Red Hat Enterprise Linux 5.0

  Red Hat Enterprise Linux WS 4.5
  Red Hat Enterprise Linux AS 4.0, updates 1, 2, 3, 4
  Red Hat Enterprise Linux ES 4.0, updates 1, 2, 3, 4
  Red Hat Enterprise Linux WS 4.0, updates 1, 2, 3, 4

  Red Hat Enterprise Linux AS 3.0, updates 1, 2, 3, 4, 5, 6, 7, 8
  Red Hat Enterprise Linux ES 3.0, updates 1, 2, 3, 4, 5, 6, 7, 8
  Red Hat Enterprise Linux WS 3.0, updates 1, 2, 3, 4, 5, 6, 7, 8

  Red Hat Enterprise Linux 2.1 — stock 2.4.9-e3

  Red Hat Linux 9.0 — stock 2.4.20-8, upgrade 2.4.20-20.9
  Red Hat Linux 8.0 — stock 2.4.18
  Red Hat Linux 7.3 — stock 2.4.18
  Red Hat Linux 7.2 — stock 2.4.7-10, upgrade 2.4.9-7, upgrade 2.4.9-13, upgrade 2.4.9-21, upgrade 2.4.9-31
  Red Hat Linux 7.1 — stock 2.4.2-2, upgrade 2.4.3-12
  Red Hat Linux 7.0 — stock 2.2.16-22, upgrade 2.2.17-14

- SUSE Linux Enterprise Server 10
  SUSE Linux Enterprise Server 9 SP4 (Beta)
  SUSE Linux Enterprise Server 9, 9 SP1, 9 SP2, 9 SP3
  (Listed versions are also supported with no service pack.)
  SUSE Linux Enterprise Server 8, stock 2.4.19

  openSUSE 10.2 (formerly known as SUSE Linux 10.2)
  SUSE Linux 10.1
  SUSE Linux 10
  SUSE Linux 9.3
  SUSE Linux 9.2, SP1)
  SUSE Linux 9.1 — stock 2.6.4-52
  SUSE Linux 9.0 — stock 2.4.21-99
  SUSE Linux 8.2 — stock 2.4.20

- Ubuntu Linux 6.10
  Ubuntu Linux 6.06
  Ubuntu Linux 5.10
  Ubuntu Linux 5.04

A Web browser is required for the Help system.

Linux Host Operating Systems (64-Bit)

Supported distributions and kernels are listed below. Workstation might not run on systems that do not meet these requirements.

NOTE As newer Linux kernels and distributions are released, VMware modifies and tests its products for stability and reliability on those host platforms. VMware makes every effort to add support for new kernels and distributions in a timely manner, but until a kernel or distribution is added to the list below, its use with VMware products is not supported. Look for newer prebuilt modules in the download area of the VMware Web site. Go to www.vmware.com/download/.

- Mandriva Linux 2006 and 2007
  Mandriva Corporate Desktop 4.0
  Mandriva Corporate Server 4.0

  Important: On 64-bit Mandriva hosts, some 32-bit compatibility libraries are required. Specifically, 32-bit `glibc`, `X11`, and `libXtst.so` are required.

- Red Hat Enterprise Linux 5.0

  Red Hat Enterprise Linux 4.5
  Red Hat Enterprise Linux AS 4.0, updates 3, 4
  Red Hat Enterprise Linux ES 4.0, updates 3, 4
  Red Hat Enterprise Linux WS 4.0, updates 3, 4

  Red Hat Enterprise Linux AS 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8
  Red Hat Enterprise Linux ES 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8
  Red Hat Enterprise Linux WS 3.0, stock 2.4.21, updates 2.4.21-15, 6, 7, 8

- SUSE Linux Enterprise Server 10
  SUSE Linux Enterprise Server 9 SP4 (Beta)
  SUSE Linux Enterprise Server 9, SP1, SP2, SP3
  (Listed versions are also supported with no service pack.)

  openSUSE 10.2 (formerly known as SUSE Linux 10.2)
  SUSE Linux 10.1
  SUSE Linux 10
  SUSE Linux 9.3
  SUSE Linux 9.2, SP1
  SUSE Linux 9.1 — stock 2.6.4-52

- Ubuntu Linux 6.10
  Ubuntu Linux 6.06
  Ubuntu Linux 5.10
  Ubuntu Linux 5.04

  Important: On 64-bit Ubuntu 6.x hosts, some 32-bit compatibility libraries are required. Specifically, 32-bit `glibc` and `X11` are required.

See the *VMware Guest Operating System Installation Guide* for version details about these operating systems. A Web browser is required for the Help system.

ACE 2 Management Server

The following sections describe the ACE 2 Management Server system requirements.

Hardware

- 1200MHz or faster compatible x86 and x86-64 architecture processor (recommended; 800MHz 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, AMD64 Opteron, Athlon 64
- Multiprocessor systems supported
- Experimental support for Intel IA-32e CPU
- Memory:

  1024MB recommended, 256MB minimum

Display

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

Disk Drives

40MB free space required for basic installation; at least 10GB free disk space recommended

Local Area Networking

Any Ethernet controller supported by the operating system

Windows Operating Systems

- Windows Server 2003 Web Edition SP1, SP2, Windows Server 2003 Standard Edition SP1, SP2, Windows Server 2003 Enterprise Edition SP1, SP2 (includes 64-bit and R2 editions)
- Windows XP Professional (includes 64-bit editions)
- Windows 2000 Server Service Pack 4, Windows 2000 Advanced Server Service Pack 4

Linux Operating Systems

- Red Hat Enterprise Linux Advanced Server 4.0 with Update 4.
- SUSE Linux Enterprise Server 9 Service Pack 3

External Databases

The SQLite database engine is embedded in the ACE 2 Management Server.

In addition, you can use external databases, through ODBC connectivity:

- For Windows-based servers: Microsoft SQL Server 2000 or higher; Oracle Database 10*g*
- For Linux-based servers: PostgreSQL 7.4 or higher.
- Red Hat Enterprise Linux Advanced Server 4.5 or higher.

Web Browsers

Required for ACE 2 Management Server configuration and ACE 2 Management Server Help Desk Web application:

- Mozilla Firefox 1.52 or higher Web browser
- Internet Explorer 6.0 or higher Web browser

Learning the Basics of Workstation ACE Edition 2

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

Terminology for This Chapter

The following terms are used frequently in this chapter. For definitions of other ACE terms, both in this chapter and in the rest of the manual, see "Glossary" on page 267.

- **ACE Option Pack** – The additional licensing required to convert an installed copy of Workstation 6 into Workstation ACE Edition.
- **Workstation ACE Edition** – The program used by the administrator to create, deploy, and update ACE packages and manage ACE instances. Workstation ACE Edition is enabled by installing Workstation 6 and entering an ACE Option Pack key.
- **ACE instances** – The virtual machines that ACE administrators create, associate to virtual rights management (VRM) policies, and then package for deployment to users. In short form, an ACE instance is an ACE.

- **ACE 2 Management Server** – A server that can optionally be installed and used by the ACE administrator for activating and tracking ACE instances and for hosting dynamic policies for ACE instances.
- **ACE master** – A virtual machine template created by the ACE administrator. The master can be configured with various policies and devices and package settings and then used as the basis for creating any number of packages to be sent to ACE users.
- **Package** – An installable bundle for distribution to users. There are several different types of packages an ACE administrator can create including a full package, Pocket ACE package, policy update package, server update package, and custom package. A full package includes an ACE master configuration file, virtual disk files, policies, package installer, and Resources files for the ACE master. It also includes the virtual runtime environment (VMware Player) application used to run ACE instances. The other package types have a subset of these components.
- **Managed ACE instance** – An ACE instance that is managed by an ACE 2 Management Server.
- **Standalone ACE instance** – An ACE instance that is not managed by an ACE 2 Management Server. Any changes to its policies or other settings are made by the administrator's distribution of updates to the user.

Setting Up Your Administrative Workstation

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

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 the *Workstation User's Manual*. If you need to use an installer on a local drive, you can use the virtual machine's networking capabilities.

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

- **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 Workstation ACE Edition can be quite large. The default location for the package files is a folder named `Packages` inside the ACE master's folder. When you create a package, you can change the location for the package's files.

  In addition, Workstation ACE Edition 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 can move or delete files on the target drives to make room for the wizard's working files.

Overview of the Workstation ACE Edition Window

You use the Workstation ACE Edition window to handle most ACE administration tasks, including

- Creating and configuring ACE masters – For details, see Chapter 5, "Creating and Configuring ACE Masters," on page 91.
- Setting policies for ACE masters – For details, see Chapter 6, "Setting and Using Policies and Customizing VMware Player," on page 107.
- Setting package settings for ACE masters – For details, see Chapter 7, "Package Settings," on page 169.
- Packaging those ACE masters with their policies and the VMware Player application (or packaging just updated policies) – For details, see Chapter 8, "Creating Packages and Deploying Them to Users," on page 187.
- Testing or previewing your ACE packages or updated policies before you distribute them – For details, see Chapter 9, "Preview, Save, Test, Publish," on page 199.

If you set up one or more ACE 2 Management Servers in Workstation ACE Edition as part of your ACE setup, you also use the controls and options in the Workstation ACE Edition window to manage the ACE masters that you associate to those servers.

Topics in this section are:

Accessing Commands in the Workstation ACE Edition Window

You have several options for accessing commands in the interface:

- Menu options
- Right-click context menus
- Commands shown in the summary view for the open ACE master

This manual will typically list just the menu option when describing procedures. You can of course use whichever access option is most convenient. When there is no menu option available—for example, Publish policies to server is only available in the summary view—then the manual describes the step using the appropriate option.

Workstation ACE Edition Window Elements

The Workstation ACE Edition window differs only slightly from the standard Workstation window. Like that window, it incorporates:

- Home page, Summary view, and Console view
- Toolbars
- Sidebar

For details of the standard Workstation window, including how to use and customize those window elements, see "Overview of the Workstation Window" in the *VMware Workstation User's Manual*.

In addition to the standard Workstation window elements, the Workstation ACE Edition window includes:

- ACE master icons in the Sidebar
- The Recent ACE 2 Management Servers segment in the Sidebar
- Summary views with layouts and commands specific to ACE masters
- New ACE Master and Open Existing VM, Team, or ACE Master icons on the Home page
- Instance view for ACE instances that are activated and tracked on an ACE 2 Management Server
- The ACE menu
- The ACE Master Toolbar, containing Edit Policies, Edit Package Settings, Create new package, Create Pocket ACE package, and Preview in Player icons
- The New ACE Master and Connect to ACE 2 Management Server commands in the File menu

The following subsections describe how to use these Workstation ACE Edition window elements.

ACE Master Icons in the Sidebar

The ACE Master icon () designates the item as an ACE master, a virtual machine template created by the ACE administrator. The master can be configured with various policies and devices and package settings and then used as the basis for creating any number of packages to be sent to ACE users.

Adding ACE Masters to ACE 2 Management Servers

If you have installed and configured one or more ACE 2 Management Servers, you can associate ACE masters to those servers and then use the servers to activate instances, track instances, and dynamically update policies, instance customization data, and other per-ACE-instance data.

See Chapter 4, "Installing and Configuring the ACE 2 Management Server," on page 53 for details on how to install and configure the ACE 2 Management Server to manage ACE deployments.

You associate an ACE master with an ACE 2 Management Server when you create the ACE master through one of these methods:

- Create a new ACE master with the New ACE Master Wizard. See Chapter 5, "Creating and Configuring ACE Masters," on page 91.
- Clone an existing virtual machine into an ACE master (Use the **Create an ACE master from an existing virtual machine** option in the New ACE master wizard or **VM > Clone to ACE Master**). See Chapter 5, "Creating and Configuring ACE Masters," on page 91.

Each method includes a step that allows you to choose an ACE 2 Management Server for the ACE master by specifying the server address and port.

Viewing ACE Masters in the Sidebar

An ACE master might not appear in the sidebar if it has been removed from the list but not deleted from the disk. If you can locate the master's configuration file on the disk, you can add the master back to the sidebar.

Using the ACE Icons on the Home Page

In addition to the standard Workstation icons, the Home page for Workstation ACE Edition contains these icons:

- New ACE Master
- Open Existing VM, Team, or ACE Master

Viewing the Summary for an ACE Master

To view a full summary of an ACE master, click the name of the ACE master in the sidebar. The summary shows all the details about the ACE master, as shown in the following screenshot:

The parts of the ACE master summary view are:

- **Header –** Contains the ACE master name, the date the ACE master was last modified, the directory containing the .vmxa file, and the name of the ACE 2 Management Server (if any) used with this ACE master.
- **Commands –** Lists commands and actions that you can perform
- **Policies –** Lists the policies that you can apply to ACE masters
- **Notes –** Provides a text area where you can enter notes about your ACE master
- **Package Settings –** Lists the package settings that you can set and have applied to every package you create
- **Package History –** Lists a history of the packages created with this ACE master. Notes that were added to the package when it was created are displayed in the list. See Step 7on page 191 for more detail on how to enter those notes. You can view the properties of the packages that you have created by double-clicking on an item in the Package History and edit the notes that are displayed in the Package History. See "Viewing Package Properties" on page 196 for detailed information.

Viewing the Summary for All ACE Instances Managed by an ACE 2 Management Server

You can view a summary of all the ACE instances managed by an ACE 2 Management Server. You can set up queries to filter these summary views. See Chapter 12, "Instance View," on page 243 for details.

ACE Menu

The ACE menu provides these commands:

- **Policies** – Opens the policy editor. See Chapter 6, "Setting and Using Policies and Customizing VMware Player," on page 107.
- **Package Settings** – Opens the package settings editor. See Chapter 7, "Package Settings," on page 169.
- **Preview in Player** – Starts the Preview feature, which allows you to preview how an ACE instance created from this ACE master will run on the user's machine in the VMware Player application. See Chapter 9, "Preview, Save, Test, Publish," on page 199.
- **New Package** – Starts the New Package Wizard. See Chapter 8, "Creating Packages and Deploying Them to Users," on page 187.

- **New Pocket ACE Package** – Starts the Pocket ACE Package Wizard. See Chapter 10, "Pocket ACE," on page 207.
- **ACE Server** – Opens the ACE Server dialog box, which allows you to choose, for a managed ACE master, a different ACE 2 Management Server than the one with which it is currently associated. See "ACE Server Settings" on page 103.
- **Clone** – Starts the Clone ACE Master Wizard. See "Cloning an ACE Master from an Existing ACE Master" on page 99.
- **Delete from Disk** – Deletes the selected ACE master from the disk. A warning message appears before the ACE master is deleted, asking whether you are sure that you want to take this irreversible action of deleting this ACE master's files.

New ACE Master, Connect to ACE 2 Management Server, and Open Hot Fix Commands in the File Menu

You use the New ACE Master command to start the New ACE Master Wizard. See "Creating a New ACE Master" on page 92 for information about using the wizard.

You use the Open Hot Fix command to respond to a hot fix request from an ACE user. See "Responding to Hot Fix Requests" on page 235 for information about hot fix requests.

You use the Connect to ACE 2 Management Server command to open the Connect to ACE 2 Management Server dialog box. See "Using the Connect to ACE 2 Management Server Command to Open an Instance View" on page 252 for information about using the command.

ACE Master Toolbar

The ACE Master Toolbar contains these icons:

- **Edit Policies** – Opens the policy editor. See Chapter 6, "Setting and Using Policies and Customizing VMware Player," on page 107 for information about policy settings.
- **Edit Package Settings** – Opens the package settings editor. See Chapter 7, "Package Settings," on page 169 for information about the settings.
- **Create new package** – Opens the New Package Wizard. See Chapter 8, "Creating Packages and Deploying Them to Users," on page 187 for information about the using the wizard to create packages.

- **Create Pocket ACE package** – Opens the Pocket ACE Package Wizard. See "Creating an ACE Package for Portable Devices" on page 208 for information about using the wizard.
- **Preview in Player** – Allows you to run an ACE instance as it will run on the user's machine as well as view the effects of changed policies as they will appear on the user's machine. See Chapter 9, "Preview, Save, Test, Publish," on page 199 for information about using the Preview mode.

Creating Packages to Distribute to Users

Using Workstation ACE Edition, create packages to distribute to your ACE users. A Full package includes:

- A virtual machine configuration file, data, policies, preferences, and resources
- The VMware Player application to run the ACE instance on the ACE user's machine, or, for Pocket ACE instances, the installer for Player
- A set of policies to control the capabilities of the ACE instance
- Other "Resource" files for the ACE master

Other package types available from the New Package Wizard are Policy Update/Server Update and Custom. For more about package types, see Step 8, "Select a package type on the Package Type page and then click Next.," on page 192. See "Creating an ACE Package for Portable Devices" on page 208 for information about creating Pocket ACE packages.

For more information on VMware Player, see Chapter 11, "Installing and Using VMware Player and ACE Instances," on page 215.

Basic Steps for Creating and Deploying ACE Packages

This section describes how to create and deploy ACE packages.

To create and deploy an ACE package

1 Create a new ACE master or clone an existing ACE master or existing virtual machine to an ACE master.

See Chapter 5, "Creating and Configuring ACE Masters," on page 91.

2 Install guest operating systems, VMware Tools, and other software in the virtual machines.

For information on installing VMware Tools, see the *Workstation User's Manual*. 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.

3 Set policies for the ACE master.

Use policies to control what your users can do with their ACE instances—for example, what network access they have from the ACE instances and what devices on their host computers they may use in the instances. See Chapter 6, "Setting and Using Policies and Customizing VMware Player," on page 107.

4 Set package settings and virtual machine settings for your ACE master.

See Chapter 7, "Package Settings," on page 169 and Chapter 5, "Creating and Configuring ACE Masters," on page 91.

5 Create packages to deploy to your users.

Workstation ACE Edition guides you through the process. See Chapter 8, "Creating Packages and Deploying Them to Users," on page 187 or "Creating an ACE Package for Portable Devices" on page 208.

6 Give the packages to your users.

Distribute the packages on CD, DVD, or portable media, or make them available on a network.See Chapter 8, "Creating Packages and Deploying Them to Users," on page 187 or "Deploying the ACE Package on a Portable Device" on page 211.

Keeping Users Up-to-Date

Workstation ACE Edition gives you tools you can use to ensure that your users are running up-to-date ACE instances. You can provide a new package—to replace an ACE master, to distribute an additional ACE master or to change the policies applied to the VMware Player application or to the ACE instance.

You might need to provide updates to users' packages. You might need to update the guest operating system or provide an update to a program running inside the ACE instance. Or you might need to update either the ACE instance itself or policies set for the package.

CAUTION If you replace an existing ACE instance by supplying a new package, your users lose any data or custom settings stored in it.

For information on these topics, see "Deploying Packages" on page 197.

Troubleshooting Users' Problems

Your users might need help with lost passwords, expired ACE instances, or copy-protected ACE instances that they have moved to a different location.

For managed ACE instances, you can fix those problems by using the Instance View in Workstation ACE Edition or by using the Help Desk Web application. See Chapter 12, "Instance View," on page 243 and "Using the VMware Help Desk Web Application" on page 237, respectively, for details.

For standalone ACE instances, you can use the vmware-acetool command-line program to fix those problems directly on the users' machines. See "ACE Tools: vmware-acetool Command-Line Tool" on page 234 for details. You can also use the hot fix feature to respond to these problems. For information on using the hot fix feature, see "Setting Hot Fix Policies" on page 154 and "Responding to Hot Fix Requests" on page 235.

You might find it useful to modify the configuration of a ACE instance on an user's computer. You can do so if you have enabled the administrator mode, providing administrator access in VMware Player to the ACE instance on the user's machine, in that package. For information, see "Setting Administrator Mode Policies" on page 152.

Installing, Configuring, and Upgrading Workstation ACE Edition

3

For information about installing, uninstalling, and configuring Workstation ACE Edition on your workstation as well as related installation, licensing, and upgrade topics, see:

ACE Option Pack and ACE Client Licenses

Many of the administrator features and controls of ACE 2 are built into Workstation 6. To expose these ACE 2 features, users of Workstation 6 must acquire the ACE Option Pack.

The ACE Option Pack is a license enablement that turns an existing copy of Workstation 6 into Workstation 6 ACE Edition. There are no new software downloads required.

The following sections describe the ACE Option Pack and ACE client licenses.

ACE Option Pack License

After entering the ACE Option Pack license into a copy of Workstation 6, your copy of Workstation will become Workstation ACE Edition. Workstation ACE Edition has the ability to generate ACE packages containing ACE virtual machines. All ACE packages require an ACE client license on the target end-user's machine. An ACE client license is

a serial number-based license key that must be entered upon powering on an ACE (if no license key is detected) or by choosing **VMware Player > Enter ACE Client License**. The ACE client license is tied to the device itself whether that device is a PC, laptop, or a portable media device such as a USB flash drive (storing a Pocket ACE).

ACE Volume Licensing Key

ACE 2 introduces a volume license key as well. This volume license key is available with both the Standard and Enterprise editions of the product. A copy of Workstation ACE Edition using a volume license key automatically embeds an ACE client license in all of your ACE packages. ACE packages with an embedded license do not require a user to enter a serial number for an ACE client license at the time of installation.

ACE Client License

An ACE client license is a device-specific license. The details of these licensing terms are covered in the End User License Agreement for ACE published on www.vmware.com. A licensed device is able to run any number of ACE instances. The ACE client license is associated with the device it is installed on and is not tied to a specific ACE instance. Devices include PCs, laptops, and portable media devices such as USB flash drives (storing a Pocket ACE).

Use of the ACE volume license key is a convenience tool for ACE administrators. The same device-specific licensing rules apply: An ACE client license must be associated with each device that has an installed ACE instance.

To enter an ACE Option Pack License key

1 Obtain the serial number for your ACE Option Pack.

2 Start up the Workstation application.

3 Chose **Help > Enter Serial Number**.

4 Type the serial number in the appropriate field and enter your name and the organization name in the dialog box.

5 Click **OK**.

6 Shut down the Workstation application and then restart it. Workstation will be converted into Workstation ACE Edition, which provides all of the features of Workstation 6, plus those features specific to ACE.

To enter an ACE Volume Licensing Key

1 Obtain the serial number for your ACE volume license key.

2 Start up the Workstation application.

3 Chose **Help > Enter Serial Number**.

4 Type the serial number in the appropriate field and enter your name and the organization name in the dialog box.

5 Click **OK**.

6 Shut down the Workstation application and then restart it. If you have already entered the ACE Option Pack license, there will be no visible differences in the product but your ACE volume license key will now be available for use during the ACE package creation process.

To enter the ACE client license key on an end-user's device

ACE packages created without the use of an ACE Volume License Key will require manual entry of an ACE client license key the first time you power-on after installation.

1 Obtain the ACE Client License serial number.

2 Double-click the desktop shortcut for the installed ACE instance.

3 At the prompt, enter the serial number in the appropriate field and enter your name and the organization name in the dialog box.

4 Click **OK**.

5 If you need to subsequently change or update the ACE Client License:

   a Choose **VMware Player > Enter ACE Client License**.

   b Enter the serial number in the dialog box. If you need to purchase a license, click **Get Serial Number** and follow the directions to get your license.

   c Click **OK**.

NOTE If you are not using an ACE volume license key, be aware that when you deploy a Pocket ACE to a portable media device, you should enter an ACE client license immediately. The Pocket ACE will run locally on that copy of Workstation ACE Edition, but if it is moved to another unlicensed device without having the ACE client license entered, it will not power on.

ACE 2 Management Server Licenses

The optional ACE 2 Management Server requires its own license. See information about how to enter that license in Step 3 on page 78 under "Configuring the ACE 2 Management Server."

NOTE If you do not configure the server and enter the license in the server setup Web application, you can't connect to the server in Workstation ACE Edition. Neither Workstation ACE Edition nor ACE instances will be able to connect to an ACE Server with an expired or non-existent license.

Setting Preferences for Workstation ACE Edition

The Preferences dialog box allows you to change a number of settings that apply to Workstation ACE Edition itself. 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.

For information on setting these preferences, see the *Workstation User's Manual*.

Installing ACE Instances on User Machines

The procedures for installing and uninstalling ACE instances from both Windows and Linux host computers are described in Chapter 11, "Installing and Using VMware Player and ACE Instances," on page 215.

The flexibility and modularity of the ACE 2 instances allow you to install and uninstall ACE instances in new ways, as described in these topics:

- "Installing Multiple ACE Instances on a Single User Machine" on page 48
- "Uninstalling Individual ACE Instances and Workstation ACE Edition" on page 49
- "Uninstalling Individual ACE Instances and Workstation ACE Edition" on page 49
- "Upgrading from VMware ACE 1.x to VMware ACE 2" on page 49

Installing Multiple ACE Instances on a Single User Machine

ACE 2 allows you or your ACE users to install multiple ACE instances on the same machine. This flexibility means that you and the ACE users can install and run ACE

instances from different vendors and that are governed by different policies, all on one system.

Uninstalling Individual ACE Instances and Workstation ACE Edition

ACE 2 allows you or ACE users to uninstall individual ACE instances and Workstation ACE Edition independently of each other. This flexibility enables ACE users to uninstall individual ACE instances or Workstation ACE Edition while leaving other ACE instances installed.

Upgrading from VMware ACE 1.x to VMware ACE 2

If you have VMware ACE 1.x projects, you can use the upgrade tool provided with Workstation ACE Edition to upgrade the virtual machines in those projects.

Before You Begin Upgrading Virtual Machines

Read the following before you begin the upgrade procedure:

- You must have both an administrator machine (has Workstation ACE Edition installed) and a user's machine (does not have Workstation ACE Edition or VMware ACE Manager software installed) to perform the upgrade procedure.
- You must also have your own notes about any VMware ACE 1.x policy settings for that you will want to manually apply to the upgraded machines. The policies for both the VMware ACE 1.x project and its virtual machines are not carried over during the upgrade. You can use these notes to configure the VMware ACE 2 policies for the virtual machines.
- If your ACE 1.x ACE instances are set to use Active Directory authentication, you must create and deploy an ACE 1.x policy update to use password authentication before you begin the ACE 2.0 upgrade procedure documented below.
  - Refer to "Setting Authentication Policies" on page 81 of the VMware ACE 1.x Administrator's Manual for information on authentication policies.
  - Refer to "Updating Virtual Machines" on page 141 of the VMware ACE 1.x Administrator's Manual for information on policy updates.
- Upgraded machines will include:
  - Upgraded hardware version
  - Guest operating system, applications, script files, and VMware Tools previously installed in the ACE 1.x virtual machine

- Connection to a VMware ACE 2 Management Server, if you choose this option during the part of the upgrade that occurs on the administrator machine
- Authentication password and revert to original installed ACE environment (RTI) snapshot – If these options were included in the VMware ACE 1.x machine, they will be carried over during the upgrade.

- Upgraded machines will not include:
  - Upgraded VMware Tools – These machines will continue to use the version of the VMware Tools installed in the VMware ACE 1.x machine, and therefore VMware ACE 2 features that require the latest Tools version will not be available on these machines.
  - The VMware ACE 1.x policies that were set for the virtual machine and for the project – During the part of the upgrade that occurs on the administrator machine, you can change ACE 2 policies and package settings. If you choose not to change any, the default ACE 2 policies and package settings are used.

Steps for Upgrading VMware ACE 1.x Virtual Machines to VMware ACE 2 Virtual Machines

To create the upgrade package

NOTE After you have completed the upgrade procedure, restart your system when you are prompted to do so.

1. Power off the ACE virtual machines in the ACE 1.x project.
2. Delete any snapshots for those virtual machines.
3. On your administrator machine, start up Workstation ACE Edition , browse to one of the ACE 1.x virtual machines in the project, and open the virtual machine by clicking the virtual machine's `<virtual_machine_name>.vmx` file icon.
4. Select **VM > Upgrade** or change version and select **Workstation 6** as the hardware version to which this machine is to be upgraded.
5. Select **VM > Clone to ACE Master**.
6. In the Clone to ACE Master Wizard, give the ACE master exactly the same name as the name of the ACE 1.x virtual machine. For example, if the 1.x name is `winXPPro.vmx`, then type **`winXPPro`** (minus the file extension, which is added automatically) into the **Name** field on the Name the ACE Master page of the wizard. The original ACE 1.x virtual machine folder name must also match the virtual machine name.

7 Complete the rest of the pages of the wizard (see "Cloning an ACE Master from an Existing Virtual Machine" on page 100 for detailed instructions on using the wizard). On the ACE Server page, choose whether or not to manage this ACE master with an ACE 2 Management Server.

8 After the Clone to ACE Master Wizard has finished, open the policy editor (**ACE > Policies**) if you want to make any changes to the default policy settings for this master.

NOTE The policies that were set for the 1.x virtual machine are not carried over to this ACE master. The default policy settings for ACE 2 are used unless you edit the policy settings and save the changes.

---

9 Edit any package settings and virtual machine settings that you want to change from the default settings for the ACE master (**ACE > Package Settings** and **VM > Settings**, respectively).

10 You do not need to update VMware Tools during the upgrade. To turn off the VMware Tools check during the package process, see "To turn off the VMware Tools check that occurs during packaging" on page 190. Be sure to close the Workstation application before editing the preferences.ini file and then restart Workstation.

11 Create a package with the New Package Wizard (**ACE > New Package**). Use the Full package type.

To deploy the upgrade package

1 Navigate to `Program Files\VMware\VMware Workstation` and run `ace_upgrade.exe` to start the upgrade wizard, which you will use to change the full package you created in Step 11 to an upgrade package. Follow the instructions in the wizard. You will be asked to browse to both the VMware ACE 1.x virtual machine and to the VMware ACE 2 package of the same name as the 1.x virtual machine.

2 If you are using a managed ACE 2 master and enterprise license, close and reopen the ACE Master and republish policies for the license to be properly updated.

3 Deploy the upgrade package you created in Step 1 to the ACE user's machine.

4 Make sure to power off all ACE 1.x virtual machines by shutting down the guest operating systems of each virtual machine.

5 From the package, run `ace_upgrade.exe` (don't run `setup.exe`). The `ace_upgrade.exe` program uninstalls ACE Player 1.x and then installs VMware Player and the ACE package.

6 Click the shortcut for the installed ACE package on the desktop to run the ACE virtual machine. Policies and the virtual hardware version are upgraded at the first run. If the ACE 1.x virtual machine had a password, you are prompted to enter that password before the ACE instance is activated.

NOTE A reimage snapshot is not taken following the completion of the upgrade procedure. Manually take a snapshot after you have performed the upgrade.

7 Go through any required steps to activate and authenticate the upgrade machine, and then power it off and exit.

8 Repeat this procedure for any other virtual machines in the VMware ACE 1.x project that you want to convert.

Installing and Configuring the ACE 2 Management Server

4

The ACE 2 Management Server allows you to manage ACE instances in real time. By including the ACE 2 Management Server in your system setup, you can:

- Manage activation of ACE packages (determine who can deploy a package).
- Manage authentication of those activated packages (determine who can run managed ACE instances).
- Dynamically deliver policy updates to managed ACE instances.
- Dynamically deliver instance customization data for managed ACE instances with Windows guest operating systems. (See "Instance Customization" on page 170 for information.)

NOTE Use of the ACE 2 Management Server is optional. If you do not need ACE 2 Management Server functionality for your ACE deployments, skip to Chapter 5, "Creating and Configuring ACE Masters," on page 91.

The following topics are covered in this chapter:

ACE 2 Management Server Setup Options

NOTE Make sure the clock on the host system that has ACE 2 Management Server installed or running the ACE 2 Management server appliance is synchronized with the client system. Use Network Time Protocol (NTP) to synchronize the clocks.

To set up an ACE 2 Management Server, you can choose any of the following options. If you set up multiple ACE 2 Management Servers, they must all be the same type.

- Install the server on a Windows host system – See page 56 for a list of supported Windows host systems.
- Install the server on a Linux host system – See page 56 for a list of supported Windows host systems.
- Download and configure the ACE 2 Management Server Appliance – See "System Requirements for the ACE 2 Management Server," the next topic, for basic information about this option.

You can download the ACE 2 Management Server appliance from the ACE 2 page and configure it as your ACE 2 Management Server.

A virtual appliance is a pre-built, pre-configured and ready-to-run software application packaged with the operating system inside a virtual machine.

The ACE 2 Management Server Appliance is a self-contained, pre-installed, pre-configured ACE 2 Management Server packaged with a small operating system in a virtual machine.

By default, the appliance attempts to configure its network by using DHCP. You can optionally configure the network settings yourself, using the supplied ACE 2 Management Server Appliance Configuration and Management Web interface. You can use that same interface to update the appliance when updates become available.

You must have access to a Web browser (Mozilla 1.52 or higher or Internet Explorer 6.0 or higher) to change network settings or obtain updates for the appliance.

NOTE You must have TLS configured on your Web browser to operate the ACE 2 Management Server. If you are using Internet Explorer, choose **Tools > Internet Options > Advanced** and scroll down to **Security**. Make sure the **Use TLS 1.0** check box is selected. Then click OK. If you are using Mozilla, choose **Tools > Options > Advanced** and make sure the **Use TLS 1.0** check box is selected. Then click **OK**.

Installation instructions for the appliance begin on page 69.

System Requirements for the ACE 2 Management Server

The following sections describe the system requirements for the ACE 2 Management Server.

Hardware

- 1200MHz or faster compatible x86 or x86-64 architecture processor (recommended; 800MHz 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™, AMD64 Opteron, Athlon 64
- Multiprocessor systems supported
- Experimental support for Intel IA-32e CPU
- Memory:

  1024MB recommended, 256MB minimum

Display

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

Disk Drives

40MB free space required for basic installation; at least 10GB free disk space recommended

Local Area Networking

Any Ethernet controller supported by the operating system

Operating Systems

The following sections describe the supported operating systems for the ACE 2 Management Server.

Supported Windows Host Systems

- Windows Server 2003 Web Edition SP1, Windows Server 2003 Standard Edition SP1, Windows Server 2003 Enterprise Edition SP1 (includes 64-bit and R2 editions)
- Windows XP Professional (includes 64-bit editions)
- Windows 2000 Server Service Pack 4, Windows 2000 Advanced Server Service Pack 4

NOTE At this release, an ACE 2 Management Server running under a Windows 2000 operating system cannot be configured for Active Directory integration.

Supported Linux Host Systems

- Red Hat Enterprise Linux Advanced Server 4.0 with Update 4.
- SLES 9 Service Pack 3

External Databases

The SQLite database engine is embedded in the ACE 2 Management Server.

In addition, you can use external databases, through ODBC connectivity:

- For Windows-based servers:
  - Microsoft SQL Server 2000 or higher
  - Oracle Database 10*g*
- For Linux-based servers: PostgreSQL 7.4 or higher

Web Browsers

One of the following Web browsers is required for ACE 2 Management Server configuration, as well as for configuration of the ACE 2 Management Server Appliance, if you choose that server option:

- The Mozilla Firefox 1.52 or higher Web browser
- Internet Explorer 6.0 or higher Web browser

NOTE Make sure that TLS is enabled on your browser.

Features of the ACE 2 Management Server

The ACE 2 Management Server has the following features:

- Scalability and reliability
  - You can increase capacity by adding network resources such as load balancers and extra server hardware.
  - For single-server small-size to medium-size deployments, the default embedded backing store provides a simple and efficient database solution. To scale the ACE 2 Management Server for large deployments, you can configure and use an external RDBMS.
  - Server requests are handled by multithreaded processes with the Windows operating system and by multiple processes in Linux operating systems. If one process dies, another takes over.
- Active Directory Integration
  - You can use Active Directory to authenticate users of ACE instances.
  - No schema change for your existing Active Directory is required.
  - LDAP is used to access Active Directory.
  - Information about Windows domain user account states is provided in clear and useful messages. Reasons for login failures are presented as “locked out” or “password expired.”
  - The ACE 2 Management Server acts as an Active Directory password change proxy.
  - You can use the instance customization feature in ACE with your own established naming conventions to associate users with machines.
- Security
  - Communications are SSL-encrypted. Communications between server and clients, over HTTPS traffic.
  - Passwords are stored securely in hashed form in the backing store.

- Database Options

  Flexible database options allow use of an embedded database or external RDBMS's to store ACE instance data and policies. (See "Database Options" on page 59 for details.)

- Simple Installation and Configuration
  - The server uses off-the-shelf software components:
    - Apache Web server 2.0
    - The default SQLite database store
  - The server setup uses industry-standard protocols:
    - HTTPS and LDAP
    - xml-rpc for message encapsulation
  - Client traffic can be proxied by off-the-shelf products.
  - The Windows installer for Workstation ACE Edition includes the installation components for the ACE 2 Management Server.
- Extensibility and Availability
  - You can create and use more than one ACE 2 Management Server. When you use more than one server, you can set the servers up so that they will share the same database for load balancing or increased fault tolerance. To use increased fault tolerance, you will have to use an external database. If your multiple servers do not need to share a database (the servers are independent of one another), you can use either the embedded database or an external RDBMS.
  - A Windows system ACE 2 Management Server can be on the same system as Workstation ACE Edition.
  - You can designate a single ACE 2 Management Server name, such as `https://ace.policyserver.company.com`, and use DNS lookup to translate the host name into an address. The address will be cached if a DNS server is not available. Additionally, different ACE 2 Management Servers can be used if users have to roam between offices in different geographic locations.

    NOTE Your server name must be either the machine name in English or the IP address. International characters are not supported.

Components of the ACE 2 Management Server

The components of the server are:

- The ACE 2 Management Server platform, based on the Apache 2.0 web server
- Backing store technology – Database layer for the server component (See "Database Options," the next topic, for details.)
- Active Directory integration
  - Permits joining an operating system that is running an ACE instance to the domain remotely.
  - In addition, provides search functions so you can quickly find a particular individual or group.
  - Enables you to use Active Directory Users and Groups to configure role-based access to the features of the ACE 2 Management Server.
- SSL certificate management – See "Using SSL Certification and Protocol" on page 61 for details.
- Event logging – See "Using Event Logs" on page 85.

Database Options

The ACE 2 Management Server offers two database options:

- Embedded SQLite database

  The default mode of the ACE 2 Management Server works with an embedded SQLite 3 database engine. The SQLite database engine is initialized during server installation and requires no special configuration. The embedded database supports up to several gigabytes of data.

- Supported external database

  If your enterprise IT environment requires the reliability and performance characteristics of a commercial database engine, you can use a supported external database as a backing store for the ACE 2 Management Server, through ODBC connectivity. Supported external database engines are Microsoft SQL Server (SQL Server 2000 or SQL Server 2005) and Oracle Database 10g for Windows-based servers and PostgreSQL 7.4 or higher for Linux-based servers.

NOTE If the ACE Management Server is deployed in the DMZ (de-militarized zone), then for security reasons you should use an external database located inside your corporate network behind a firewall.

Some common benefits of using an external database with the ACE 2 Management Server are:

- Online backup: You don't have to shut down the ACE 2 Management Server to back up the database.
- Enhanced security model: You can fine-tune permissions to access sensitive data. The SQLite database engine provides file-system based security.
- Performance fine-tuning.
- Ability to use external database management and reporting tools.

If your setup includes load-balanced ACE 2 Management Servers, you must use an external RDBMS as the backing store, because the SQLite database cannot be shared across processes running on multiple machines.

NOTE The SQLite database is file-based and is not designed to be effectively shared across multiple processes. If you use third-party tools to access the database for a read operation, therefore, you cannot depend on transactional isolation of the pending write operations of the ASM.

About Database Backup

If you are using an external database, you can use the backup/recovery strategy that you have determined is appropriate for your database system.

CAUTION We recommend that you back up your ACE 2 Management Server database on a regular basis to ensure that the database can be recovered promptly if needed.

If you are using the embedded database, you can use standard file-backup tools, such as `ntbackup` or `dd`. The data is stored in one of:

On Windows servers:

```
C:\Program Files\VMware\VMware ACE Management Server\db\acesc.bin.
```

On Linux servers:

```
/var/lib/vmware/acesc/db/acesc.bin
```

If you are using the embedded database in a production environment: Because SQLite is file-based, the database file could be modified by the ACE 2 Management Server process at the same time it is being copied for backup. Therefore, an inconsistent database snapshot potentially could be produced. This problem is unlikely to occur —because the file is usually not large and is copied quickly. To avoid the possibility of an inconsistent snapshot, however, you should: (1) stop the server, (2) copy the file to

an alternative location from which you will do the backup, and then (3) restart the server.

