vmware®

VMware® ACE

Best Practices for Setting Up VMware ACE 2.0 Enterprise Edition

This technical note explains how to set up VMware Workstation with ACE option pack to most efficiently create and manage ACE masters.

Note: The guidelines in this document are general in nature. VMware ACE 2.0 Enterprise Edition is a powerful and flexible product. By no means does this document explain every detail of setting up and using it. Nor is there any guarantee that the recommended practices and settings described here make sense for your particular environment. Always refer to the *VMware ACE Administrator's Manual* if you have questions or for more detailed information on any aspect of VMware ACE 2.0 Enterprise Edition.

This document contains the following topics:

About VMware ACE 2.0 Enterprise Edition

VMware ACE 2.0 Enterprise Edition extends virtual machine technology to address security issues in a networked computing environment. VMware ACE 2.0 Enterprise Edition enables you to apply corporate IT policies to a virtual machine containing an operating system, enterprise applications, and data to create a secure, isolated PC environment known as an "ACE virtual machine."

A primary of advantage of using VMware ACE 2.0 Enterprise Edition is that you create a standard, self-policing PC environment for your users. This means:

- Users can run standard PC applications without modification.
- Users can connect to the corporate network with standard networking protocols.

- Users can work whether connected to the corporate network or not; when the user is not connected, IT policies, such as authentication and access to devices and networks, are still enforced.

With VMware ACE 2.0 Enterprise Edition, you create a virtual machine master, or template, and apply a set of Virtual Rights Management policies to it. From the ACE master, you can create any number of ACE virtual machines to deploy to users. Policies enable you to:

- **Protect data and control access**— Protect data on the ACE virtual machine through encryption and control access through password and directory service authentication; restrict the location from which the virtual machine may be run.
- **Protect the integrity of the ACE virtual machine** — Verify that the ACE virtual machine's resource files have not been tampered with.
- **Control the life-cycle of a virtual machine**— Set an expiration date, after which the ACE virtual machine is disabled. For example, you can limit guest workers to the length of a contract, or reclaim licenses that have expired.
- **Enforce updates** — Determine how often a virtual machine needs to check the server for updated policies and how long it can run without connecting to the server.
- **Provide troubleshooting capabilities** — Enable users to request help for specific problems and allow an administrator to access a user's machine.
- **Control network access** — Restrict the networks that the ACE virtual machine or host can access. For example, you can require that the ACE virtual machine connect to the corporate network through a VPN server only and restrict the host machine from any access to the corporate network.
- **Control device access** — Restrict access of the ACE virtual machine to some or all of the host's devices, such as CD-ROM/DVD, floppy and USB drives, to create a totally isolated environment.

After you create an ACE master, set policies, and install software, you create an installable package. You can easily supply the newly created package to employees, contractors or business partners as needed for them to install ACE virtual machines. ACE virtual machines are of two types, managed and standalone.

Managed ACE

Managed virtual machines require connection to the ACE Management Server. The ACE Management Server allows you to manage ACE virtual machines, to dynamically publish policy changes for those virtual machines, 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 access and secure SSL communication.

You can deploy the ACE Management Server in either of two ways:

- Install it manually on an existing physical or virtual Windows or Linux host machine.
- Deploy the ACE Management Server appliance, which you can run from the VMware Workstation ACE Edition administrator console, or which you can deploy to a VMware Server environment.

The ACE Management Server provides a view that allows an administrator to see all managed ACE virtual machines and to make policy updates as desired.

Standalone ACE

A standalone virtual machine does not require access to a management server to run. Its policies take effect when the package is installed and the virtual machine is activated. If IT policies change, or if particular users need to change policies, you can easily create a new set of policies and distribute an update package with the new policies to your end users.

Basic Terminology

The following terms are important in the context of this document:

Guest operating system — An operating system that runs inside an ACE virtual machine.

Host computer (or machine) — The physical computer on which the VMware ACE 2.0 Enterprise Edition software is installed. It hosts ACE virtual machines. The operating system on a host machine is referred to as the host operating system.

Virtual Rights Management policies — Policies control the capabilities of an ACE virtual machine. You set policies by using the policy editor in VMware Workstation ACE Edition.

Network quarantine policy A policy that controls the access of an ACE virtual machine to networks and machines. Network quarantine policies can be either static or dynamic. A static policy is installed with the ACE virtual machine and cannot be updated except by updating the entire virtual machine. A dynamic policy resides on a Web server or on an Active Directory server, and can be updated as necessary without updating the ACE virtual machine.

ACE master A virtual machine template created by an ACE administrator that can be configured with various policies, devices, and package settings and then used as the basis for creating any number of packages to be sent to ACE users.

ACE Virtual Machine The virtual machine that ACE administrators create, associate to virtual rights management (VRM) policies, and then package for deployment to users.

Standalone ACE An ACE virtual machine that is not managed by an ACE Management Server.

Managed ACE An ACE virtual machine that is managed by an ACE Management Server. The server may or may not be integrated with Active Directory.

Prerequisites for VMware Workstation ACE Edition

This section discusses some general guidelines to keep in mind when you install and use VMware Workstation ACE Edition. For more detailed information about requirements for ACE, see Appendix — Requirements for VMware Workstation ACE Edition on page 29.