Other alternatives for backing up an open database, as recommended by members of an SQLite community, as discussed in this forum thread, are noted below:

http://marc.10east.com/?l=sqlite-users&m=111487876701133&w=2

- Log in to the SQLite database using the `sqlite3` command-line tool. Use the `.dump` command, store the result in a separate file, and back up that result file. It is a SQL script that will recreate the database.
- Using the Shadow Volume Copy mechanism on Windows systems or LVM volume snapshots on Linux (and the crash-restore feature of SQLite), back up the complete database directory, including journal files if they are present. This method is actually easier than it sounds: On a Windows XP SP1 or later operating system, just use `ntbackup` on the database directory. When the database is restored it should work fine.
- Log in to the database as described in the first method. Issue BEGIN EXCLUSIVE, copy the database file, and then issue COMMIT.

Integrating the ACE 2 Management Server with Management Tools or Automated Scripts

If you need to use your company's own management or reporting tools or automated scripts with the data in the VRM database, see "Appendix: Using the VMware ACE 2 Management Server Database Schema and Querying the Audit Event Log Data," which describes the schema for the database.

Using SSL Certification and Protocol

NOTE The ACE 2 Management Server must be configured to use SSL. For more information on configuring ACE 2 Management Server to use SSL, see "Configuring Multiple ACE 2 Management Servers to Use SSL" on page 65.

By default, the ACE 2 Management Server uses the SSL protocol to provide encrypted, secure communications. The server connects to its managed instances using SSL. If the server is integrated with an Active Directory service, it communicates with the service through an SSL-protected link.

The SSL (Secure Sockets Layer) protocol was developed by Netscape Communications Corporation to be used for secure document transmission over the Internet. SSL encrypts data through the use of a public-key/private-key pair: the public key is known

to everyone and the private key is known only to the message recipient. URLs that require an SSL connection start with https.

The following is a description of how the ACE 2 Management Server uses SSL.

At ACE 2 Management Server installation, two files are created:

- An RSA 1024-bit key (file name: server.key) – This is the private key.
- A *self-signed* certificate (file name: server.crt) – It is "self-signed" because its signature is verified by the public key, which is embedded in the certificate.

By default, these files are stored in the SSL directory in the VMware ACE 2 Management Server program directory.

The self-signed certificate, which is a public certificate, is valid for 10 years from the date and time at which the server is installed. The certificate file is encoded in PEM format. You can browse the file to see its properties as follows:

- On a Windows host system: In Windows Explorer, navigate to the location of the server.crt file and double-click the file name.
- On a Linux host system, use this command:

```
openssl x509 –in /var/lib/vmware/acesc/ssl/server.crt –text
```

NOTE As noted above, the self-signed certificate is valid for 10 years. If you should need to replace an expired certificate, you can do that by deploying the affected ACE masters in an update package, which would include the new certificate. Do not modify certificates to make them permanent.

When an ACE master connects to an ACE 2 Management Server, it downloads the public certificate for that server and any *chain of certificates* required to verify the server's public certificate. A server certificate might have a chain of several certificates that must be verified step by step until the verification process reaches the root (trusted) certificate in the certificate store. The first time a connection is made to a server by any ACE master on a Workstation ACE Edition administrator machine, the certificate is downloaded to the Workstation ACE Edition host system.

The store or collection of certificates that is downloaded when an ACE master connects to a server is included in each ACE package that you create with that ACE master. It is saved in the ACE Resources directory. When you deploy and run an ACE instance of this master, the VMware Player application uses the certificates included in the package to verify connections made to the ACE 2 Management Server. It verifies that the certificates that are in the ACE package match those provided by the server. If they do not match exactly, VMware Player displays an error message and does not run the instance.

NOTE If you change the custom SSL certificate for your ACE 2 Management Server, you need to update the Resource directory for all of your existing ACE instances. You can do this by creating and distributing a custom package that contains only Resources. See Chapter 8, "Creating Packages and Deploying Them to Users," on page 187 for more information.

VMware Player does an integrity check of the certificate store included in the package every time it communicates with the server.

The VMware Player application does not use any certificates stored in the host system, because their integrity cannot be verified.

NOTE ACE 2 Management Server only supports public key certificates that have been signed using the SHA1 algorithm. Any other algorithms will result in an error when the ACE is deployed.

Because the Player does not trust any certificates stored on the host machine that it is running on and instead relies on a complete certification chain that is included in the ACE package, the use of self-signed certificates is adequate for most security needs.

If, however, your enterprise requires the use of a certificate signed by a certificate authority (internal or commercial), you can set up that type of key/certificate pair for the ACE packages to use. A *certificate authority, or CA*, is an entity that issues and signs public-key certificates, typically for a fee. See "Setting Up Your Own Self-Signed Certificates, Third-Party Signed Certificates, or Certificates from an Internal Certificate Authority," below, for details.

Setting Up Your Own Self-Signed Certificates, Third-Party Signed Certificates, or Certificates from an Internal Certificate Authority

If you want to use custom SSL certificates, either your own self-signed certificates or those of a third-party or internal CA (certificate authority), you must provide the various needed certificate, key, and (in the case of CAs) certificate chain files. These files must be PEM-encoded. After you have created or obtained these files, you place them in the correct directory by uploading them from the Custom SSL Certificates page in the server setup Web application.

NOTE Workstation ACE Edition only supports certificate signatures that use the SHA1 algorithm digest.

To set up your own self-signed certificates, third-party signed certificates or certificates from an internal certificate authority

1 Ensure that you have configured the ACE 2 Management Server through the server configuration Web application.

2 Create or provide the needed files:

   a For your own self-signed certificate, use `openssl` to create a new self-signed certificate.

   b For a third-party CA or internal CA, obtain an SSL certificate signed by that CA, and a certificate-verification chain file.The chain file is a concatenation of every certificate required to verify the new SSL certificate you created or obtained.

   c A private key file.

   All these files must be PEM-encoded.

   Steps for obtaining the certificate chain vary depending on which host operating system you are using and on the source from which the CA certificate is obtained.

3 After you have obtained the items in Step 2, rename them as follows:

   - Private key file: Rename to `server.key`.
   - Certificate file: Rename to `server.crt`.
   - Certificate chain file: Rename to `chain.crt`.

4 Use the ACE 2 Management Server configuration Web application to upload the files. See Step 4 on page 82, under "Configuring the ACE 2 Management Server."

5 Stop and restart the Apache service. See "Stopping and Starting the Apache Service Manually" on page 85.

To update any existing ACE masters to use a new certificate and key file

1 Open the ACE master.

2 Create an update package.

   The package will contain the new certificate file and certificate chain.

Configuring Multiple ACE 2 Management Servers to Use SSL

The following describes various scenarios in which you might configure multiple ACE 2 Management Servers to use SSL.

- Multiple servers behind one or more proxy servers
  - Each server can have its own SSL key/certificate (ACE 2 Management Server and proxy server).
  - The cert_chain file must contain the certificate file and verification chain for the SSL certificates being used by the proxy servers. Place this cert_chain file in each of the ACE 2 Management Servers. (Follow instructions above on how to do that.)
  - In the case of self-signed certificates being used, the actual certificate is the verification chain, so the chain file would contain each self-signed certificate being used by the proxies.
  - It is also possible to use the same key/certificate for every server and proxy. In this case, it is not necessary to create a cert_chain file (unless you use CA signed certificates; then follow the instructions above for CA signed certificates).
  - Each certificate must have a unique common name.
- Multiple servers using DNS round robin
  - Each server can have its own SSL key/certificate (ACE 2 Management Server and proxy server).
  - The cert_chain file must contain the certificate and verification chain for every certificate being used by the servers. Place this certificate chain file in each of the ACE 2 Management Servers. (Follow instructions above on how to do that.)
  - In the case of self-signed certificates being used, the actual certificate is the verification chain, so the chain file would contain each self-signed certificate being used by each of the servers.
  - It is also possible to use the same key/certificate for every server. In this case, it is not necessary to create a cert_chain file (unless you use CA signed certificates; then follow the instructions above for CA signed certificates).
- Multiple servers without any round robin or behind any proxy servers: You don't need to do anything for this case. Because there is no DNS round-robin or proxy server, the ACE master behaves as if there is only one server it can talk to.

Installing the ACE 2 Management Server

Follow the instructions provided below for installing the server on your Windows or Linux system or for installing the ACE 2 Management Server Appliance.

NOTE Before you can create a managed ACE master, you must have an ACE 2 Management Server set up and configured. The New ACE Master Wizard requires connection to an ACE 2 Management Server before creation of an ACE master can be successfully completed.

Target hardware platform support for the ACE 2 Management Server is driven almost exclusively by the number of ACE instances being supported and the frequency with which they are configured to communicate with the server. VMware recommends that production deployments be installed on either a dedicated server or a virtual platform with sufficient available resources to ensure performance and stability. Refer to the sizing white paper for more detailed information on VMware performance testing. However, the ACE 2 Management Server has been tested and can be installed on desktop or workstation platforms to support a small number of clients or non-production evaluations.

Topics in this section are:

Default Port Assignments for the ACE 2 Management Server

The default port assignments used by the ACE 2 Management Server are:

Table 4-1. Port Assignments, Default Settings, for the ACE 2 Management Server

Port	Used For:
https port 443	Communications between the ACE 2 Management Server and ACE instances
https port 8000	ACE 2 Management Server Setup (configuration) Web application
	ACE Help Desk Web application
https port 8080	ACE 2 Management Server Appliance configuration

NOTE If you have another Web server installed that uses any of these default ports, you might need to resolve the conflict. See "Unblocking Port Traffic and Changing Port Assignments" on page 87.

Installation Options for the ACE 2 Management Server

Follow the installation instructions for your server installment option:

- "Installing the ACE 2 Management Server on a Windows System" on page 67
- "Installing the ACE 2 Management Server on a Linux System" on page 67
- "Installing the ACE 2 Management Server Appliance" on page 69

Installing the ACE 2 Management Server on a Windows System

Install the ACE 2 Management Server by launching the `vmware-ace-management-server` application from the server that the ACE 2 Management Server will reside on. The `vmware-ace-management-server.exe` file is available as a separate downloadable file in the same download location as the one for the Workstation ACE Edition application.

To install the server, follow the prompts in the installation wizard.

CAUTION On the Server Information page in the wizard, ensure that the server name you use matches the name of the machine on which you are installing the ACE 2 Management Server. If you set the server name to something other than this, you will not be able to log in to the ACE 2 Management Server after you finish the installation and ACE instances might have trouble making required connections to the server during activation.

NOTE If you are installing the server on a host computer that has a firewall enabled, you might see a message at the end of the installation asking whether you want to unblock the Apache service. Choose **Unblock**. The ACE 2 Management Server will not work properly if you do not unblock the service.

Installing the ACE 2 Management Server on a Linux System

You can install the ACE 2 Management Server on the following Linux systems:

- Red Hat Enterprise Linux 4
- SUSE Linux Enterprise Server 9 SP3

Before you install the ACE 2 Management Server on a Linux system:

- You must have a working installation of Apache 2.0 on the system. (The rpm for a Web server comes with your RHEL4 or SLES9 installation.) Verify that the Apache Web service is operating normally and is receiving requests for SSL http.
- You must have the `mod_ldap` and `mod_ssl` modules available on your system.
- The following packages are dependencies of the ACE 2 Management Server rpm:

  `curl, openldap, openssl, apache, gdbm`

  You must have these packages installed on your RHEL4 or SLES9 system before you install the ACE 2 Management Server.

  If you are going to use the external database option, then the following packages are dependencies as well:

  For RHEL4: `unixODBC`

  For SLES9: `unixODBC`, as well as `unixODBC-gui-qt` if you want to use the X11 graphical configuration tool

To install the ACE 2 Management Server on a Red Hat Enterprise Linux 4 or SUSE Linux Enterprise Server 9 system:

1 Run the appropriate `rpm` installer for the ACE 2 Management Server:

```
vmware-ace-management-server-<build_number>.i386-rhel4.rpm
vmware-ace-management-server-<build_number>.i386-sles9.rpm
```

2 For an SLES9 server, ensure that the LDAP module (`mod_ldap`) has been configured for loading:

   a Using a text editor, open this file:

   `/etc/sysconfig/apache2`

   b Add the config option "`ldap`" to the variable `APACHE_MODULES`.

   c Save and close the file.

Now continue with "Configuring the ACE 2 Management Server."

Installing the ACE 2 Management Server Appliance

To install the ACE 2 Management Server Appliance

1 Download the zipped file for the appliance from the ACE 2 release download page:

`VMware-ACE-Management-Server-Appliance-2.0.0-<NNNNN>.zip`

where <NNNNN> is the ACE build number.

2 Extract the zipped files to the directory where you want to have the server located.

3 Start up VMware Workstation ACE Edition and then choose **File > Open** to open and run `ams_appliance.vmx`.

4 At the password prompt, enter a password and confirm it. This password is used for both root and network accounts.

NOTE You must remember this password so that you can use it for later appliance management operations from the console and the Web.

At this point in the process the appliance attempts to configure its network by using DHCP.

NOTE The console view displays the following information:

- The current network settings
- The URLs for remotely administering the appliance and configuring the ACE Management Server itself:

  For the Appliance Management and Configuration application:

  `https://<hostIPaddress>:8080/`

  For the ACE 2 Management Server Setup application:

  `https://<hostIPaddress>:8000/`

(This information is displayed above each login prompt. If you press **Return** at the login prompt, the information is displayed again.)

---

5 At the time zone prompt, accept the current setting or make a change as needed.

6 Optional: If you would like to reconfigure the network—for instance, to configure the server to use a static IP address or to specify a proxy server—you can reconfigure the network settings from the current console view, by following the prompts and instructions on the screen. You can also reconfigure the network

settings by using the Appliance Management and Configuration application, as follows:

a Leave the ACE 2 Management Server Appliance running.

b Browse to:

```
https://<hostIPaddress>:8080/
```

c In the connection dialog box, type "**root**" in the user name field and your network/root password in the password field.

d Click the **Network** link on the first page of the Appliance Configuration and Management Web application to open the Network Configuration page.

e To view instructions about configuring network settings, click the **Help** link in the upper right of the Web page.

f After you've made the changes you want to make to the network settings, click **Apply**. If you want to revert to the settings that were on the page before you started making changes, click **Reset**.

7 Optional: You can obtain updates to this appliance when they become available. If you would like to reconfigure any update options—for example, if you want to disable automatic downloads of updates—you can do that by using the Appliance Management and Configuration application, as follows:

a Leave the ACE 2 Management Server Appliance running.

b Browse to:

```
https://<hostIPaddress>:8080/
```

c In the connection dialog box, type "**root**" in the user name field and your network/root password in the password field.

d Click the **Update** link on the first page of the Appliance Configuration and Management Web application to open the Appliance Update page.

e To view instructions about configuring update options, click the **Help** link in the upper right of the Web page.

8 When you have finished configuring any network or update settings, navigate to the ACE 2 Management Server Setup Web application to configure the server. To access that application, choose one of these methods:

- From within the Appliance Management and Configuration Web application page, click the **ACE Login** link at the top right of the page.

- Browse to the ACE 2 Management Server Setup Web application:

  `https://<hostIPaddress>:8000/`

9 Click **Configuration** to open the Web application.

Continue with the next topic, "Configuring the ACE 2 Management Server."

Configuring the ACE 2 Management Server

After you have installed the ACE 2 Management Server, you must use the ACE 2 Management Server Setup Web application to configure the server.

You need to provide your ACE 2 Management Server license before you can configure the server features ensure that you the license information available before you start the server setup application.

Before you start up the server setup application, you must complete the tasks described below if you will use any of the following optional features:

- Active Directory integration (using LDAP)
- An external database
- Custom SSL certificates

Tasks to Complete Before You Configure the Server

Before you start up the server setup Web application to configure the server, complete the procedures in this section that are applicable to your ACE 2 Management Server option.

- "Obtain Your ACE 2 Management Server License Information" on page 71
- "Using Active Directory Integration (Using LDAP)" on page 72
- "Using an External Database" on page 72
- "Using an External Database With the ACE 2 Management Server Appliance" on page 77
- "Setting Up Your Own Self-Signed Certificates, Third-Party Signed Certificates, or Certificates from an Internal Certificate Authority" on page 63

Obtain Your ACE 2 Management Server License Information

Obtain your license information (serial number) for the ACE 2 Management Server before you begin using the server setup Web application to configure the server. If you do not have a serial number available at the initial server configuration, you will not be

able to complete the configuration. As a result, the ACE 2 Management Server functionalities will not be available. These functionalities include but are not limited to connecting to the server from Workstation ACE Edition, assigning masters to be managed by the server, and using the Help Desk Web application.

See Step 3 on page 78 for information about how to enter the serial number for your ACE 2 Management Server in the server setup Web application.

See "ACE 2 Management Server Licenses" on page 48 for information about the license requirements for the server.

Using Active Directory Integration (Using LDAP)

This section describes how to use Active Directory integration.

To use Active Directory integration (using LDAP)

1 Create a user that the ACE 2 Management Server will use to connect to the LDAP server and use for querying. Find out what the user principal name is for that user.

   For example, create a user called `aceuser` whose UPN is `aceuser@vmware.com`.

2 Create an ACE Administrators group in the domain.

3 Add users who will be ACE administrators to that group.

4 If you will permit certain users to perform Help Desk tasks from with the Help Desk Web application but do not want to give them access to other administrative tasks, create a Help Desk group and assign users to it for the Help Desk role.

NOTE You can log into the Help Desk Web application with your administrative LDAP credentials or password. Creating a Help Desk role allows you to permit certain users to perform Help Desk tasks from within the Help Desk application but does not give them access to other administrative tools.

Using an External Database

This section describes how to use an external database.

To use an external database with any ACE 2 Management Server option

1 Install the RDBMS:

- On Windows – Microsoft SQL Server 2000 or higher and Oracle Database 10*g* are supported.
- On Linux – PostgreSQL 7.4 or higher is supported.

The external database does not have to be installed on the same server as the ACE 2 Management Server.

NOTE The ACE 2 Management Server will create the database schema automatically, provided proper access rights are granted.

2 Configure a database. Make sure you have a dedicated database (see the Note below) and a user account that has full access to this database, including rights to create tables. Ensure that you didn't give this database user permissions that it doesn't need; for example, for reading or writing to other databases managed by your RDBMS.

NOTE All tables in the database have a name starting with a `PolicyDb_` prefix and indices with `PdbIns_` or `PdbLf_` prefixes, so potentially you could provide the ACE 2 Management Server with a DSN to a database that it would share with some other application, if the database count is at a premium.

3 If you plan to have the ACE 2 Management Server connect to the database over the network (TCP socket connection), ensure that TCP connectivity is enabled in the database configuration options. Also ensure that the TCP connection is not blocked by firewall settings on either the database server or the ACE 2 Management Server system. Additionally, if you are using a PostgreSQL external database, you must configure per-user permission to connect to the database over the network. Configure that permission in the file `pg_hba.conf`, which is located in the root folder of your database.

4 To ensure smooth configuration of the ACE 2 Management Server, you could also verify the server's connectivity to the configured database with the configured user credentials by running a command-line or graphical SQL tool on the ACE 2 Management Server machine. Examples of such tools are sqlcmd.exe for SQL Server, sqlplus.exe for Oracle, and psql for Postgres. Refer to the respective database user manual for database configuration and verification instructions.

5 Create a System DSN entry on the ACE 2 Management Server machine. The only required information in DSN configuration is the DSN name, server IP address or host name, and the database name. In other words, you don't have to provide a user name and password in the DSN configuration. Any values entered here will

be ignored. You will provide a user name and password when configuring your ACE 2 Management Server using the Web Setup application.

NOTE Ensure that you create a System DSN and not a User DSN. If you were to create a User DSN, it would be visible only to your user account. The ACE 2 Management Server runs under the local system account, so a User DSN would not be visible to and therefore not usable by the server.

- For Windows-based systems:

  Using the ODBC Data Sources plugin (**Control Panel > Administrative Tools > Data Sources (ODBC)**), create a System DSN entry for connecting to this database using the proper driver (refer to your operating system and database documentation).

  NOTE ACE 2 does not support ODBC using an SQL Native Client driver on Windows 64-bit systems.

  If the DSN Setup wizard provides this option, test the connection to verify that it is working with the database user credentials.

  NOTE If your ACE 2 Management Server is running on a 64-bit Windows host system, do not use the default Control Panel plug-in to create the DSN. Using that default plug-in will result in your creating a DSN for a 64-bit subsystem, and that DSN will not be visible to the ACE 2 Management Server. Instead, navigate to %WINDIR%\syswow64\odbcad32.exe, and use that program to create a DSN for a 32-bit subsystem.

- For Linux-based systems:

  You must have the `unixODBC` rpm package installed on your Linux system for the external database option to be available in the ACE 2 Management Server Setup Web application.

  The `unixODBC` package provides an ODBC API to programs running on Linux systems that is similar to the Windows ODBC API. The package contains the `libodbc` shared library, providing the ODBC Driver Manager API to other programs, a set of configuration utilities, and ODBC drivers for popular databases. On both RHEL4 and SLES9, the ODBC driver for PostgreSQL is included in the `unixODBC` binary distribution package. To use the X11 graphical configuration tool `ODBCConfig` for setting up a DSN on your SLES9 system, you have to have the `unixODBC-gui-qt` package also installed (this utility is included in the RHEL `unixODBC` package).

Because `libodbc` is a shared library that implements industry-standard ODBC APIs, the ACE 2 Management Server application is not sensitive to the particular version of the `unixODBC` package installed on your Linux system, but we recommend that you update the package to the latest version released for your specific Linux distribution.

The DSN configuration for the `unixODBC` package is stored in the `/etc` directory (`/etc/unixODBC` for SLES) on your system (`odbc.ini` for DSNs and `odbcinst.ini` for driver and general ODBC system configuration). You can edit these plain-text files manually, or you can edit them more conveniently by using the `ODBCConfig` graphical (X11) utility. You have to be logged in as a root user to access the configuration files or run the ODBCConfig utility.

NOTE If you are using the ACE 2 Management Server Appliance, see the information about setting up an ODBC connection on page 77.

The `ODBCConfig` utility mimics the Windows ODBC Data Sources Control Panel plugin. When configuring a DSN for your database connection, ensure that you are using the correct ODBC driver (typically, `/usr/lib/libodbcpsql.so` or, on SLES 9, `/user/lib/unixODBC/libodbcpsql.so.2`). You also must configure the server address and the database name in the DSN settings.

See http://www.unixodbc.org/ for additional information about using `unixODBC`.

6 Make a note of the database information: database DSN, user name, and password. You need to enter that information during server setup.

Performance Optimization Tips for External Database Use

The following two subsections provide tips for optimizing server performance:

- "Ensure That the Server Has a Sufficient Number of Database Connections" on page 75
- "Enable Database Connection Pooling If Not Already Enabled" on page 77

Ensure That the Server Has a Sufficient Number of Database Connections

For the optimal server performance, the ACE 2 Management Server starts multiple parallel threads (on Windows) or processes (on Linux) listening for the incoming connections from the clients. Every client connection typically executes a database transaction, so it needs to open a database connection. It is possible that under a high load all available listening threads or processes would be processing client requests at

the same time, so that the ACE 2 Management Server would require at least as many database connections available for its use. If the server runs out of database connections, the clients might start receiving connection errors.

To ensure smooth operation of the server with an external database option, ensure that the server has a sufficient amount of database connections available for it. The maximum number of remote connections allowed to the database is a database configuration option (check your database manual for the information on how to configure it). You should configure at least as many connections as there could be parallel threads or processes in the Apache HTTP server running the ACE 2 Management Server component (or allow an unlimited number of connections).

To find out how many parallel threads or processes your Apache server could start, inspect the Apache configuration file, looking for the "prefork" or "MPM" section. The number of allowed clients is the lower bound for the required number of database connections. You can either reduce this number or increase the number of the allowed remote connections in the database.

As a rough guide, here is the location of the Apache configuration file per platform and the typical default number of connections:

On the Windows platform:

```
C:\Program Files\VMware\VMware ACE Management Server\Apache2\
               conf\httpd.conf
```

250 client connections (WinNT MPM section)

On the Linux RHEL 4 platform:

```
/etc/httpd/conf/httpd.conf
```

256 client connections (prefork MPM section)

On the Linux SLES 9 platform:

```
/etc/apache2/server-tuning.conf
```

150 client connections (prefork MPM section)

On the ACE 2 Management Server Appliance:

```
/etc/httpd/apache2.conf
```

20 client connections (prefork MPM section)

The default installation of the PostgreSQL database on RHEL Linux allows only 100 remote connections, which is less than the number of parallel threads started by the Apache server by default on the same platform, so you might want to change this number if you expect a high volume of client requests to your server (basically, if you have more than 100 active clients).

Enable Database Connection Pooling If Not Already Enabled

A useful performance optimization tip for servers on Linux platforms is to enable database connection pooling in the ODBC Driver Manager (it is disabled by default).

To enable database connection pooling on Linux platforms

1 Start the ODBCConfig utility as a root user.

2 Click the Advanced tab.

3 Select the checkbox for Connection Pooling.

Enabling this option can give a substantial performance gain under high load, as the ACE 2 Management Server can reuse the database connections rather than opening new one for every request.

On Windows platforms, ODBC connection pooling is enabled by default, so you don't have to take any additional configuration steps.

Using an External Database With the ACE 2 Management Server Appliance

The ACE 2 Management Server Appliance does not contain a PostgreSQL database server. You must use an external server to which the server appliance connects over the network. One possibility you might consider is whether an appliance version of a database server would suit your setup.

To set up an ODBC connection to your PostgreSQL external database

1 Log in to the server appliance console as `root`, using the password you created during your first run of the server appliance.

2 Open the `/etc/odbc.ini` file in a text editor; for example:

```
vaos# vi /etc/odbc.ini
```

This file contains a setting for the ODBC DSN called `postgres_dsn`.

3 Uncomment all lines in the `postgres_dsn` file except the first two (that is, remove the leading '#' symbol in each line).

4 Replace placeholders <...> with the PostgreSQL database server DNS name or IP address, and the database name in this server.

5 If you have configured your PostgreSQL server to listen on a non-default port number, use that port number in the configuration; otherwise, keep the default port number setting.

6 Save the file.

These steps ensure that "`postgres_dsn`" will appear in the dropdown box on the Database tab in the server setup application.

Using the ACE 2 Management Server Setup Application

Ensure that you have completed any necessary pre-configuration tasks. See "Tasks to Complete Before You Configure the Server" on page 71.

To configure the server

1 Start up the configuration application:

- On Windows: Choose **Start > VMware > VMware ACE Management Server** and click the **Configuration** link.
- On Linux: Open a browser, point it to the address for the host system on which you installed the server, and open the Web page. Click the **Configuration** link on the page.

2 On the Welcome page for the server setup application:

- If this page says **This server has not been configured**, click **Start**.
- If this page says **This server is configured**, click the tab for the page on which you want to make a configuration change.

3 On the Licenses page:

To set up the license at the initial configuration of your ACE 2 Management Server:

a Enter the serial number for the server.

b Optionally, enter a user name and company name.

c Click **Next.**

If you are reconfiguring the server, the current licensing information is displayed at the top of the page. The **License Expiration** field shows either **No Expiration** or a date, for permanent and expiring licenses, respectively.

If the system on which you have installed the ACE 2 Management Server currently has more than one valid server license, just one license is displayed on that page.

To make changes to the license information:

a Click **Change**.

b (Optional) Type in the new user name or company name.

c Enter the serial number (if you are not changing the serial number at this reconfiguration, enter the existing number).

d Click **Apply** and then click **Restart** or **Later**. If you click **Later**, you will need to restart the server manually. See "Stopping and Starting the Apache Service Manually" on page 85.

4 On the Database page, select one of:

- **Embedded Database** – Select this option if you plan to use the default embedded SQLite database engine. Then click **Next**.
- **External Database (ODBC-compatible)** – Select this option to use an external database, either Microsoft SQL Server or Oracle Database 10*g* (Windows) or PostgreSQL (Linux). Provide the database DSN, user name, and password.

  After you enter the database connection credentials, the setup application checks for an existing database. If the database is present, the setup application offers an option to re-initialize it (erase all data, restoring the database to its default state; the default setting for the option is "No"). You can also use the reinitialization option at a later time (after setup is complete, by revisiting this page) to reset the database.

  If the database setup is unsuccessful, the server setup will fail and the server won't be able to start.

NOTE If you are upgrading the server from the previous release, the database schema will be upgraded automatically and you will not lose your previous data. The upgrade will be done on the first start of the upgraded server, even if you do not rerun the setup application. See the release notes for information about upgrading from a previous ACE 2 release to this release.

Continue with the server configuration in one of the following ways:

- If this is the initial configuration of the server, click **Next**.
- If you are reconfiguring the server, click **Apply** and then click **Restart** or **Later**. If you click **Later**, you will need to restart the server manually. See "Stopping and Starting the Apache Service Manually" on page 85.

5 On the Access Control page, if you want to integrate the ACE 2 Management Server to an existing LDAP directory, in this case an Active Directory service, select **Domain Account (LDAP)**.

Specify credentials that the ACE 2 Management Server will use to connect to and query the domain controller:

- **Host Name** – Enter the host name of the LDAP server, using the name you created during the procedure in "Using Active Directory Integration (Using LDAP)" on page 72.
- **Query User UPN** – Enter the UPN (User Principal Name) for the LDAP server. Together with the Query User Password, this parameter will be used by the Management Server to connect to the LDAP server.
- **Query User Password** – Enter the password for the query user.
- **Default Domain** – Enter the default domain on which you will authenticate users.

See the example below.

NOTE The query user can be any user who has read access to the locations where user and group objects reside in the LDAP server.

Click **Next** or **Apply**.

a Select the ACE Administrators group. The specified group will be used by the administrator to authenticate and authorize users. (You set up this group when you prepared for Active Directory integration before you started the server configuration.)

b If you want to set up a separate role for the Help Desk application, enable **Helpdesk LDAP Group** and select a group to log in to the application. If this

option is not enabled, then anyone who logs in to the Help Desk application must be a member of the ACE Administrators group.

6 Still on the Access Control page: If you select **Local Account** (you do not plan to use an Active Directory service), specify the password for ACE 2 Management Server administrators. Administrators must enter this password before they can modify the server's configuration. If you want to enable a role for using the Help Desk Web application, select **Enable Helpdesk Role** and specify a password that users must enter when they start up the Help Desk application. See "Using the VMware Help Desk Web Application" on page 237 for details about that application.

NOTE If you are reconfiguring the server, you will notice that any passwords you entered previously are shown as a 12-character display rather than as the actual number of password characters.

CAUTION If you lose your administrator password (you set this password if the server is configured not to use LDAP), there is no way to retrieve that password. You will have to delete the server configuration file, setting the server back to its initial state, and then reconfigure the server and set an administrator password during the reconfiguration.

To delete the ACE 2 Management Server configuration file and set a new administrator password

1 If you used complex settings in your configuration file, you might want to save a copy of the file so that you can look at those settings while you are reconfiguring the server.

2 Navigate to the location of the ACE 2 Management Server configuration file:

On Linux systems:

```
/var/lib/vmware/acesc/conf/acesc.conf
```

On Windows systems:

```
C:\Program Files\VMware\VMware ACE Management Server\conf\acesc.conf
```

3 Delete the configuration file.

Navigate to the server setup Web application and configure the server again, specifying a password on the Access Control page.

Continue with the server configuration in one of the following ways:

- If this is the initial configuration of the server, click **Next**.
- If you are reconfiguring the server, click **Apply** and then click **Restart** or **Later**. If you click **Later**, you will need to the server manually. See "Stopping and Starting the Apache Service Manually" on page 85.

4 On the Custom SSL Certificates page

If you are setting up the server to use custom SSL certificates, either your own self-signed certificates or those of a third-party or internal CA (certificate authority), then use this page to upload the PEM-encoded files to the correct directory. You created the files earlier; see "Setting Up Your Own Self-Signed Certificates, Third-Party Signed Certificates, or Certificates from an Internal Certificate Authority" on page 63.

To upload files for your own self-signed certificates or for third-party or internal CAs:

a Click the appropriate **Browse** button to navigate to and upload the key and certificate files you created.

b If you are using CAs, upload the chain file.

c Click **Upload certificates**.

d Verify that the summary page shows that the correct files have been uploaded.

If you upload an invalid certificate file, the server setup application fails when you click **Apply** and then **Restart** and you won't be able to restart the Apache service. To fix this problem, restore the backup certificate file for the corresponding certificate. The backup certificate files are in the following format:

`<certificate_filename>.<date>-<time>`

where `<certificate_filename>` is one of:

`server.crt` for the server public certificate

`server.key` for the server private key

`chain.crt` for the certificate chain

`<date>` is in the format YYYYMMDD (year, month, day).

`<time>` is in the format HHMMSS (hours, minutes, seconds).

The backup files are in the ACE 2 Management Server directory, with the filename appended with the date and time; for example, `server.crt.20070216–095344`.

Save the file in the correct location as `ssl/<filename>.crt`. Then restart the Apache server manually to complete the restoration process and to bring up the VMware ACE 2 Management Server Setup Web application again and continue the configuration.

e Click **Close** to close the summary page.

f Continue with the server configuration in one of the following ways:

If this is the initial configuration of the server, click **Next**.

If you are reconfiguring the server, click **Apply** and then click **Restart** or **Later**. If you click **Later**, you will need to restart the server manually. See "Stopping and Starting the Apache Service Manually" on page 85.

5 On the Logging page:

At this release, the server by default collects log entries for events that change the data in the database. You can set the logging levels and set an option for purging log entries.

However, if you enable the Debug logging level, the logs will include entries for events that do not change the database state, such as getting instance information and so on.

To set the logging options:

a Set the log-type categories. Each category covers several server RPC interfaces and contains several distinct event types. The categories are:

ACE Administration – Logs events for ACE instance creation, update, and destruction.

Package Administration – Logs events for package creation and update.

Policy Administration – Logs events for policy-set update and publish, instance customization, and user access control changes by an ACE administrator.

Instance Administration – Logs instance lifecycle events: creation, copying, revocation, re-enablement, and deletion, instance password change by a user, instance password change by an administrator, changes of per-instance expiration, changes of instance guest or host OS information, and setting instance custom fields. The debug level can be used to log the most ubiquitous

traffic—policy update requests from active instances. Failed instance verifications are only logged at the debug level.

Authentication – Logs events for every authentication request. Administration or helpdesk authentication attempts (at the normal level), instance authentication (at the informational level), and remote LDAP password change. (You might want to set logging for this category to as minimal a level as is practical for you; otherwise, this category can generate a large volume of entries.)

b Set the detail level individually for each of the logs. The detail levels are:

None: No log entry will be made for this event.

Critical: The log will provide entries for the critical category of events, which are those having broad and critical effects; for example, an event that would remove all packages, instances, and policies associated with an ACE master.

Normal: The amount of information given in the entry will be sufficient to answer most queries.

Informative: The log will provide entries for nondestructive events that have limited effect.

Debug: The log will provide entries for every client access of the server. It will provide more records of certain event types, creating potentially orders of magnitude more logging entries than other log levels. It logs all informational transactions, such as instance status and so on. You would use this setting only when debugging running servers in the field.

c Use the **Event Log Purging** feature to specify whether to keep log entries indefinitely, keep log entries for at least a minimum specified number of days, or keep at least a minimum specified number of log entries after each purge. The oldest entries are purged first. The purge maintenance process runs approximately every 6 hours.

d Continue with the server configuration in one of the following ways:

If this is the initial configuration of the server, click **Next**.

If you are reconfiguring the server, click **Apply** and then click **Restart** or **Later**. If you click **Later**, you will need to restart the server manually. See "Stopping and Starting the Apache Service Manually" on page 85

6 When you see the message about the completion of server setup, click **Restart**. If you click **Later**, you will need to manually restart the server to have the configuration changes take effect. See "Stopping and Starting the Apache Service Manually" on page 85.

NOTE At this point, the new configuration has been written. The system must be restarted for the ACE 2 Management Server to use the configuration.

7 On the Login page, type your admin password. Then click **Login**.

8 The Welcome page reappears, this time displaying a success message. Close the window.

Using Event Logs

At this release, the server collects log entries for events that change the database. You can set the logging levels and set an option for purging log entries. See information about setting these levels and options in Step 5 on page 83, under "Configuring the ACE 2 Management Server."

Stopping and Starting the Apache Service Manually

This section describes how to restart the Apache service on each of the supported server types.

To restart the Apache service manually on a Windows host server

1 Click the Apache icon in the taskbar.

2 Click **Stop**, and then click **Start**. Ensure that you click **Stop** and **Start**, not **Restart**.

On a Red Hat Enterprise Linux 4 host server:

1 Log in to your host console.

2 As `root`, type the following command:

```
/etc/init.d/httpd stop
/etc/init.d/httpd start
```

To restart the Apache service manually on a SUSE Linux Enterprise Server 9 SP3 host server

On an SUSE Linux Enterprise Server 9 SP3 host server:

1 Log in to your host console.

2 As `root`, type the following command:

```
/etc/init.d/apache2 stop
/etc/init.d/apache2 start
```

To restart the Apache service manually on an ACE 2 Management Server appliance

On the ACE 2 Management Server appliance:

1 Log in to your host console.

2 As `root`, type the following command:

```
/etc/init.d/apache2 stop
/etc/init.d/apache2 start
```

Logging On to the ACE 2 Management Server

Communications between Workstation ACE Edition and the ACE 2 Management Server take place over a secure SSL connection.

When you attempt to access the ACE 2 Management Server for the first time in a Workstation ACE Edition session, a login dialog box appears. You need to supply the appropriate login information:

- If the server is not integrated with LDAP (Active Directory) service, type in the administrator password that you set when you configured the server.
- If the server is integrated with Active Directory service, enter your administrative credentials (username, password, and domain) in one of the formats shown in Table 4-2.

Table 4-2. Logon Options for ACE 2 Management Servers with Active Directory Service

Logon	Notes
long name + password + domain name	The long name is the "First_name Last_name" format; for example, "ACE User".
long name + password	The long name is the "First_name Last_name" format; for example, "ACE User". Leave the domain field blank.
short name + password + domain	The short name is the sAMAccountName; for example, "ace" as the shorter form of long name "Ace User".
short name + password	The short name is the sAMAccountName; for example, "ace" as the shorter form of long name "Ace User". Leave the domain field blank.
email address + password	This logon option can only be used for a domain that is accessed through a direct connection. Leave the domain field blank.

Table 4-2. Logon Options for ACE 2 Management Servers with Active Directory Service (Continued)

Logon	Notes
NETBIOS DOMAIN NAME\username + password	The NetBIOS name is a short name for domains that is registered in the NetBIOS Name Service (WINS). Leave the domain field blank.
username + password + NETBIOS DOMAIN NAME	The NetBIOS name is a short name for domains that is registered in the NetBIOS Name Service (WINS).

Using the ACE 2 Management Server

After the ACE 2 Management Server has been installed and configured, you can use it to:

- View the instances on the server in the Workstation ACE Edition user interface.
- Revoke and re-enable an instance.
- Push out a dynamic policy update.
- Fix various problems with the ACE instances as reported by instance users, through the Instance View in the Workstation ACE Edition interface or through the Help Desk Web application.

See Chapter 12, "Instance View," on page 243 and "Using the VMware Help Desk Web Application" on page 237 for more information about these tasks.

Unblocking Port Traffic and Changing Port Assignments

The following two topics describe how to deal with these port-related issues:

- "If Your ACE Instance on a Linux Host Computer Cannot Contact the ACE 2 Management Server" on page 87
- "If You Need to Change the Port Assignment for the Server" on page 88

If Your ACE Instance on a Linux Host Computer Cannot Contact the ACE 2 Management Server

If your ACE instance cannot contact the server, check to see whether a firewall or proxy setting is blocking or rerouting https traffic on port 443. By default, https traffic from the VMware Player to ACE 2 Management Server is routed on port 443. Disable the firewall or turn off the proxy setting to allow the Player-to-server traffic on that port.

If You Need to Change the Port Assignment for the Server

The ACE 2 Management Server is a module running on the Apache 2.0 platform. If you need to change the port that the server listens on, you must manually edit the Apache configuration file.

To change the port that the ACE 2 Management Server listens on

1 Using a text editor, open the ACE 2 Management Server component http configuration file, which is located at

On a Windows host server:

```
C:\Program Files\VMware\VMware ACE Management Server\Apache2\conf\
                httpd.conf
```

On a Red Hat Enterprise Linux 4 host server:

```
/etc/httpd/conf.d/acesc.conf
```

On an SUSE Linux Enterprise Server 9 SP3 host server:

```
/etc/apache2/conf.d/acesc.conf
```

NOTE This path will be different if you installed VMware ACE 2 Management Server in a different location. Use the path you established for your server.