What You Need

To complete the procedures in this document requires the following:

- VMware Workstation ACE Edition
- System software to install on the ACE master
- Any software applications required by end users of the ACE virtual machine
- A network share to use for creating and storing ACE virtual machines, masters, and packages

Before starting the step-by-step procedures in this document, make certain you have the *VMware ACE Administrator's Manual* available.

Managing Files and Folders

You need to provide adequate disk space for two types of files that you create with VMware Workstation ACE Edition:

- **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.

  It is recommended that you create virtual machine files on a network share where they are accessible to other VMware Workstation ACE Edition users.

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

  In addition, VMware 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 Create Package Wizard displays information about the amount of space needed and the locations where the space is needed. If you do not have enough free space, the wizard displays an error message. You may move or delete files on the target drives to make room for the wizard's working files.

Installing an ACE Management Server

When you create an ACE master, you may specify whether to manage it with an ACE Management Server or not. Using an ACE Management Server is optional, but highly recommended. An ACE Management Server provides a number of ways to manage ACE virtual machines in real time, such as:

- Managing activation of ACE packages (determine who can deploy a package)
- Managing authentication of those activated packages (determine who can run managed ACE virtual machines)
- Dynamically delivering policy updates to managed ACE virtual machines
- Dynamically delivering virtual machine customization data for managed ACE virtual machines with Windows guest operating systems

If you plan to create managed virtual machines, you must first install an ACE Management Server before running the New Master Wizard. The New Master Wizard requires you to identify the ACE Management Server for the new ACE master.

You may install the ACE Management Server to an existing Windows or Linux physical or virtual host, or deploy the ACE Management Server appliance, which is a pre-built, pre-configured and ready-to-run software application packaged inside a virtual machine. The ACE management server can be hosted on a VMserver system with-in your enterprise.

Note: ACE Masters are tied to the specific IP address of their ACE Management Server. When a managed virtual machine powers on, it must find its ACE Management Server — otherwise, it cannot power on. Moving an ACE Master to a different Management Server is a

complicated and time-consuming process, so it is recommended that you install the ACE Management Server with a static IP address on a server that is always available. For example, if you have a round-robin server arrangement, install the ACE Management Server on the load-balancing server.

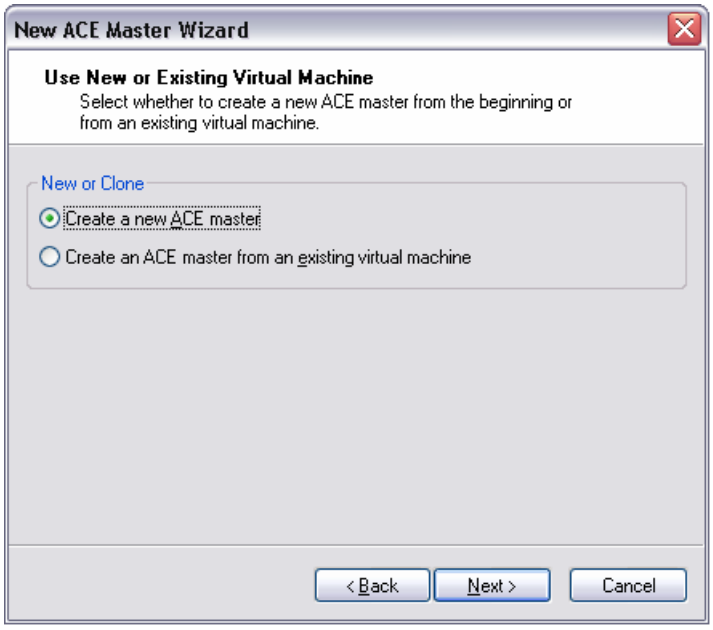
See the *VMware ACE Administrator's Manual* for information on installing and configuring an ACE Management Server.

Creating an ACE Master

In VMware Workstation ACE Edition, you create an ACE master that you can configure with various policy, device, and package settings. You can then use the master to create packages to install ACE virtual machines on host machines. In addition to creating an ACE master from scratch, you can create an ACE master from an existing virtual machine or you can clone an existing ACE master. This section assumes you are creating a new ACE master from scratch.

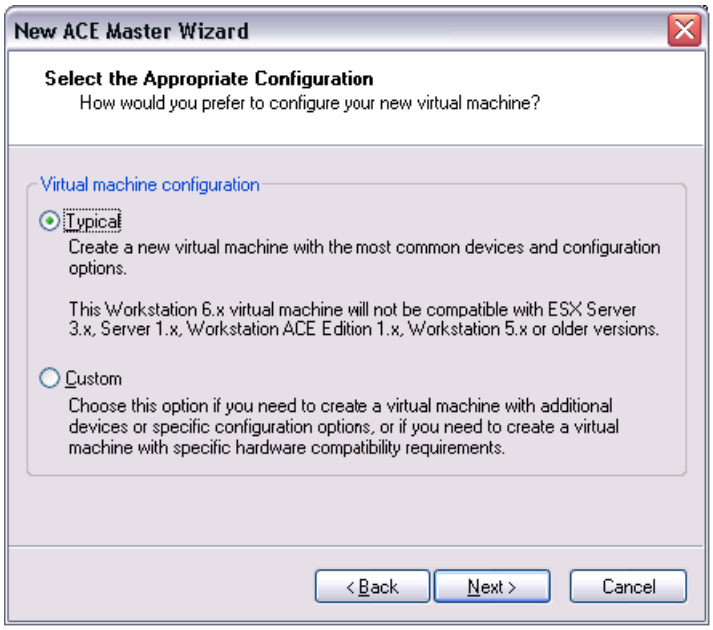
To create an ACE master, run VMware Workstation ACE Edition and complete the following steps:

1. Click File > New > ACE Master to start the New ACE Master Wizard.
2. Click Next to enter the wizard. The Use New or Existing Virtual Machine panel appears.
3. Select Create a new ACE master and click Next.