2 Locate the line entry in the file that reads `Listen 443` and then change the port number to the desired port configuration.

3 Locate the Virtual Server configuration for port 443. It starts with the line

```
<VirtualHost –default_:443>
```

and ends with the line

```
</VirtualHost>
```

4 Change the port number in the section header to the desired port number (for example, to change to port 8443, change `443` to `8443`.

5 Save the file.

6 Stop and start the Apache service. See "Stopping and Starting the Apache Service Manually" on page 85.

The ACE 2 Management Server is now listening on the specified port.

NOTE Port 8000 is used by the server for configuration, and port 8080 is used for the ACE 2 Management Server Appliance, so you cannot choose those ports.

When you create an ACE master, you can specify which port is to be used to talk to the ACE 2 Management Server.

Creating and Configuring ACE Masters

5

This chapter discusses how to create and configure ACE masters.

Topics in this chapter are:

Creating an ACE Master

You have four options for creating an ACE master:

- Create a new ACE Master. Choose **File > New > ACE Master**, select **Create a new ACE master**, and then follow the instructions in the New ACE Master wizard.
- Create a new ACE Master optimized for Pocket ACE. Choose **File > New > ACE Master**, select **Create a new ACE master optimized for Pocket ACE**, and then follow the instructions in the New ACE Master wizard.
- Create from an existing virtual machine. Select a virtual machine in the Favorites list or choose **File > Open** and select the virtual machine, then choose **VM > Clone to ACE Master**. You can also choose **File > New > ACE Master** and select the **Create**

an ACE master from an existing virtual machine option. Then follow the instructions in the Clone to ACE Master Wizard.

- Clone an ACE Master. Select an ACE master in the Favorites list or choose **File > Open** and select the ACE master, then choose **ACE > Clone**.

You can clone virtual machines created with certain other VMware products and convert the clones into ACE masters. Virtual machines created with the following products can be used in Workstation ACE Edition:

- VMware Workstation 5.x and later
- VMware Server

Creating a New ACE Master

As you use the New ACE Master Wizard, you are prompted to make decisions about many aspects of the ACE master. Before you begin using the wizard, review the topics under "Setting Up a New Virtual Machine" in the *Workstation User's Manual*. The subsections there under "Before You Begin" describe considerations for making configuration choices, particularly for the custom configuration. These subsections describe, for example, what to consider when choosing a guest operating system. They provide information about the issues involved so that you can determine which choices you want to make before running the wizard.

To create a new ACE master

1 Click **File > New > ACE Master**. Click **Next** on the Welcome page. The Use New or Existing Virtual Machine page appears.

2 Select whether you want to create a completely new ACE master, an ACE master optimized for Pocket ACE, or an ACE master cloned from an existing virtual machine.

If you select **Create a new ACE master** and click **Next**, the Configuration page appears.

If you select **Create a new ACE master optimized for Pocket ACE**, the Select a Guest Operating System page appears. Proceed to Step 5 if you selected the Pocket ACE option.

NOTE Choose the **Create a new ACE master optimized for Pocket ACE** option if you intend to use this ACE master as a Pocket ACE and store it on a portable device. This option chooses appropriate values for the virtual machine configuration, policies, and package settings so that the ACE master you create can be easily used as a Pocket ACE.

This option allows you to specify the guest operating system, name and location, and specify the disk size. Choose a disk size that will fit on the portable device on which you intend to deploy the Pocket ACE. The wizard shows the minimum amount of free space needed on the portable device. Adjust the size of the disk so that it has enough space for a guest operating system, your applications, and data.

In addition to the disk size there are some additional required files that must be present on the portable device. The ACE master wizard will show you the space required for these files.

You can also choose to include VMware Player on the portable device so that the Pocket ACE can be used on a host that does not have VMware Player already installed (you will need administrator privileges on the host to install VMware Player if it is not installed already). When you package the Pocket ACE for deployment to the portable device you can include VMware Player in a Pocket ACE package. The size required for VMware Player is also shown on the Disk Capacity page of the New ACE Master wizard (marked as optional). The size required for VMware Player is not included in the total size required. If you intend to include VMware Player on the portable device, make sure you account for the additional required space.

If you select **Create an ACE master from an existing virtual machine**, the Select a Virtual Machine page opens. After you select a virtual machine to create your ACE master from, the Clone to ACE Master Wizard opens. For information about using that wizard, see "Cloning an ACE Master from an Existing Virtual Machine" on page 100.

3 Select the method you want to use for configuring your ACE master.

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

- The guest operating system
- The ACE master name and the location of the ACE master's files
- The network connection type
- Disk size

- Allocation of space for the disk
- Splitting the disk into 2GB files
- Specifying an ACE 2 Management Server if you want to manage the ACE master's instances with a server

Select **Custom** if you want to:

- Make a different version of virtual machine than what is specified in the preferences editor (from the Workstation menu bar, choose **Edit > Preferences**, and see the setting for **Default hardware compatibility**).
- 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.

  In order to find out what type of virtual disk would be created by default for a particular operating system, select the **Custom** option and click **Next** through the wizard pages, select the desired guest operating system, and then continue through the wizard until you get to the page called Select a Disk Type. The default is already selected.
- Use an existing virtual disk rather than create a new virtual disk.
- Set memory options that are different from the defaults.
- Assign more than one virtual processor to the virtual machine.

Click **Next**.

4 If you selected Typical, skip to Step 5.

If you selected **Custom**, the Virtual Machine Hardware Compatibility page appears. Specify whether you want to create a Workstation 5 or 6 virtual machine and click **Next**. When you make a selection from the Hardware Compatibility list, you will see a list of other VMware products and versions that are compatible with your selection. You will also see a list of features that will not be available for that version. Click **Next**.

5 The Guest Operating System page appears.

This page asks which operating system you plan to install in the ACE master. Select both an operating system and a version.

The New ACE Master Wizard uses this information to select appropriate default values, such as the amount of memory needed.

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

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.

6 Enter a name and folder for the ACE master on the Name the Virtual Machine page.

Each ACE master 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 ACE master is C:\Documents and Settings\<username>\My Documents\My Virtual Machines\Windows XP Professional.

If you are creating an ACE master optimized for Pocket ACE, skip to Step 14.

If you selected **Typical** as your configuration path, skip to Step 9.

7 If you selected **Custom** as your configuration path, select the number of virtual processors to use, one or two. Then click **Next**.

8 Continuing with **Custom** configuration, adjust the memory settings or accept the defaults.

When choosing the ACE master 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 users' computers and the amount of RAM required by the host operating system. Do not set the ACE master memory below the amount recommended for the guest operating system. If you set ACE master 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 ACE master memory no higher than half the amount of RAM you expect to find on users' host computers.

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

Click **Next** to continue.

9 Configure the networking capabilities of the ACE master.

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 ACE instance deployed from the ACE

master (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 ACE instance but the ACE instance must be able to connect to the Internet, select **Use network address translation (NAT)**. NAT also allows the user to share files between the ACE instance and the host operating system.

For more details about networking options, see the *Workstation User's Manual*.

Click **Next** to continue.

If you selected **Typical** as your configuration path, skip to Step 14.

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

10 Select the type of SCSI adapter you want to use with the ACE master.

An IDE adapter and a SCSI adapter are installed in the ACE master. 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 ACE master.

Click **Next** to continue.

11 Select the disk you want to use with the ACE master.

- **Create a new virtual disk.**

  Virtual disks are appropriate for any ACE masters 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. Click **Next** to continue.

- **Use an existing virtual disk.** If you select this option, click **Next** and then skip to Step 13.

12 If you chose to create a new virtual disk, now select a disk type: 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.

Click **Next** to continue, then skip to Step 14.

13 If you chose to use an existing virtual disk, select the disk you want to use. Click **Next** and then click **Finish**.

14 Specify the capacity of the virtual disk.

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

See the *Workstation User's Manual* for more information about using virtual disks.

Enter the size of the virtual disk that you wish to create. If you are creating an ACE master optimized for Pocket ACE, click **Next** and skip to Step 17 after entering your virtual disk size. If you are creating a typical or custom ACE master, continue with this step.

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 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 might be stored on a FAT32 file system.

If you plan to distribute the 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 when distributing the package on DVD.

Click **Next** to continue.

15 If you selected **Typical** as your configuration path, skip to Step 17.

16 If you selected **Custom** as your configuration path, specify the location of the virtual disk's files. Click **Next**.

17 On the Specify ACE Management Server page, choose whether you want to use the ACE 2 Management Server to manage the instances created from this ACE master.

- Select **Use server** (the default choice) to have an ACE 2 Management Server manage the instances created from this ACE master.

  Then enter the server name and port or choose the server from the dropdown list of previously chosen servers. The port assigned to that server appears in the Port box. Click **Next**.

- Select **Don't use server** if you do not want to have an ACE 2 Management Server manage the ACE instances created from this ACE master.

NOTE You can't change the ACE master at a later time from **Use server** to **Don't use server** or the reverse. The ACE master will always be either managed or standalone.

Click **Next** to continue.

18 If you selected a server that is integrated with an Active Directory service, the Active Directory page appears. Select whether to use Active Directory with this ACE master. Then click **Next**.

CAUTION When you choose an ACE 2 Management Server with Active Directory integration during ACE master creation, ensure that your Workstation ACE Edition administrator machine is in the same domain as that server. If the machine is not in that domain, you won't be able to preview the instance or add users to the ACE master.

19 The Ready to Complete page appears. Click **Finish** to complete the New ACE Master Wizard.

Cloning an ACE Master from an Existing ACE Master

For detailed information about full and linked clones, see the *Workstation User's Manual*.

To clone an ACE master from an existing ACE master

1 Choose **File** > **Open** to navigate to and open the ACE master you want to clone, and then choose **ACE > Clone**. The Welcome page of the Clone ACE Master Wizard appears. Click **Next**.

2 The Clone Source page appears. Under **Clone from**, select one of:

- The current state **in the virtual machine**
- **An existing snapshot (powered off only)**.

Click **Next**.

3 On the Clone Type page, select **Create a linked clone** or **Create a full clone**. Click **Next**.

4 Select a name and folder for the ACE master in the Name of the New ACE Master page.

Each ACE master 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 ACE master is `C:\Documents and Settings\<username>\My Documents\My Virtual Machines\Windows XP Professional`.

5 On the ACE Management Server page, choose whether you want to use the ACE 2 Management Server to manage the instances created from this ACE master.

- Select **Use server** to have an ACE 2 Management Server manage the instances created from this ACE master.

  Then enter the server name and port or choose the server from the dropdown list of previously chosen servers.The port assigned to that server appears in the Port box. Click **Next**.

- Select **Don't use server** if you do not want to have an ACE 2 Management Server manage the ACE instances created from this ACE master.

NOTE You can't change the ACE master at a later time from **Use server** to **Don't use server** or the reverse. The ACE master will always be either managed or standalone.

Click **Next** to continue.

6 If you selected a server that is integrated with an Active Directory service, the Active Directory page appears. Select whether to use Active Directory with this ACE master. Then click **Next**.

7 On the Ready to Complete page, click **Next**.

The Cloning ACE Master page shows progress and then displays a success or failure message.

8 Click **Close** to exit the wizard.

Cloning an ACE Master from an Existing Virtual Machine

For detailed information about full and linked clones, see the *Workstation User's Manual*.

To clone an ACE master from an existing virtual machine

1 Choose **File > New > ACE Master** and select the **Create an ACE master from an existing virtual machine** option in the New ACE Master wizard or, if you have already opened the virtual machine you want to clone, choose **VM > Clone to ACE Master**. The Welcome page of the Clone to ACE Master Wizard appears. Click **Next**.

2 The Clone Source page appears. Under **Clone from**, select one of:

- The current state **in the virtual machine**
- **An existing snapshot (powered off only)**

Click **Next**.

3 On the Clone Type page, select **Create a linked clone** or **Create a full clone**. Click **Next**.

NOTE Deployed instances of this master will always include a complete copy of the virtual machine.

---

4 Select a name and folder for the ACE master on the Name of the New ACE Master page.

Each ACE master 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 ACE master is `C:\Documents and Settings\<username>\My Documents\My Virtual Machines\Windows XP Professional`.

5 On the ACE Management Server page, choose whether you want to use the ACE 2 Management Server to manage the instances created from this ACE master.

- Select **Use server** (the default choice) to have an ACE 2 Management Server manage the instances created from this ACE master.

  Then enter the server name and port or choose the server from the dropdown list of previously chosen servers. The port assigned to that server appears in the Port box. Click **Next**.

- Select **Don't use server** if you do not want to have an ACE 2 Management Server manage the ACE instances created from this ACE master.

NOTE You can't change the ACE master at a later time from **Use server** to **Don't use server** or the reverse. The ACE master will always be either managed or standalone.

Click **Next** to continue.

6 If you selected a server that is integrated with an Active Directory service, the Active Directory page appears. Select whether to use Active Directory with this ACE master. Then click **Next**.

7 On the Ready to Complete page, click **Next**.

The Creating ACE Master from Virtual Machine page shows progress and then displays a success or failure message.

8 Click **Close** to exit the wizard.

Cloning a Virtual Machine from an ACE Instance

You might need to convert an ACE instance into a standard virtual machine for troubleshooting or repair purposes. All the ACE policies that were on the ACE instance will be removed on the cloned virtual machine.

You must have Administrator Mode configured to clone a virtual machine from an ACE instance. If your package is tamper resistant or encrypted you must also have a recovery key. Enable your recovery key on the access control page in the policy editor.

To enable ACE 2 to clone a virtual machine from an ACE instance

1 Choose **Edit policies > Administrator Mode** and select the **Enable administrator mode** check box. Enter and confirm your administrator password.

2 Choose **Access control** and click the **Recovery key** button to choose or configure a recovery key.

3 Choose **Create new package** to create a package with these policy changes.

To clone a virtual machine from an ACE instance

1 At the command line, change directories to the directory where you have the vmware-acetool.exe application stored.

For example,

```
cd \Program Files\VMware\VMware Player
```

or

```
cd \Program Files\VMware\VMware Workstation
```

2 Enter the cloneToVM command, using the following format:

```
vmware-acetool.exe cloneToVM <ACE 2 instance path name> <target virtual
                machine name> <recovery key>
```

For example,

```
vmware-acetool.exe cloneToVM C:\Documents and Settings\All
                Users\Application Data\VMware\VMware
                ACE\clonetovm\Windows XP Professional.vmx
                C:\cloneToVM\test.vmx C:\Documents and
                Settings\<username>\recovery keys\rec key.priv
```

3 Enter the administrator password and recovery key password when prompted. The following message should appear:

```
Cloning: 100% done.
Operation succeeded.
```

The virtual machine clone has been created from the ACE instance.

Networking ACE Instances

In the ACE instances you create for your users, you are most likely to use NAT or bridged networking with an IP address provided by a DHCP server.

For details on networking, see the *Workstation User's Manual*.

ACE Master Settings

See "ACE Menu" on page 39 for a complete list of ACE master settings and descriptions of how to apply the settings.

ACE Server Settings

You can use the ACE Server dialog box in the ACE menu to change the server that manages an ACE master.

To change the ACE 2 Management Server for an ACE master

1 Select the ACE master whose server setting you want to change.

2 Choose **ACE > ACE Server**.

3 In the ACE Server dialog box, select a server from the drop-down list or type the server address in **Server**.

You can change from a server that uses an Active Directory service to one that does not, but you can only make this change if the selected ACE master is not using Active Directory. Also, if you change from a server that does not use Active Directory to one that does, the selected ACE master will not use Active Directory.

NOTE The icon next to the server name indicates whether this server is integrated with Active Directory. The icon in the example is for a server with Active Directory. A key icon appears for a server that is not integrated with Active Directory.

---

4 The default port is 443. Type a new port number in **Port** if appropriate.

NOTE The information in the **ACE master Information** area of the dialog box applies to the ACE master and not to the server. Therefore, in the example, "**Active Directory: Yes**" indicates that this ACE master uses Active Directory.

---

5 Click **OK** to save the settings and close the dialog box.

Reassigning an ACE Master to a Server When the Master's Record Cannot Be Retrieved

When you open a managed ACE master, VMware Workstation ACE Edition will contact the management server that the ACE master is using to retrieve this ACE master's record. If Workstation ACE Edition cannot contact the management server, the ACE master record cannot be retrieved and the ACE master cannot be opened.

A server record for an ACE master might be unavailable for various reasons, including:

- The server address has changed.
- The record for the ACE master has somehow been deleted.

The solution to these problems is to assign the ACE master to a new server address.

When you attempt to open an ACE master whose management server cannot be contacted, Workstation ACE Edition displays a message that tells you that the server cannot be contacted and asks whether you want to select a new server address.

If the new address that you provide is simply the updated address for the original server—for example, the address obtained from DHCP servers has changed—then the ACE master's record will be intact in the new server location.

If the original server is unavailable or the ACE master's record has been deleted, then when you open the ACE master, Workstation ACE Edition offers to create a new record for the ACE master. Some data that was contained in the original record is lost—such as access lists, key lists, and domain-join passwords—because that data was maintained on the server.

To reassign an ACE master to a new server address

1 When you see the message that prompts you to select a new server, select or type in a new server address and port.

  If the ACE master was using Active Directory, then you can only reassign it to a new management server that is integrated with Active Directory. If the ACE master was not using Active Directory, then it can be reassigned to any management server.

2 Click **OK**. Select **ACE > New package**, provide the name and location of the package in the wizard, and then select the Server Update package type.

CAUTION If you reassign an ACE master to a new server, be aware that unless the new server has access to the old database or to a copy of it, existing instances of that ACE master will not continue to run.

Why Would You Need to Reassign an ACE Master to a Different Server Address?

Every time you open a managed ACE master, Workstation ACE Edition looks up the ACE master's record on the ACE 2 Management Server and downloads the master's policies and other information from the server. If Workstation ACE Edition fails to contact the server or cannot find a record for the ACE master, it cannot open the master and the master becomes unusable. In this case, you can choose to change the server address of the ACE master's ACE 2 Management Server.

When Do You Need to Reassign an ACE Master?

Common situations when you might need to reassign an ACE master to an new server address:

- The address of the ACE 2 Management Server changes (for example, if it was a DHCP-assigned address or if you change the server's network address).
- The database used by the ACE 2 Management Server gets corrupted.

In either of these cases, the ACE master's database record cannot be retrieved and an attempt to open the ACE master will fail. You will be offered a choice to specify the new address of the server. If the address has changed, specify the new address of the server. If the database was corrupted, you can specify the address of another ACE 2 Management Server. The ACE master will now use this new ACE 2 Management Server. However, all your deployed instances will continue to use the old server (you can reassign them by creating and distributing a server update package).

How Does Reassigning the Master to a New Server Address Work?

If the address of the ACE 2 Management Server has changed, you can specify the new address of the server. Workstation ACE Edition searches for a record for this ACE master on the new server. If the record is found, the ACE master will use this existing record along with all the settings stored for this record. (Caveat: If the ACE master was using password-based activation before it was reassigned, this access control setting will be changed to no activation. After reassigning the master, you will need to change it to use password activation and specify the activation password).

If an existing record for this ACE master is not found on the new ACE 2 Management Server, Workstation ACE Edition will create a new record for the ACE master on the new server. However, in this case the following settings will be lost and you will need to re-enter them:

- Activation password (if using password-based activation)
- Activation token list (if using token-list based activation)

- Allowed users (if using Active Directory based access control)
- Domain join password (if instance customization and domain join are enabled)
- Remote domain join password (if instance customization and remote domain join are enabled)

What Does Reassigning an ACE Master to a New Server Address Do?

Note that reassigning the ACE master to a new server address only copies the record for the ACE master. The records for the ACE instances are not copied. After the master has been reassigned, all the deployed instances of the master will continue to attempt to contact the old server. If the old server cannot be contacted, the instances will use their cached policies (if offline policy usage is enabled) until their cache expires. If you want to change your deployed instances to contact the new server, you will need to do two things:

1. Make sure the new server can access the same database that your old server was using, either by copying it if it was an embedded database or by configuring your new server through the server setup Web application if it is using an external database.
2. Create a server update package, distribute it to all your users, and have them install it.

Virtual Machine Settings

You can change the settings for devices and options for an ACE master that you have selected. See the *Workstation User's Manual* for details on these settings and options.

Setting and Using Policies and Customizing VMware Player

6

The following sections guide you through the steps for setting policies for an ACE master and ACE instances and customize the VMware Player interface:

Taking Advantage of Policies

Policies give you control over many aspects of the ACE instances you distribute to your users. You can, for example

- Permit the ACE instance to be used only by certain users and groups defined in an Active Directory domain.
- 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.
- Set an expiration date for an ACE instance.

You set policies with the policy editor. See "Using the Policy Editor" on page 108.

You can change some or all of the policies for an ACE instance at any time by editing the policies, then creating and distributing a new package that contains only the policies.

For ACE masters managed by the ACE 2 Management Server, you can dynamically change some policies and deploy those changes to the ACE instances on the users' machines.

Using the Policy Editor

You set policies using the policy editor. You can start the policy editor in any of the following ways:

- Click the ACE master in the Sidebar, then choose **ACE > Policies**.
- Click the ACE master in the Sidebar, then click **Edit Policies in the summary view.**
- Click the Edit Policies icon in the toolbar.
- Right-click the ACE master in the Sidebar, then choose **Policies**.

NOTE The default Update Frequency—the rate at which managed instances check the server for changes—is 5 minutes.

Setting Policies

You can set the following policies for ACE instances:

- "Setting Access Control Policies – Activation and Authentication" on page 109
- "Setting Host-Guest Data Script Policies" on page 121
- "Setting Expiration Policies" on page 122
- "Setting Copy Protection Policies" on page 123
- "Setting Resource Signing Policies" on page 125
- "Setting Network Access Policies" on page 126
- "Setting Removable Devices Policies" on page 142
- "Setting USB Device Policies" on page 142
- "Setting Virtual Printer Policies" on page 146
- "Setting Runtime Preferences Policies" on page 147
- "Setting Snapshot Policies" on page 150
- "Setting Administrator Mode Policies" on page 152
- "Setting Hot Fix Policies" on page 154
- "Setting Policy Update Frequency" on page 155

For information about encrypting ACE packages and instances, see "Encryption" on page 181.

Setting Access Control Policies – Activation and Authentication

Set activation and authentication policies to control access to installed ACE packages and the instances created from those packages.

When you choose settings for these policies, those choices in turn determine the default settings to be used for package and ACE instance encryption policies, which protect the ACE packages and files in transit. See "Encryption" on page 181 for more information about those encryption settings.

The **activation policy** specifies who can access an installed ACE package and turn it into an ACE instance.

The **authentication policy** specifies who can run (power on) an ACE instance.

The particular settings for these policies and how they are implemented vary depending on how your ACE instances are managed and (optionally) tracked. The possible management setups are:

- **Server, with Active Directory:** ACE instances are managed by an ACE 2 Management Server, and the server is integrated with Active Directory.
- **Server, no Active Directory:** ACE instances are managed by an ACE 2 Management Server, and the server is not integrated with Active Directory.
- **Standalone:** ACE instances are standalone; they are not managed by a server.

To get started with setting activation and authentication policies

1. Click **Edit Policies** in the ACE master summary view or choose **ACE Master > Policies**.
2. Click the **Access Control** page link in the left pane of the Policy Editor window.
3. To choose settings options, see the subsection that applies to your ACE management setup:
   - "Activation and Authentication for Managed Instances with Active Directory Service" on page 110
   - "Activation and Authentication for Managed Instances Without Active Directory Service" on page 113
   - "Activation and Authentication for Standalone Instances" on page 117

Activation and Authentication for Managed Instances with Active Directory Service

If you are using a managed ACE master with a server that is integrated with Active Directory, use the following information to set activation and authentication policies:

The user must enter Active Directory user credentials each time the ACE instance is run.

Only the user who activates the instance can authenticate (run) the instance.

The activation step is performed whenever an ACE package has been installed.

In addition to the user's input of the correct user credentials, the server also verifies these items before the instance can be authenticated and run:

- The revocation flag is not set and the instance is not blocked from running because of any policy errors.
- The expiration date set for the instance, if any, has not been reached.

Dynamic changes to the authentication policy: You can add or remove users from the list of those who can activate ACE packages. User-list changes are effective at the next startup of this instance.

NOTE You cannot change activation and authentication policies that use Active Directory to policies that do not use Active Directory, nor can you make the reverse change of "without Active Directory" to "with Active Directory."

Activation and Authentication

Under **Activation and authentication**, you can edit the list of users and groups who can activate and authenticate (run) the instance:

- Click **Add** to open the Active Directory users and groups dialog box. Select the users and groups who can activate and authenticate the instance.

  NOTE Ensure that your administrator machine (the one on which you're running Workstation ACE Edition) is on the same domain as the one that the ACE 2 Management Server is configured to interoperate with. If it is not, you won't be able to add users.

- To remove a user or group from the list, select the entry in the User or Group/Domain table and click **Remove**.

Active Directory Password Change Proxying

You can provide additional security for your ACE instances by integrating with Active Directory.

You can specify password expiration and change requirements, set up the domain to expire passwords, and require password changes periodically. These settings are in addition to ACE access control policy settings.

In cases in which Active Directory users need to change their passwords, you can configure the ACE 2 Management Server as an Active Directory password change proxy. In this mode, the ACE 2 Management Server makes the password change request to the Active Directory domain controller on the user's behalf.

Allowances

Under **Allowances**: In **Total number of activations,** choose how many instances can be activated from this package:

- **Unlimited**
- **Maximum of**. Type the number or choose it from the drop-down list.

By default, users can activate one instance per ACE package. Select **Allow multiple activations per user** to allow individual users to activate more than one instance.

Advanced Setting for Power-On Script

You can provide a script that runs when an ACE instance powers on that determines whether the ACE instance can be run. This script provides a customizable way of controlling access to an ACE instance in addition to the authentication policy.

To include a power-on script in the ACE master's packages

1 Create the script and save it in the ACE Resources folder.

2 On the access control policy page, click the **Advanced** button at the bottom right. The Choose Power-on Script dialog box appears.

If the deployment platform setting in package settings is set to **Both Windows and Linux**, then the Choose Power-on Script dialog box contains text fields for both Windows and Linux script specifications.

3 Select **Use power-on script**.

4 Click **Set** to open the Set Custom Script dialog box. See page 119 for details on setting custom scripts.

5 If you are enabling the power-on script after you have already deployed packages with this ACE master, provide the script to the user using a policy/server update package or a custom package with ACE Resources.

NOTE The script is signed before deployment to prevent tampering. See page 125 for more information about resource signing.

When the script runs on the user's system, the script should print "TRUE" (power on) or "FALSE" (power off), and should conform to standard script exit code rules.

The following is a sample power-on script:

```
#
#   VMware Sample Script
#
#   Sample script for ACE power-on hook
#
#   Description:
#   This sample script implements a power-on hook for ACE. This can be used
              in addition
#   to authentication to control the circumstances under which an ACE is
              allowed to run.
#
#   This script assumes that the username is defined in the environment
              variable TEST_USERNAME
#   (a ficticious environment variable used for this sample) and returns TRUE
              if the user
#   is allowed to run, and FALSE otherwise.
#
#   Input to script:
#   None.
#
#   Returns:
#   TRUE if username is on white list.
#   FALSE if username is not on white list or is undefined.
#
#   Expected output:
#   One of the strings "TRUE" or "FALSE"
#
#

my @white_list = ("alan", "bob", "mary", "sonia", "chris");

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
   print "FALSE";
   exit(0);
}
```

```
my @grepNames = grep(/$username/, @white_list);
if (@grepNames == 1) {
   print "TRUE";
   exit(0);
}


print "FALSE";
exit(0);
```

NOTE Scripts can be in any language. A script provides Workstation ACE Edition with a command line executable or a script file (for example, .bat on Windows operating systems, perl or sh on Linux operating systems) in the ACE Resource directory. The guidelines a script must follow depend on which policy the script is implementing.

There are some general rules. The script must exit with a 0 (zero) value to be considered a success. Any other output results in failure. Upon success, the stdout output of the script will be examined. For a given policy this should be something specific (for example, the power on script output should be TRUE or FALSE), the authentication script output is used as a password, the host-guest data script is a string in a particular format (for example, “guestinfo.var1=”value1”\nguestinof.var2=”value2””).

Activation and Authentication for Managed Instances Without Active Directory Service

If you are using a managed ACE master with a server that is not integrated with Active Directory, use the following information to set activation and authentication policies.

Activation

The activation step is performed whenever an ACE package is installed.

Dynamic changes to the activation policy:

- To change the activation setting type: Edit the policy and publish it. The policy takes effect when a new instance from this package is installed and activated.
- To change the activation key: Edit the policy and publish it. The policy takes effect when a new instance from this package is installed and activated.You can also edit an imported keyword list and publish the change.

Under **Activation**, select one activation type:

- **None** – No password or key is required; any user can activate this instance.
- **Password** – The user must enter the password specified by you to activate this ACE instance. You must provide the user with the password through email or other means.

- **Activation key** – The user must enter a key that is in the key list you have created for this ACE instance. Click **Set key list** to open the Activation keys dialog box.

  NOTE Activation keys are essentially serial numbers that can be tracked as used or unused by the server. The admin can enter the keys they want to use in the dialog or import them into the dialog from a text file. After an ACE instance or ACE master has been activated using a key, that key can't be used to activate another instance.

  - To add keys: Click **Add**. Type in the free-form string.
  - To import keys: Click **Import** and browse to the file that contains the list of activation tokens you want to import. Each token is one line in the file. Blank lines are ignored.
  - To remove keys: Select the entry or entries you want to remove in the table. Click **Remove,** then click **Yes**. Removing a key does not affect an instance that has been activated with that key.

Authentication

The user must authenticate the ACE instance each time the user runs the instance, unless the authentication type (see below) is set to **None**.

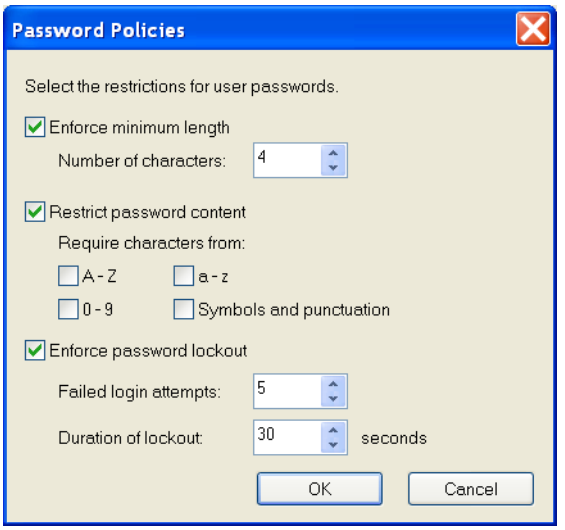
In addition to the user's input of the correct password or the key resulting from the successful execution of the script, the server also verifies these settings before the instance can be powered on:

- The revocation flag is not set and the instance is not blocked from running because of any policy errors.
- The expiration date set for the instance, if any, has not been reached.

Under **Authentication**, select one authentication type:

- **None** – No password is required; any user can activate this instance.
- **User-specified password** – Select this option to specify that the instance does not run until the user enters the correct password. Each user must set a password during activation, at first power-on. To set the minimum length or required

character types for the password, click **Set password policies** to open the Password Policies dialog box.



Choose one, two, or all three of:

- **Enforce minimum length.** Type the number or choose it from the drop-down list.
- **Restrict password content**. Select one to four options for character type.
- **Enforce password lockout**. Select the number of times the user can attempt to enter the password before an error message appears that tells the user that the number of allowed password attempts has been reached. Also specify the amount of time in seconds that the user must wait before making another attempt to log in.

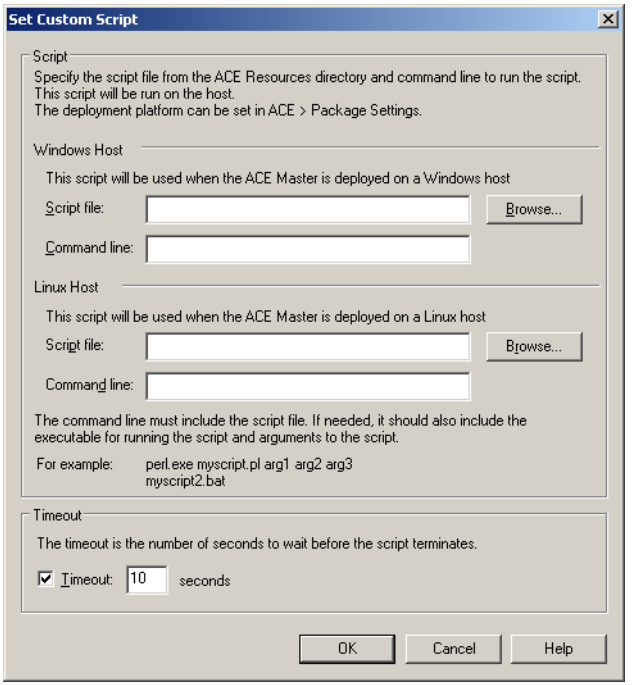
- **Script** – Select this option to use your own custom script to determine who can use the instance.

To provide a script in packages created with this ACE master

1 Create the script and save it in the ACE Resources directory for the ACE master.

2 In the access control policy page, click **Set** to open the Set Custom Scripts dialog box.

If the deployment platform setting in package settings is set to **Both Windows and Linux**, then the Set Custom Script dialog contains text fields for both Windows and Linux.



3 Browse to the script file and click **Open**.

4 Type the command for running the script. Include the script file in the command line, as well as any needed executable for running the script and any arguments to the script.

5 (Optional) Select **Timeout** and type in a timeout interval in seconds, in case the script does not run to completion. The user will be denied access if the timeout interval elapses before the script runs to completion.

6 Click **OK**.

7 If you are enabling an authentication script after you have already deployed packages with this ACE master, provide the script to the user using a policy/server update package or a custom package with ACE Resources.

NOTE The script is signed before deployment to prevent tampering. See page 125 for more information about resource signing.

Allowances

Under **Allowances**: In **Total number of activations,** choose how many instances can be activated from this ACE master:

- **Unlimited**
- **Maximum of**. Type the number or choose it from the drop-down list.

Advanced Setting for Power-On Script

You can provide a script to run at ACE instance power on that determines whether the ACE instance can be run.

See "To include a power-on script in the ACE master's packages" on page 111 for the procedure.

Activation and Authentication for Standalone Instances

If you are using a standalone ACE master, you can set the policies described in the following sections.

Activation

The activation step is performed whenever an ACE package has been installed.

Under **Activation**, select one activation type:

- **None** – No password is required; any user can activate this instance.
- **Password** – The user must enter the password specified by you to activate this ACE instance. You must provide the user with the password through email or other means. For standalone ACE masters, the password is provided during the packaging process.

Authentication

The authentication step is performed whenever the user runs the instance, unless **Authentication** is set to **None**. Under **Authentication**, select one authentication type:

- **None** – No password is required; any user can run this instance after it has been activated.
- **User-specified password** – Select this option to specify that the instance does not run until the user enters the correct password. Each user must set a password during activation, at first power-on.

  NOTE If a user enters an incorrect password a specified number of times, the user will be unable to try to enter the password again for a specified amount of time. The default values are five attempts and 30 seconds.

  To set the minimum length or required character types for the password, click **Set password policies** to open the Password Policies dialog box.

  Choose one, two, or all three of:

  - **Enforce minimum length.** Type the number or choose it from the drop-down list.
  - **Restrict password content**. Select one to four options for character type.
  - **Enforce password lockout**. Select the number of times the user can attempt to enter the password before an error message appears that tells the user that the number of allowed password attempts has been reached. Also specify the amount of time in seconds that the user must wait before making another attempt to log in.
- To set a recovery key:

  You can specify the key to be used for access to encrypted ACE instances. If you specify password protection for an ACE master and want to be able to reset the password for a deployed ACE instance from that master, you must specify a recovery key before you create the package that includes the virtual machine.

  a Click **Set recovery key**. The Recovery Key dialog box appears.

  b In the Recovery Key dialog box, select **Use recovery key** to configure a recovery key.

  c 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.

d Enter a name and location for the key pair.

e Enter and confirm the password to protect the private key.

f 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. The two parts of the key are stored in the location you indicated, with the names you specified followed by extensions ".pub" and ".priv" for the public and private portions of the key respectively.

NOTE You must know the password for the private key and the location of the private key file to reset a user's password.

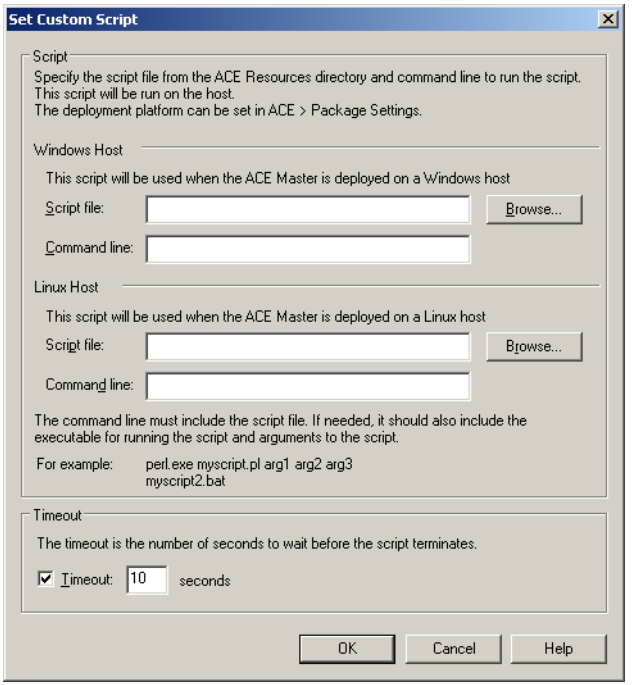
- **Script** – Select this option to use your own custom script to determine who can use the instance.

To provide this script in packages created with this ACE master

1 Create the script and save it in the ACE Resources directory for the ACE master.

2 In the access control policy page, click **Set** to open the Set Custom Scripts dialog box.

If the deployment platform setting in package settings is set to **Both Windows and Linux**, then the Set Custom Script dialog contains text fields for both Windows and Linux.



3 Browse to the script file and click **Open**.

4 Type the command for running the script. Include the script file in the command line, as well as any needed executable for running the script and any arguments to the script.

5 (Optional) Select **Timeout** and type in a timeout interval in seconds, in case the script doesn't run to completion.

6 Click **OK**.

7 If you are enabling this script for an ACE master that you have already deployed, include the script in the update package you distribute to your users, so that existing instances can be updated to use the new authentication script.

NOTE The script is signed before deployment to prevent tampering. See page 125 for more information about resource signing.

- To change the authentication setting from one type to another: Create a policy update package and distribute it to the user.
- To change the script: Create a new package with the new script and distribute the package to the user.

Advanced Setting for Power-On Script

You can provide a script to run at ACE instance power on that determines whether the ACE instance can be run.

See "To include a power-on script in the ACE master's packages" on page 111 for the procedure.

Setting Host-Guest Data Script Policies

You can provide a host-guest data script that runs when the ACE instance is powered on, and can be used to pass values to the guest operating system. The script, which runs on the host operating system, should output a set of key/value pairs, which become available to the applications running inside the guest operating system. The facility to do this is provided by the VMware Tools Service.

Use this policy setting to share specific host information with the guest operating system when the ACE instance is powered on.

The set of acceptable keys consists of `machine.id` and keys prefixed with `guestinfo`, such as `guestinfo.ipAddress`.

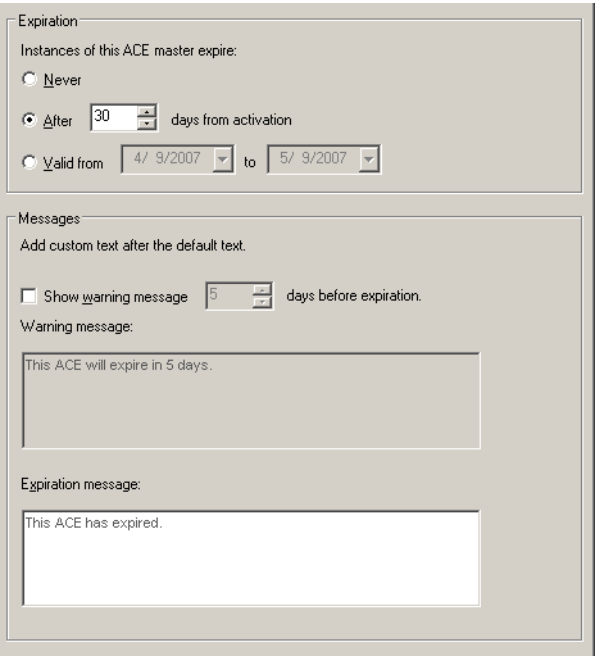
If the ACE master for this instance is configured to be deployed to both Windows and Linux platforms, you can provide scripts for both Windows and Linux systems.