4. The Select the Appropriate Configuration panel appears.

Select Typical and then click Next.

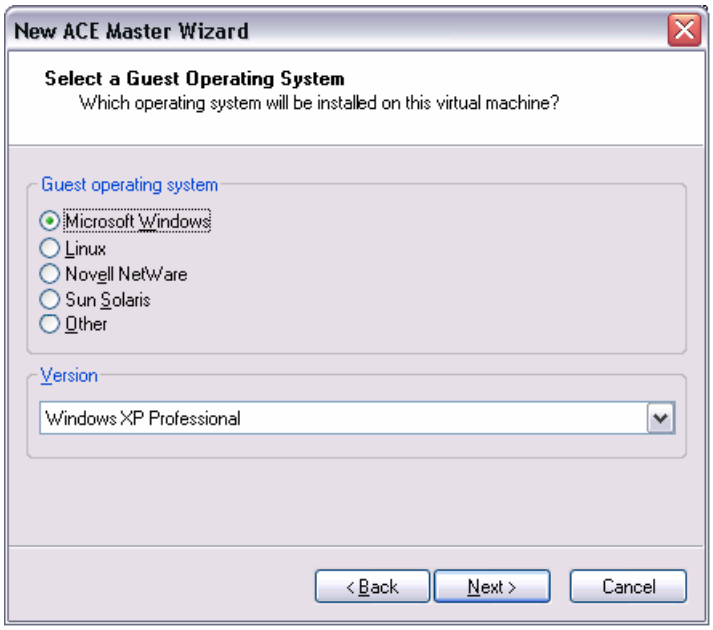


Select Custom only if you want to do any of the following:

- Make a different version of a virtual machine than what is specified in the preferences editor (choose Edit > Preferences, select the Workstation tab, 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.
- Use a physical disk rather than a virtual disk (for expert users).
- 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.

See the *VMware ACE Administrator's Manual* for more information.

5. Select a guest operating system.

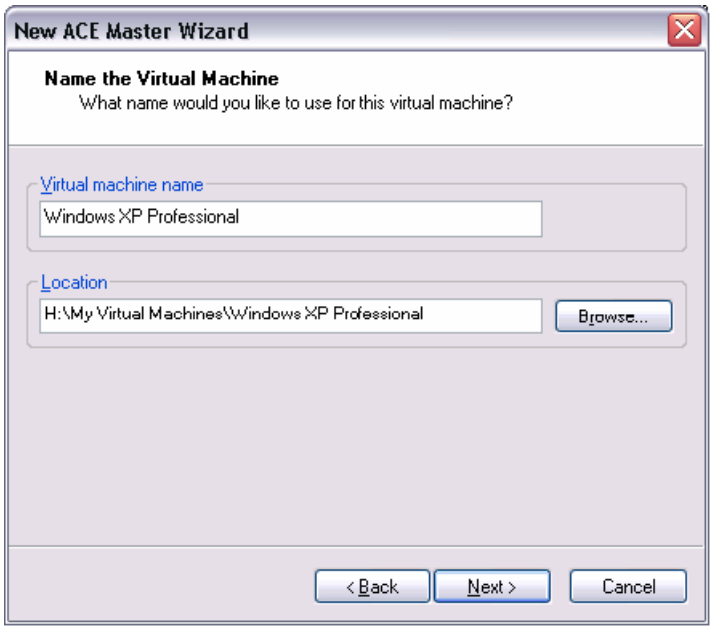


This panel asks which operating system you plan to install in the virtual machine. Select both an operating system and a version.

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

If the operating system you plan to use is not listed, select Other for both guest operating system and version. The rest of this procedure assumes you selected Microsoft Windows.

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

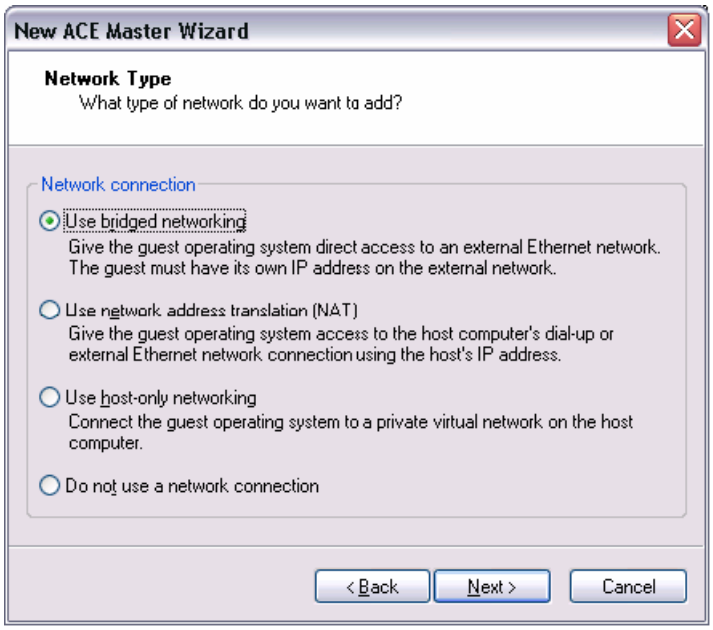


The name specified here is used as the name of the folder where the files associated with this virtual machine are stored.

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

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

7. Configure the networking capabilities of the virtual machine.



The default setting, Use network address translation (NAT), is generally the safest option because you may not be certain if your end users' networks can provide a separate IP address to the virtual machine. For example, many home cable modems use a static IP address instead of a DHCP server, and do not provide the virtual machine with its own IP address. NAT is more likely to work in all situations.

On the other hand, if the package is to be installed on a host computer that is on a network and a separate IP address is available for the virtual machine (or it can get one automatically from a DHCP server), select Use bridged networking. This setting is most likely to be appropriate if the package is to be installed on a computer connected to an office network. If you are planning to use advanced network quarantine settings to set host quarantine policies, use bridged networking.

Select Use host-only networking to connect the guest operating system to a virtual private network on the host computer, which generally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the same network.

You may also choose to provide no network access to the virtual machine by selecting Do not use a network connection.

Note: After you add the virtual machine, you can still change the selection at any time, if necessary, before you create the package to distribute to end users.

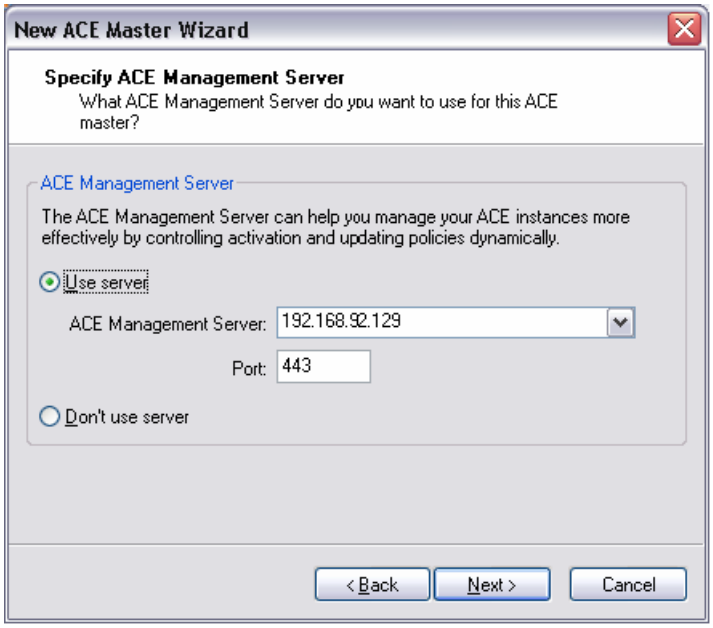
8. Specify the capacity of the virtual disk.

The default setting for disk capacity is 8 GB, which is generally too small for corporate environments. It is difficult to add hard disk space after the virtual machine package is deployed — you must redeploy the entire virtual machine — so you should choose a large capacity now, such as 80GB, to be certain that the virtual machine does not run out of hard disk space.

Caution: Do not check the option: Allocate all disk space now. Doing so provides a small performance improvement but creates massively large files. When you leave this option unchecked, the disk starts small and grows to the specified capacity over time. If an end user's computer does not have the specified capacity, the disk grows until the computer's hard drive is full.

Check the option: Split the disk into 2 GB files. This improves the performance of package creation and installation.

9. Specify an ACE Management Server to use.



Using an ACE Management Server is optional, but highly recommended. See Installing an ACE Management Server on page 4 for some reasons to use a management server. For information on setting up and using an ACE Management Server, see *VMware ACE Administrator's Manual*.

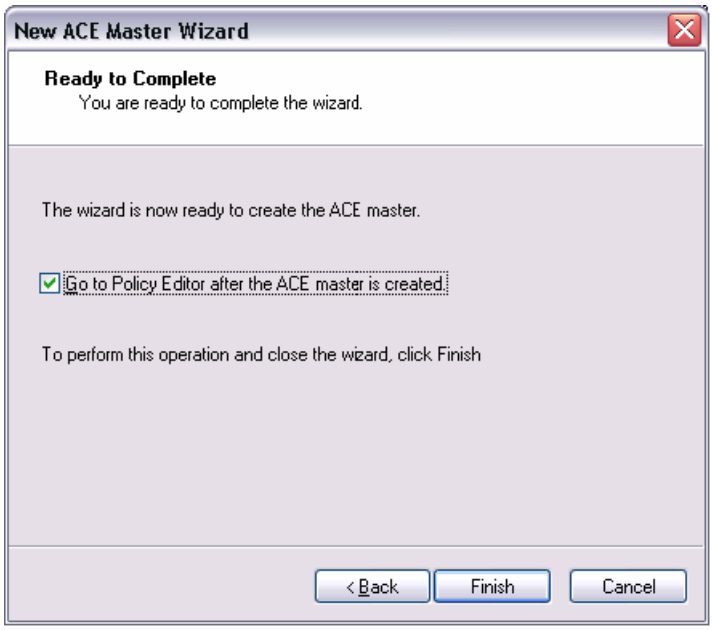
To specify an ACE Management Server, select Use server and enter the name or IP address that you assigned to your server earlier.