To provide a host-guest data script to be run in the guest operating system, enable **Run a host-guest script at power on**. Then click **Set** to open the Set Custom Script dialog box and specify the scripts you want to run in the guest operating system. See page 115 for information about setting up custom scripts.

NOTE If you change a script for a deployed ACE instance, create an update package that contains the script and deploy it to the user's machine.

Setting Expiration Policies

Select **Expiration** from the Policy Editor window to set an expiration date for the ACE instance. When an instance expires, the files remain on the user's computer, but the instance cannot be used.



You can select one of the following options for expiration:

- **Never** – The instance does not expire.
- **After x days from activation** – The instance runs for the specified number of days after the package is installed and activated; it cannot be used after that time.
- **Valid from <date> to <date>** – The instance can be powered on and run no earlier than the **from** date and no later than the **to** date. It cannot be used before the **from** date or after the **to** date.

You can deploy ACE instances with expired date ranges.

You can set a warning message that appears each time an instance powers on as the expiration date approaches. You can customize the text of the warning message. Add your text after the gray text in the message box; the gray text cannot be edited.

The expiration message appears when the instance has expired. You can customize the text of this message as well, adding your text after the gray text, which cannot be edited. When the expiration message appears, the instance cannot be powered on.

With a standalone ACE instance, the fixed expiration date or the fixed date range is established at activation time. Each time the user powers on the instance, the date/date range is checked. If the date at power-on is beyond the specified date or outside the date range, an expiration message appears and the instance cannot be powered on. Expiration checks are also performed while the instance is running. If the expiration is reached, the expiration message appears and the instance is suspended.

With a managed ACE instance, the expiration policy works similarly as for standalone instances, but the expiration policy value can be specified on a per-instance basis, and all expiration values, both for ACE masters and for all ACE instances, are dynamic. A valid date range for an ACE master applies to each of its associated ACE instances until an instance is individually configured with its own date range. After that configuration, any changes to the ACE master's expiration policy do not affect the instance.

Setting Copy Protection Policies

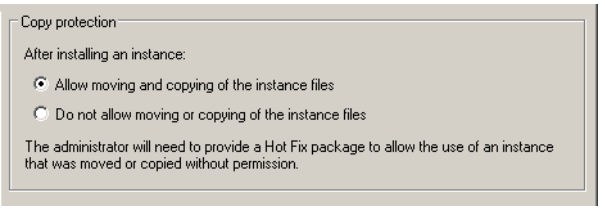
Copy protection policies let you ensure that an ACE instance can run only from the location where it was originally installed.

Every ACE has a CPID (copy protection identifier) that contains the path of the ACE on the host filesystem and either the system's BIOS ID (used for standard ACE instances) or filesystem ID (used for pocket ACE instances). If copy protection is on, Workstation ACE Edition compares the current CPID with the stored CPID. If they don't match, the instance has been moved or copied. For managed ACE instances, the CPID is stored on the server and can be updated by the administrator. For standalone ACE instances, the CPID can be set using vmware-acetool or hot fixes (onWindows systems, if hot fixes are enabled).

If you copy protect an ACE instance, it is still possible for the instance's files to be moved or copied. However, the copy-protected instance cannot be run from the new location.

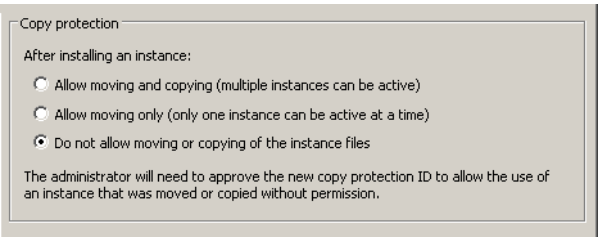
Copy protection is applied to individual ACE instances.

Copy Protection Policies for Standalone ACE Instances



To apply copy protection to a standalone ACE instance, click Copy Protection in the left pane of the policy editor. Select **Allow moving and copying of the instance files** to enable users to run their instances after moving or copying the instances. Select **Do not allow moving or copying of the instance files** to restrict users from moving or copying instance files.

Copy Protection Policies for Managed ACE Instances



You can dynamically change the copy protection settings for managed ACE instances, toggling the settings so that moved or copied instances will run or not run.

To view and change copy protection settings for a managed ACE instance, click **Copy Protection** in the left pane of the policy editor.

Select **Allow moving and copying (multiple instances can be active)** to enable users to run their instances after moving or copying the instances. Select **Allow moving only (only one instance can be active at a time)** to enable users to move their instances but not copy them. Select **Do not allow moving or copying of the instance files** to restrict users from moving or copying instance files.

In the Instance View for the server, a replaced and no longer active instance has a red "do not enter" sign on top of its icon.

If the policy allows copies and moves, a replaced instance can be reenabled if the user runs it.

If the user moves or copies the instance and tries to run the instance from that new location but either moves or moves and copies are not allowed without approval, VMware Player displays an error message that tells the user that this action is not allowed. The message also lists an alphanumeric string for the user to send to the system administrator or help desk assistant if the user wishes to request permission to move or copy the instance.

Administrators and help desk assistants can then reset the copy protection ID if they choose, allowing the moved or copied instance to be run. The administrator can apply this change in the Instance View in Workstation ACE Edition, and the administrator or help desk assistant can apply this change from the Help Desk Web application. See Chapter 12, "Instance View," on page 243 or "Using the VMware Help Desk Web Application" on page 237, respectively, for details about these two options.

Setting Resource Signing Policies

You can set the resource signing policy so that an ACE instance cannot be run if resource files, such as policy scripts or custom EULA text files, have been tampered with.

A "resource," for these cases, is any file that is in the ACE Resources directory during packaging. (Files that are put in this directory on the user's machine are not "resources" in this sense and are not signature-checked.)

Signature checking is performed, on the user's machine, at power on and then every time a script is run.

Select **Verify the integrity of all files in the ACE Resources folder** if you wish to protect against tampering with any resource files.

Select **Verify the integrity of policy scripts in the ACE Resources folder only** if you wish to protect against tampering with any policy scripts that have been saved in ACE Resources.

Select **No verification** if you do not want to verify that the resource files have not been tampered with.

NOTE If you set the encryption package setting options to **None**, any verification specified in the resource signing policy will not be performed. The encryption package setting overrides the resource signing policy setting. See "Encryption" on page 181 for more information about that package setting.

If you are creating a package that has substantial resources—for example, an ISO image that is hundreds of megabytes in size—and are using many policy scripts, you might

want to set the resource signing option to verify scripts only or no verification because signature checking could take a long time.

Setting Network Access Policies

Network access policies give you fine-grained and flexible control over the network access you provide to users of your ACE instances.

Using a packet filtering firewall, the network access feature of ACE 2 lets you specify exactly which machines or subnets an ACE instance or its host system may access. This means that you can, for example, configure the instance so it is allowed to connect only to your VPN server, which then controls access to other resources.

You can also customize the network access settings to filter on the basis of network addresses, traffic direction, protocol, and ports.

Workstation ACE Edition provides methods for you to perform the following tasks from within the user interface:

- Define network zones
- Define network access for your ACE instances' host machines (also known as "host network access")
- Define network access for your ACE instances' guest systems (also known as "guest network access")

Network access policies can be dynamic if the ACE instance is associated with an ACE 2 Management Server. This means, for example, that you can quickly lock ACE instances out of all or part of your network to help combat the spread of a worm or virus without deploying updated packages.

Topics in this section include:

Before You Begin: Read These Notes About Host Policies

Keep these facts in mind as you set host policies:

CAUTION A host machine for ACE instances can have only one host policy file. If you try to install an ACE package with a host policy file on a machine that already has a host policy file and the new package is from an ACE master that is different from the one already installed, the package install fails.

CAUTION Host policy settings might 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 http://www.vmware.com/info?id=110.

- A host policy is in effect even when no ACE instances are running. The policy effect starts immediately after installation and comes up every time the host system boots.
- "Host policy" can refer to both host network access policy settings and to host network configuration settings (for more about the latter, see "Network Properties Packaging" on page 141).
- You need to create and deploy a new package in order for the host policy to take effect. If you create packages with a managed ACE master that do not contain a host policy and then later edit the master's network access policy to include a host policy and publish the change, instances created from packages of that master will not have a host policy applied. A warning appears on the network access policy page if you attempt to apply a host policy in this way.
- You can package just the host policy in a Custom package, keeping the package size quite small.
- If you set up network access by using the Network Access Wizard through the Laptop Configuration option (described on page 109) and you do not modify any of the default settings provided by the wizard, then even though 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.
- Any restrictions on the host's network access also restrict network access for an ACE instance using NAT networking, because the NAT connection is affected by all the policies you apply to the host. If you set up restricted host access by using the ruleset and rules editors rather than the Network Access Wizard, ensure that you have configured the ACE master's virtual NICs to use bridged networking.

- If you are setting up a managed ACE master, then you must allow the host to access the ACE 2 Management Server, communicating through TCP over the appropriate port that you configure.

- Host policies do not apply to Pocket ACE instances. If you specify a restricted host policy for an ACE master and then attempt to create a Pocket ACE package with that master, the package will be created but the host policy will not be included in the package.

- You cannot view changes to host policies in the Preview mode. If you want to test the effects of such changes, you must do a test deployment. See Chapter 9, "Preview, Save, Test, Publish," on page 199 for details on test scenarios.

Getting Started with Setting Network Access

To get started: In the policy editor, select **Network Access** and then choose one of the following options:

- **Full network access** for both the ACE instance and its host – This option allows full network access, with no restrictions. This is the default setting. If you don't need to restrict network access, verify that this option is selected and then click **OK**.

- **Restrict network access** of the ACE instance and/or its host – This option allows restricted network access that is based on rules that you specify.

If you chose **Restrict network access**, you can now specify the access rules. Workstation ACE Edition provides you with two methods for setting up the rules:

- Use the Network Access Wizard to set up access quickly, using the default settings. See "Using the Network Access Wizard to Configure Network Access" on page 129.

- Skip the wizard and configure network access options by using the zone, ruleset, and rule editors. See "Using the Zone, Ruleset, and Rule Editors to Configure Network Access" on page 132.

NOTE Actually, you can combine the two methods by using the wizard to set the basic settings and using the editors to reconfigure and fine-tune the settings.

Using the Network Access Wizard to Configure Network Access

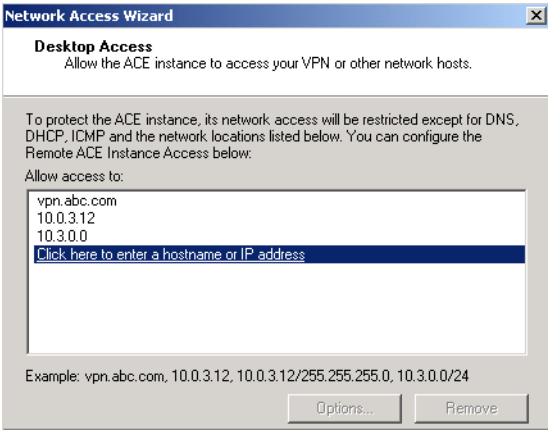
1 Click **Quick Setup Wizard** to start the Network Access Wizard. Click **Next** on the welcome page.

2 On the Network Configuration Type page, select one of the following options and then click **Next**:

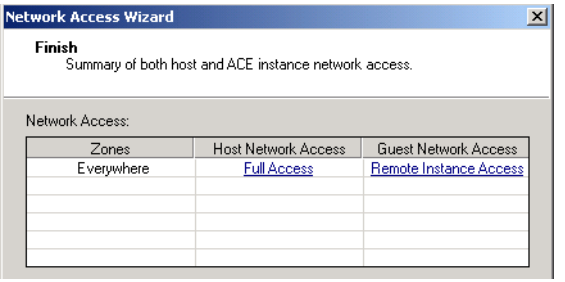
- **Desktop Configuration** – Select this option to set network access for ACE instances on host machines that connect indirectly to the corporate network. This option allows you to restrict ACE instance access to your VPN or specified hosts. Continue with Step 3.
- **Laptop Configuration** – Select this option to set network access for ACE instances on host machines that are sometimes connected remotely to the corporate network and sometimes connected directly to the corporate network. Configure network access to protect your internal network from an infected host and to protect the ACE instances against infection from untrusted networks. Continue with Step 4.

3 If you selected **Desktop Configuration**:

a On the Desktop Access page, click the link in the table and type the host names or IP addresses that the ACE instance is allowed to access in addition to the default DNS, DHCP, and ICMP protocols and ports.You can optionally enter subnet masks, in dotted quad format or in slash notation. When you have finished entering names and addresses, click **Next** at the bottom of the Desktop Access page.

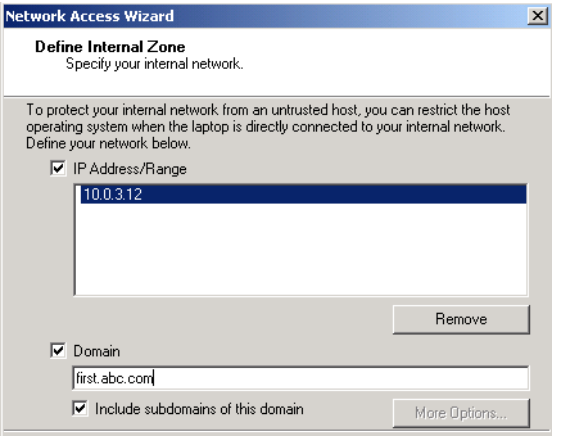


b The summary of the settings appears in the table on the Finish page. Click **Back** if you want to make any changes to the access you just configured. When you are satisfied with the configuration, click **Finish**.



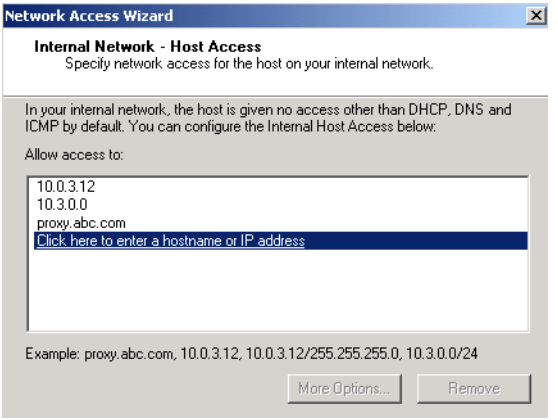
4 If you selected **Laptop Configuration**:

a On the Define Internal Zone page, specify the conditions that identify your internal (corporate) network. You specify this internal zone by IP address and range and/or by domain/subdomain. **IP Address/Range** is selected by default. If you don't want to use this option, deselect it. To use it, click the link in the table and type the IP addresses or address ranges. If you select **Domain**, type the domain name. Select **Include subdomains of this domain** (see the descriptions of **Allow subdomains of this domain** and other zone conditions on page 134) if you wish to include them when the software searches for a domain name match. When you have finished entering addresses and/or the domain name, click **Next**.

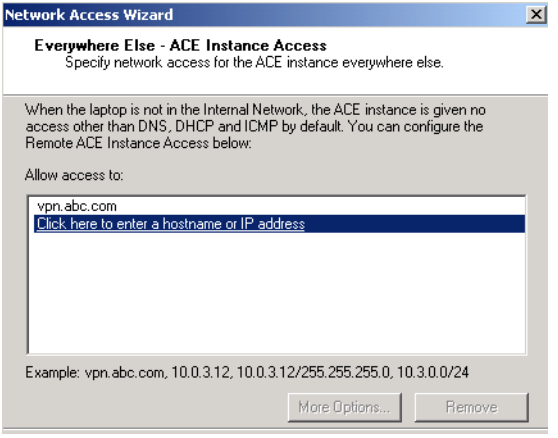


b On the Internal Network – Host Access page, type any host names and addresses for internal network locations that you want to allow this host

machine to access in addition to the default DNS, DHCP, and ICMP protocols and ports and then click **Next**.

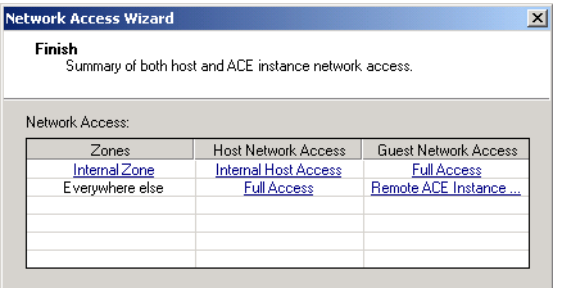


c On the Everywhere Else – ACE Instance Access page, type host names or IP addresses for locations that this ACE instance can access—in addition to the default DNS, DHCP, and ICMP protocols and ports—when the instance is outside the internal network. Then click **Next**.



d The table on the Finish page summarizes the access settings. Click **Back** if you want to make any changes to the access you just configured. When you are satisfied with the configuration, click **Finish**. The summary of the network

access settings you have chosen appears in the table on the Network Access policy page.



You have finished setting up network access for the ACE instance and its host. The current settings for all zones, with the labels you have applied, appears on the Network Access policy page. If you want to, click on the links and buttons in the policy page to open the zone, ruleset, and rule editors and then to reconfigure and fine-tune the access settings. See "Using the Zone, Ruleset, and Rule Editors to Configure Network Access."

Using the Zone, Ruleset, and Rule Editors to Configure Network Access

You can configure and edit network access settings with the zone, ruleset, and rule editors by clicking the links in the table on the Network Access policy page. The use of those editors is described in the following sections:

Using the Zone Editor to Set Up and Configure Network Zones

Zone descriptions describe the characteristics of a network zone. Workstation ACE Edition 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 for any adapter in any of the zone definitions.

The zones are checked in the order they appear in the network access table, from the top down. When the host connects to a network, checking begins to see whether the network matches the conditions for a zone. The checking starts with the topmost zone in the table and continues down the table until a match is made or the Everywhere Else zone is reached. When a match is made, the zone checking stops and filter rules for that zone are applied.

Details about zone matching are:

- A zone can be specified by using up to six conditions:
  - Domain
  - Subnet
  - DNS servers
  - DHCP servers
  - Gateway servers
  - WINS servers

  For a match to occur, *all* specified conditions must be met.
- All zone conditions except the domain condition allow users to specify a list of addresses. The match is made if the host's address matches *any* of the address-list entries in a specified condition.

Guidelines for Choosing Zone Conditions

Choose the characteristics you specify carefully.

There are trade-offs between using shorter and longer lists of conditions.

If you use a longer list, you minimize the chances of a false-positive or a misidentification. Minimizing the chance of a false-positive or a misidentification can be important if you are providing an 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 and instance access policies are applied—even if the host is not connected to your network.

In some cases, however, using a longer list might also increase the likelihood that an 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 Network address, or Network address and DNS server information).

Another point to consider is that the addresses or names of certain servers can change over time. Such changes can also introduce detection issues.

Using a smaller set of information—for example, using only the network address and the subnet mask—in a zone description lessens the chance that the detection mechanism fails 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.

Descriptions of the Zone Condition Settings

Each zone description must contain one or more of the following setting options describing the conditions of the zone:

- **Domain** – Specifies the domain name of the network—for example, `mycompany.com`. Only one entry can be used. You can't use a list of entries. The interpretation of this option is governed by the value of **Allow subdomains of this domain** (below).
- **Allow subdomains of this domain** – Modifies the **Domain** option (above). It specifies whether, for the **Domain** zone condition to be met, a domain name must exactly match the domain name specified in the **Domain** box or whether a match of the domain name is made anytime the string contains `<domain_name>`. For example, if this option is selected, then `corp.mycompany.com` is considered a match for `mycompany.com`. If this option is not selected, then `corp.mycompany.com` is not considered a match for `mycompany.com`. The default setting for this option is deselected.
- **Network address** – Specifies an IP address or subnet range that is used by the network. The value of `<subnet>`, if you include a subnet range, must be the number of bits in the netmask. A network adapter matches this condition if it is using an IP address that lies within any of the specified ranges.
- **DNS servers** – Specifies one or more IP addresses or host names for DNS servers on the network. A network adapter matches this condition if it is using at least one of these servers.
- **Match at least** – Modifies the **DNS servers** option. A network might have multiple DNS servers, and a host might 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.

- **DHCP servers** – Specifies one or more IP addresses or host names for DHCP servers on the network. A network adapter matches this condition if it is using at least one of these servers.
- **Gateway servers** – Specifies one or more IP addresses or host names for default gateways on the network. A network adapter matches this condition if it is using at least one of these gateways.
- **WINS servers** – Specifies one or more IP addresses or host names for WINS servers on the network. A network adapter matches this condition if it is using at least one of these servers. WINS server settings are ignored by Linux hosts during zone detection.
- **Match at least** – Modifies the **WINS servers** option. A network can have multiple WINS servers, and a host might 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.

Steps for Adding or Editing a Network Zone

NOTE You cannot delete or rename the default zone, which is named "Everywhere" if it is the only zone or "Everywhere else" if there is more than one zone.

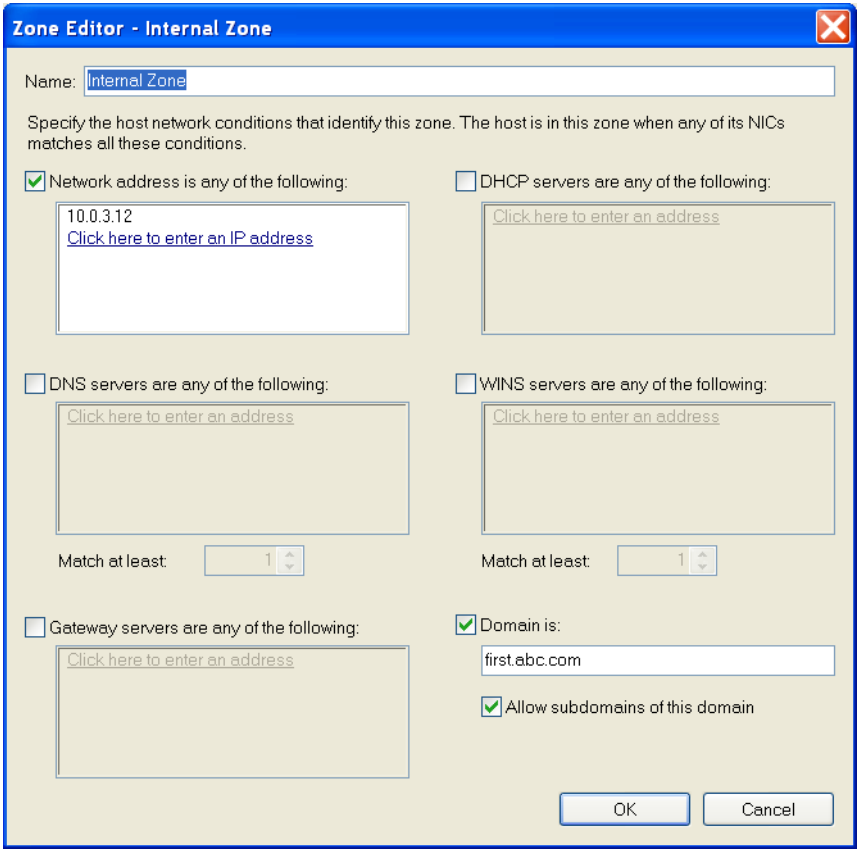
To add or edit a network zone

1. If you want to add a new zone, click **Add Zone** on the Network Access policy page and then click the **New Zone** entry in the table. The zone editor appears.
2. If you want to edit an existing zone, click the name of the zone in the table on the policy page. The zone editor appears.
3. If you want to name a new zone or rename the existing zone, type the new name in the **Name** box.
4. Select the checkboxes for any host network conditions that you want to use to identify this zone. Type addresses or host names as appropriate.

   NOTE For guidelines on choosing these settings and for detailed descriptions of the zone conditions, see "Guidelines for Choosing Zone Conditions" on page 133 and "Descriptions of the Zone Condition Settings" on page 134.
5. If you have specified DNS servers or WINS servers for the zone, select the minimum number of servers that must be matched to meet the zone conditions. WINS server settings are ignored by Linux hosts during zone detection.

NOTE Because there are multiple methods for assigning DNS domain names to a Linux host, using just the DNS domain name to define a zone can be error-prone. We recommend that you use criteria in addition to the DNS domain name to define a zone for Linux hosts.

6 When you have finished making your zone condition selections, click **OK**.



Using the Ruleset and Rule Editors to Configure Host and Guest Access

Each access setting for the ACE instance's host machine and for the ACE instance's guest system is based on a set of access rules. Whenever you create a host or guest access setting with the Network Access Wizard, a default ruleset is used. You can change the parameters of those rules by using the ruleset and rules editors.

Before You Begin Configuring Rulesets and Rules: Details on Filtering Action

Network access policies are applied by filtering on the IP address, the protocol number from the IP header, the direction of traffic, and TCP and UDP port values. The filtering does not involve deep packet inspection. For DNS and DHCP access, the TCP and UDP ports on which those services traditionally reside are opened.

Note the following aspects of the filtering actions:

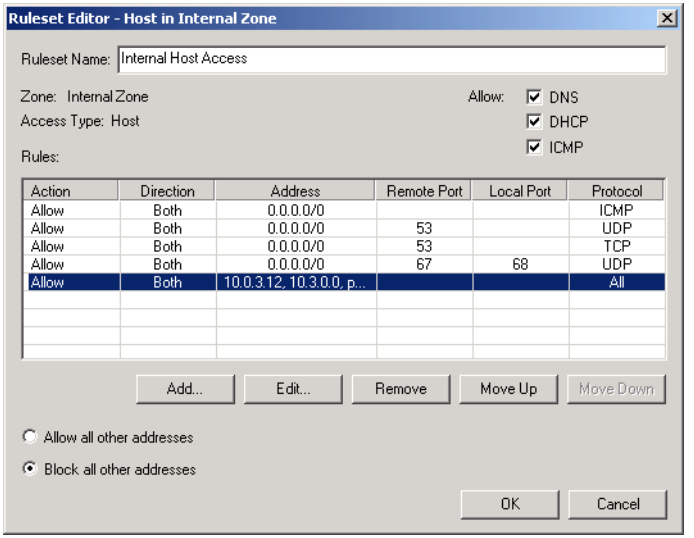
- If you move your services to different ports, the network access rules for those services won't work.
- The host or instance is open to all traffic on these protocols and ports.

To understand the particulars of how traffic is being blocked or allowed for DNS, DHCP, and ICMP protocols and ports, you can look at the rules displayed in the ruleset editor.

Steps for Adding or Editing Rulesets and Rules

To add and edit rulesets and rules for network access

1 In the Network Access policy page, click the link in the table for the access setting you want to edit. The ruleset editor appears. The Zone and Access Type information just below the Ruleset Name box shows the name of the zone and whether the access setting applies to the host or to the guest.



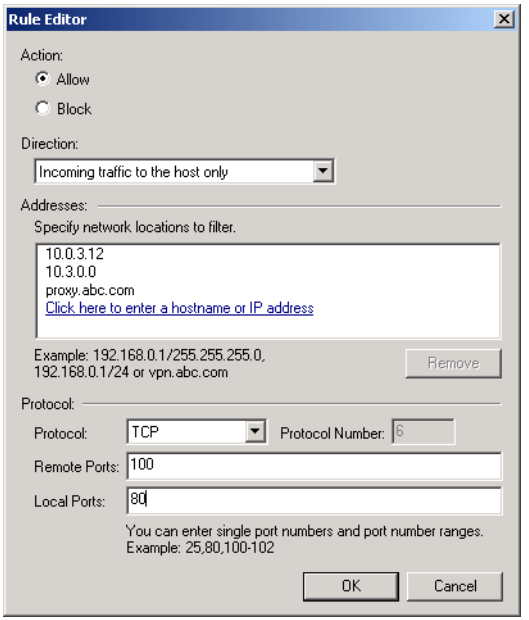
2 If you want to change the name of the ruleset, enter the new name in the **Ruleset Name** box.

3 By default, **DNS**, **DHCP**, and **ICMP** are included in the network access setup. Generally, we recommend that you keep DHCP and DNS selected, as they are important for zone detection, for both host and instance access. Deselect them if you do not want them included in the access setting.

- **DNS** – Keep this option selected if the ACE instance needs to resolve IP addresses using a DNS server that is not included in any other network access setting for the instance.
- **DHCP** – Keep this option selected if the ACE instance needs to get its IP address from a DHCP server that is not included in any other network access setting for the instance.
- **ICMP** – Keep this option selected if you need support for the ping command—for example, to check network connectivity to and from the virtual machine.

4 If you want to add or edit a rule, click **Add**. If you want to change a specific rule's settings, click the row for that rule in the table in the ruleset editor and then click **Edit**.

The rule editor appears.

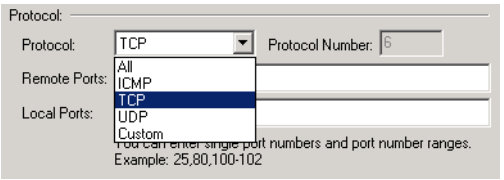


5 To change the action for this rule, select the new action, **Allow** or **Block**, as appropriate.

6 To change the direction of traffic for the rule, select the option you want from the drop-down list under **Direction**.

7 To add a host name or IP address for the rule, click the link in the table under Addresses and type the new name or address. The wildcard setting for all IP addresses is 0.0.0.0/0. If you want to edit an existing host name or address, click that item and edit it. To remove a host name or address, click the item and then click **Remove**.

8 To change the protocol used for this rule, select the new protocol you want from the **Protocol** drop-down list.



Select **Custom** if you want to allow or block communication for a specific protocol. The protocols are defined by their protocol numbers, which range from 0 through 255. The number is in the packet. If that number matches the number supplied in the Custom field, the packet is allowed or blocked as specified by the rule. Type the protocol's number in the Protocol number box.

You can find the protocol number with the protocol's RFC at http://www.ietf.org/rfc.html for protocol numbers. You can also see a listing of protocols and their numbers at http://www.iana.org/assignments/protocol-numbers.

NOTE The protocol number is used in the protocol field of IPv4 packets. Most protocol numbers are permanently assigned.

---

9 If you are using either TCP or UDP and want to qualify the rule with specific port numbers for this type of traffic, type the port numbers or port-number ranges in the **Remote Ports** and **Local Ports** boxes as appropriate.

The wildcard port setting is "" (double quotation marks).

Usually you specify filtering on one or the other port type, not both, because both specifications have to meet the match for the rule to be applied. (DHCP represents an exception to this general rule.)

- Local port – Filters on the port from the local machine, either host or guest. The local port is the source port for outgoing packets and the destination port for incoming packets. Typically you specify a local port when the host or guest is being used as a server getting remote connections on some port.
- Remote port – Filters on the port from the remote machine. The remote port is the source port for incoming packets and the destination port for outgoing packets. Typically you specify a remote port when the host or guest is a client and is contacting a remote server on some port.

10 When you have finished making all the changes you want to make in the rule, click **OK**. The ruleset editor reappears, with the changes now appearing in the rule that you edited.

11 If you want to remove a rule, select the row for the rule in the table and click **Remove**.

12 If you want to move a rule up or down in the table to change the order in which the rules are applied, select the row for the rule in the table and click **Move Up** or **Move Down** as needed. Precedence for rule application starts with the rule at the top of the table. See "Packet-to-Rule Comparison" on page 141 for details.

Packet-to-Rule Comparison

The rules in the ruleset editor are listed in the order in which they are to be evaluated. When a network traffic packet arrives or is to be sent from the host or guest, it is compared with each rule in the ruleset, in order from the top down. If the packet's settings (that is, source address for incoming packets, destination address for outgoing packets, protocol, and ports) match the rule conditions, the packet is allowed or blocked according to the rule's action. The packet is compared to each rule in order until either it matches a rule or it has been compared with all of the rules. When a match is made, the packet-to-rule comparison ends; the packet is not compared to subsequent rules in the ordered list. If it has been compared to all rules without a match, the default rule action is applied.

Network Properties Packaging

You can use the network properties packaging feature of the network access policy to specify the IP address range for the virtual network VMnet8 on the ACE instance's host system. You deploy this network properties setting with the ACE package.

CAUTION If you set this property, the setting affects all the ACE instances and virtual machines on this instance's host system.

NOTE The network properties packaging setting is not a dynamic policy setting. You can only change the setting by changing it in the policy, then creating a new ACE package and deploying the package.

To specify the subnet range for VMnet8

1. For the ACE master you want to package with these network properties, select **Policies > Network Access**.
2. Click **NAT Settings** on the policy page. The Virtual Network Settings dialog box appears.
3. Select **Assign IP addresses from this subnet**.
4. Type the subnet IP address you want to use, entering zero (0) as the last byte in the address.
5. Click **OK**.

Understanding the Interaction of Host Access and Guest Access Filters With Tunneling Protocols

Host access and guest access filters can differ in their interactions with tunneling protocols.

A host network access filter sees traffic before packets have been encapsulated in the tunneling protocol (for example, VPN), but a guest network access filter sees traffic after the packets have been encapsulated in the tunneling protocol.

Because of this guest access filter behavior, it might be possible for a user to circumvent guest access restrictions through use of tunneling protocols or proxies.

Setting Removable Devices Policies

Removable devices policies allow you to control whether users can connect and disconnect removable devices from their ACE instances.

A Removable Devices policy is applied to an ACE master and affects all users of all instances created from that ACE master.

To apply a removable devices policy, click **Removable Devices** in the left pane of the policy editor. All removable device types for this ACE master are visible in the list. To enable all users of ACE instances created from this master to connect and disconnect a device, select the device in the **Allow** column.

NOTE To add devices, use the virtual machine settings editor (**VM** > **Settings**).

Setting USB Device Policies

You can set USB device policies to restrict the ACE user's access to USB devices to protect the integrity of ACE instances and your network. The policies are dynamic, so you can allow and then block access to USB devices.

You can set restrictions at various levels of specificity, and you can mix levels of restriction in a policy setting. The levels of restriction are:

- **Specific USB device** – For example, allow use of a specific type of digital camera but disallow use of iPod mobile digital devices.
- **Device class** – For example, allow use of HIDs (human input devices), such as mice and keyboards, but disallow use of communications devices, such as modems and cell phones.
- **All USB devices** – Allow or deny access to all connected USB devices.

NOTE Rule application and precedence: Access control is applied at the most granular level, and the most restrictive rule is always applied. That is, if a rule exists for a specific device, then that rule overrides any rules set for device classes in which the device belongs. In the same way, specific device class settings override the default setting for all other device classes. If no specific device rule exists, and there is more than one device class rule that applies to the device, then the most restrictive rule is applied. For example, if one applicable device class is blocked, then the device is blocked, even if other applicable classes are allowed.

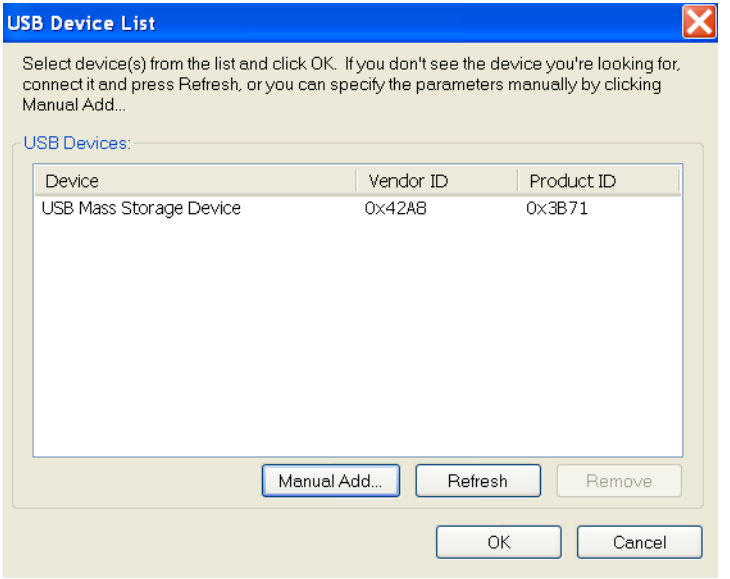
To set a USB device policy

1 To specify USB policy by specific device: You can allow or block a device in the **Device** list. You can add a device by clicking the **Add** button below the **Device** list.

All entries in the Device list are maintained in a device database that is included with the files for this ACE master.

a To select a device to be used with instances from this ACE master, click the device in the Device list and then select the checkbox under **Allow**. To disallow the specific device, click **Block**.

b To add a device or manually enter information about a device, click the **Add** button below the Device list. The USB Device List dialog box appears.



NOTE You can copy and share the database. Note, however, that it is not write-protected. The default location for the file is `C:\Documents and Settings\All Users\Application Data\VMware\VMware Workstation\usbhistory.ini`.

- You can add devices to the list in two ways:

  (1) Plug in the device and click **Refresh** to add it.

  When the system recognizes the device, the device appears as an entry at the end of the Device list in the USB Device List dialog box after one of two occurrences: (1) The dialog box has just been opened or (2) you clicked **Refresh**.

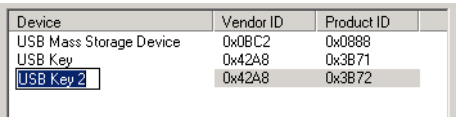
  The device is added to the device database and is maintained there as an entry even after you unplug the device.

  (2) Click **Manual Add** to open the Add USB Device dialog box.

  In that dialog box, type a name for the device in the **Name** box. Then type the vendor ID and product ID in the appropriate boxes. (Vendor IDs are assigned to manufacturers by the USB Implementers Forum; the USB-IF Web site is http://www.usb.org. Product IDs are assigned by manufacturers to their individual products.) Click **OK**. The device appears as an entry at the end of the Device list in the USB Device List dialog box.

- To make changes to the details of a device in the list:

  To edit a device name, click **Add** in the USB Devices policy page. The USB Device List dialog box appears. Double-click the device to select it. The name is highlighted in its own editable text box. Edit the name.



  To alter the Vendor or Product IDs for a device already in the list, click **Add** in the USB Device List dialog box. Type in the name of the device, then make changes as needed in the ID fields. Then click **OK**.

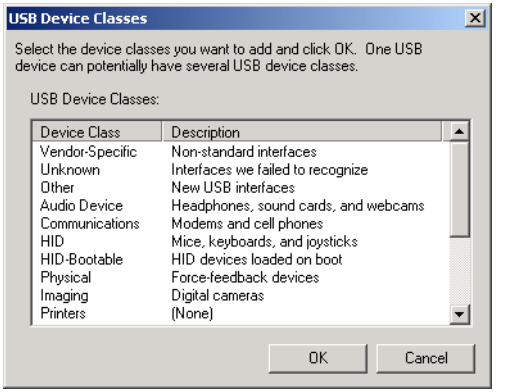
c When you are finished adding devices and changing device details, select the devices in the USB Device list that you want to add to the policy page and then click **OK**. The devices appear in the **Device** list on the policy page. The **Allow** checkbox is automatically selected when you add a device.

2 To select a device class to be used with instances from this ACE master: Under **General access to all USB devices**, you can select a device class already in the list or add a device class by entering information in the USB Device Classes dialog box. USB devices all belong to one or more classes, each of which has a class identifier. For example, the mass storage class contains devices such as memory sticks and Apple iPods.

a To select a device class, click the class in the USB Device Classes list and select the checkbox under **Allow**. To disallow the device class, click **Block**.

b To add a class, click **Add** in the **Default Policies** area of the page. The USB Device Classes dialog box appears. Select the classes you want to add and click **OK**. The **Allow** checkbox is automatically selected when you add a device class.

NOTE A specific USB device can have more than one interface (for example, a device might include both a fax function and a print function) and therefore can belong to more than one class. As noted earlier, the most restrictive rule is always applied. For the example just given, if one rule blocks a fax device but another rule allows a print device, then a combination fax/print device is blocked.



3 To select the default device policy to be used for all other USB devices (that is, any devices not already specifically allowed or blocked with device or device class settings) with instances from this ACE master, click either **Allow** or **Block** next to **Default for other device classes**.