If you do not plan to use an ACE Management Server, select Don't use server.

10. The ACE master attempts to connect to the ACE Management Server and when successful, prompts you for a password.

Enter the password you configured earlier and press OK.

11. Click Finish to create the virtual machine. You can leave the option Go to Policy Editor after the ACE master is created checked.



Restricting Access to an ACE Virtual Machine

This document discusses many different aspects of creating and configuring an ACE master, including configuring the virtual hardware and using policies for a variety of reasons. However, the basic function of an ACE virtual machine is to provide a secure computing environment. WIth that in mind, this section serves as a checklist of the policies and other settings that you should use to restrict access to an ACE virtual machine.

Do the following to restrict access to an ACE virtual machine:

- Disable drag and drop and copy and paste between the ACE virtual machine and the host machine; see Setting Configuration Options on page 12.
- Do not create any shared folders for the ACE virtual machine; see Setting Configuration Options on page 12.
- Enable encryption for the package containing the ACE master and for the ACE virtual machine to be installed by the package; see Setting Encryption Policies on page 27.
- Block access to USB devices of class mass storage, other, and unknown; see Setting Removable Devices Policies on page 23.
- Disable network access; see Setting Network Access Policies on page 25

Configuring the Virtual Hardware

The following sections guide you through the steps to configure the hardware for the virtual machine.

Specifying the Memory

To edit the memory setting, click Edit virtual machine settings in the Commands panel, or double-click Memory in the Devices panel. The Memory panel appears.

If you specified Typical when you created the virtual machine, VMware Workstation ACE Edition calculates the amount of memory to allocate based on the amount of RAM on the computer on which you are running VMware Workstation ACE Edition. The panel shows the minimum, recommended, and maximum effective settings. You can accept this amount or use the slider or arrow keys to adjust the amount. You must specify the size in multiples of 4MB.

Select the option Allow automatic adjustment of memory size. When you power on the virtual machine, the VMware ACE 2.0 Enterprise Edition application automatically decreases the amount of RAM used by the virtual machine, if necessary, to fit the amount of free RAM available on the host machine. If you do not specify this option, the machine does not power on if the amount of available RAM on the host machine is below the specified minimum.

When you are finished specifying memory, go to the next section.

Adding Devices

Add all the devices you think end users may need because it is difficult to add devices after the virtual machine has been deployed. Also, if you use the same virtual machine for multiple groups that have different device needs, you don't want to be continually editing devices in the Settings panel.

VMware Workstation ACE Edition adds a number of devices by default. Be certain the Devices panel is still open — if not, click Edit virtual machine settings in the Commands panel. Select each device in turn and unselect the Connect at power on option in the Device status panel. To add a device, click Add and choose the type of device to add. For each device. unselect the Connect at power on option.

If you want to restrict the virtual machine from access to devices on the host machine, you can use policies to take away access privileges for each device. See Setting Removable Devices Policies on page 23.

When you are finished adding devices, go to the next section.

Setting Configuration Options

Shared folders enable an end user to share files between a virtual machine and the host machine. To enhance security, you should disable this feature.

To disable shared folders, if the Devices panel is still open, click the Options tab. If it is not open, click VM > Settings > Options and click Shared Folders.

Select Disable Shared Folders. Click OK to disable shared folders and accept the other device settings you made, and exit the Settings editor.

To disable drag and drop and copy and paste between the ACE virtual machine and a host machine, select Guest Isolation.

Clear the settings:

- Enable drag and drop to and from this virtual machine
- Enable copy and paste to and from this virtual machine

Using ACE Masters

VMware ACE 2.0 Enterprise Edition manages policies through ACE masters. If you have different groups of users that require different policies, create a separate master for each group.

For example, employees with desktop machines (who by definition work onsite), guest workers with laptop machines (who work on site as well as off site), and contract employees, who work off site, require completely different network quarantine policies. You could create three ACE masters, Employees, Guests, and Contractors, to manage these groups of workers.

An end user may have more than one virtual machine installed on the host machine, but all of these virtual machines must come from the same ACE master.

Setting Policies for the ACE Master

Policies are at the heart of managing virtual machines. The following sections describe policies you should set for the ACE Master:

Set the following policies to manage ACE virtual machines and to make it easier for end users to request troubleshooting assistance, and to set up their environment:

- Responding to Help Requests on page 13 explains how to enable users to request help and administrators to respond for standalone and managed ACE virtual machines.
- Setting Administrator Mode on page 15 explains how to create an administrative password that enables you to work at an end user's host machine and modify the configuration of the virtual machine, or fix a number of specific problems, such as resetting the user's password so they can run the virtual machine.
- Setting Policy Update Frequency Policies on page 16 explains how to set policies that determine how often a managed ACE virtual machine must connect to the ACE Management Server to download policy updates, and how long it is available for use without connecting to the server.
- Setting Expiration Policies on page 18 describes how to use expiration policies to track which users are installing your VMware ACE 2.0 Enterprise Edition packages.