Setting Virtual Printer Policies

VMware ACE includes a virtual printer that allows users to print to any printer available to the host computer from applications inside a virtual machine without installing additional drivers in the virtual machine.

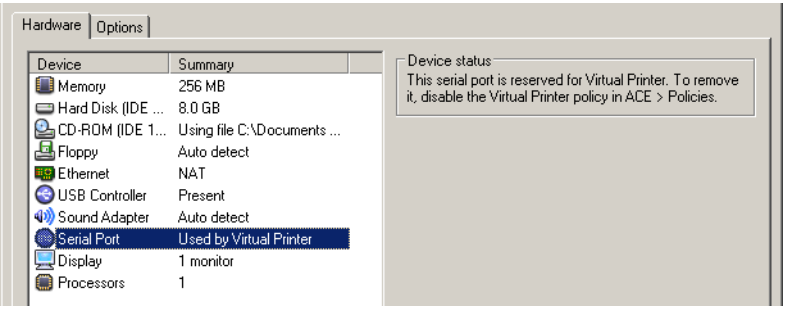
NOTE The virtual printer feature is available for ACE instances running with these Windows host and guest operating systems:

- Host: Windows 2000, XP, 2003, or Vista, 32-bit only
- Guest: Windows 2000, XP, 2003, Vista (32- and 64-bit), Linux RHEL 4 (32 bit only), Ubuntu, and SUSE

Select **Enable virtual printer for instances** to allow users to print to the virtual printer.

After you have enabled this policy, a serial port appears on the **Hardware** tab of the virtual machine settings editor, with the summary **Used by Virtual Printer**. You can

only add or remove this serial port by enabling or disabling the option in the Virtual Printer policy.



NOTE If the ACE master already has four serial ports, you won't be able to add another serial port for the virtual printer. To enable the virtual printer, delete an existing serial port.

The user will be able to print to any of the host printers that are available in the printer selection list from the Print dialog box. The user can control which printers are available in that list by opening the tray icon for the print application in the host taskbar notification area and selecting the printers to use. The tray icon is visible when the ACE instance is running.

Setting Runtime Preferences Policies

You can set options on the runtime preferences policy page to specify which Workstation ACE Edition runtime attributes the user can choose.

Runtime Preferences

If you select **Always run in full screen**, VMware Player fills the full screen when it starts, hiding the host operating system. You might find this useful, for example, to avoid user confusion about the differences between the host system environment and that of the ACE instance.

The user can minimize the Workstation ACE Edition 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.

NOTE If the user has more than one monitor, full screen mode fills only one display, and the host system is available on the other display.

If you select **Always run in appliance view**, the ACE instance will open in Appliance mode and the user will not have the option of running the instance in Console mode.

NOTE You must enable the appliance view in virtual machine settings (**VM > Settings > Options > Appliance**) for this runtime option to work. If you select **Always run in appliance view** in this policy but do not enable the appliance view setting in virtual machine settings, an error message appears when the user attempts to start up the ACE instance.

If you select **Do not allow users to modify the memory allocation**, the Change Memory Allocation command does not appear in the **VMware Player > Troubleshoot** menu of VMware Player, so the user cannot alter memory allocation for the ACE instance.

Exit Behavior

If you select **The user determines the exit behavior**, the user has access to both Suspend and Power off choices in the Preferences dialog box (**VMware Player > Preferences**).

If you select either **Suspend the ACE instance** or **Power off the ACE instance**, that option is selected by default in the Preferences dialog box (VMware Player > Preferences), and the user cannot change the option. The instance exits with that default behavior if the user chooses **VMware Player > Exit** or clicks the Close icon on the Player window.

If you select **Remove the power commands from the Player Troubleshoot menu**, the Reset and Power off and exit options do not appear in the VMware Player > Troubleshoot menu, and the user can power off or suspend the ACE instance only by exiting VMware Player. The actual exit behavior is specified in the VMware Player Preferences dialog box.

Enhanced Keyboard Filter (for Windows Host Systems Only)

Select **Always use the enhanced keyboard filter** if you want ACE instances created with this ACE master to always run with this feature.

You must also turn on the enhanced keyboard filter feature in virtual machine settings. To do that, go to **VM > Settings > Options > General** and select **Use enhanced virtual keyboard** under **Miscellaneous**. Click **OK** on the General settings page. You can apply the feature to existing ACE masters or virtual machines and clones of these masters and virtual machines by enabling it in the virtual machine settings.

The enhanced keyboard filter provides an alternate method for the way a Windows host system ordinarily processes keyboard input. The filter provides a solution to these problems:

- Certain key combinations are reserved by Windows operating systems and are processed at a very low level. For example, if you press Ctrl+Alt+Delete while the running ACE instance has keyboard focus, the host system, as well as the guest system, acts on the entered command.
- Keyboard input is passed quickly through the operating system driver stack and possibly through other low-level keyboard handlers, providing opportunities for malware to log keystrokes intended for an ACE instance.
- International keyboards or keyboards with extra keys might not be handled well.

The enhanced keyboard filter provides a new keyboard input path for Windows host systems. It processes raw keyboard input as soon as possible, bypassing Windows keystroke processing and any malware that's not already at a lower layer.

For example, with the enhanced keyboard filter, Ctrl+Alt+Delete works in the guest system only if the instance has keyboard focus.

The virtual machine settings editor has the enhanced keyboard filter option setting enabled by default. With that setting, the virtual machine or ACE instance runs in VMware Player with the enhanced option as long as the needed keyboard filter driver has been included in the virtual machine/instance's files.

If you enable this runtime preference policy, then an ACE instance created with this setting must use the enhanced keyboard filter option. If the driver is not available to the instance at power-on, the instance will not run.

Keyboard-filter installation requires a host-system restart.

Setting Snapshot Policies

You can set policy options for two types of snapshots:

- Reimage snapshots – The program automatically takes a reimage snapshot of an ACE instance when the ACE is created. It takes the snapshot after all the required instance setup steps are complete (including, if applicable, encryption, instance customization, and domain join). The snapshot is taken while the ACE instance is powered off.

  NOTE You can manually disable the automatic reimage snapshot by editing the ACE master's aceMaster.dat file. Edit the option packaging.takeReimageSnapshot.

- User snapshots – You can enable users to take a user snapshot of the ACE instance either when the instance is running or immediately after powering it off, and you can also enable them to delete that user snapshot. If you enable options in this policy for this user snapshot, Snapshot appears in the VM menu when the ACE instance is powered on. Only one user snapshot can be saved at a time.

The two snapshot types differ in these ways:

- **Primary uses** – Reimage snapshots allow the ACE administrator, or the user if the administrator enables reimage snapshot options for the user, to revert the ACE instance to its known good starting state or to the known good updated reimage state. The administrator might tell the user to revert to the reimage snapshot to fix a problem with the virtual machine. The administrator also might patch the virtual machine or install new software, retake the reimage snapshot, and then revert the machine to the snapshot or instruct the user to do so. User snapshots enable the user to return the virtual machine to a known stable state.
- **When they are first taken** – The reimage snapshot is first taken automatically after the ACE instance is created but before it is run for the first time. A user snapshot is taken whenever the user chooses after powering on the ACE instance.
- **Precedence** – The reimage snapshot must always be older than the user snapshot. Taking a new reimage snapshot deletes any existing user snapshot. User snapshots can be taken, reverted to, and deleted without affecting the reimage snapshot.
- **Power state when taken** – User snapshots can be taken both in powered-on and powered-off states. The reimage snapshot is only taken in a powered-off state.

NOTE You can't take snapshots of a Pocket ACE instance. For more about Pocket ACEs, see Chapter 10, "Pocket ACE," on page 207.

To select options for the user snapshot

Choose the options you want the user to have:

- **Take the user snapshot**
- **Revert to the user snapshot**

If you select either or both of those options, the **Snapshot** command appears in the VMware Player menu when the instance is powered on. If the user is allowed to take the snapshot, the user can take a snapshot while the ACE instance is running or have VMware Player power off the ACE instance, take the snapshot, and then power the instance on again (**VMware Player > Snapshot > Take Snapshot**).

Taking the snapshot when the instance is powered off provides two benefits:

- Gives the snapshot greater mobility – A snapshot taken when the virtual machine is powered on might become unusable as it is moved between host computers.
- Takes up less disk space than a snapshot taken when the virtual machine is powered on.

If an ACE instance gets stuck during the taking of a powered-off snapshot (for example, at a message that says you can power off your machine), the user can issue the command to take a powered-off snapshot again to force the machine to power off. The machine will be powered on again and the snapshot will have been taken.

All power and snapshot operations, including exiting VMware Player, are disabled while the software is taking a powered-off snapshot.

If **Revert to the user snapshot** is enabled, the user can choose **VMware Player > Snapshot > Revert to Snapshot** whenever a user snapshot exists.

If **Take a user snapshot** is enabled, the user can delete the user snapshot by selecting **VMware Player > Snapshot > Delete Snapshot**.

NOTE If the user or the administrator takes a reimage snapshot, the user snapshot is deleted.

To select options for the reimage snapshot

Choose the options you want the user to have:

- **Replace the reimage snapshot**
- **Revert to the reimage snapshot**

If you select either or both of those options, the appropriate commands to execute the options appear in the **VMware Player > Troubleshoot** menu.

You might want to give the user the ability to replace the reimage snapshot. Because the reimage snapshot is taken when the ACE instance is created, any changes that have been made to the ACE instance after instance creation are lost if the user reverts to that reimage snapshot. If the ACE instance has been updated and this option is enabled, you can tell the user to replace the reimage snapshot so that it will include those changes. To replace the reimage snapshot, the user chooses **VMware Player > Troubleshoot > Take Reimage Snapshot**.

If the user chooses **VMware Player > Troubleshoot > Revert to Reimage Snapshot**, 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 the ACE administrator.

NOTE If you choose not to enable the reimage snapshot options for the user, you can replace the reimage snapshot or revert to it on the user's machine by providing administrator mode access through the Administrator Mode policy. See "Setting Administrator Mode Policies" on page 152.

Setting Administrator Mode Policies

You can use the administrator mode policy to set an administrative password so you can do any of the following:

- Run the ACE instance on the user's machine and enter the administrator mode to access the virtual machine settings and make changes to the instance's configuration (on Windows systems only). You can only edit the settings; you cannot add or remove devices.
- Run the ACE instance on the user's machine and enter the administrative mode to access all the snapshot commands, including Take Snapshot, Take Powered Off Snapshot, Revert to Snapshot (these first three refer to the user snapshot), Take Reimage Snapshot, and Revert to Reimage Snapshot. See "Setting Snapshot Policies" on page 150 for information about the user snapshot and the reimage snapshot.
- Use the vmware-acetool command-line program directly on an ACE user's system to fix a limited set of problems for standalone ACE instances.

To use these features, select **Enable administrator mode** in this policy.

To edit the virtual machine settings or use snapshot commands not available to the user on the ACE user's machine, select **VMware Player > Troubleshoot > Enter**

Administrator Mode. Enter and confirm the password to be used for administrator access. Then choose the appropriate commands as follows:

- To edit virtual machine settings from the user's machine (on Windows systems only), select **VMware Player > Troubleshoot > Virtual Machine Settings**.
- To use the user snapshot commands, select them from the Snapshot menu (**VMware Player > Snapshot**).
- To use the reimage snapshot commands, select them from the Troubleshoot menu (**VMware Player > Troubleshoot**).

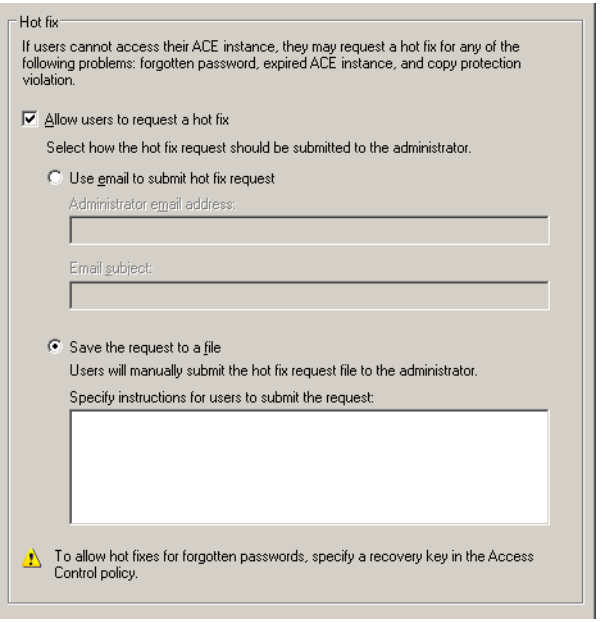
When you are finished resetting the virtual machine settings or using the snapshot commands, select **VMware Player > Troubleshoot > Exit Administrator Mode**.

For detailed information about using the ACE Tools, see "ACE Tools: vmware-acetool Command-Line Tool" on page 234.

Setting Hot Fix Policies

You can use the hot fix policy to specify that users can request hot fixes for specific problems.

NOTE Hot fixes can be used only with standalone ACE instances. You can use the Help Desk Web application or the Instance View in Workstation ACE Edition to fix problems with managed instances. See "Using the VMware Help Desk Web Application" on page 237 for information about using that application and Chapter 12, "Instance View," on page 243 for information about using the Instance View.



If you enable the hot fix feature, 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 a user's password for encrypted or tamper-resistant ACE instances, you must enable a recovery key in the access control policy. See page 118 for details on enabling a recovery key.

- Expired ACE instance
- Copy-protected ACE instance run from a new location

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

The hot fix request is a file that the user must submit to an administrator for action. After enabling the hot fix feature, you must select the preferred way for the 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 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 Hot Fix Request wizard saves the hot fix request file. The user must submit this file to an administrator manually.

  The 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 user an opportunity to save the hot fix request as a file. The 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 235.

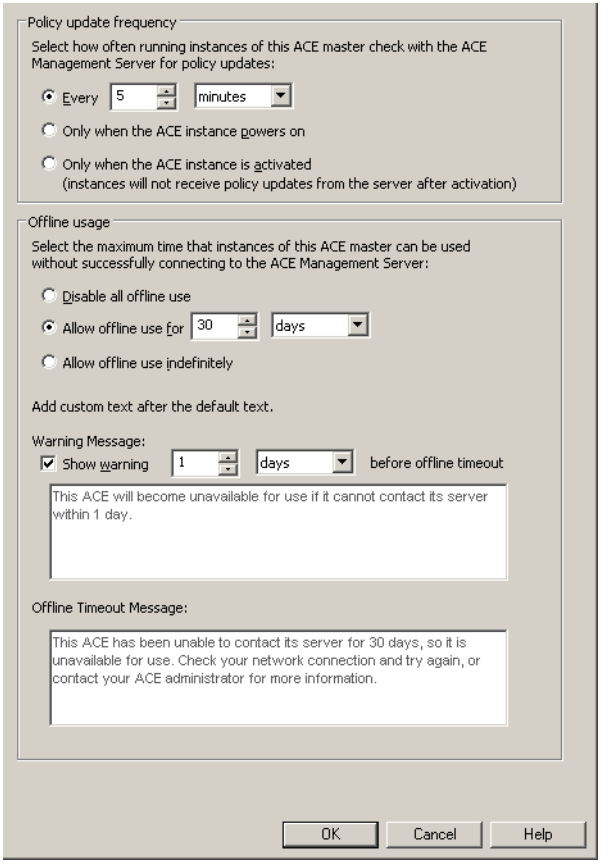
For details on how the user interacts with the Hot Fix Request Wizard, see "Requesting a Hot Fix" on page 126.

Setting Policy Update Frequency

You can use this policy to control:

- **Policy update frequency** – How often a managed ACE instance must connect with the ACE 2 Management Server to download any policy updates while it is running
- **Offline usage** – How long a managed ACE instance is available for use without connecting to the ACE 2 Management Server. "Offline" in this usage refers to the instance not being connected to the server; the instance might be running with other active network connections.

NOTE This policy applies only to managed ACE instances. Policy updates for standalone ACE instances are applied as policy update packages. Policy changes are applied when the instance is started up after the update package has been installed.



To set the policy update frequency

1 In Policy Update Frequency, select one of:

- **Every [x] [time_unit]** – Set **x** to the number of minutes, hours, or days and set **time_unit** to **minutes**, **hours**, or **days** that the ACE instance can run before it must connect to the server and retrieve any updated policies.
- **Only when the ACE instance powers on** – The instance connects to the server at power on and retrieves any updated policies.
- **Only when the ACE instance is activated** – Choose this option if you do not need to have contact with the ACE instance after it has been activated.

2 In Offline Usage,

a Select one of:

- **Disable all offline usage** – The ACE instance must be connected to the server while it is being used so that policy updates are transmitted to the instance at the update frequency rate (default setting is five minutes).
- **Allow offline use for [x] [time_unit]** – Set **x** to the number of minutes, hours, or days, and set **time_unit** to **minutes**, **hours**, or **days** that the ACE instance is available for use before it must connect to the server to check for policy updates. When the limit is reached, the ACE instance cannot be powered on and used.
- **Allow offline use indefinitely** – The ACE instance can be used for an indefinite period of time without any requirement that it connect to the server to retrieve policy updates.

b If you chose **Disable all offline usage** or **Allow offline use for [x] [time_units]**, the text in the Offline Timeout message box appears to ACE users when they power on the ACE instance or when the offline use limit has been reached. You can customize the message text. Add your text after the gray text in the message box. You cannot edit the gray text.

c If you chose **Allow offline use for [x] [time_units]**, you can choose to have a message displayed to the user that warns that the ACE instance will soon become unavailable for offline use. To do this, select **Display warning [x] [time_unit] before policy expiration**. Set **x** to the number of minutes, hours, or days, and set **time_unit** to **minutes**, **hours**, or **days**. You can customize the message text. Add your text after the gray text in the message box. You cannot edit the gray text.

Policy updates take effect while the instance is running, with these exceptions:

- **Authentication policies** – User and group lists, passwords, and scripts can be updated. Changes take effect the next time the instance is powered on.
- **Policy update frequency policies** – If Policy Update Frequency is set to **Only when the ACE instance powers on**, changes take effect the next time the instance is powered on.

Writing Plug-In Policy Scripts

You may write your own scripts to control certain policies in VMware Player. You may use any language that is supported on the user's computer.

For security reasons, scripts must be deployed as part of a package and installed by the package installer. They cannot be deployed separately to users' computers and cannot be modified by the end user.

Your scripts must write the appropriate values to StdOut. Output to StdOut maybe up to 4096 bytes long.

Place any scripts you want to use for a package in the `ACE Resources` directory. They must be in the main `ACE Resources` directory, not in a subdirectory under that folder. If the scripts need any additional resource files, place those files in the main `ACE Resources` folder, too. Your script should reference those resources using relative paths.

Your scripts may also write messages to StdErr. Output to StdErr maybe up to 4096 bytes long. Any messages generated on StdErr are captured in the 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.

Table 6-1 describes the environment variables that are set in the script execution environment.

Table 6-1. Environment Variables

Variable	Description
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 scripts run each time the end user launches VMware Player or resets the virtual machine. Some may run more often. For example, an expiration script is run once each 24 hours.

The sample scripts presented in "Sample Scripts" on page 139 are installed with VMware Player. The default location is `C:\Program Files\VMware\VMware Player\Samples`.

The following descriptions give the format for the output that your scripts must write to StdOut to control various policies.

Authentication Scripts

Table 6-2 outlines the basic information you need to write authentication scripts.

Table 6-2. Writing Authentication Scripts

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.

Table 6-2. Writing Authentication Scripts (Continued)

Question	Explanation
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?	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.

Sample Scripts

The following sections contain sample policy scripts.

Sample Authentication Script

The following sample script is written in C. It is installed by Workstation ACE Edition as `sampleAuth.c`. You may compile it with a C compiler if you want to run it.

```
#
#   VMware Sample Script
#
#   Sample script for ACE script authentication
#
#   Description:
#   This sample script lookups the user as defined in the environment
variable
#   TEST_USERNAME and returns seed data that is used to make a key for
authentication
#   purposes.
#
#   It assumes that the username is defined in the environment variable
TEST_USERNAME
#   (a ficticious environment variable used for this sample) and returns the
seed data
#   from a harcoded map of username to seed data.
#
#   Input to script:
#   None.
#
#   Returns:
#   0 if successful (user is correctly authenticated).
#   -1 if TEST_USERNAME is not set, or the user is unrecognized.
#
#   Expected output:
#   Seed data for creating script authentication key on stdout.
#
```

```
#   Notes:
#   If the script returns success, its output will be used to create a key.
#   Therefore, it is important that the output of this script be unique for
#   each user, and that there is enough data to make a meaningful key (at
#   least 16 bytes).
#
#

my %user_map= ( 'charlie'         => 'E1C4F612135B4D98A33B2C9BD595025D',
                'kathy'           => 'C79AFFEF773D61225751C2566858DB08',
                'beth'            => '05B169B439B26AAB2EA4F755B7E3800C',
                'ernie'           => '8CE63D4AA2068BD8AFF2D1B05F3495A5',
                'bert'            => '"172B1619B2EFBE0E4F381AA1C428F049'
                 );

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
   print "You should set the TEST_USERNAME environment variable.\n";
   exit(-1);
}


my $key_seed = $user_map{$username};
if (! defined $key_seed) {
   print "Unrecognized username.\n";
   exit(-1);
}

print $key_seed;
exit(0);
```

Sample Host-Guest Data Script

The following sample script is written in Perl. It is installed by Workstation ACE Edition as sampleQuarantine.pl. You need a Perl interpreter to run this script.

```
#
#   VMware Sample Script
#
#   Sample script for ACE Host-Guest Data script
#
#   Description:
#   This sample script passes information defined on the host to the guest.
#   It assumes that the machine name is defined in the environment variable
TEST_MACHINENAME
#   and that the asset tag is defined in the environment variable
TEST_ASSETTAG.
#   (These are fictitious variables used for this sample).
#
```

```
#   Input to script:
#   None.
#
#   Returns:
#   0 if successful.
#
#   Expected output:
#   Set of acceptable key/value pairs where the values are fetched from the
environment variables.
#   These values can be retrieved from within the Guest operating system
using the VMware Tools.
#

my $machine_name = $ENV{TEST_MACHINENAME};
my $asset_tag = $ENV{TEST_ASSETTAG};
my $host_mac = $ENV{TEST_MACHINEMAC};

if (defined $machine_name) {
   print "machine.id = " . $machine_name . "\n";
}

if (defined $asset_tag) {
   print "guestinfo.assetTag = " . $asset_tag . "\n";
}

if (defined $host_mac) {
   printf "guestinfo.mac = " . $host_mac . "\n";
}

exit(0);
```

Sample Power-On Hook Script

The following sample script is written in Perl. It is installed by Workstation ACE Edition as sampleQuarantine.pl. You need a Perl interpreter to run this script.

```
#
#   VMware Sample Script
#
#   Sample script for ACE power-on hook
#
#   Description:
#   This sample script implements a power-on hook for ACE. This can be used
in addition
#   to authentication to control the circumstances under which an ACE is
allowed to run.
#
#   This script assumes that the username is defined in the environment
variable TEST_USERNAME
```

```
#   (a ficticious environment variable used for this sample) and returns TRUE
if the user
#   is allowed to run, and FALSE otherwise.
#
#   Input to script:
#   None.
#
#   Returns:
#   TRUE if username is on white list.
#   FALSE if username is not on white list or is undefined.
#
#   Expected output:
#   One of the strings "TRUE" or "FALSE"
#
#

my @white_list = ("alan", "bob", "mary", "sonia", "chris");

my $username = $ENV{TEST_USERNAME};
if (! defined $username) {
   print "FALSE";
   exit(0);
}

my @grepNames = grep(/$username/, @white_list);
if (@grepNames == 1) {
   print "TRUE";
   exit(0);
}

print "FALSE";
exit(0);
```

Customizing the VMware Player Interface

You may customize several aspects of the VMware Player 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.

To specify a skin file

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 Player Icons

VMware Player 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 Player uses whatever size is specified in the system preference for icon size. The small (16x16) icon is used in the VMware Player title bar and on the Windows taskbar button for VMware Player.

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 Player extracts the icon of the appropriate size for each use.

Customizing the Title Bar Text

You may specify what text appears in the VMware Player 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.

Table 6-3 describes the VMware Player title text parameters.

Customizing the Removable Device Display

Table 6-3. VMware Player Title Text Parameters

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 user's computer)
`player.title.font.size`	integer	32	Point size for the text

Removable devices are shown in the VMware Player interface either by buttons on a toolbar or by menu items on a Devices 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 user may make in the VMware Player preferences dialog box.

Table 6-4 describes the parameter you use to control whether devices are shown as toolbar items.

Table 6-4. Toolbar Items Parameter

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 Table 6-5.

Table 6-5. Removable Devices Parameters

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`		
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. Table 6-6 provides the shortcut key values.

Table 6-6. Shortcut Key Values

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`.

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.ethernet0.buttonStyle = "icon"
# player.deviceBar.ide1:0.buttonStyle = "icon"
# player.deviceBar.audio.buttonStyle = "icon"
```

Package Settings 7

Package settings enable you to configure package characteristics, such as instance customization and encryption, and then apply those settings to as many packages as you choose. The ability to set these package characteristics and then apply them to every package you create saves you the time and effort required to set each of these details every time you create a package. Changes to package settings affect only packages created after the changes were made; they do not apply to existing packages.

The following sections describe the package settings you can choose to apply to your ACE masters:

- "Custom EULA" on page 170
- "Instance Customization" on page 170
- "Package Lifetime" on page 181
- "Encryption" on page 181
- "Deployment Platform" on page 183

Specific information about how to join an ACE instance to a remote domain, a procedure that requires you to set particular parameters in the instance customization package settings, is provided under

- "Setting Up a Remote Domain Join" on page 183

Some troubleshooting tips about DNS setup issues appear at the end of the chapter:

- "Troubleshooting Setup Issues" on page 185

Custom EULA

You can provide a custom EULA (end-user license agreement) that appears when an ACE instance is activated. You can use this feature to display a custom license-agreement message that the user must see and accept before the instance can be run for the first time.

To specify a custom EULA

1 Create a text file for the custom EULA and save it in the ACE Resources directory for the ACE master.

NOTE The file format can be either `.txt` or `.rtf` for an ACE instance running on a Windows system. It must be a `.txt` file for an ACE instance running on a Linux system. If you have selected either **Both Windows and Linux** or **Linux** in the Deployment Platform package setting, ensure that your custom EULA file is a `.txt` format file.

---

2 Select **Display specified EULA text file** in the custom EULA package setting.

3 Click **Browse** and navigate to the file.

4 Click **OK** on the package setting page.

Instance Customization

NOTE Instance customization applies only to ACE instances that have a Windows guest operating system installed.

Topics in this section:

For detailed information on closely related topics, see:

- "Setting Up a Remote Domain Join" on page 183
- "Creating a Package" on page 188

Benefits of Instance Customization

The instance customization feature enhances and streamlines the preparation and deployment of ACE instances. The instance customization process is built around the standard Microsoft Sysprep deployment tools.

- It automates the Sysprep process (the use of the Microsoft Sysprep deployment tools), allowing you to use just one tool—one user interface, and so on—to do all the tasks. It gives you better control of some Sysprep parameters, such as computer name.
- It provides you with an automated way to join ACE instances to a domain from a remote site, with your VPN client. For details, see "Setting Up a Remote Domain Join" on page 183.

  NOTE Your VPN client must support a command-line interface.

- For managed ACE instances, the instance customization process on the user's machine reports back the status—success or failure of the process—to the server. The information is available in the Instance View of Workstation ACE Edition. (See Chapter 12, "Instance View," on page 243 for details on the view.) Besides status, the process also reports back the MAC address and the new computer name.

Overview of the Instance Customization Process

This section provides an overview of instance customization.

To customize an instance

On the Workstation ACE Edition machine, during packaging:

1. A snapshot of the ACE master is taken and saved.
2. The master is powered on, and all the required deployment tools and files, including the appropriate Microsoft Sysprep tools, are copied into the guest. There is no visible indication of the copying process. See "Downloading the Microsoft Sysprep Deployment Tools" on page 174 for more information.
3. The Microsoft deployment tools run inside the guest operating system to seal the guest and prepare for deployment.

4 The guest operating system shuts down (this is visible, of course).

NOTE If the guest operating system does not shut down, the problem might be that the Sysprep tools were not in place. If the guest operating system fails to shut down promptly—after approximately 10 minutes, generally—the operation is cancelled and an error message tells you that instance customization failed. See "Downloading the Microsoft Sysprep Deployment Tools" on page 174.

5 After a successful guest operating system shutdown, the following steps are taken to prepare the deployment package:

   a The master is cloned into the package directory: that is, the virtual machine files are copied into the directory, encrypted if needed, and, if specified in the package distribution setup, divided up to be put on media.

   b The master reverts to the snapshot, and then the snapshot is deleted.

   c The installer files are copied into the package directory.

On the ACE user's machine, after the instance has been activated:

6 All the required information for resolving placeholder variables is obtained.

7 Placeholder variables are resolved and are replaced with the actual values for the ACE instance. (See "Placeholder Values to Use in Instance Customization" on page 177 for details.)

8 The Microsoft Mini-Setup process runs unattended. Additional commands to execute other scripts that you have specified in the instance customization package settings are executed at the end of this process.

9 If you have set up instance customization to include joining a remote ACE instance to a domain, the software executes the script specified in the instance customization package settings, which is used to connect to the VPN server. Then the machine is joined to the domain.

10 For managed instances, instance customization is reported to the server if it is successful.

Remote domain join requires that you perform some additional steps beyond those required for instance customization. See "Setting Up a Remote Domain Join" on page 183 for further information.

Before You Specify Instance Customization Settings, Perform These Tasks

NOTE Instance customization is available for both managed and standalone ACE instances. You don't have to use an ACE 2 Management Server to take advantage of the feature.

Before you specify instance customization settings, perform the following:

- Install one of the following Windows guest operating systems on your ACE master:
  - Windows 2000
  - Windows XP Professional
  - Windows Server 2003
  - Windows Vista
- Install the latest version of VMware Tools on the guest operating system. For information about installing and updating VMware Tools, see the *Workstation User's Manual*.
- Download the Microsoft Sysprep tools. See "Downloading the Microsoft Sysprep Deployment Tools" on page 174 for more information.

NOTE *A Best Practice:* When you install Workstation ACE Edition, download the Microsoft Sysprep deployment tools for all the guest operating systems you plan to deploy.

You will need the following information before you specify instance customization settings:

- The Windows product ID for the guest operating system installation
- If the ACE instance will be joined to a domain (whether the instance is local or remote to the domain), the user name and password for an account that has permission to add computers to the domain
- Remote domain join parameters if a remote ACE instance will be joined to a domain: See "Setting Up a Remote Domain Join" on page 183 for more information.

Downloading the Microsoft Sysprep Deployment Tools

NOTE Microsoft Sysprep deployment tools are automatically installed with the Windows Vista operating system installation, so you do not need to download Sysprep tools if your guest operating system is a Windows Vista system.

To ensure that the tools are on your admin machine when you need them

1 Go to http://www.microsoft.com and search for Sysprep deployment tools.

2 Follow the instructions on the site for downloading the Sysprep deployment tools. Download all versions of the Sysprep deployment tools that correspond to the guest operating systems that you will deploy. The Sysprep deployment tools you might need are:

- Sysprep deployment tools for Windows XP Professional SP1 and SP2. The SP1 version works with Windows XP Professional with no service pack and Windows XP Professional SP1. The SP2 version is, of course, for Windows XP Professional SP2.
- Sysprep deployment tools for Windows 2000.
- Sysprep deployment tools for Windows 2003. Two versions of these tools are available for Windows 2003. Both versions will work, so you can download either version.

3 Download the zip files and unzip them into the directory where Workstation ACE Edition is installed.

The default installation directory for Workstation ACE Edition is:

```
C:\Program Files\VMware\VMware Workstation
```

Specifying Package Settings for Instance Customization

Make sure you have installed all required files for customization scripts before you specify package settings.

NOTE Instance customization applies only to ACE instances that have a Windows guest operating system installed.

To specify package settings for instance customization

1 See "Before You Specify Instance Customization Settings, Perform These Tasks" on page 173.

2 Choose **ACE > Package Settings** to open the package settings editor.

3 On the Instance Customization page:

a Select **Enable instance customization**.

b Type the product ID for the guest operating system software you have installed in the ACE master.

The Instance Customization sub-pages are disabled and cannot be accessed if the **Enable instance customization** option is not selected. Similarly, you cannot type in the **Product ID** box if the **Enable** option is not selected.

---

4 On the System Options page:

NOTE You can use placeholder variables for the system name, organization name, and computer name. For details on the placeholder variables, including an example, see "Placeholder Values to Use in Instance Customization" on page 177.

---

a Enter a system name.

b Enter an organization name.

c Enter a computer name.

CAUTION For Windows Vista guest operating systems, the computer name must be 15 characters or less in length. If the name is more than 15 characters, the Mini-Setup process fails on the user machine.

NOTE Do not enter **`administrator`** in the Name field or the Computer Name field of the System Options page.

If you type the text **`administrator`** in those fields, instance customization will fail during the Mini-Setup process.

If you set the `%logon_user%` placeholder in those fields and the placeholder variable resolves to `administrator`, the software automatically changes the value to a random alphanumeric string of 10 characters.

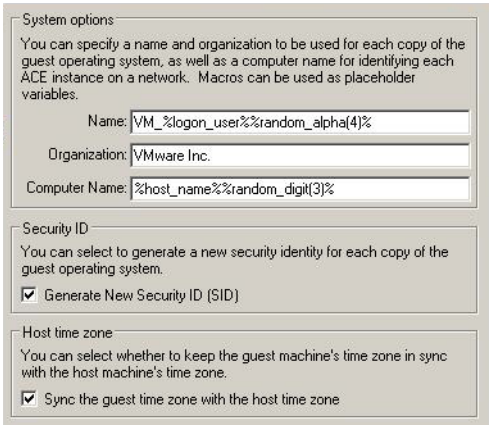
---

d Select **Generate new security ID (SID)** if you want to have a new security ID generated for each copy of the guest operating system.

NOTE A new SID is always generated for Windows Vista guest operating systems, regardless of the setting you choose here in the package settings editor.

---

e Select **Sync the guest time zone with the host time zone** if you want to have that synchronization take place automatically.



5 On the Initialization Scripts page, type the additional commands to run scripts in the guest operating system at the end of the Mini-Setup process on the ACE user's machine. See the Microsoft deployment tools documentation for information about additional commands.

CAUTION Specify the path to the batch file without using quotation marks. The quotation marks will be added automatically.

For more information about specifying command-line parameters to your script, see the Microsoft knowledge base article at http://support.microsoft.com/kb/177462.

6 On the Workgroup or Domain page:

a Enter the name of the workgroup or domain that this instance will use to access the network.

b If you selected **Domain** and have entered the domain name, now enter the user name for an account that can join a new computer to the domain.

NOTE Instance customization only supports DHCP, not static IP addresses.

c If you want to allow this ACE instance to join the domain from a location remote to the domain, select **Enable remote domain join** and then type the command to run the script that establishes a VPN connection. See "Setting Up

a Remote Domain Join" on page 183 for more information about joining remote ACE instances to a domain.

NOTE If the ACE master is managed, then passwords and commands specified on this page are stored on the ACE 2 Management Server. If the ACE master is standalone, then passwords and commands are stored with the package.

If the ACE master is not managed, you should encrypt the package and ACE since the passwords are kept inside the virtual machine.

Now create the package; see "Packaging with Instance Customization Enabled" on page 178.

Placeholder Values to Use in Instance Customization

Placeholder values are values to be used inside the guest operating system during the Mini-Setup procedure on the ACE user's machine to construct individualized field names.

The available placeholders are:

- `%logon_user%` or `%logon_user(n)%` – The logged-on user on the host machine at the time the Microsoft Mini-Setup process begins.

  You can use `%logon_user(n)%`, where <n> is the maximum number of characters obtained from the actual logged-on user name when the name is resolved, if you need to ensure that the user name is resolved to no more than a certain number of characters. For example, if you specify that 3 random characters are to be added to the actual logged-on user name and you want to limit the maximum length of the resolved name to 15, then set <n> to 12. Your entry in the **Name** field in System Options would be `%logon_user(12)%%random_alpha_digit(3)%`.

  Including `(n)` in the placeholder is optional. If you don't use it (that is, you use `%logon_user%`) or if you set <n> to zero (that is, you use `%logon_user(0)%`), the placeholder will resolve to the full logged-on user name.

- `%host_name%` or `%host_name(n)%` – The name of the host computer (usually used with some additional random number or name).

  You can use `%host_name(n)%`, where <n> is the maximum number of characters obtained from the actual computer host name when the name is resolved, if you need to ensure that the host name is resolved to not more than a certain number of characters. For example, if you specify that 3 random characters are to be added to the actual host name and you want to limit the maximum length of the resolved

name to 15, then set <n> to 12. Your entry in the **Computer Name** field in System Options would be `%host_name(12)%%random_alpha_digit(3)%.`

Including `(n)` in the placeholder is optional. If you don't use it (that is, you use `%host_name%`) or if you set <n> to zero (that is, you use `%host_name(0)%`), the placeholder will resolve to the full actual computer host name.

- `%random_alpha_digit(n)%` – A randomly generated string of alphabetic and numeric characters, where <n> is the number of characters. You must specify <n>.
- `%random_alpha(n)%` – A randomly generated string of alphabetic characters, where <n> is the number of characters. You must specify <n>.
- `%random_digit(n)%` – A randomly generated string of numeric characters, where <n> is the number of characters. You must specify <n>.

Make sure that computer names on Windows Vista systems work in mini-setup. The computer name must be 15 characters or less for your ACE instance with a Windows Vista guest operating system in order for the Mini-Setup process to run successfully on the user's machine.

To meet this computer-name requirement, specify placeholder values that give you control of the resolved-value length, such as placeholders for random strings, host name, and logged-on user.

CAUTION If you do not ensure that the host computer name will not exceed the 15-character limit, Mini-Setup will fail on the user machine if the name is too long.

Packaging with Instance Customization Enabled

CAUTION Ensure that you have downloaded the current Sysprep deployment tools from Microsoft Corporation's Web site and copied them to your machine as described in "Downloading the Microsoft Sysprep Deployment Tools" on page 174 *before* packaging with instance customization enabled begins. If the tools are not available at packaging time, the operation fails during the packaging process. Because packaging can take a long time, and the failure might not occur until well into the packaging process, you could lose substantial time if the process failed because the tools weren't available.

To create a new package with instance customization enabled

1. Choose **ACE > New Package** to start the New Package Wizard.
2. Follow the steps defined in the wizard (for details, see "Creating a Package" on page 188).

3 If the ACE master you are creating is a standalone ACE master, the Password page of the wizard will appear. Enter any passwords for domain join and, if needed, for the VPN connection.

4 On the Package Summary page, click **Next** to begin the packaging process.

5 Finish the steps for the New Package Wizard (for details, see "Creating a Package" on page 188).

NOTE See "Overview of the Instance Customization Process" on page 171 for details on what happens during the packaging process.

CAUTION Before you deploy the package, preview the ACE instance to verify that all settings are working correctly.

During the preview, verify that instance customization runs unattended—that is, no dialog boxes appear that require user interaction. For example: If an invalid Windows product ID was entered, then a dialog box requiring a product key entry appears during Mini-Setup in the Preview run.

When you preview the ACE instance, VMware Player runs in interactive mode so that you can see any instance customization errors and make corrections as needed. VMware Player does not run in interactive mode when you have deployed the package to the user's machine.

NOTE If the ACE instance is configured for automatic login and automatic login fails, then instance customization also fails. It fails because the VMware Tools service is required during instance customization for sealing the ACE master and preparing it for deployment, but the Tools service does not start if automatic login fails. To fix this problem, power on the ACE master, fix the automatic login problem, and then preview the ACE master to verify that instance customization runs successfully.

Specifying Additional License Information for Windows Server Products

In order to supply additional license information for Windows Server products, you can add a file named `sysprep_license.txt` to the <ACE_master_name> directory in which you can specify two parameters: `AutoMode`, which can have either of two values, `PerSeat` or `PerServer`, and `AutoUsers`, which indicates the number of client licenses purchased for the server (in the `PerServer` case). See
http://technet2.microsoft.com/WindowsServer/en/library/c4f0b57a-f4f7-478b-9667-ca20af32611d1033.mspx?mfr=true
for more information about these values.

If this file is not found in the <ACE_master_name> directory, a default is used: `AutoMode` is set to `PerServer` with 5 client licenses.

If you choose to supply this file, you won't see any change to the license portion of the Mini-Setup process during preview. Even if you supplied `AutoMode=PerSeat`, you will still see `AutoMode=PerServer` and `AutoUsers=5` in the Mini-Setup user interface. This is the expected behavior. The license information will be set correctly by the Mini-Setup process nonetheless.

Next Steps for Instance Customization

You have completed the steps for instance customization on the Workstation ACE Edition machine. Continue with "How ACE Instance Customization Completes on the ACE User's Machine."

How ACE Instance Customization Completes on the ACE User's Machine

To customize an instance

1. The ACE user installs the ACE package on her machine and activates the instance.
2. All the required information for resolving placeholder variables is obtained.
3. The placeholder variables are resolved and are replaced with the actual values for the ACE instance.
4. The Microsoft Mini-Setup process runs.
5. If the Mini-Setup process fails, the ACE instance shuts down.

   NOTE After this failure, the ACE instance is not runnable.

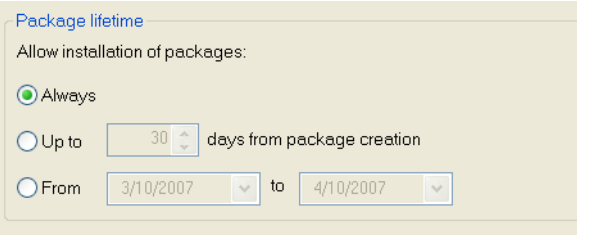
6. At the end of the Mini-Setup process, the additional commands are executed.
7. If the remote domain join procedure is selected, the software executes the script provided in the instance customization package settings, which is used to connect to the VPN server. The machine is then joined to the domain.
8. At the end of this process, if this is a managed instance, the results of instance customization, the instance's MAC address, and new computer names are reported to the server.

After instance customization runs on an ACE instance with a Windows Vista guest operating system, what happens before the ACE instance is ready to be used differs slightly from what occurs with other Windows guest operating systems. The user will

see a message saying that the machine is going to be restarted, next the login screen will appear, and then the system will reboot. No user interaction is required at any point.

Package Lifetime

You can specify a time period during which an ACE package is installable. If a user attempts to install a package outside of this time period, an error message appears and the package will not be installed.



The default setting for package lifetime is **Always**. A package with this setting can be installed at any time after it is deployed.

If you want to allow package installation for a certain number of days after the package's creation date, choose **Up to [x] days from package creation** and select the number of days from the dropdown list.

If you want to set package installation boundary dates, choose **From [date] to [date]**. Use the dropdown list arrows to open the calendar and specify the first date on which the package can be installed and then the last date on which the package can be installed.

The administrator can change the package lifetime settings on managed packages. Settings can be changed before or after package creation. To change the package lifetime setting, right-click the package you want to change under the Package History heading at the bottom of the interface. Select **Properties > Settings** to change the package lifetime settings or select **Deactivate** to deactivate the package immediately.

Encryption

Encryption settings are of two types:

- **Package encryption** – Protects package files from being copied or altered while in transit.
- **ACE instance encryption** – Protects ACE instance files from being copied or altered.

NOTE You can choose to encrypt the package while leaving the ACE instance files unencrypted or to encrypt instance files while leaving the package unencrypted.

The Workstation ACE Edition software applies encryption settings to the package and files by using defaults that are determined by the settings in place for the activation and authentication policies. See "Setting Access Control Policies – Activation and Authentication" on page 109 for more information on those settings.

NOTE Changing activation and authentication settings resets encryption settings to their default settings.

In general, VMware recommends that you not override the default encryption settings. In circumstances when you might want to do so—for instance, if you want to test-deploy a package and don't need to have the files encrypted—you can change the encryption settings on the Encryption page.

To change encryption settings

1 Click **Edit Package Settings** in the ACE master summary view.

2 Click the **Encryption** page link in the left pane of the Package Settings window.

NOTE If you change these settings after you have created a package, the changes affect only new packages, not existing ones.

To protect the contents of the ACE package, you can specify that the New Package Wizard encrypts the virtual machine when the package is created. To do so, select **Encrypted** under **Package protection**. Each installation of the virtual machine is encrypted differently.

You must specify an authentication method if you want the installer to encrypt the ACE instance. See "Setting Access Control Policies – Activation and Authentication" on page 109 for details about authentication policies.

If you encrypt the package or the ACE instance, configuration and policy files are automatically protected against viewing and tampering. Even if you do not encrypt the virtual machine, you can select **Tamper resistant**.

NOTE If you set the encryption settings to **None**, any verification specified in the resource signing policy will not be performed. The encryption package setting overrides the resource signing policy setting. See "Setting Resource Signing Policies" on page 125 for more information about those settings.

Deployment Platform

If you want to change the platform that your ACE package is deployed to, select the Deployment Platform setting. The default setting is **Windows**.

To change the platform to which an ACE package is deployed

1 Select the ACE master whose Deployment Platform setting you want to change.

2 Choose **ACE > Package Settings** to open the package settings editor.

3 Click the **Deployment Platform** setting in the left-hand pane.

4 Select the deployment platform by choosing **Windows**, **Linux**, or **Both Windows and Linux**.

5 Click **OK** to save the setting and close the page.

Setting Up a Remote Domain Join

The remote domain join feature allows you to manage ACE instances that are outside the corporate network as if they were inside that network. The process of joining an ACE instance to an Active Directory domain is automated for both instances that are local to the domain and those that are remote to it.

To join an ACE instance to a domain, you must provide:

- The domain name
- The user name for an account that can join a new computer to the domain
- The account password

In addition to those items, to join an ACE instance from a remote location to the domain, you must provide a way to establish a secure connection with your network.

To establish a secure connection to the network, you must install a VPN client in the guest and set it up to allow remote login to the domain. You must supply a script to establish the secure connection to the VPN server.

NOTE Your VPN client must support a command-line interface.

After you install the VPN client, with the script file, in the guest, you must specify remote domain join settings in the package settings editor in Workstation ACE Edition.

To specify remote domain join settings in the package settings editor

1 In the package settings editor, enable instance customization.

2 On the Workgroup or Domain page, enter the domain name, the user name for an account that can join a new computer to the domain, and the account password.

3 On that same page, select the **Enable remote domain join** option and enter the command that will execute the script.

4 On the Initialization Scripts page, specify a VPN connect script to a list of scripts to be run after Mini-Setup is complete.

NOTE You can take advantage of a password placeholder variable (%password%) by entering it in the **Password** field under **Remote Domain Join**. The placeholder variable is resolved and replaced with the actual value when the script executes.

See Step 6 on page 176 for details about these package settings.

After you have saved the package settings, you create a package. See "Packaging with Instance Customization Enabled" on page 178 for details. Then you deploy the package. After the package has been installed on the ACE user's machine and the ACE instance has been activated and authenticated, the Microsoft Mini-Setup process runs. The script for joining the remote ACE instance to the domain executes at the end of that process, and the machine is joined to the domain.

Troubleshooting Setup Issues

If you or your ACE users have problems with logging back into a domain after invoking the Revert to Installed snapshot or with domain validation and name resolution, see if the following descriptions and resolutions are applicable to those problems:

Problem: The ACE user can't log the ACE instance back into a domain after the Revert to Installed snapshot has been invoked.

Description: An ACE instance has been configured both to log into a domain and to use the Revert to Installed snapshot. The ACE instance has a Windows guest operating system installed and the machine account password for the domain is periodically renewed by default. If the password has been renewed by the time the user reverts the ACE to the snapshot, the snapshot's password will be invalid and the login will fail.

Solution: To avoid this problem, ensure that the following security policy is enabled: **Refuse machine account password changes.**

You can enable this policy on the ACE master (affecting all instances created from it) or on the primary domain controller. For details on how to change the policy, see these Microsoft articles:

- Local Security Policies: http://support.microsoft.com/kb/175468
- PDC Security Policies: http://technet2.microsoft.com/WindowsServer/en/library/bd36a5c9-e757-4658-9554-593bfa30f0761033.mspx?mfr=true

---

Problem: When you try to join an ACE master to a domain, domain validation or name resolution isn't working.

Description: Some ACE masters with certain network configurations might demonstrate these problems.

Solution: Consult the following Microsoft knowledge base article: http://support.microsoft.com/kb/314108.

Problem: An ACE instance running under a Windows Vista guest operating system cannot join the local domain and that instance customization failed with NetDomainJoin function Error 1722: Could not join domain.

Description: ACE instances running in the Windows Vista operating system might have this problem.

Solution: Tell the user to power off the instance and then power it on again to retry instance customization. The problem is intermittent and restarting might solve the problem.

Creating Packages and Deploying Them to Users

8

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

Reviewing the Configuration of the ACE Master and Installing Software

To finish preparing your ACE master and its files before packaging, review its configuration and policies, and ensure that the appropriate operating system and software are installed in it.

Review Policies

Review the policy settings for this ACE master.

To change the policies, click **Edit policies** in the summary view, then change the settings as needed.

Review Package Settings

Review the package settings for this ACE master.

To change the package settings, click **Edit package settings** in the summary view, then change the settings as needed.

Review Virtual Machine Settings

Review the devices and options configured for this ACE master and make any needed changes.

Installing an Operating System, Applications, and VMware Tools in the ACE Master

Before deploying a package to your users, be sure the ACE master has the necessary operating system and software installed.

See the *Workstation User's Manual* for details about installing the guest operating system, applications, and VMware Tools.

Creating a Package

After you have created an ACE Master and configured policies, devices, and package settings, use the New Package Wizard to create a package to deploy instances to users.

NOTE To create a Pocket ACE package for distribution on portable devices, use the Pocket ACE Package Wizard rather than the New Package Wizard. See "Creating an ACE Package for Portable Devices" on page 208.

This section has the following topics:

Overview of Package Creation

A Full package includes an installer and the additional files needed to install an ACE package and the VMware Player application that runs the ACEs. A Full package allows you to create a completely new ACE instance. A Policy Update package includes just the policy-related files. A Server Update package allows you to update the ACE 2

Management Server and server usage for a managed ACE master. A Custom package allows you to choose specific items to deploy.

The components for a Pocket ACE package vary slightly from those for the Full package. For information about the Pocket ACE package, see "Creating an ACE Package for Portable Devices" on page 208.

The package settings and device settings that you already set for this ACE master allow you to create multiple packages quickly, because you can use those same settings over and over again. You don't have to set them for each individual package.

You can 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.

Package Validation

Package validation does the following:

- Checks that all files required by the ACE master are present. Those files include:
  - Disk/snapshot files
  - Script files (if any policy is using scripts)

  NOTE Package validation does not check for device files (ISO images, flp images, and so on). To include device files in the package, put the files in the ACE Resources folder for the ACE master and set the devices to point to that location.
- Checks that the ACE master is cloneable: the master is powered off, multiple snapshots are enabled, and the master is not read-only.
- Checks that the latest version of VMware Tools is installed.
- If instance customization is enabled, checks that the SysprepTools directory for the ACE master's guest operating system is not empty.
- If the guest operating system is Windows 2000, Windows XP, or Windows 2003, checks that the folders in the Program Files\VMware\VMware Workstation\Resources\SysprepTools directory are not empty.

CAUTION Ensure that you have downloaded the current Sysprep deployment tools from Microsoft Corporation's Web site and copied them to your machine as described in "Downloading the Microsoft Sysprep Deployment Tools" on page 174 *before* packaging with instance customization enabled begins. If the tools are not available at packaging time, the operation fails during the packaging process. Because packaging can take a long time, and the failure might not occur until well into the packaging process, you could lose substantial time if the process failed because the tools were not available.

NOTE If you do not have the latest version of VMware Tools installed in the guest operating system, the wizard fails to create the package. If you need to create packages without installing the latest Tools version each time—for example, if you want to do a test deployment of these packages and don't need the latest Tools in the resulting instances in order to run your tests—you can have the wizard ignore the Tools check.

To turn off the VMware Tools check that occurs during packaging

1 Close Workstation ACE Edition.

2 Use Notepad or another text editor to open the `preferences.ini` file, which is located in `<username>\Application Data\VMware`.

3 Add this line to the file:

```
pref.ignoreToolsPkgCheck = "TRUE"
```

4 Save and close `preferences.ini`.

To reinstate the VMware Tools check during packaging

1 Open `preferences.ini` again with your text editor.

2 Delete the added line or change `TRUE` to `FALSE`.

3 Save and close the file.

Steps for Creating a Package

To create a package

1 Start Workstation ACE Edition and open the ACE master you want to use as the basis for the package.

2 To ensure that the package is as compact as possible, defragment virtual disks before you create the package. Run a disk defragmentation utility inside the virtual machine to defragment each virtual disk.

3 Ensure that the guest operating system and VMware Tools are installed in the ACE master.

NOTE Ensure the version of VMware Tools provided with Workstation ACE Edition is installed in the guest operating system. A number of key features in ACE 2 are provided by the VMware Tools package.

---

4 If instance customization is enabled for this package and the guest operating system is Windows XP, Windows 2000, or Windows 2003, ensure that the correct Sysprep deployment tools are available in the correct directory. See the Caution page 190.

5 Ensure that the virtual machine in the package is configured as you want it, then ensure it is shut down and powered off.

You can use the Preview mode to see how an ACE instance created from this ACE master will run on the user's machine in the VMware Player application. When you quit the VMware Player interface, the ACE instance is suspended, not shut down and powered off.

6 Choose **ACE > New Package** to start the New Package Wizard. Click **Next** on the Welcome page.

7 On the Name the Package page:

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

b 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.

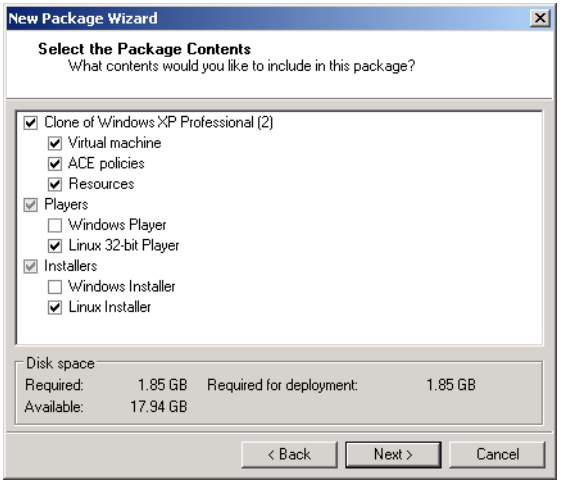
c Use the **Notes** field to enter any background information you want to store for the package. Your users do not see this information.

d Click **Next**.

8 Select a package type on the Package Type page and then click **Next**.

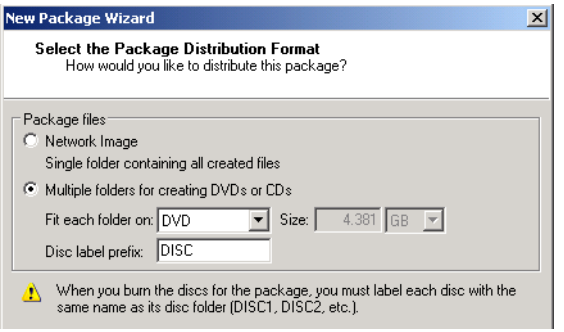
- **Full** – Packages default package contents, including the ACE master configuration file, virtual disk files, and policies; Player applications per the selected platform; package installer; and Resources files for the ACE master.
- **Policy Update / Server Update**— Packages the policies for this ACE master. If this is a managed ACE master, this option reads "Server Update". A server update package allows you to either change the server that the ACE master is associated with or change an "activation-only" server setup to an "activation and tracking" setup.
- **Custom** – Packages the particular package elements that you select.

9 If you chose a Custom package, the Package Contents page appears. Select the items to be included in the package and deselect any default-selected items that you do not want to have in the package.



10 Select a package distribution format and then click **Next**.

NOTE This page does not appear for any packages that are being deployed only to Linux host machines.



- If you plan to distribute the package through network distribution, select **Network image**. Then click **Next**.
- If you plan to distribute the package on CD or DVD, select **Multiple folders for creating 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 can set the maximum file size (must be at least 10MB) for the media you plan to use.

  When the New 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 can 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. The labels must include this prefix.

  If you use multiple discs, ensure 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 New 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 a warning message. You can move or delete files on the target drives to make room for the wizard's working files.

11 If passwords are required for activation for a standalone ACE instance; domain join; or VPN connection, the Package Password page appears. The page might request one, two, or three passwords, depending on the access control policy setting and instance customization package setting for domain and remote domain join that you have configured for this ACE master. The three password types that might be included are described below. Enter the required information and then click **Next**:

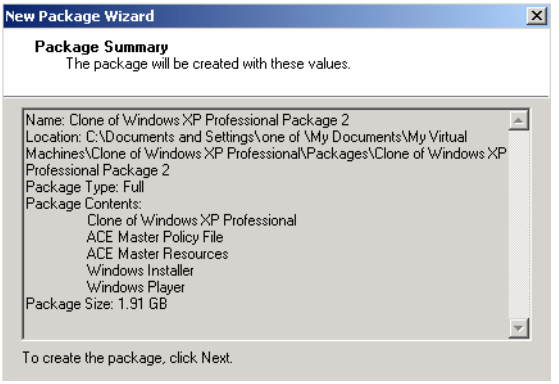
   a Activation password – Access control policy for a standalone ACE instance is set to password. Enter a password and then type it in again to confirm it.

   b Domain join credentials – Access control policy for the ACE instance is set to password, and the Instance Customization package setting for **Domain** is enabled.

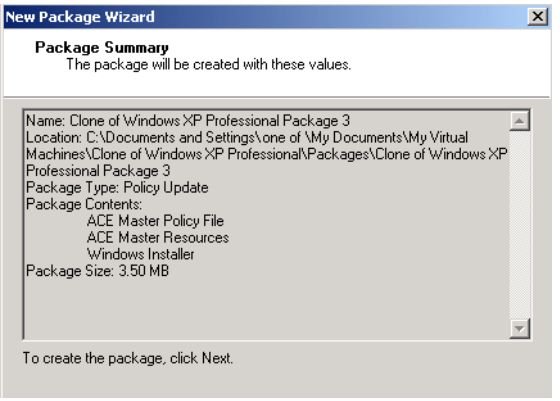
   c Domain join credentials and VPN credentials – The Instance Customization package setting for **Enable remote domain join** is enabled. Enter the password for the user account that has permission to add computers to this domain. Enter the password for the user account that has permission to access this VPN connection.

12 The Package Summary page appears.

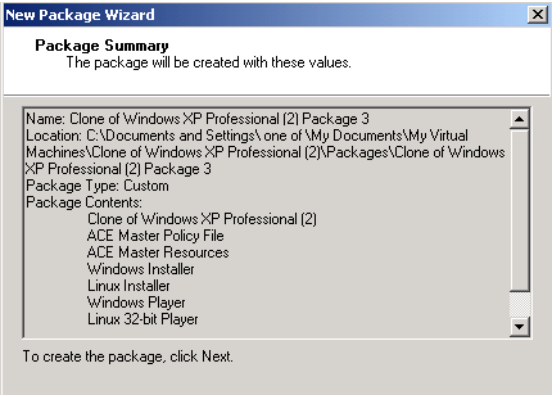
   Full package:



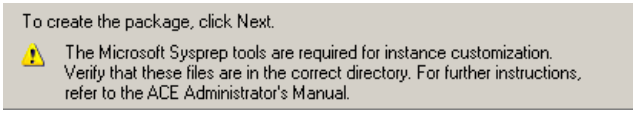
Policy Update/Server Update package:



Custom package:



CAUTION The Caution text shown at the bottom of the Package Summary page only appears if instance customization is enabled for this package. See the information in the Caution on page 190 for details about obtaining the Microsoft Sysprep deployment tools and why it is important to have them in place before package creation begins.



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

13 The Package Creation page appears and displays a progress bar. It can take quite some time to complete this step, especially for packages that include large virtual machines or instance customization settings. (See "Instance Customization" on page 170 for detailed information about instance customization.)

The Package Creation Complete page appears when the process has finished. It lists the location of the newly created package and provides a link to the package directory.

14 If you created a single file for network distribution, you can copy the file to the appropriate location on a network.

15 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 Ensure 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.

Also ensure that you burn the contents of each disc onto the top level of the disc. The package installer expects to find the contents of each folder on a disc with the same name as the folder name. It expects to find only the contents of the folder—at the root level on the disc—not the folder itself. If you burn the folder onto the disc, then when someone tries to install the contents of the second or subsequent discs on the user's machine, error 1309, "`Error reading from file <filename>`", appears.

---

16 You are finished creating the package. Continue with "Deploying Packages" on page 197.

Viewing Package Properties

You can view the properties of the packages that you have created by double-clicking on an item in the Package History from the ACE master summary view. The Package Properties dialog box also enables you to edit the notes that are displayed in the Package History. These notes will not be seen by the users of your packages and are only visible from your Workstation ACE Edition window.

The Package Properties dialog box has three tabbed pages:

- **Summary** page – Displays the package name, creation date, deployment media, package type, size, location, and components. You cannot edit information on this page.
- **Settings** page – Displays values for package settings that have been applied to this package. You cannot edit information on this page.
- **Notes** page – Displays and allows you to edit notes for this package. These notes could have been entered into the Name the Package page when the package was created using the New Package Wizard, or they could be notes that have been edited from this page.

Deploying Packages

To deploy a package:

- If this is a Full, Policy Update/Server Update, or Custom package, you can give the package to your user. You can distribute the packages on CD or DVD, or you can make them available on a network. See Chapter 11, "Installing and Using VMware Player and ACE Instances," on page 215 for information on installing packages.
- If this is a Pocket ACE package, see "Deploying the ACE Package on a Portable Device" on page 211.

9 Preview, Save, Test, Publish

Before you deploy a new or updated ACE package or updated policy, you might want to test it. This section describes test options that allow you to see the ACE instance working exactly as the ACE user will see it.

NOTE You can run any ACE master directly in Workstation ACE Edition to be sure the guest operating system and applications perform as expected. However, an ACE master running in Workstation ACE Edition does not respect any policies that restrict its functionality.

The following subsections describe:

Understanding Test Terminology

- **Live copy of policies** – The currently deployed policy set. The active ACE instances on the ACE users' machines are using these policies.
- **Working copy of policies** – The policy set that you are using to make changes. For managed masters, these are "unpublished" policies. For standalone masters, these are policies that you have not yet packaged or distributed for deployment.

- **Preview** – A mode that allows you to run the ACE instance as it will run on the user's machine as well as see the effects of changed policies as they will appear on the ACE user's machine without your having to package and install them. (The Preview mode displays the working copy of the policies.) See a full description of the Preview mode on page 200.
- **Publish Policies to Server** – (Applies only to managed ACE masters) A command that commits the changes you made in the working copy to the live copy.

Choosing a Test Option

Recommended test options: You can use Preview mode as a test option without having to install a package. Because Preview mode is available as part of the Workstation ACE Edition interface, and Workstation ACE Edition runs only on Windows hosts, you cannot use Preview mode to run ACE instances as they will run on Linux hosts. You also cannot test a host policy in Preview on your administrator machine. For ACE instances that will be deployed on Linux hosts or for which you want to test a host policy, use one of the other test options, either pre- or post-deployment end-to-end testing, as applicable, rather than using Preview mode.

The test option you choose depends on what you are deploying:

- If you are deploying minor policy changes, see "Quick and Easy Test with Preview Mode" on page 200.
- If you are deploying a new ACE package, see "Pre-Deployment End-to-End Test" on page 202.
- If you are deploying an updated ACE package, see "Post-Deployment End-to-End Test" on page 203.

Quick and Easy Test with Preview Mode

This subsection provides:

- "Understanding Preview Mode" on page 200
- "Run a Quick and Easy Test in Preview Mode" on page 201

Understanding Preview Mode

Preview mode allows you to run the ACE instance as it will run on the user's machine as well as see the effects of changed policies as they will appear on the ACE user's machine without your having to package and install them. It also allows you to see many of the effects of your setup choices for an ACE package without having to expend the time and effort required for a full package deployment and installation.

You click the **Preview in Player** icon in the toolbar to create a preview instance. A package based on a linked clone is created in a new directory, Preview Deployment, inside the ACE master's directory on your administrator machine. The snapshot for the linked clone is taken of the ACE master's current state. Unlike a package that is deployed to an ACE user's machine, this package is not installed.

VMware Player starts up, and the preview instance events are the same as those for a standard ACE package deployment: activation of the ACE instance; instance customization (if any); encryption. You can then run the instance, checking for the effects of any changes you made to the ACE master.

You can only have one preview instance per ACE master. When you click **Preview in Player** for the ACE master a second or subsequent time, a message asks if you want to (1) replace the current preview instance with a new deployment or (2) use the existing deployment.

The preview mode saves you time because you don't have to create a full package and install it. Furthermore, the saved mode in Preview, which allows you to use an existing deployment, can save you additional time by allowing you to skip activation and instance customization steps that were done during the first preview instance for this ACE master.

You can switch from running the ACE instance in preview mode back to the Workstation ACE Edition interface without having to shut down the preview if you wish. You can't start up another preview run, however, because only one preview instance is allowed per master. You can start up a preview of a different ACE master.

Run a Quick and Easy Test in Preview Mode

This test allows you to view and test changes without having to take the time to create a full package and install that package.

To run a quick and easy test with Preview mode

1 Open the ACE master you want to test and invoke the policy editor.

2 Select the page for the policy you want to change and make the change.

3 Click **OK** on the policy page to save the change.

4 Click the **Preview in Player** icon in the toolbar to invoke VMware Player. Player allows you to activate and authenticate the ACE instance (if those policies are set) and starts up the guest operating system.

5 Test the change in the running ACE instance to ensure that it is the one you want to make.

6 *For managed ACE masters only:* After you are satisfied that the change is correct, click **Publish Policies to Server**. A pop-up dialog box tells you that the policy has been published.

Pre-Deployment End-to-End Test

You can run an end-to-end test on a new ACE package before you deploy it to ACE users. Preview mode cannot be used to test host policies or ACE packages that will be deployed on a Linux host. Instead, you must perform end-to-end testing.

- **For managed ACE masters** – Designate a separate ACE server as a test server. On the ACE master you are testing, change the target ACE server to the test server. Publish and package your changes. Deploy the new package to a test client machine and the instance will use the test server. When you have finished testing and the ACE instance works as you want it to, switch the target ACE server back to the original server. Then delete the activated ACE instance from the test server. See "To run an end-to-end pre-deployment test using an ACE 2 Management Server test server" on page 202 for more information.
- **For standalone ACE masters** – Package the ACE master, deploy it on another computer, and test it there. See "To run an end-to-end pre-deployment test on another computer" on page 203 for details.

NOTE This test might take a long time because packaging and encryption processes can be lengthy.

To run an end-to-end pre-deployment test using an ACE 2 Management Server test server

1 Select the ACE master in its server location and then choose **ACE > ACE Server** to open the ACE Server dialog box.

2 Enter the name and port number of the server you will use as a test server, or select the server from a history list, and then click **OK**.

3 Click **Create New Package** to start the New Package Wizard, and then follow the wizard steps to create the package. (See details at "Creating a Package" on page 188).

4 Navigate to the package location, copy the package to a client test machine, then run setup.exe. Follow the wizard steps to install the package.

5 Start up VMware Player and then use it to activate and run the ACE instance. Verify that the ACE instance is configured as you had intended and runs as you had planned.

6 In the Workstation ACE Edition interface, select the ACE master in the server location where you tested it and then choose **ACE > ACE Server** to open the ACE Server dialog box.

7 Choose the original server for the ACE master from the server history list, and click **OK**.

NOTE After you have reassigned the ACE master back to the original server, you must create a new package. The package you created in the test will refer to the server you used for testing. Instances created from that package would refer to that server.

To run an end-to-end pre-deployment test on another computer

1 Open the ACE master you want to test, click **Create New Package** to start the New Package Wizard, and then follow the wizard steps to create the package. (See details in "Creating a Package" on page 188).

2 Install the package on your test system, and start up `setup.exe` to open the Installation Wizard. Follow the wizard steps to install the package.

3 Start up VMware Player and then use it to activate and run the ACE instance. Verify that the ACE instance is configured as you had intended and runs as you had planned.

4 Shut down the guest operating system in the ACE instance and then exit from Player.

Post-Deployment End-to-End Test

You can run an end-to-end test on an updated package to replace a deployed ACE package without affecting active ACE instances. Preview mode cannot be used to test host policies or ACE packages that will be deployed on a Linux host. Instead, you must perform end-to-end testing.

- **For managed ACE masters** – Create a clone of the ACE master, move the clone to a server that you have designated as a test server, make the desired changes in the clone, and then package, install, and test it. After you have verified that the changes are correct, duplicate the changes that you made on the clone to your original ACE master. Finally, delete the clone. See "To run an end-to-end post-deployment test using an ACE 2 Management Server test server" on page 204 for details.

- **For standalone ACE masters** – Package the ACE master, install it on another computer, and test it there. See "To run an end-to-end post-deployment test on another computer" on page 205 for details.

NOTE This test might take a long time because packaging and encryption processes can be lengthy.

To run an end-to-end post-deployment test using an ACE 2 Management Server test server

1. Select the ACE master and choose **ACE > Clone** to open the Clone to ACE Master Wizard.
2. On the Clone Source page, select **From current state**, and click **Next**.
3. On the Clone Type page, select **Create a linked clone**, and click **Next**.
4. On the Name of the New ACE Master page, accept the default name and location by clicking **Next**.
5. On the ACE Management Server page, enter the name and port number of the test server, or select the server from the history list, and click **Next**.
6. On the Cloning ACE Master page, click **Done** after checkmarks appear next to all steps on the page.
7. Edit policies and other settings to make the needed changes and then save them.
8. Click **Create New Package** to start the New Package Wizard, and then follow the wizard steps to create the package. (See details at "Creating a Package" on page 188).
9. Navigate to the package's location on your system and start up `setup.exe` to open the Installation Wizard. Follow the wizard steps to install the package.
10. Start up VMware Player and then use it to activate and run the ACE instance. Verify that the ACE instance is configured as you had intended and runs as you had planned.
11. In the Workstation ACE Edition interface, select the ACE master in the server location where you tested it and then choose **ACE > ACE Server** to open the ACE Server dialog box.
12. Choose the original server for the ACE master from the server history list, and click **OK**.

To run an end-to-end post-deployment test on another computer

1 Open the ACE master that you made changes to and want to test, click **Create New Package** to start the New Package Wizard, and then follow the wizard steps to create the package. (See details in "Creating a Package" on page 188).

2 Install the package on your test system and start up `setup.exe` to open the Installation Wizard. Follow the wizard steps to install the package.

3 Start up VMware Player and then use it to activate and run the ACE instance. Verify that the ACE instance is configured as you had intended and runs as you had planned.

4 Shut down the guest operating system in the ACE instance and then exit from Player.

Pocket ACE 10

The Pocket ACE feature allows you to store ACE instances on portable devices such as USB keys (flash memory drives), Apple iPod mobile digital devices, and portable hard drives. Your ACE users attach these portable devices to x86 host computers, run their ACE instances with VMware Player, and then detach the portable devices. The next time they need access to their ACE instances, they can attach the devices to the same host computers or to different ones.

You can thus package a daily computing environment and allow your users to take that environment—including their documents, settings, applications, and even VPN access—wherever they need to go.

This chapter describes how to create, deploy, and run Pocket ACE instances.

Portable Devices Requirements

You can install ACE packages on the following types of devices:

- Flash memory drives (USB keys)
- Flash-based Apple iPod mobile digital device

- Hard drive-based Apple iPod mobile digital device
- Portable hard drives

NOTE Use USB2 high-speed devices only.

Space Requirements for Your Pocket ACE

When you create a new ACE master that you will use it to create a Pocket ACE package, make sure that the removable device you intend to use to store your Pocket ACE has enough space to store the virtual disk's total capacity, memory, and approximately 300MB for overhead. When a Pocket ACE package is deployed to a removable device, the virtual disk is preallocated to the full capacity for enhanced performance.

Creating an ACE Package for Portable Devices

You can package any ACE master for a portable device, if the device has enough space to hold the files. Select **ACE > New Pocket ACE Package** or click **Create New Pocket ACE package** in the ACE master summary view to open the Pocket ACE Package Wizard.

This section contains the following topics:

Policies and Package Settings That Do Not Apply to Pocket ACEs

Host and snapshot policies will be ignored by Pocket ACE instances. If you attempt to create any of these policies for an ACE master and then attempt to create a Pocket ACE package with that ACE master, the package will be created but the policy will not be included in the package.

In addition, administrators are not able to revert to reimage snapshots when running a Pocket ACE in administrator mode in VMware Player.

To create an update package for a deployed Pocket ACE, use the New Package Wizard and select the Update package type in that wizard.

If you enable a restricted host policy or any options in the snapshot policy, those settings are ignored when the update package is created.

Steps for Creating a Pocket ACE Package

To create a Pocket ACE package

1 Start Workstation ACE Edition and open the ACE master you want to use as the basis for the package.

2 Ensure that the guest operating system and VMware Tools are installed in the ACE master.

NOTE Ensure the version of VMware Tools provided with Workstation ACE Edition is installed in the guest operating system. A number of key features in ACE 2 are provided by the VMware Tools package.

---

3 Ensure that the virtual machine in the package is configured as you want it, then ensure it is shut down and powered off.

If an ACE instance is suspended on one host computer, it cannot be resumed reliably on a host computer with different hardware. As a result, you must ensure that the ACE instance is powered off, not just suspended, when you create a package.

4 Choose **ACE > New Pocket ACE Package** to start the Pocket ACE Package Wizard. Click **Next** on the Welcome page.

NOTE If you are creating an update package for a Pocket ACE, you use the New Package Wizard and select the Update package type. Remember not to include a restricted host policy or a snapshot policy in this update for your Pocket ACE.

See "Steps for Creating a Pocket ACE Package" on page 209 for information about creating an update package with the New Package Wizard.

---

5 On the Name the Package page:

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

b 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.

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

d Click **Next**.

CAUTION When you select the Location on the Name the Package page, note that you are choosing a location, usually on the administrator machine, in which to store the package. Do NOT select the portable device to which the package will be deployed. If you do that, the package will not work. You will deploy the package to the device at a later time; see the instructions under "Deploying the ACE Package on a Portable Device" on page 211 for details.

6 On the Select Player page, select the Player installers you want to include in the package.

All the contents needed for a Pocket ACE are packaged, including the installers for Player. The Player installers that are packaged will be for the operating systems selected in the Deployment Platforms page of the package settings editor.

The Disk Space area on the page includes a value for **Required on portable device**.

Click **Next**.

7 The Pocket ACE Deployment Password page appears. If you supply a password here, anyone who attempts to deploy the package to a portable device will have to enter the password during deployment.

- For most Pocket ACE packages, you must specify a deployment password. Type in a password and confirm it.
- Specifying a Pocket ACE deployment password is optional if the ACE master has either of these qualities:
  - Package protection (in the Encryption package setting) is set to **None**.
  - This is a standalone ACE master and the access control policy's authentication type is set to **None**.

  To set the password in those situations, select **Protect Pocket ACE package with password**, and then type in a password and confirm it. Then click **Next**.

8 The Package Summary page appears.

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

9 The Package Creation page appears and displays a progress bar. It can take quite some time to complete this step, especially for packages that include large virtual machines.

The Completing the Pocket ACE Package Wizard page appears when the process has finished. If you want to deploy the package immediately, select **Deploy to a portable device now**.

Whenever you're ready to deploy the package, you can navigate to the package location (the one you specified in the Name the Package page) on your machine and then follow the instructions in "Deploying the ACE Package on a Portable Device."

Deploying the ACE Package on a Portable Device

You can deploy multiple ACE packages on a single portable device. The only limitation on the number of packages is the amount of available space on the device. You run `deploy.exe` to deploy individual ACE instances or `bulkDeploy.exe` to deploy ACE instances to multiple devices.

The wizard automatically pre-allocates disk space and splits the disk into 2GB segments.

The following procedures describe how to deploy packages.

To deploy a package on a portable device

1 Click `deploy.exe`.

2 If the Enter Password dialog box appears, enter the deployment password.

3 On the VMware Pocket ACE Deploy Utility page:

   a Select the removable drive or browse to the folder where you want to deploy the ACE package. Click **Refresh** if you need to refresh the drive list.

   b Click **Deploy**. A progress screen appears.

   c When the deployment is finished, click **Deploy** to deploy more instances or click **Close** if you are done deploying instances.

The Pocket ACE instance is re-encrypted during the deployment instead of after the user's first run of the instance. For this re-encryption, the policy applied is the package protection policy that was in place at the time of packaging.

NOTE When you distribute the Pocket ACE, give it directly to the user and tell the user to keep the Pocket ACE secure until the user runs the ACE and changes the user password.

To bulk deploy packages

1 Change directories to your bulk deployment directory. For example,

```
cd C:\Documents and Settings\Administrator\My Documents\
               My Virtual Machines\My ACE Master\Packages\
               Pocket ACE Package\
```

2 In the command line interface, enter the bulk deploy command and specify the necessary parameters (see Table 10-1):

```
bulkDeploy.exe <drive> <parameters>
```

Table 10-1. Bulk Deploy Command Parameters

Parameter	Usage
-p	Deployment password. Required when the package is password protected.
-s	If you are performing your bulk deployment from outside of the Pocket ACE package, specify the path to the VMX file on the host system.
-q	By default the bulk deployment feature will report progress after you enter the command. Include this parameter if you do not want the command to report progress.
-t	Include this parameter to run a Pocket ACE performance test. If the test fails, the bulk deployment will fail.

For example,

```
bulkDeploy.exe C: –p password –s C:\pocketACEPackage\VM\packagedVMX.vmx
               –q –t
```

If the performance test is run, a result of 0 is returned if the test is successful and negative values result if the test fails.

Running the Pocket ACE Instance

The following steps describe what happens when the user runs the ACE instance from the portable device.

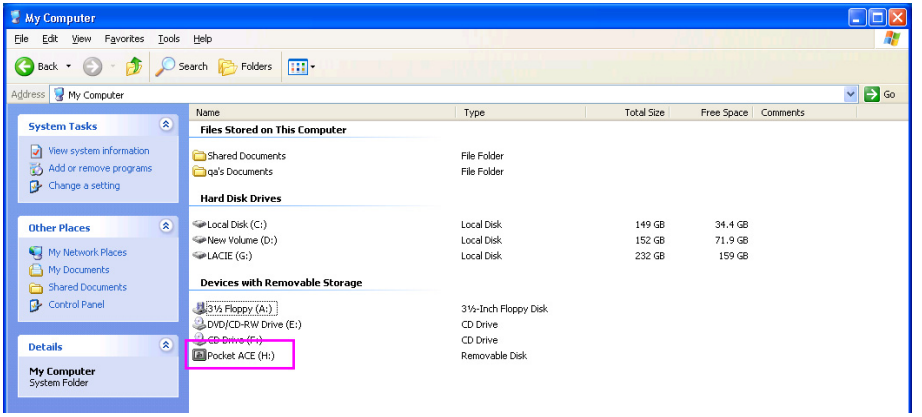
NOTE Tell your users that the host computers that they move Pocket ACEs among must have their clocks set to the correct time. If they move a Pocket ACE from one host computer to another and the clock of the second host is behind that of the first, the Pocket ACE will not run.

---

1 The user plugs the portable device into the host computer.

2 Depending on the host system autorun configuration, users might have to manually start their Pocket ACE.

- For Windows host systems, autorun is included in the package. autorun checks to see if VMware Player is installed. If not, Player is installed automatically. If the instance does not start automatically, choose **Start > My Computer**, and browse to the removable device and run the Pocket ACE.



- For Linux systems, you must install VMware Player from the Player directory on the USB drive; for example, if the USB drive is mounted at /media/USBFLASH, navigate to

  `/media/USBFLASH/player/VMware-player.i386.tar.gz`

  Install the Player as described in "Installing VMware Player on a Linux Host Computer" on page 219. Then navigate in Player to the .vmx file and start up the ACE instance (see "Running the ACE Instance on a Linux Host Computer" on page 221).

3 Both disk and checkpoint caches are initialized. If the Pocket ACE has a session on this host, that session continues. Otherwise a new session is started. (The checkpoint state and virtual disk are cached on the host during use and synced back to the portable device later. The checkpoint state and virtual disk are protected with the same encryption level used for the ACE instance on the portable device.)

4 The Pocket ACE runs primarily from the host cache, although it occasionally reads from the parent disk on the portable device. The ACE does not write to the parent disk.

5 When the user finishes using the instance and executes a close command in Player, a dialog box appears that offers a choice of leaving the session open on the host computer or closing the session and syncing it back to the portable device. Here are the scenarios that can result from the choice the user makes:

   a If the user closes the session and syncs it back to the portable device, the user can then take the device to another host computer and start up the Pocket ACE there.

   b If the user closes the session but doesn't sync it back to the portable device, the session remains on the host computer. The user can unplug the device and take it elsewhere, but VMware does not recommend that the user actually run the Pocket ACE on another computer.

   c The user can discard the session, much like a snapshot reversion, and all changes made to the virtual machine since the last synchronization are discarded.

   NOTE Tell your ACE users that they should safely unplug or eject the portable device before they disconnect it.

6 If the user does not close the Pocket ACE and unplugs the device, the ACE remains in a Suspend state; the result is the same as in Step 5b.

NOTE If the user leaves the Pocket ACE in a Suspend state and then moves the Pocket ACE to a different host computer, it is recommended that the two host computers have the same CPU type. If the host CPUs are different, the user should shut down the Pocket ACE on the first machine before moving it to the second machine.

Installing and Using VMware Player and ACE Instances

11

This chapter describes how to install and run VMware Player and ACE instances on ACE user machines. Topics in this section are:

Installing the ACE Package on a Windows Host Computer and Running the ACE Instance

The administrator creates an ACE package, which includes the ACE instance and VMware Player.

NOTE If this is the first installation of an ACE instance on the user machine, then an administrator (a user with administrator privileges) must install VMware Player before the ACE user can install and run ACE instances.

Installing VMware Player on a Windows Host Computer

Only a user with administrator privileges can install and uninstall VMware Player.

To install VMware Player on a Windows host computer, log on with administrator privileges and then follow the instructions for installing an ACE instance. The installation program installs VMware Player before it installs the virtual machine files if VMware Player is not already on the machine.

NOTE Although you must be logged in as an administrator to install VMware Player, a user with normal user privileges can run the program after it is installed.

Installing an ACE Instance on a Windows Host Computer

Any user can install an ACE instance, unless the ACE instance includes a host policy. That virtual machine must be installed by a user with administrator privileges.

An ACE package contains an ACE instance that will become an ACE instance after it has been installed and activated.You can install a package from a location on the network or from one or more CDs or DVDs. In either case, take the following steps:

To install VMware Player and an ACE instance on a Windows host computer

1 If VMware Player is not yet installed on the user's machine, log on to your Microsoft Windows host as the Administrator user or as a user who is a member of the Windows Administrators group.

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 it to start the installer.

4 Follow the instructions in the installation wizard.

The installer asks where you want to place the virtual machine files. The default location on Windows XP systems is `C:\Documents and Settings\All Users\Application Data\VMware\VMware ACE\<ACE Name>`. The default location on Windows Vista systems is `C:\ProgramData\VMware\VMware ACE\<ACE Name>`. If you want to place the files in a different location, you can click **Browse** and navigate to the new location or enter the path 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 Click **Finish** to complete the installation. The wizard closes.

Installing an ACE Package Silently on a Windows Host Computer

If you are installing a VMware ACE package on a number of Windows host computers, you might 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 ACE package, issue the following command:

```
instmsiw.exe /Q
```

This section outlines what you need to do to install an 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:

```
setup.exe /s/v"/qn"
```

This command installs the package and application (if included) into the default locations and creates a shortcut for the ACE instance on the desktop. The default location for the VMware Player application is `<ProgramFiles>\VMware\VMware Player`. The default location for the virtual machine files on a Windows XP system is `C:\Documents and Settings\All Users\Application Data\VMware\VMware ACE\<ACE Name>`.

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

- Installation directory for the ACE instance
- Installation directory for the VMware Player 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"
PLAYER_INSTALLDIR="C:\VMware\VMware Player" /qn
```

Enter the command on one line.