Set the following policies to protect the integrity of ACE packages and virtual machines and to control user access and access to data on ACE virtual machines:

- Setting Resource Signing Policies on page 18 describes policies that verify that the ACE virtual machine resource files have not been tampered with.
- Setting Copy Protection Policies on page 19 describes policies that ensure the ACE virtual machine only runs from the location in which it is installed.
- Setting Access Control Policies on page 20 describes policies that enable you to secure the data and the virtual machine itself through encryption and password protection. When you password-protect a virtual machine, you should also enable a recovery key and hot fixes in case the end user forgets the password.
- Setting Removable Devices Policies on page 23 describes how to set device policies that restrict access for the virtual machine to the host's devices such as DVD/CD-ROM, floppy and so on. This prevents data on the virtual machine from being exposed when the host machine is outside the corporate network.
- Setting Network Access Policies on page 25 describes some of the uses of network quarantine policies and contains links to other documents that describe specific use cases for network quarantine policies.

Responding to Help Requests

For standalone ACE virtual machines, hot fixes allow users to request help and administrators to respond. See Enabling Hot Fixes for the VMware ACE 2.0 Enterprise Edition Application.

For managed ACE virtual machines, administrators may use the Help Desk application to view virtual machines and respond to requests by ACE users. See Using the Help Desk on page 15.

Enabling Hot Fixes for the VMware ACE 2.0 Enterprise Edition Application

Hot fixes make it easy for users of standalone ACE virtual machines to request help and for an administrator to respond to the request. A user who cannot access a virtual machine for any of the following reasons can request a hot fix to solve the problem:

- Forgotten password.
- The expiration date has passed.
- Trying to run a copy-protected machine from a different location.

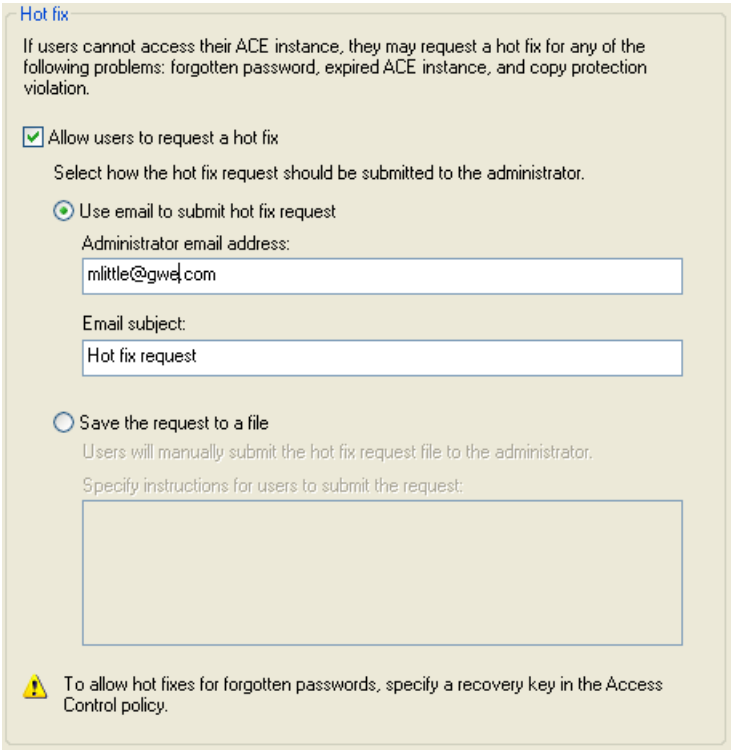
For hot fixes to be available, you must enable them for the ACE virtual machine that runs on a user's host machine. When hot fixes are enabled, a user can use the Hot Fix Request Wizard to generate a hot fix request file that can be sent to the ACE administrator. The ACE administrator, in turn, can respond to the request by opening the hot fix file in VMware Workstation ACE Edition and taking the appropriate action, such as extending the expiration date.

To enable hot fixes:

1. In VMware Workstation ACE Edition, select the ACE master and click ACE > Policies.

   The Policies panel appears. Select Hot Fix.

2. The Hot Fix panel appears.



   Select Allow users to request a hot fix.

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

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

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

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

You must enable recovery on each virtual machine if you want end users to be able to request hot fixes for a forgotten password on that machine. See Setting Access Control Policies on page 20.

3. Click OK to set the hot fix policy you have specified.

When you are finished, go to the next section.

Using the Help Desk

The Help Desk Web application allows help desk assistants or administrators to view ACE virtual machines that are managed by a particular VMware ACE Management Server and to provide some fixes requested by users of those virtual machines.

Help desk assistants can access the ACE virtual machine through the Help Desk Web application and can fix ACE virtual machine problems, such as reactivating a virtual machine, changing the virtual machine's expiration date, or resetting the user password if the user has lost or forgotten it.

Unlike Hot Fixes, which you must configure with a policy, the Help Desk requires no policy settings. However, you do need to set up a password for a help desk assistant in the ACE Management Server Setup. See the *VMware ACE Administrator's Manual* for details.

To access the Help Desk application:

- On Windows: Choose Start > All Programs >VMware > VMware ACE Management Server > Helpdesk.
- On Linux: Open a browser and point it to `https://<hostname>:8000`. Click the Helpdesk link on the page.

You can integrate the Help Desk with Active Directory to support role-based access. For example, you can create a Help Desk role that permits specific users to perform tasks from within the Help Desk application but does not give them access to other administrative tools.

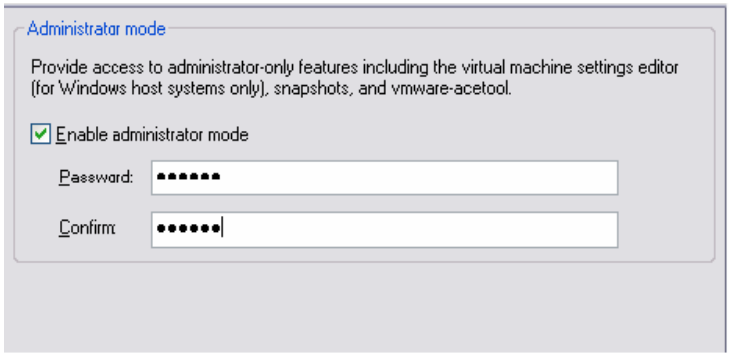
Setting Administrator Mode

The administrator mode policy allows you to set an administrator password so you can work at an end user's computer and run the ACE virtual machine in a special troubleshooting application. When you enable administrator mode, you can do the following:

- Run the ACE virtual machine on a user's machine and enter administrator mode to make changes to the virtual machine's configuration. Note that you can only do this on Window's machines and you can only edit settings; you cannot add or remove devices.
- Run the ACE virtual machine on a user's machine and enter administrator mode to access all the snapshot commands.
- Run the ACE-Tools command-line program on an ACE user's system to fix any of the following problems:
  - Set the user's password so the user can run the ACE virtual machine.
  - Set copy protection so the user can run the ACE virtual machine in a new location.
  - Set the expiration date so the user can continue to use an ACE virtual machine that has reached its scheduled expiration date.

To set administrator mode:

1. In VMware Workstation ACE Edition, select the ACE master and open the policies editor (click ACE > Policies), then select Administrator Mode.



2. Select the Enable administrator mode option.
3. Enter and confirm a password.

   Be certain to record the password in a safe place.

When you are finished, go to the next section.

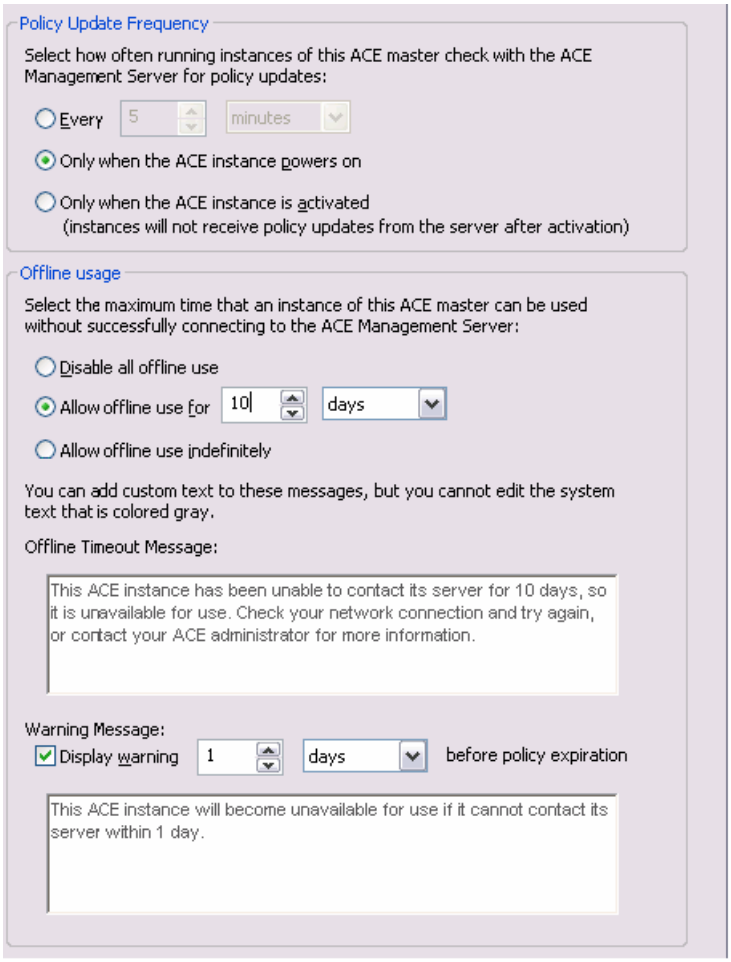
Setting Policy Update Frequency Policies

This policy only applies to managed virtual machines. You can use this policy to specify:

- Policy update frequency — How often a managed ACE virtual machine must connect to the ACE Management Server to download policy updates while it is running.
- Offline usage — How long a managed ACE virtual machine is available for use without connecting to the ACE Management Server.

To set policy update frequency policies:

1. In VMware Workstation ACE Edition, select the ACE master and open the policies editor (click ACE > Policies), then select Policy Update Frequency.



2. In Policy Update Frequency, select one of:
   - Every *x time_unit*. and specify the number of minutes, hours, or days that the ACE unit can run before it must connect to the server to retrieve any updated policies.
   - Only when the ACE virtual machine powers on to connect the virtual machine to the server at power-on to retrieve any updated policies.