Option	Description
DESKTOP_SHORTCUTS	When set to 0, skips installation of the ACE instance shortcut on the desktop. The default is 1.
INSTALLDIR	Sets the root installation directory for the ACE instance.
PLAYER_INSTALLDIR	Sets the root installation directory for the VMware Player application.

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

Uninstalling VMware Player from a Windows Host Computer

To uninstall VMware Player

1 Navigate to **Start > Control Panel > Add or Remove Programs > Change or Remove Programs**.

2 Select the program and click **Remove**.

Uninstalling an ACE Instance from a Windows Host Computer

To uninstall an ACE instance from a Windows host computer

1 Find the `setup.exe` file for the package for this instance, and double-click it to start the installer or remove the package by choosing **Settings > Control Panel > Add or Remove Programs**.

2 Follow the instructions in the installation wizard to remove the ACE instance.

3 Click **Finish** to complete the installation. The wizard closes.

The uninstaller reclaims everything, including the ACE instance's data files, shortcuts, and registry entries. Then the uninstaller quits.

NOTE The uninstaller does not uninstall the VMware Player application.

Running the ACE Instance on a Windows Host Computer

To run the ACE instance either double click the icon on the desktop or single click on the icon in the start menu.

Installing the ACE Package on a Linux Host Computer and Running the ACE Instance

The administrator creates an ACE package, which includes the ACE instance and VMware Player. The ACE package must be accessible to the Linux user machines for installation.

NOTE If this is the first installation of an ACE instance on the user machine, then an administrator must install VMware Player before the ACE user can install and run ACE instances.

Installing VMware Player on a Linux Host Computer

Only a user with administrator or root privileges can install and uninstall VMware Player.

Player will be automatically installed when you run vmware-install.pl as root or sudo. Manually install Player on systems where the end user will not have root access. The manual installation procedure is described below.

To install VMware Player on a Linux host computer

1 In a terminal window, become the root user so you can perform the initial installation steps:

```
su –
```

2 Mount the ACE package, and locate the player installer in the package directory:

```
VMware-player-i386.tar.gz
```

Or

```
VMware-player-x86_64.tar.gz
```

3 Copy the tar archive to a temporary directory on your hard drive, in this example, `/tmp`:

```
cp VMware-player-i386.tar.gz /tmp
```

Or

```
cp VMware-player-x86_64.tar.gz /tmp
```

4 Change to the directory to which you copied the file:

```
cd /tmp
```

5 Unpack the archive:

```
tar zxf VMware-player-i386.tar.gz
```

Or

```
tar zxf VMware-player-x86_64.tar.gz
```

6 Change to the installation directory:

```
cd vmware-player-distrib
```

7 Run the installation program:

```
./vmware-install.pl
```

Accept the default directories for the binary files, library files, manual files, documentation files, and the initiation script.

8 Select **Yes** when prompted to run `vmware-config.pl` and accept the default values for the remaining prompts.

NOTE If you do not enable host-only networking when you install VMware Player, you cannot allow a virtual machine to use both bridged and host-only networking.

9 When installation is completed, exit from the `root` account:

```
exit
```

Installing the ACE Instance on a Linux Host Computer

Any user can install an ACE instance, unless the ACE instance includes a host policy. That virtual machine must be installed by the root user.

NOTE Only the user who installs the ACE instance or a user with necessary permissions (such as `root`) is allowed to run that ACE instance.

To install the ACE instance on a Linux host computer

1 Run `vmware-install.pl` from within the package.

2 When prompted, select the directory in which you want to install the ACE instance.

The ACE instance is installed in the selected directory.

Installing an ACE Package Silently on a Linux Host Computer

The following installs an ACE package and the VMware Player as an automated (default) install:

```
/tmp/path/to/package/ACE_Pkg/vmware-install.pl --default
```

Uninstalling an ACE Instance from a Linux Host Computer

ACE users can only uninstall their own ACE instances. Only the root user can uninstall others' ACE instances.

To uninstall an ACE instance from a Linux host computer

- In the command-line interface, type either

  ```
  run <path to instance directory>/vmware-uninstall-ace.pl
  ```

- or change directories to the instance directory and then type

  ```
  run ./vmware-uninstall-ace.pl
  ```

The uninstaller reclaims everything, including data files, the global registration, and so on. Then the uninstaller quits.

Uninstalling VMware Player from a Linux Host Computer

To uninstall VMware Player, run:

```
/usr/bin/vmware-uninstall.pl
```

Running the ACE Instance on a Linux Host Computer

To run the ACE, enter the following on the command line:

```
vmplayer <path_to_installed_package_directory>/<name_of_ACE_vmx_file>.vmx
```

Or run the ACE instance from the VMware ACE menu.

Controlling Which Virtual Machines and ACE Instances Run on a Host

You can control which virtual machines and ACE instances can be run on a host by editing your aceMaster.dat file.

To control which virtual machines and ACEs can be run on a host on which you have deployed an ACE instance, edit the following entries in the aceMaster.dat file:

NOTE The aceMaster.dat file is located in the same directory as the configuration file (.vmxa) for your ACE master.

`allowVMs = "0" or "1"`.

This entry corresponds to a host policy that controls whether non-ACE virtual machines can be run on the host. An entry of "1" (the default) indicates that all non-ACE virtual machines can be run on the host. An entry of "0" indicates that only ACE instances can be run on the host.

`creatorID = "<id string>"`. The default is "".

`requiredCreatorID = "<id string>"`. The default is "".

The creatorID and requiredCreatorID entries enable you to tag ACE instances you create with a specific identifier, and to set an identifier to run on a given host.

For example,

```
requiredCreatorID = "created by x"
```

```
creatorID = "created by x"
```

These changes to the aceMaster.dat file would tag all ACE instances created from this ACE master as "created by x" and specify that only ACE instances tagged with "created by x" can be run. You can only set requiredCreatorID once per host. Set the requiredCreatorID and creatorID to the same value on an ACE master and install that ACE master first on each of your client hosts. Then for each additional ACE master you create which is intended to be installed on the same hosts, set creatorID to the same value. The ACE masters you create with your creatorID value can be installed on the same hosts but ACE instances from ACE masters created by anyone else cannot run on those hosts.

Note that the ID string is in plain text in the aceMaster.dat file on the administrator's machine, but will be hidden in the policy file. If you publish the policy set of an ACE instance to `requiredCreator=yourPolicySetting` and install it on a host, nobody but you (or others with access to the administrator files) will know what the creator ID is. Without knowing the requiredCreator policy setting, you will not be able to create your own ACE instance that can run on the host.

Editing the aceMaster.dat File

The aceMaster.dat file should only be edited when the ACE master tab is not open in the Workstation ACE Edition interface. The aceMaster.dat file can be edited using any

text editor. After you have finished editing the aceMaster.dat file, reopen the ACE master in the Workstation ACE Edition interface. If the ACE master is managed and the policy values have changed, then the "needs publish" warning should appear. The policies will need to be published before the changes can take effect. Apply changes to standalone instances by using an update package.

Host Policies

Both the `requiredCreatorID` and `allowVMs` entries control host policies (the `creatorID` policy is not a host policy). A host policy applies to the entire host the policy is deployed to and not just the particular ACE instance. Another example of a host policy is the host network access policy.

Make sure to consider the following when you make changes to host policies:

Only one set of host policies can be deployed to a particular host. If a package contains host policies and the host already contains host policies from another ACE master, then the second package will fail to be installed.

A package containing host policies requires administrator rights for installation.

Host policies for managed ACE masters are stored on the ACE Management Server and can be edited at any time. However, changes to host policies will not take effect on a host unless that host has had a package installed from that ACE master that contains the changed host policies.

Running VMware Player

This section provides an overview of the most used features of VMware Player. You might not see all these features in the VMware Player installed on your computer. Certain features are available only if the administrator who created the package included them.

See also the VMware Player online help for general information on using the Player.

Starting VMware Player

To start VMware Player, double-click the ACE icon on the desktop or single-click an ACE instance in the Start menu.

Depending on how the administrator has configured your ACE, you might be required to enter zero, one or even two passwords when you run the instance for the first time. The various possibilities are:

- You don't have to enter any passwords, either at the first run of the instance or on subsequent runs.
- You must enter one password at the first run, and that password has been supplied to you by the administrator. On subsequent runs of the instance, you don't have to enter any passwords.
- You must enter one password at the first run, a password that you create. On subsequent runs of the instance, you have to enter that password.
- You must enter two passwords at the first run, both an administrator-supplied password and one that you create. On subsequent runs of the instance, you only have to enter the password that you created.

For any passwords, your administrator might require that you include numbers or punctuation marks or that you mix capital and lowercase letters. The password dialog box shows what requirements your administrator has set.

If this ACE requires you to enter a user password and your system administrator has configured this ACE with password lockout settings, then an error message appears if the number of password tries has reached the set limit, and you will not be able to try to log in again for the specified lockout time.

After you have entered any required passwords, VMware Player starts.

Click inside the VMware Player window to begin using the guest operating system and the applications installed in the ACE. In general, you use the operating system and applications just as you would if they were running directly on a physical computer.

After the ACE has started running, you can change a password that you created by choosing **Player** > **Change Password** and typing in a new password.

Entering a Client License in VMware Player for an ACE Instance

If the Enter Serial Number dialog box appears when you attempt to power on an ACE instance, enter the serial number provided by your ACE administrator, or click **Get Serial Number**. You can also choose **Player > Enter ACE Client License** to enter a new serial number.

Quitting VMware Player

Quit VMware Player before you shut down the host computer—the computer where VMware Player is running.

To quit VMware Player, do one of the following:

- Choose **Player > Exit** (on Windows) or **Player > Quit** (on Linux).
- Click the **X** in the upper-right corner of the toolbar.

Depending on the configured exit behavior, the ACE either suspends or shuts down and the window closes.

If your system administrator has enabled the appropriate controls, you can change the exit behavior in the Preferences dialog box (**Player > Preferences**).

You can specify the following:

- **Confirm before exiting the application** — If selected, when you give the command to exit VMware Player, a dialog box appears. You can confirm the intention to exit VMware Player or click **Cancel** to continue using VMware Player.
- **Suspend the virtual machine** when exiting — If selected, VMware Player suspends the ACE and closes. The next time you launch VMware Player, the ACE resumes operation from the point where it was suspended.
- **Power off the virtual machine** when exiting — If selected, VMware Player powers off the ACE. The next time you launch VMware Player, the ACE starts from a powered-off state and the guest operating system boots.

Enlarging VMware Player to Fill the Screen

Click the maximize button on the VMware Player window to run your ACE 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 disappears if it is unpinned. 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 Player 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**.

If your system administrator has configured VMware Player 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 Player window is minimized and you see the host operating system.

Understanding VMware Player Status Indicators

Your ACE has several indicators to keep you aware of its status. The activity indicator shows that your ACE is running. It is represented by the VMware logo of three interlocking squares.

- On Windows, this indicator appears in the lower-right corner of the VMware Player window in windowed mode, but is not visible in full screen mode.
- On Linux, this indicator appears in the top of your window in both windowed and full screen mode.

While your ACE is running, the activity indicator is animated.

The status icon tray (on Windows host systems only) is at the lower-right corner of the VMware Player window or immediately left of the activity indicator on the toolbar. The status icon tray might display one or both of the following:

- The network access indicator is a shield-shaped icon. If your ACE uses network access 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 access status icon to open the ACE Information dialog box, which displays a detailed summary of your ACE's network access status.

- If the ACE has a host network access policy:

  - On Windows, the host access 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 access status. Click the icon to open the VMware ACE

Host Network Access Info dialog box, which displays a summary of the host network access status.

- On Linux, you can use the following commands to set the log level and to see the current zone and log level.

  Usage:

  ```
  vmnet-detect [-d]
  -d <PID file>: daemon mode
  -l <log level>: set the log level
  -g:get the current zone and log level
  ```

  Valid log levels are `mute`, `terse`, `normal`, and `verbose`.

  Sample output from a `-g` command:

  ```
  Current zone: Default Zone
  Not blocking network traffic
  Current log level: verbose
  ```

  Sample output from a `-l` command:

  ```
  Log level set to normal.
  ```

Viewing Messages, Notifications, and the ACE Information Dialog Box

VMware Player displays pop-up notifications about changes in network access settings and other status information. Those notification messages appear in the lower-right corner of the Player window when you start up the ACE. You can close the messages by clicking the **X** in the upper-right corner of the message box.

You can view messages that have been displayed for this ACE by selecting **Player > Troubleshooting > Message Log**. The Message Log dialog box allows you to open and view the past messages and to remove any or all messages from the log.

You can view information about the ACE's network access settings and other settings, such as expiration date for the ACE, in the ACE Information dialog box. To access this dialog box, choose **Player > Troubleshoot > ACE Information**.

Controlling Devices Attached to VMware Player

Your administrator might have configured VMware Player to give the ACE 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 Player Preferences" on page 228), those devices might appear in the toolbar or on the **Devices** 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 **Devices** menu, click the name of a device to toggle it off and on. A check mark next to the name of a device indicates that it is connected. If there is no check mark, the device is disconnected.

Only one machine—either the host computer or the ACE —can use disk drives and USB devices at any one time. If your ACE 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 ACE. The Ethernet adapter can be shared by the host computer and the ACE.

Setting VMware Player Preferences

You can set preferences that control the behavior of VMware Player. The options available to you depend on choices made by your system administrator. To change the preferences, choose **Player** > **Preferences**. The Preferences dialog box appears.

If your system administrator has made them available, you can set the preferences described below.

The exit behavior preferences allow you to specify the following:

- **Confirm before exiting the application** — If selected, when you give the command to exit VMware Player, a dialog box appears. You can confirm the intention to exit VMware Player or click **Cancel** to continue using VMware Player.
- **Suspend the virtual machine** when exiting — If selected, VMware Player suspends the ACE and closes. The next time you launch VMware Player, the ACE resumes operation from the point where it was suspended.
- **Power off the virtual machine** when exiting — If selected, VMware Player powers off the ACE. The next time you launch VMware Player, the ACE starts from a powered-off state and the guest operating system boots.

The option to **Check the web for updates on startup** is not available when you are running an ACE.

Removable devices 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 Player. Select one of the following:

- **Show 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 as menu** – To disconnect and reconnect the devices from the **Devices** 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.

Taking Snapshots in VMware Player

If your system administrator has enabled the option to take a user snapshot, you can take a single snapshot of the ACE. Choose **Player > Snapshot > Take Snapshot** and either choose to take the snapshot while the ACE is running or have VMware Player power off the ACE, take the snapshot, and power the ACE on again. (The software shuts down the ACE and restarts it after taking the snapshot. You don't need to power off or restart the machine yourself.)

All snapshot and power operations, including exiting VMware Player, are disabled while the software is taking a powered-off snapshot.

NOTE If an ACE instance gets stuck while taking a powered-off snapshot (for example, at a message that says you can power off your machine), issue the command to take a powered-off snapshot again to force the machine to power off. The machine will be powered on again and the snapshot will have been taken.

You can also replace an existing user snapshot. Choose **Player > Snapshot > Take Snapshot** and choose **Yes** in the message dialog that appears asking if you want to replace the previous snapshot.

If the administrator has enabled the option to revert to the user snapshot, you can revert the ACE to the existing snapshot by choosing **Player > Snapshot > Revert to Snapshot**.

If you are permitted to take a user snapshot, you can also remove it. Select **Player > Snapshot > Delete Snapshot**.

Using Shared Folders

Shared folders allow you to share files between a ACE and the host computer.

You cannot change the shared folder options in the Shared Folders dialog box (**Player > Shared Folders**) for an ACE unless it is running in administrator mode. See "About the Enter Administrator Mode Command on the Troubleshoot Menu" on page 233 for information about that mode.

Printing from VMware Player

If your system administrator has enabled the print feature for your ACE, you can print from applications in the ACE as you would on the host system.

You can choose which host printers are available for use by the guest operating system by clicking the tray icon for the print application in the taskbar notification area of the host system and selecting the printers you want to use. When you execute the Print command in the guest operating system, those printers appear in the printer selection list.

Troubleshooting Problems

If you encounter problems while running your ACE, contact your system administrator for assistance. Topics in this section are:

Requesting a Hot Fix

NOTE This feature is available only if your system administrator has enabled the feature.

When certain problems occur, VMware Player 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 ACE
- Copy-protected ACE run from a new location

The hot fix request includes the nature of the problem. The Hot Fix Request Wizard allows you to include an additional message to your system administrator. The wizard 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 might have configured your ACE to submit the hot fix request automatically. If not, or if the automatic submission fails, you can save the hot fix request in a file and submit that file to your administrator. Note the path to the file shown in the final page of the Hot Fix Request Wizard. Also note any submission instructions the administrator provides. The wizard displays those instructions in the page 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 your ACE so a password is required, and you try to log on with an incorrect password, you receive an error message. Click the **Request Hot Fix** button in the error message to start the Hot Fix Request Wizard.

If your system administrator approves your hot fix request, the administrator supplies you with a new temporary password by whatever method of communication the administrator has set up. After applying the hot fix, use that temporary password to run your ACE. Then choose **Player** > **Change Password** to set a password of your choice.

Expired ACE – If your system administrator configured your ACE to run for a limited time, you receive an error message if you try to run the ACE after it has expired. To

request an extension of the time you are authorized to run the ACE, click the **Request Hot Fix** button in the error dialog box. This starts the Hot Fix Request Wizard.

Copy-Protected ACE Run from a New Location – If your system administrator has applied copy protection to your ACE, it runs only from the location where it is installed by the 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 ACE from the new location, click the **Request Hot Fix** 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 might ask you to reset or power off your ACE. These commands are on the VMware Player menu. Choose **Player** > **Troubleshoot** > **Reset** or **Player** > **Troubleshoot** > **Power Off and Exit**.

The reset command affects your ACE 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 ACE the same way 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 ACE closes. The next time you run your ACE, you see a VMware startup screen for a few moments before the operating system in your ACE begins to run.

Reverting to the Reimage Snapshot

If you encounter serious problems with your ACE, your system administrator might tell you to use a menu choice to revert to the reimage snapshot of your ACE. The reimage snapshot is first taken automatically when the ACE is created. The administrator might have retaken the reimage snapshot or enabled the option to allow you to do so.

If you do revert to the reimage snapshot, you lose all changes made to your ACE since the time that snapshot was taken, including any data you have saved in the ACE, 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.

NOTE Taking a reimage snapshot deletes the user snapshot.

To revert to the ACE reimage snapshot, choose **Player** > **Troubleshooting** > **Revert to Reimage Snapshot**. To take the reimage snapshot, choose **Player** > **Troubleshooting** > **Take Reimage Snapshot.**

These menu items are available only if your system administrator has enabled them.

About the Enter Administrator Mode Command on the Troubleshoot Menu

If the administrator mode has been enabled for your ACE, the **Enter Administrator Mode** command appears in the **Troubleshoot** menu. The command is for use by administrators, allowing them to:

- Edit virtual machine settings for your ACE (on Windows systems only).
- Take a reimage snapshot or revert to it, and take a user snapshot or revert to it, if those options are not enabled in the menu. Snapshot operations are not available on Pocket ACEs.
- Change Shared Folder settings (**Player > Shared Folders**).

The feature requires the administrator to enter the administrator mode password.

Troubleshooting Tools

VMware ACE includes some troubleshooting tools that allow administrators and help desk assistants to fix some common problems that users have with their ACE instances, such as forgotten user passwords. The tools are:

- For standalone ACE instances
  - The ACE Tools, a command-line tool – See "ACE Tools: vmware-acetool Command-Line Tool" on page 234.
  - Hot fixes – See "Responding to Hot Fix Requests" on page 235, as well as the instructions about requesting a hot fix that you can provide to your users, in "Requesting a Hot Fix" on page 231.
- For managed ACE instances
  - The Help Desk Web application – See "Using the VMware Help Desk Web Application" on page 237.
  - The Instance View in Workstation ACE Edition – See Chapter 12, "Instance View," on page 243.

ACE Tools: vmware-acetool Command-Line Tool

The vmware-acetool command-line program is a troubleshooting tool that allows ACE administrators to fix a limited set of problems for standalone ACE instances directly on an ACE user's system.

NOTE You can actually use the vmware-acetool program to reset passwords and fix expiration dates on another machine, but you must have the .vmx, .vmpl, and ace.dat files from the user all set up in the same directory.

The vmware-acetool is distributed with VMware Player and is available for both Windows and Linux systems.

Problems you can fix with vmware-acetool are:

- Set the user's password, so the user can run the ACE instance.
- Set copy protection, so the user can run the ACE instance in a new location.
- Set the expiration date, so the user can continue to use an ACE instance that had reached its scheduled expiration date.

NOTE For you to use vmware-acetool to fix a problem, the configuration file for the targeted ACE instance must be on the ACE user's machine. That is, you cannot use the tool to make fixes to files associated with the instance unless the configuration file is on the same machine as those files. It should be run on the user's machine, in place.

Usage: `vmware-acetool <command> <ACE configuration file> [parameters]`

Command	Parameters	Description
`setPassword`	Path to recovery key file	Set the ACE instance's password
`setExpirationDate`	New expiration date	Set the ACE instance's expiration date
`allowCopy`		Allow the ACE instance to run from its current location

Password Prompts

All commands prompt for the administrative tools password. See "Setting Administrator Mode Policies" on page 152.

The `setPassword` command also prompts for the recovery key password for the private recovery key file, a new ACE instance password, and confirmation of that new password. See page 118 for information about the recovery key password.

Expiration Dates

The new expiration date can be passed as one of:

- A number of days from the current date
- An absolute date in the format `YYYY-MM-DD`
- A start date and an end date in the format `YYYY-MM-DD YYYY-MM-DD`
- The special value `"never"`, so that the instance will never expire
- The special value `"expired"`, so that the instance expires immediately

Examples

```
vmware-acetool setPassword myACE.vmx recKey.priv

vmware-acetool setExpirationDate myACE.vmx 30

vmware-acetool setExpirationDate myACE.vmx 2007-06-16

vmware-acetool setExpirationDate myACE.vmx "never"

vmware-acetool allowCopy myACE.vmx 30
```

Responding to Hot Fix Requests

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

- Lost or forgotten password
- Expired ACE instance
- Copy-protected ACE instance run from a new location

NOTE For information on enabling the hot fix feature, see "Setting Hot Fix Policies" on page 154. For information on setting a recovery key, which you must have to send a hot fix for a lost or forgotten user password, see page 118.

The user runs the Hot Fix Request Wizard, which generates a hot fix request file. The user can 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 on which you are running Workstation ACE Edition.

2 In Workstation ACE Edition, open the ACE master for the instance requiring the hot fix.

3 Choose **File** > **Open**.

4 Navigate to the location of the hot fix request file and click **Open**.

A hot fix tab opens in the Workstation ACE Edition window. The hot fix tab displays the user's name and email address, the problem that led to the hot fix request and any additional note the user entered.

5 Click **Approve hot fix** to open a dialog box in which you can make the appropriate settings to approve the request. Click **Deny hot fix** to deny the request.

6 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. (See page 118 for information about creating a recovery key.) Enter the password for the private part of the recovery key. Enter and confirm a temporary password for the user. You must communicate this temporary password to the user separately.
- Expired ACE instance – Set the new expiration information for the ACE instance. You can extend use by a specified number of days or set a new expiration date.
- Copy-protected ACE instance run from a new location – The dialog box displays the path to the location from which the user wants to run the ACE instance.
- Denied request – The dialog box provides a field in which you can enter a message to the user.

7 Select one of the following methods for sending the response:

- Click **Send hot fix** on the hot fix tab.Then click **OK**.
- Send the hot fix file (in the same folder as the hot fix request; the file extension for the fix file is .vmhf).

8 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 user applies the hot fix by double-clicking the hot fix file.

Using the VMware Help Desk Web Application

The VMware Help Desk Web application allows help desk assistants or administrators to view ACE instances that are managed by a particular VMware ACE 2 Management Server and to provide some fixes requested by users of those instances.

Help desk assistants can access the ACE instance through the VMware Help Desk Web application and can fix just a limited set of ACE instance problems, such as reactivating an instance, changing the instance's expiration date, or resetting the user password if the user has lost or forgotten it.

To set up a password for help desk assistants: Open the ACE 2 Management Server Setup Web application (see "Using the ACE 2 Management Server Setup Application" on page 78 for information for details) and choose **Enable Help Desk Role** on the Access Control tab. Type in a help desk password and confirm the password.

To access the Help Desk application

- On Windows: Choose **Start > All Programs > VMware > VMware ACE Management Server**. Click the Help Desk link on the page.
- On Linux: Open a browser and point it to `https://<hostname>:8000`. Click the **Help Desk** link on the page.

The VMware Help Desk opens to the Instances page, which contains a summary table of all the instances managed by that server.

The Instances Page

On the Instances page, you can

- "Set Up Queries to Search for Instances" on page 238
- "Reactivate/Deactivate an Instance" on page 239
- "Reset Expiration Dates by Clicking Reactivate" on page 239
- "Sort Instances by Column Heading" on page 240
- "Access the Instance Details Page" on page 240

To navigate through the Instances page, click the previous and next arrows at the right of the status bar at the bottom of the Instances table. The indicator at the left edge of the status bar displays which instances of the total number of instances managed by this server are shown on this page. For example, "11 - 20 / 150" indicates that instances 11 through 20 of 150 instances appear on the current page.

Set Up Queries to Search for Instances

You can use the advanced search function in the VMware Help Desk to query the ACE 2 Management Server database to find one or more particular ACE instances.

To search for an ACE instance

1 Click **Search** in the upper left of the Instances page. The Search window appears.

2 Specify the criteria to be included when the database is queried. Type your entries in the fields that you want to query.

- Activated by

  ("Activated by" refers to the activation method, such as password or activation key. If there is no such activation method, then N/A appears in the column.)

- Activated
- Deactivated
- Valid
- ACE Master Name
- Package Name
- Host Name
- Host IP Address
- Guest Name

  NOTE The Guest Name, which is the computer name resolved on the user's machine during instance customization (a feature for Windows systems only), is always shown in the help desk view as 15 characters or less. The NetBIOS name is reported here, and it is a maximum of 15 characters in length. Even if the actual computer name contains more characters, the name is always shown as the NetBIOS name.

- Guest IP Address
- Guest MAC Address

[custom_column_name]

Any custom columns that you have specified appear directly below the Guest MAC Address criterion.

If you select the option **Exact match only** for a search category, only instances with values that are exact matches of the value specified in that category field are listed in the search results. Exact-match values are case-sensitive.

Specify dates in the format MM/DD/YYYY.

Search criteria are joined with AND, not OR, operations.

You can save a search by entering a name in the Save as field in the Advanced Search dialog box. Saved searches are specific to each server. If you go to the instance view of another server, that server will have a unique set of saved searches. You can edit or delete your saved searches by selecting the name of a saved search in the **Saved Searches** drop-down list and then clicking the **Options** button.

3 Click **Reset** in the Search dialog box if you want to clear entries in the search fields.

4 When you have finished specifying the search criteria, click the **Search** button. The Search dialog box closes and the search results are displayed.

5 Click **Back to all instances** in the upper left of the window if you want to refresh the display with the total list of instances.

6 If the results list cannot all be displayed on one page of the Instances table, you can click the Next arrow at the bottom right of the table to see the next page of results.

Reactivate/Deactivate an Instance

You can immediately deny or allow access to an instance by deactivating or reactivating it.

To reactivate or deactivate an instance, select the instance by clicking the instance row once, and then click the appropriate icon, **Deactivate** or **Reactivate**, in the upper left of the Instances page.

The change is made as soon as you click the icon.

Reset Expiration Dates by Clicking Reactivate

You can reset the expiration dates for an expired instance by selecting the instance row, clicking **Reactivate**, resetting the expiration dates in the dialog box, and clicking **OK**.

Sort Instances by Column Heading

You can re-order the instances in the table and change column widths as follows:

- Re-order the list alphabetically or numerically, depending on the selected column's contents, in ascending or descending order. Click to the right of the column heading that you want to sort the column. Click again to re-sort in the opposite (ascending or descending) order.
- Re-size column width by clicking on a column divider and dragging the column edge to a new width.

Access the Instance Details Page

To access the details page for an instance, double-click the instance row. You can also select the row and click the **Details** icon in the upper left of the Instances page.

The Instance Details Page

On the Instance Details page, you can:

- View Details for the Instance
- Reactivate/Deactivate an Instance
- Reset the Instance Expiration Date
- Change the Copy Protection ID
- Reset the Password
- View Network Access Details

View Details for the Instance

The general details for the instance appear at the top of the Instance Details page. The rest of the page provides details about any instance customization results, the guest MAC address, and the various policy settings. Removable devices shows the settings for the removable devices policy, including details about which devices are allowed and blocked. See "View Network Access Details" on page 241 for more information about the display for network access policy settings.

Reactivate/Deactivate an Instance

You can immediately deny or allow access to an instance by deactivating or reactivating it.

To reactivate or deactivate an instance, click the appropriate icon, **Deactivate** or **Reactivate**, in the upper left of the Instance Details page. The change is made as soon as you click the icon.

Reset the Instance Expiration Date

You can reset the expiration date by selecting or deselecting **Use the date range specified for the ACE master**, typing in **Valid From** and **Valid Until** dates, and selecting or deselecting **Never expire**. You must click the **Save** button in the upper left of the page to institute the changed expiration date.

Change the Copy Protection ID

You can change the copy protection ID to allow the user to run a moved or copied instance. Select the alphanumeric string in the Copy Protection ID box and replace it with the new copy protection ID (generally, the user sends you a request to allow a moved or copied instance to run and includes the new ID in that request message).

The Copy Protection ID field is always active, so you can change the ID whenever you want.

CAUTION If you enter a change in the Copy Protection ID field for an active instance, a warning appears to let you know that if you change the ID, the original instance will no longer run.

You must click the **Save** button in the upper left of the page to institute the changed ID.

Reset the Password

If this is an instance that has an authentication (user-specified) password, you can reset the password by clicking **Reset Password** and then specifying a new password. Ensure that the number of characters in the password is greater than zero. You must then send the new password to the user in an e-mail message.

The change is made as soon as you click **OK** in the password dialog box.

View Network Access Details

Click the links under **Zone** (if "**Zone**" is anything other than "**Everywhere**" or "**Everywhere else**"; those zones do not require further definition), **Host Access,** or **Guest Access** to view the Zones or Rules Detail page for this zone or this type of network access.

Preserving the State of an ACE Instance

ACE 2 offers two ways to preserve the state of an ACE instance:

- Suspend and Resume
- Snapshots

See the *Workstation User's Manual* for information on these features.

12 Instance View

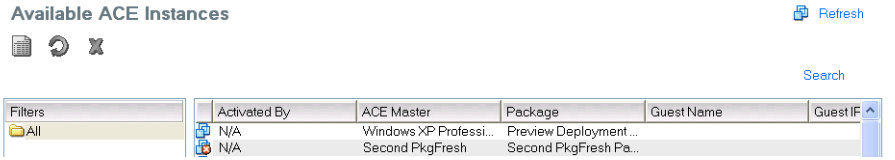
The Instance View provides you with a central management point for all instances managed by a particular ACE 2 Management Server. A summary table provides instance status (activated, deactivated, or blocked by policy violation) and validity dates (expiration) for the instances, as well as many details such as who the instance was activated by, ACE master for this instance, package name, guest name and IP address, and host name.

You can select an instance in the table and then deactivate or reactivate the instance. You can also open a details view for each instance that shows the instance's general statistics and policy settings.

The topics in this section are:

Opening a View of All Instances Managed by a Server

To open a view of all instances managed by a server, click the server in the Sidebar. An example of an Instance View appears below.



An instance has one of three status types:

- Active – The instance is active. It is available for immediate use.
- Blocked by policies – The instance is still active but is blocked (cannot be run) due to a violation of a policy such as expiration or copy protection. For details on the reason for the blockage, you can view the server's log for the instance.
- Deactivated – This instance has been purposely deactivated. You must reactivate it to make it usable again.

Expiration dates are shown in the Instance View in the **Valid From** and **Valid Until** column. If there is no expiration date set for the instance, those columns don't contain dates.

Setting Up Queries to Search for Instances

You can use the advanced search function in the Instance View to query the ACE 2 Management Server database to find one or more particular ACE instances.

To search for an ACE instance

1 Click **Search** in the upper right of the Available ACE Instances page of the Instance View. The Advanced Search dialog box appears.

2 Specify the criteria to be included when the database is queried. Type your entry in the fields that require text. Choose dates from the calendar pop-ups for date fields. In the date fields, you can enter a start date and leave the end date empty if you wish.

- Activated by
- Activated
- Deactivated

- Valid
- ACE Master Name
- Package Name
- Host Name
- Host IP Address
- Guest Name

  The Guest Name, which is the computer name resolved on the user's machine during instance customization (a feature for Windows systems only), is always shown in the Instance View as 15 characters or less. The NetBIOS name is reported here, and it is a maximum of 15 characters in length. Even if the actual computer name contains more characters, the name is always shown as the NetBIOS name.
- Guest IP Address
- Guest MAC Address

You can search on custom columns by selecting **Show custom values** and specifying the search values for those columns.

If you select the option **Exact match only** for a search category, only instances with values that are exact matches of the value specified in that category field are listed in the search results. Exact-match values are case-sensitive.

Specify dates in the format MM/DD/YYYY.

Search criteria are joined with AND, not OR, operations.

You can save a search by entering a name in the **Save as** field in the Advanced Search dialog box. Saved searches are specific to each server. If you go to the instance view of another server, that server will have a unique set of saved searches. You can edit or delete your saved searches by selecting the name of a saved search in the **Saved Searches** drop-down list and then clicking the **Options** button.

3 Click **Reset** in the Advanced Search dialog box if you want to clear entries in the search fields.

4 When you have finished specifying the search criteria, click the **Search** button. The search results are displayed. An indicator in the lower right corner of the page displays **Showing [number of results in view] out of [total number of results]**; for example, **Showing 24 out of 55**.

The query is remembered for the length of the Workstation ACE Edition session.

To clear a query

1 Click **Search** in the Instance View.

2 Click **Reset** in the Advanced Search dialog box.

3 Click **Search**.

Showing, Hiding, Moving, and Resizing Columns in the Instances Table

You can show, hide, and move columns that appear in the Instance View table. You can also resize the width of a column.

NOTE The column setup – the visible columns and their positions – is saved for each server view you work with. If you rearrange the view for one server, the views of other servers that you open are not affected by that rearrangement.

To show or hide a column

Right-click the column heading row and then select (check) or deselect (uncheck) the column you want to show or hide. If you show a column that was previously hidden, the column is added to the right side of the table.

To move a column

Click the column header, drag the column to a new location, and release the mouse button.

To resize column width

Resize column width by clicking on the right side of a column divider and dragging the column edge to a new width.

Adding Custom Database Fields by Adding Columns

You can create up to nine custom columns in the Instance View table so that you can view additional categories of information about the instances managed by this server.

In the Instance View table, you can add, delete, and rename custom columns.

To specify a value that will appear in a custom column, go to the Details view for the instance. See "Custom Details View" on page 252.

To add a custom column

1 Right-click anywhere in the column heading row and choose **Add Custom Column**. The Custom Column Name dialog box appears.

2 Type a name for the new column in the **Name** text box and click **OK**.

NOTE If you have added nine custom columns, the **Add Custom** command in the right-click menu is dimmed and you can't select it. You must delete one of the nine existing custom columns before you can add another one.

To delete a custom column

Right-click on the column header for the custom column and choose **Delete Column s**from the context menu.

To edit a custom-column name

1 Right-click on the column header for the custom column and choose **Edit Title** from the context menu.

2 Type the new name in the **Name** field of the Custom Column Name dialog box and click **OK**.

Changing the Sort Order of the Instances Table

You can change the sort order for the rows in the instances table.

To change the column sort order

Choose either of:

- Click the column heading for the column you want to sort by. An arrow appears at the right of the column heading cell, showing whether sorting is currently ascending or descending. Click again to reverse the order.
- Right-click the column heading and choose **Sort**.

Deactivating and Reactivating Instances from the Instance View

To deactivate an active instance

1 Click the instance in the right pane of the view, so that the instance row is highlighted.

2 Click the **Deactivate** icon at the top left of the view.

3 Verify that the icon is dimmed.

To reactivate a deactivated instance

1 Click the instance in the right pane of the view, so that the instance row is highlighted.

2 Click the **Reactivate** icon at the top left of the view.

3 Verify that the icon is no longer dimmed.

Resetting Expiration Dates for an Expired Instance by Clicking Reactivate

You can reset the expiration dates for an expired instance in the Instance View by selecting the instance row, clicking **Reactivate**, resetting the expiration dates in the dialog box, and clicking **OK**.

NOTE You can press Ctrl+click or Shift+click to select multiple instances and then reactivate or deactivate them all at once.

Using the Details View

To open a details view of an instance

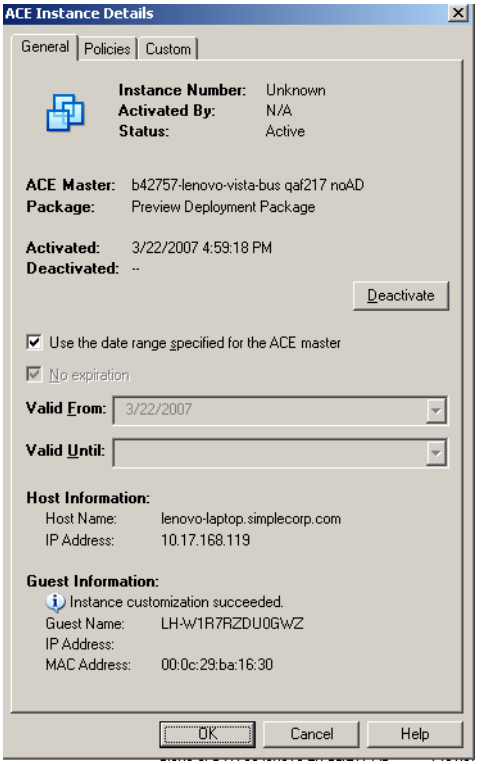
Do one of the following:

- Double-click the instance row in the right pane of the view.
- Click the instance in the right pane of the view, so that the instance row is highlighted, and then click the **Details** icon at the top left of the view.

General Details View

The **General** details view shows statistics for this instance, including:

- Instance number, activated by, and activation status
- ACE master name and package name
- Activation and deactivation dates
- Expiration date/range
- Guest Name, IP address, and MAC address
- Host name and IP address



To activate or deactivate the instance or reset the expiration date

1 To activate or deactivate the instance, press the **Reactivate** or **Deactivate** button.

2 To reset the expiration date for the instance, check or uncheck **Use the date range specified for the ACE master** or select dates in the **Valid from** and **Valid until** dropdown lists. Check **No expiration** if you do not want the instance to expire.

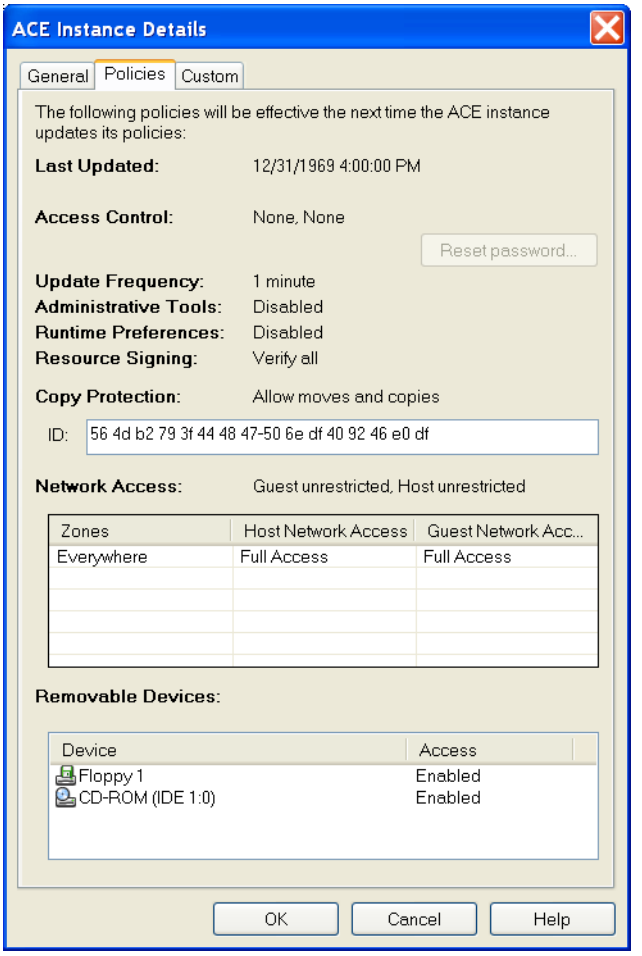
3 When you are finished making changes, click **OK**.

Policies Details View

The **Policies** details view shows current policy information for this instance, including:

- The date and time that the instance last retrieved the policies from the server
- The current policy values, including the network access table and the list of removable devices

- The copy protection ID



To reset the password for this ACE instance

1 Press **Reset Password**. The Password dialog box appears.

2 Type the password in the first text box and then retype it to confirm it in the second text box. Then click **OK**.

To change the copy protection ID for this ACE instance

1 Select the alphanumeric string in the **Copy Protection ID** box.

2 Type the new ID over the old one. Then click **OK**. (Generally, the user provides the new alphanumeric string to you with a request to allow a moved or copied instance to run.)

The Copy Protection ID field is always active, so you can change the ID whenever you want.

If you enter a change in the Copy Protection ID box for an active instance, a warning appears to let you know that if you change the ID, the original instance will no longer run.

Custom Details View

The **Custom** details view shows values for any custom columns that you have created.

To specify values for custom columns

1 In the Instance View table, click the row for the instance that has custom columns for which you need to set values.

2 Click the **Details** icon.

3 In the Details view, click the **Custom** tab.

4 Type a string value for each custom column in the appropriate text box. There are no character or format restrictions on your entries. You can even leave the fields empty.

5 When you have finished adding and editing values, click **OK**.

Using the Connect to ACE 2 Management Server Command to Open an Instance View

To open the Instance View for a particular ACE 2 Management Server, you can click the server in the list of Recent ACE 2 Management Servers in the Sidebar of the Workstation ACE Edition interface.

If the server you want does not appear in the list, choose **File** > **Connect to ACE Management Server**. Enter the server address and port number in the dialog box and click **OK**.

In addition to using the Connect to ACE 2 Management Server command to open a server connection, you can open the connection by:

- Creating a new master and assigning it to the server
- Opening an existing master that is already assigned to the server
- Opening an existing virtual machine, cloning it to create a new master, and then assigning the master to the server

See Chapter 5, "Creating and Configuring ACE Masters," on page 91 for details about these tasks.

Appendix: Using the VMware ACE 2 Management Server Database Schema and Querying the Audit Event Log Data

Tables in the VMware ACE 2 Management Server database represent the major configuration objects of ACE 2 Management Server: Ace, Package, Instance, Access Policy, Runtime Policy, and User Data (which contains image customization settings and other per-user data). Administrator and user actions are audit logged in the Event table in the database, while possible event types are listed in the EventType table. This Appendix shows the format of the data stored in the database, and the best ways to access this data.

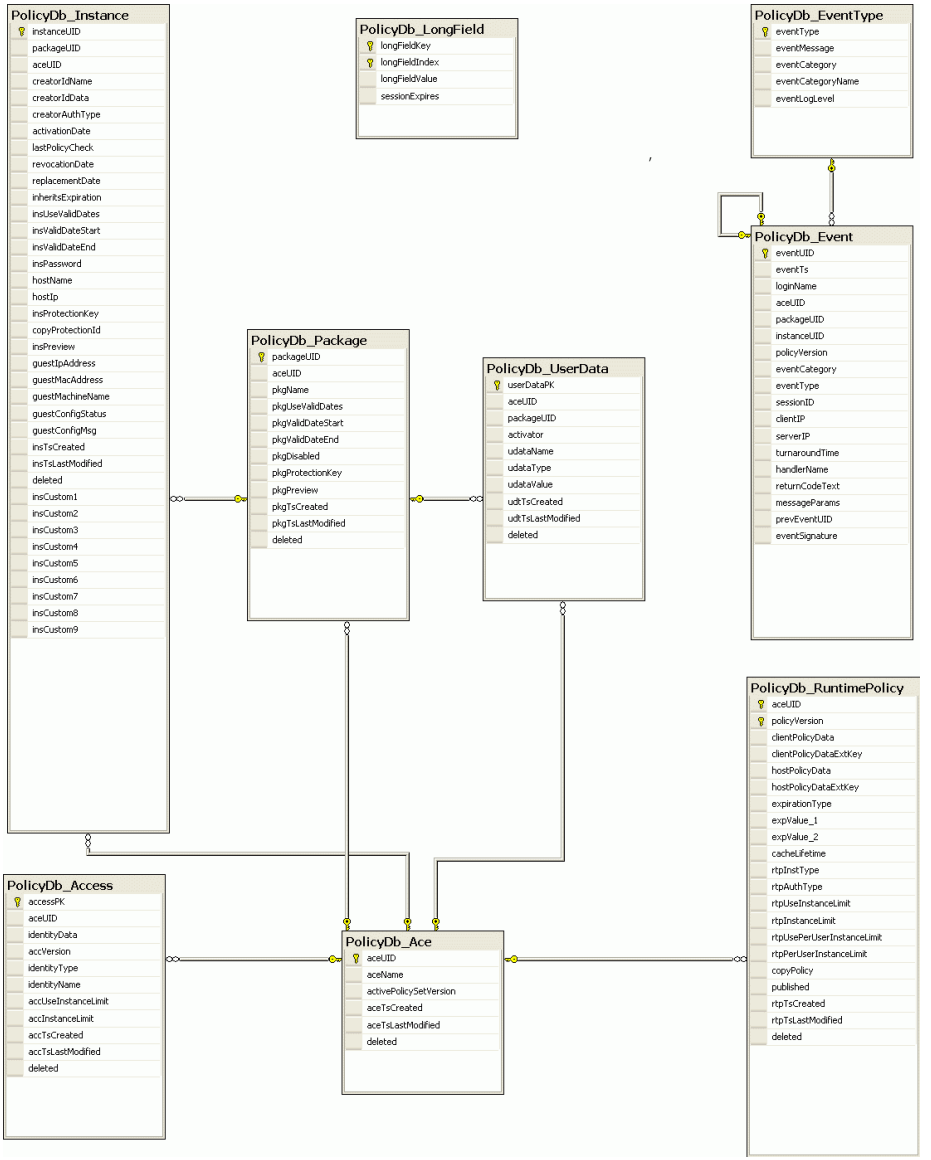
For a big installation, you might choose to use a third-party database management or reporting tool with the VMware ACE Server database. While VMware Workstation ACE Edition provides powerful tools to inspect the current state of the system (the Advanced Instance Query dialog, for example), you might want to create custom reports of the system state using a reporting tool such as Crystal Reports. You can also use a reporting tool to inspect the audit trail of the administrator or user actions stored in the Event table. For example, you might look for active instances that have not updated their ACE policy with the latest ACE policy set changes, or for excessive failed authentication attempts.

The VMware ACE 2 Management Server Database Schema

CAUTION The data stored in the database is protected by the RDBMS access control mechanism. Make sure that you do not allow the database user account used by your reporting tool to have a higher than necessary level of access to the data; otherwise you could compromise the security of your VMware ACE system. For example, reporting tools typically do not need write access to the database. Instead, you can create a separate read-only account for the reporting tool. You might also want to disallow read access to database fields that contain sensitive information, such as user passwords, instance customization data (which may have the domain administrator logon), or instance disk encryption keys. (See the schema in the following section). The embedded SQLite database does not support authentication, so access can be protected only by "all or nothing" file-based security.

Figure A-1 shows the VMWare ACE 2 Management Server Database Schema.

Figure A-1. Database Schema Diagram



The following is the Database Schema script.

```
/* Name - value pairs of service information, e.g. DB schema version number */
CREATE TABLE PolicyDb_MetaInfo (
  name VARCHAR(128),                        /* Name of the name-value pair */
  value VARCHAR(1024),                      /* Value of the name-value pair */
  PRIMARY KEY(name));

/* This table holds data for guest and host policy sets, split in 2K chunks */
/* Select all fields for the key in the order of index and append strings together */
/* to reconstruct the policy set */
CREATE TABLE PolicyDb_LongField (
  longFieldKey VARCHAR(128),                /* Unique ID of the long field series */
  longFieldIndex INTEGER,                   /* Index in the series */
  longFieldValue VARCHAR(2000),           /* Up to 2000 chars of field value chunk */
  sessionExpires VARCHAR(21),           /* Optional field for storing session blob */
  PRIMARY KEY (longFieldKey, longFieldIndex));

/* ACE Master data */
CREATE TABLE PolicyDb_Ace (
  aceUID VARCHAR(128),                      /* Unique ID (primary key) */
  aceName VARCHAR(128),                     /* Name of this ace */
  activePolicySetVersion INTEGER NOT NULL,  /* Soft foreign key to active RT policy*/
  aceTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  aceTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY(aceUID));

/* Package data */
CREATE TABLE PolicyDb_Package (
  packageUID VARCHAR(128),                  /* Unique ID (primary key) */
  aceUID VARCHAR(128) NOT NULL,             /* The ACE it belongs to. */
  pkgName VARCHAR(128),                     /* UI visible name. */
  pkgUseValidDates VARCHAR(7)
     DEFAULT 'FALSE' NOT NULL,              /* Use validity dates or always valid */
  pkgValidDateStart VARCHAR(21) NOT NULL,   /* The package is valid from this date.*/
  pkgValidDateEnd VARCHAR(21) NOT NULL,     /* The package is valid till this date.*/
  pkgDisabled  VARCHAR(7) DEFAULT 'FALSE' NOT NULL,  /* Is the package disabled */
  pkgProtectionKey VARCHAR(1024),         /* The key used for package distribution */
  pkgPreview VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* Is preview package */
  pkgTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  pkgTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY(packageUID),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* Access Control object data (single item of the list, associated with ACE master)*/
CREATE TABLE PolicyDb_Access (
  accessPK VARCHAR(128),                    /* Unique ID (primary key) */
  aceUID VARCHAR(128),                  /* Ace for which this access policy is (FK)*/
```

```
  identityData VARCHAR(128),                /* Internal representation, SID in AD */
                                            /* case, token value goes here. */
  accVersion INTEGER NOT NULL,              /* Access object version number */
  identityType INTEGER NOT NULL,            /* AD User, Group, or Token Value */
  identityName VARCHAR(128),               /* UI visible user/group name in AD case */
  accUseInstanceLimit VARCHAR(7)
     DEFAULT 'FALSE' NOT NULL,          /* Limit number of instances for this ID?  */
  accInstanceLimit INTEGER NOT NULL,        /* Max no. of ACE instances allowed */
  accTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  accTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY(accessPK),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* ACE Instance object data */
CREATE TABLE PolicyDb_Instance (
  instanceUID VARCHAR(128),                 /* VM instance ID (primary key) */
  packageUID VARCHAR(128) NOT NULL,         /* The package it belongs to. */
  aceUID VARCHAR(128) DEFAULT '' NOT NULL,  /* The ACE Master it belongs to */
  creatorIdName VARCHAR(128) NOT NULL,  /* Display name of the activator user      */
  creatorIdData VARCHAR(256),          /* Fully qualified name of the activator   */
  creatorAuthType INTEGER NOT NULL,     /* The type of access check at activation  */
  activationDate VARCHAR(21) NOT NULL,  /* The date and time for the activation.   */
  lastPolicyCheck VARCHAR(21) NOT NULL, /* Last time when the player called server */
  revocationDate VARCHAR(21) NOT NULL,  /* When the instance was revoked */
  replacementDate VARCHAR(21) NOT NULL, /* When replaced because of Copy Protect.  */
                                        /* policy      */
  inheritsExpiration
     VARCHAR(7) DEFAULT 'FALSE' NOT NULL,   /* Use expiration info from Ace Policy
                Set */
  insUseValidDates
     VARCHAR(7) DEFAULT 'FALSE' NOT NULL,   /* Use validity dates or always valid */
  insValidDateStart VARCHAR(21) NOT NULL,   /* The instance is valid from this date*/
  insValidDateEnd VARCHAR(21) NOT NULL,     /* The instance is valid till this date*/
  insPassword VARCHAR(128),                 /* The login password for non-AD */
                                            /* authentication for this instance */
  hostName VARCHAR(128),                 /* The name of the host PC the VM runs on */
  hostIp VARCHAR(128),                  /* The IP addr of the host the VM runs on  */
  insProtectionKey VARCHAR(1024),           /* Instance VM disk encryption key */
  copyProtectionId VARCHAR(1024),           /* Stores location of the copy */
  insPreview VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* Is preview instance */
  guestIpAddress VARCHAR(128) DEFAULT '',   /* Reported VM IP address */
  guestMacAddress VARCHAR(128) DEFAULT '',  /* Assigned VM MAC address */
  guestMachineName VARCHAR(128) DEFAULT '', /* The guest (VM) OS host name */
  guestConfigStatus INTEGER DEFAULT 0,      /* The completion status of guest */
                                            /* auto-configuration */
  guestConfigMsg VARCHAR(512),              /* Message for the guest auto-config */
  insTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  insTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
```

```
  insCustom1 VARCHAR(255),                  /* User-defined field */
  insCustom2 VARCHAR(255),                  /* User-defined field */
  insCustom3 VARCHAR(255),                  /* User-defined field */
  insCustom4 VARCHAR(255),                  /* User-defined field */
  insCustom5 VARCHAR(255),                  /* User-defined field */
  insCustom6 VARCHAR(255),                  /* User-defined field */
  insCustom7 VARCHAR(255),                  /* User-defined field */
  insCustom8 VARCHAR(255),                  /* User-defined field */
  insCustom9 VARCHAR(255),                  /* User-defined field */
  PRIMARY KEY(instanceUID),
  FOREIGN KEY(packageUID) REFERENCES PolicyDb_Package(packageUID),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* MAC Address Pool (reserved for future use) */
CREATE TABLE PolicyDb_MacPool (
  macPoolUID VARCHAR(128),                  /* primary key */
  aceUID VARCHAR(128) NOT NULL,             /* ACE for which this MacPool is used */
  macPoolName VARCHAR(128),                 /* User visible name */
  description VARCHAR(128),                 /* name and description of the MAC pool*/
  rangeStart VARCHAR(21) NOT NULL,          /* Start address of the MAC pool */
  rangeEnd VARCHAR(21) NOT NULL,            /* End address of the MAC pool */
  lastAssigned VARCHAR(21) NOT NULL,        /* Last assigned address */
  mplTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  mplTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY(macPoolUID),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));
/* Instance customization data */
CREATE TABLE PolicyDb_UserData (
  userDataPK VARCHAR(516),                  /* Primary key */
  aceUID VARCHAR(128),                   /* ACE for which this UserData is defined */
  packageUID VARCHAR(128),              /* Package for which this UserData is used */
  activator VARCHAR(128),                   /* The user */
  udataName VARCHAR(128),                   /* User data entry name */
  udataType INTEGER NOT NULL,               /* Attribute of the date */
  udataValue VARCHAR(2048),                 /* User data entry value */
  udtTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  udtTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID),
  FOREIGN KEY(packageUID) REFERENCES PolicyDb_Package(packageUID),
  PRIMARY KEY(userDataPK));

/* ACE Master policy set */
CREATE TABLE PolicyDb_RuntimePolicy (
  aceUID VARCHAR(128),                      /* The ACE it belongs to. */
  policyVersion INTEGER,                  /* Version of the RT Policy for this ACE */
  clientPolicyData VARCHAR(2000),           /* Runtime policy for the guest OS */
  clientPolicyDataExtKey VARCHAR(128),     /* If too long store in LongField table */
  hostPolicyData VARCHAR(2000),             /* Runtime policy for the host OS (NQ) */
```

```
  hostPolicyDataExtKey VARCHAR(128),       /* If too long store in LongField table */
  expirationType INTEGER NOT NULL,          /* Expiration Type (enum) */
  expValue_1 VARCHAR(21) NOT NULL,          /* Expiration value (depends on type) */
  expValue_2 VARCHAR(21) NOT NULL,          /* Expiration value (depends on type) */
  cacheLifetime VARCHAR(21) NOT NULL,       /* How long could work without server */
  rtpInstType INTEGER NOT NULL,        /* Instantiation authentication check type */
  rtpAuthType INTEGER NOT NULL,             /* Runtime authentication check type */
  rtpUseInstanceLimit VARCHAR(7)
     DEFAULT 'FALSE' NOT NULL,        /* Limit number of instances for this ACE? */
  rtpInstanceLimit INTEGER NOT NULL,        /* Max no. of ACE instances allowed */
  rtpUsePerUserInstanceLimit VARCHAR(7)
     DEFAULT 'FALSE' NOT NULL,              /* Limit number of instances per user? */
  rtpPerUserInstanceLimit INTEGER NOT NULL, /* Max no. of ACE instances per user */
  copyPolicy INTEGER DEFAULT 0 NOT NULL,    /* Behavior if VM instance is copied */
  published VARCHAR(7) DEFAULT 'FALSE' NOT NULL,/* Policy published (update locked)*/
  rtpTsCreated VARCHAR(21) DEFAULT 0 NOT NULL,   /* Creation timestamp */
  rtpTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL,  /* Last modified timestamp */
  deleted VARCHAR(7) DEFAULT 'FALSE',       /* Is this entry deleted (tombstone) */
  PRIMARY KEY (aceUID, policyVersion),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* ACE Management Server info - reserved for future use */
CREATE TABLE PolicyDb_AcescServer (
  serverHostname VARCHAR(128),              /* Host name of the server computer */
  serverPort INTEGER,                  /* TCP port number server is listening on */
  secure VARCHAR(7) DEFAULT 'FALSE' NOT NULL,  /* Whether HTTPS is enabled */
  sslCertificateExtKey VARCHAR(128),        /* SSL Certificate data, key to stored */
                                            /* in LongField table */
  sslCertificateChainExtKey VARCHAR(128),   /* SSL Certificate Chain data, key to */
                                            /* stored in LongField table */
  PRIMARY KEY (serverHostname, serverPort));

/* Audit Event Log Event Types lookup table */
CREATE TABLE PolicyDb_EventType (
  eventType INTEGER,                        /* Event Type code (PK) */
  eventMessage VARCHAR(1024),              /* Printable message for this event type */
  eventCategory INTEGER,                    /* Event Category code */
  eventCategoryName VARCHAR(128),           /* Event Category printable name */
  eventLogLevel INTEGER,                    /* Event Log Level */
  PRIMARY KEY (eventType));

/* Audit Event Log data */
CREATE TABLE PolicyDb_Event (
  eventUID INTEGER,                      /* Primary key of the table (sequential) */
  eventTs VARCHAR(21),                 /* Timestamp of the event creation in uSec */
  loginName VARCHAR(128),                   /* Login user name of the actor */
  aceUID VARCHAR(128),                      /* UID of the ACE affected by event */
  packageUID VARCHAR(128),                  /* UID of the package affected by event */
  instanceUID VARCHAR(128),                /* UID of the instance affected by event */
  policyVersion INTEGER,               /* Version of ACE policy affected by event  */
```

```
eventCategory INTEGER,               /* Event Category as defined in EventType   */
eventType INTEGER,                       /* Event Type as defined in EventType */
sessionID VARCHAR(128),                  /* Ace Server Session ID */
clientIP VARCHAR(128),                /* IP Address of the client machine (resvd) */
serverIP VARCHAR(128),                /* IP Address of the Ace Server (reserved)  */
turnaroundTime VARCHAR(21),              /* Server-side execution time in ms */
handlerName VARCHAR(128),              /* Name of the ClientLib handler (debug) */
returnCodeText VARCHAR(128),          /* Text error code returned to the client */
messageParams VARCHAR(1024),             /* Tab separated list of event data */
prevEventUID INTEGER UNIQUE,             /* UID of the previous recorded event */
eventSignature VARCHAR(128),         /* Event signature, signed with server key  */
FOREIGN KEY(eventType) REFERENCES PolicyDb_EventType(eventType),
FOREIGN KEY(prevEventUID) REFERENCES PolicyDb_Event(eventUID),
PRIMARY KEY (eventUID));
```

Note the following about the database schema:

- A few tables with system internal information and indices are not listed.
- Boolean values are stored as strings with TRUE or FALSE value.
- Timestamps are stored as decimal 64-bit number strings showing the number of microseconds from 12:00AM 01/01/1970.
- Other dates/times are stored as decimal strings showing the number of seconds from 12:00AM 01/01/1970.
- ACE, Package, Instance, Access, and UserData records are never deleted from the database, but rather marked as deleted with the deleted field set to TRUE, so that the previous information can be inspected for audit purposes.
- The guest and host operating system portions of the ACE policy set are stored in the PolicyDb_RuntimePolicy table in respective fields as strings, if their length is less than 2000 bytes. If the length of the policy component exceeds 2000 bytes, the string is split in 2000-byte chunks and stored in the PolicyDb_LongField table. In this case, the value for the respective ExtKey field in the RuntimePolicy table will contain the foreign key pointing to the corresponding series of strings in the LongField table (see the notes in the table definition).

Querying the Audit Event Log Data

In the ACE Server Component it is possible to create an audit trail for all transactions that are performed by the server. This system can be used by administrators to track down usage, security breaches, policy errors, performance, etc.

The ACE Server Component Event Logging infrastructure is flexible enough to provide detailed logging when necessary, without overwhelming the system by causing a significant performance slowdown when in operation.

The Event Logging mechanism captures enough information to answer the questions like these:

- Who activated instance X?
- When was instance X activated?
- Who revoked instance X?
- Who turned off copy protection policy?
- What changes to policy were made on such a date?
- Who is failing to authenticate?

The mechanism does not necessarily answer these questions directly, but provides enough data so that an administrator can view event logs and find answers to those questions. The data being logged meets the following requirements:

- Provide details of each transaction served.
- Centralize the gathering of event log data when multiple servers are used.
- Provide a means for administrators to select which type of transactions they care to log information about.
- Can be configured to provide more or less logs when necessary.

Some of this audit trail is already in plain view by other features of the product.For example, the instance viewer displays the date of the last policy get operation, or the expiration date, etc. The event logging mechanism can answer more difficult questions (or ones that are not often asked), such as: which administrator made which policy changes, which administrator revoked such instance, which administrator deleted this ACE.

The following data is stored in a log entry (fields in the PolicyDb_Event table):

- Audit log event ID (PK) – an incrementing integer
- Log timestamp (in microseconds from 12:00 AM 01/01/1970, stored as a decimal string)
- Logon user name
- Affected Ace UID (FK)
- Affected Package UID (FK)
- Affected Instance UID (FK)
- Affected Policy Set Version
- Event Category (Auth, AceAdmin, PkgAdmin, PolicyAdmin, InstAdmin)
- Event Type code (FK) – references PolicyDb_EventType table
- Session ID (debug)
- Incoming IP Address (reserved for future use)
- Server IP Address (reserved for future use)
- Operation Turnaround Time (time spent in server in ms)
- Operation Handler Name (debug)
- Return code text (success/failure/specific error)

- Message Parameters (tab separated list; see below)
- Previous event UUID to prevent unauthorized record deletion or insertion (log integrity)
- Event record hash with a server key to reveal modification of the record (log integrity)

ACE, package, and instance UIDs and policy version provide "coordinates" of the log event in the space of ACE Server objects. They help to identify the event with the state of the system. By using database query tools such as Crystal Reports, the administrator can, for example, find all ACE administration events that affected a particular ACE, from its moment of creation until it was deleted (since we never delete objects from the database, but rather mark them as deleted).

Not all coordinates have to be present for all events. For instance, if a package expiration date update is logged, the instance UID field is not set, since all instances within the package will be affected.

If the data in the log event is stored permanently elsewhere in the database and it is immutable, it is not duplicated in the log entry. For example, when a new policy gets published, we do not include the complete policy text in the log entry, but rather reference its version number, so that the complete data of the event can be reconstructed from PolicyDb_ RuntimePolicy and PolicyDb_Access tables if necessary.

NOTE ACE Server does not log sensitive data like passwords or encryption keys.

The event type code is associated with a lookup table PolicyDb_EventType, which contains a text message template for each type of event, category, and log level of the event. The message may contain parameter placeholders `%s`, in which case the message parameters field in the log entry will contain a (tab-delimited) list of values for these parameters. For example, an instance administration event with type = 4110 will have the message

```
4110 –> "Instance Set Guest Info requested, IP address = %s, MAC
address %s, configuration message \"%s\", machine name \"%s\",
configuration status %s"
```

And the Message Parameters field will show

```
10.17.0.3     00:0C:29:1A:2B:3C       OK    ACETest       0
```

The resulting parameters should replace the `%s` placeholders in the message template.

The current list of event types is illustrated in Figure A-2. This list might grow, as new functionality is added to the ACE Server.

Figure A-2. Event Types

eventType	eventMessage	eventCategory	eventCategoryName	eventLogLevel
0	No event	0	N/A	5
10	Handler invoked	0	N/A	4
1000	Authentication-related handler invoked	1	Authentication	4
1010	Manager Authenticate: type = %s, administrator = %s, helpdesk = %s	1	Authentication	2
1020	LDAP user remote change password requested	1	Authentication	2
1030	Instance Authenticate and Get Key requested, supplied credentials: %s	1	Authentication	3
2000	Ace administration-related handler invoked	2	ACE Administration	4
2010	Ace "%s" Create requested, active policy set version %s	2	ACE Administration	2
2020	Ace "%s" Destroy requested	2	ACE Administration	1
2030	Ace "%s" Update requested, new name ="%s"	2	ACE Administration	2
3000	Package administration-related handler invoked	3	Package Administration	4
3010	Package "%s" Create requested, %sdisabled = %s, preview = %s	3	Package Administration	2
3020	Package "%s" Update requested, new name = "%s", %sdisabled = %s, preview = %s	3	Package Administration	2
4000	Instance administration-related handler invoked	4	Instance Administration	4
4020	Instance Create requested, supplied instantiation credentials: %s	4	Instance Administration	2
4030	Instance Copy requested, supplied instantiation credentials: %s, replace = "%s", copy policy = "%s", new instance UID = "%s"	4	Instance Administration	2
4040	Instance Revoke requested	4	Instance Administration	2
4050	Instance Enable requested, supplied instantiation credentials: %s	4	Instance Administration	2
4060	Instance Set Custom Field requested for field # %s, new value "%s"	4	Instance Administration	3
4070	Instance Set All Custom Fields requested, values "%s", "%s", "%s", "%s", "%s", "%s", "%s", "%s", "%s", "%s"	4	Instance Administration	3
4080	Set Custom Instance Field Name requested for field # %s, new value "%s"	4	Instance Administration	2
4090	Instance Set Password requested, value = "*********"	4	Instance Administration	2
4100	Instance Change Password requested, new value = "*********"	4	Instance Administration	2
4110	Instance Set Guest Info requested, IP address = %s, MAC address %s, configuration message "%s", machine name "%s", configuration status %s	4	Instance Administration	3
4120	Instance Set Host Info requested, IP address = %s, machine name "%s"	4	Instance Administration	3
4130	Instance Set Expiration requested, inherit from ACE = %s, enable expiration = %s, start date = %s, end date = %s	4	Instance Administration	2
4140	Instance Set Copy Protection ID requested	4	Instance Administration	3
4150	MAC Address For a New Instance requested, returned address %s	4	Instance Administration	3
4160	Instance Clear Custom Field # %s for all instances requested	4	Instance Administration	2
4170	Instance Delete requested	4	Instance Administration	2
5000	Policy administration-related handler invoked	5	Policy Administration	4
5010	Access Control add requested, identity type = %s, name = "%s", details = "%s"	5	Policy Administration	2
5020	Access Control remove requested, found Access Control object with identity type = %s, name = "%s", details = "%s"	5	Policy Administration	2
5030	Update Working Policy version %s requested	5	Policy Administration	3
5040	Publish Working Policy version %s requested	5	Policy Administration	2
5050	Add User Data For Ace requested, name = "%s", value = "*********", type = %s	5	Policy Administration	3
5060	Add User Data For Package requested, name = "%s", value = "*********", type = %s	5	Policy Administration	3
5070	Remove User Data For Ace requested, name = "%s"	5	Policy Administration	3
5080	Remove User Data For Package requested, name = "%s"	5	Policy Administration	3
5090	MAC Address Pool Add requested, UID = "%s", name = "%s", description = "%s", range start %s, range end %s	5	Policy Administration	2
5100	MAC Address Pool Remove requested, UID = "%s", name = "%s", description = "%s", range start %s, range end %s, last assigned MAC Address %s	5	Policy Administration	2

ACE Server event logging contains an experimental tamper evidence feature. Every record in the event log (except the first one) must have a unique reference to the previous event, further enforced by the database foreign key / unique constraint. Each successive record has a Unique ID incremented by 1, so missing records are immediately evident. If a user with direct access to the database changes, adds, or removes some records, he must change either the previous event pointer or other data in the remaining event record(s). Data within very record is hashed together with a server key, and is stored in the eventSignature field. The integrity of the log data can be verified by a separate utility, which will be available from VMware support.

Event categories, configuring levels of event logging per category, and purging of the old events to keep the table size in check are described in the Logging Page section of "Using the ACE 2 Management Server Setup Application" on page 78.

Glossary

ACE instances
The virtual machines that ACE administrators create, associate to virtual rights management (VRM) policies, and then package for deployment to users. In short form, an ACE instance is an ACE.

ACE 2 Management Server
A server that can optionally be installed and used by the ACE administrator for activating and tracking ACE instances and for hosting dynamic policies for ACE instances.

ACE master
A virtual machine template created by the ACE administrator. The master can be configured with various policies and devices and package settings and then used as the basis for creating any number of packages to be sent to ACE users.

Activation
A step in ACE instance setup that includes package protection and setting up the ACE instance's runtime authentication policy. The successful completion of activation makes the packaged virtual machine, with its policies and other settings, into an ACE instance. The activation setting in the access control policy determines who can access an installed ACE package and turn it into an ACE instance.
See also Authentication.

Authentication
A step in ACE instance setup that includes instance protection. The successful completion of the authentication step allows the user to run the instance.
See also Activation.

Bridged networking
A type of network connection between an ACE instance and the rest of the world. Under bridged networking, an ACE instance 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 ACE instance's display fills the entire screen.

Guest operating system
An operating system that runs inside an ACE instance.
See also Host operating system.

Host computer
The physical computer on which the VMware Player software is installed. It hosts the ACE instances.

Host-only networking
A type of network connection between an ACE instance and the host. Under host-only networking, an ACE instance 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 and Network address translation (NAT).

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.

Instance customization
The act of customizing an ACE instance, thus making it unique from all other instances. The instance customization process automates the actions of the Microsoft sysprep utility. It also provides the ACE administrator with features needed to set up an automated remote domain join process of the ACE instance to a company VPN network.

Live copy of policies

The currently deployed policy set. The active ACE instances on the ACE users' machines use this set.

Managed ACE instance

An ACE instance that is managed by an ACE 2 Management Server.
See also ACE 2 Management Server.

Network address translation (NAT)

A type of network connection that allows you to connect your ACE instances 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 ACE instance does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your ACE instance gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more ACE instances and the external network. It identifies incoming data packets intended for each ACE instance and sends them to the correct destination.

Network access

Policies that give you fine-grained and flexible control over the network access you provide to users of your ACE instances. Using a packet filtering firewall, the network access feature of ACE 2 lets you specify exactly which machines or subnets an ACE instance or its host system may access.

New ACE Master Wizard

A point-and-click interface for convenient, easy creation of an ACE master configuration. To launch it, choose **File > New ACE Master**. It prompts you for information, suggesting default values in most cases. It creates files that define the ACE master.
See also Virtual machine settings editor.

Package

An installable bundle for distribution to users. A full package includes an ACE master configuration file, virtual disk files, and policies; package installer; and Resources files for the ACE master. It also includes the VMware Player application used to run ACE instances.

Package settings

A set of rules and settings associated with a package, such as Revert to Installed and Instance Customization settings. These settings cannot be changed after packaging. The only way to change package settings is to create a new package.

Pocket ACE

An ACE feature that allows the ACE administrator to distribute an ACE instance on a removable device such as a USB key, Apple iPod mobile digital device, or portable hard drive. The user of a Pocket ACE instance can plug the device into a host computer, run the instance, save data from the session and close it, and then unplug the device. The user can then take the instance to another host computer and use it in that new location.

Policy

A policy controls the capabilities of an ACE instance. Policies are set in the policy editor.

See also Live copy of policies; Working copy of policies; and Publish.

Preview

An operating and viewing mode that an administrator can use to preview the ACE instance as it will run on the user's machine. The administrator can use this feature to see the effects of policy and configuration settings without having to go through the packaging and deployment steps. The preview mode displays the working copy of the policies.

See also Working copy of policies.

Publish

To publish policies (applies only to managed ACE instances) is to make those policies part of the live copy of the policy set. Publishing copies the working copy of the policies over to the live copy.

See also Policy; Live copy of policies; and Working copy of policies.

Resume

Return an ACE instance to operation from its suspended state. When you resume a suspended instance, all applications are in the same state they were when the instance was suspended.

See also Suspend.

Snapshot

A snapshot preserves the ACE instance (or ACE master) just as it was when you took the snapshot—the state of the data on all the ACE instance's disks and whether the instance was powered on, powered off or suspended.

Standalone ACE instance

An ACE instance that is not managed by an ACE 2 Management Server. Any changes to its policies or other settings are made by the administrator's distribution of updates to the user.

Suspend

Save the current state of a running ACE instance. To return a suspended ACE instance to operation, use the resume feature.
See also Resume.

Virtual disk

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 an ACE master 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. The managed virtual machine that has policies and other settings associated with it is known as an ACE instance.
See also ACE instances.

Virtual machine configuration

The specification of what virtual devices (disks, memory size, etc.) are present in a virtual machine (an ACE instance) and how they are mapped to host files and devices.

Virtual machine configuration file

A file, with file extension .vmx, containing an ACE instance configuration. It is used by VMware Player to identify and run a specific ACE instance. An ACE master's configuration file has the file extension `.vmxa`.
See also ACE instances; ACE master.

Virtual machine settings editor

A point-and-click editor used to view and modify the virtual machine settings of an ACE master. You can launch it from the **VM** menu.
See also New ACE Master Wizard.

Virtual Network Editor

A point-and-click editor used to view and modify the networking settings for the virtual networks created by ACE 2. You can launch it from the **Edit** menu.

.vmxa

The file extension for an ACE master configuration file.

VMware Player
A simple application that allows an user to run an ACE instance.

Workstation ACE Edition
The program used by the administrator to create and deploy and update ACE packages and manage ACE instances. Formerly named "VMware ACE Manager."

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 page, 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 ACE instance is running.

Working copy of policies
The policy that the ACE administrator uses to make and try out policy changes. For managed ACE masters, the working copy contains "unpublished" policies. For standalone masters, the working copy contains policies that have not yet been packaged or distributed. Manipulating the working copy for a managed ACE master does not affect any existing instances associated with that master.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Updates for the VMware ACE Administrator's Manual

VMware ACE 2

Last Updated: October 19, 2007

This document provides updates to the VMware ACE 2.0.2 version of the *VMware ACE Administrator's Manual*. Updated descriptions, procedures, and graphics are organized by page number so you can easily locate the areas of the guide that have changes. If the change spans multiple sequential pages, this document provides the starting page number only.

The following is a list of *VMware ACE Administrator's Manual* page updates in this document:

Updates for Running a Pocket ACE Instance

The procedure for closing a Pocket ACE, described in "Running the Pocket ACE Instance" on page 213, has changed. You can now select the behavior you want when you close a Pocket ACE.

To set your Pocket ACE close behavior

1 Choose **Edit Policies > Runtime Preferences**.

2 In the Pocket ACE section of the Runtime Preferences dialog box, select from the following options:

- Let the user choose

  When closing ACE, you will be given the opportunity to choose from the following options:

  - Shut down and synchronize
  - Suspend and stay connected to this computer
  - Show advanced options (Suspend and synchronize, Revert to last sync)
- Always synchronize changes (Requires power off on exit)

  When you select this option, the virtual machine powers off and synchronizes any changes to the device where the virtual machine is stored. The exit behavior automatically becomes "Power off the ACE instance."

- Do not synchronize changes (ACE remains linked to the host)

  When you select this option, your virtual machine is suspended or powers off depending upon the user preferences. No synchronization occurs. To return to the state of the Pocket ACE when it was closed, you must open the virtual machine on the same computer. If you open the virtual machine on another computer, you have the option to revert to the last synchronized state.

- Always discard changes (Requires power off on exit)

  When you select this option, no synchronization occurs and any changes made to the virtual machine are discarded. The exit behavior automatically becomes "Power off the ACE instance."

In addition, if you are using a virtual machine and you encounter a policy violation, the virtual machine is suspended and adheres to the configured Pocket ACE closure policy.