   Do not select Only when the ACE virtual machine is activated unless you do not need to have contact with the ACE virtual machine after it has been created.
3. In Offline Usage, select one of:
   - Allow offline use for *x time_unit*. and specify the number of minutes, hours, or days that the ACE virtual machine is available for use before it must connect to the server to check for policy updates. This is the recommended setting because it forces the virtual machine to look for policy updates while allowing it to run in case the server is unavailable for any reason.

- Disable all offline usage. This setting is the most restrictive in that it forces virtual machines to be connected at all times to the server. This policy provides maximum control for enforcing policy updates but does not take into account that the management server could be down, effectively disabling all ACE virtual machines that depend on it for updates.

Do not select Allow offline use indefinitely if you want to force ACE virtual machines to update policies as you make them available on the server.

Setting Expiration Policies

Typically, you use expiration policies to limit the lifetime of a virtual machine. For example, you can provide a computing environment for a contractor and limit its use to the duration of the contract; or you can set a virtual machine to expire to provide a time-limited demonstration to potential customers.

When a virtual machine expires, the files remain on the end user's computer but the virtual machine cannot be used.

For a standalone ACE instance, the expiration date is fixed at activation time. Each time the user powers on the instance, the date or date range is checked, and if beyond the date or outside the range, the instance cannot be powered on. Expiration checks are also performed while the instance is running, and if expiration is reached, the expiration message appears and the instance is suspended.

For a managed ACE instance, the expiration policy works similarly, but the expiration policy value can be specified on a per instance basis (using Instance View on the ACE Management Server), 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.

To set an expiration date for the virtual machine:

1. Select Expiration from the Policy list.
2. In the policy editor, select one of the following options for expiration:
   - After *x* days from activation — The virtual machine runs for the specified number of days after the package is installed, then cannot be used. Consider this option for such uses as time-limited demonstrations.
   - Valid from *x* to *x* — The virtual machine can be run between the specified dates. It cannot be used before or after the specified dates. Consider this option for such uses as computing environments for contractors.
3. For a machine that is set to expire, you may optionally change the warning and expiration messages, as well as specify at which point a warning message is displayed when the virtual machine is powered on.

Setting Resource Signing Policies

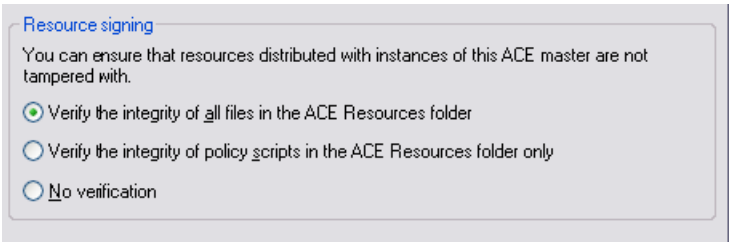
You can set the resource signing policy so that an ACE virtual machine cannot be run if resource files, such as policy scripts or custom EULA text files, have been tampered with.

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 end user's machine are not *resources* in this sense and are not signature-checked.)

Signature checking is performed, on the end user's machine, at power on and then every time a script is run.

To set resource signing policies:

1. Select the ACE master and click ACE > Policies > Resource Signing.



2. For the maximum level of protection, leave the default selected, Verify the integrity of all files in the ACE Resources folder.

   Note: 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.

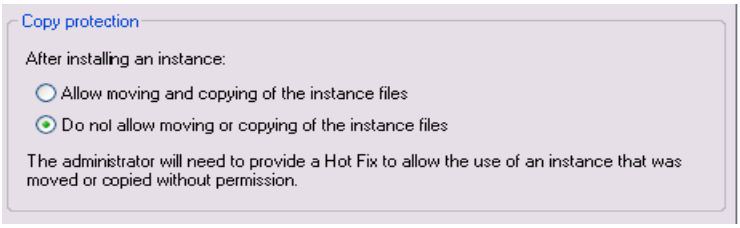
Setting Copy Protection Policies

Copy protection policies let you ensure that an ACE virtual machine can run only from the location in which it was installed.

To set copy protect policies:

1. Select the ACE master and click ACE > Policies > Copy Protection.
2. For a standalone virtual machine, select Copy protect instances of this ACE master.

   The virtual machine may only be run from the location in which it is installed.
3. For a managed virtual machine, the default setting, which provides the highest level of protection, is to clear both of the following options:
   - Do not allowing moving or copying of the instance files



   Copy protection policies are dynamic for a managed virtual machine. You can toggle the settings so that moved or copied virtual machines will run or not run.

   With the default settings, if the user moves or copies the virtual machine and tries to run it from the new location, VMware Player displays an error message 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 to request permission to move or copy the virtual machine.

Administrators and help desk assistants can then reset the copy protection ID if they choose, allowing the moved or copied virtual machine 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 the *VMware ACE Administrator's Manual* for more information about instance view and the Help Desk Web application.

Setting Access Control Policies

Access control policies have two parts:

- Activation policies allow you to control access to installed ACE packages so the ACE virtual machine is protected while it is in transit to the end user. You can require a password to activate a virtual machine.
- Authentication policies allow you to control access to ACE virtual machines created from the installation packages.

To set access control policies:

1. Start the policy editor (select the ACE master and click ACE > Policies; or under Policies, click Edit policies).
2. Select Access Control

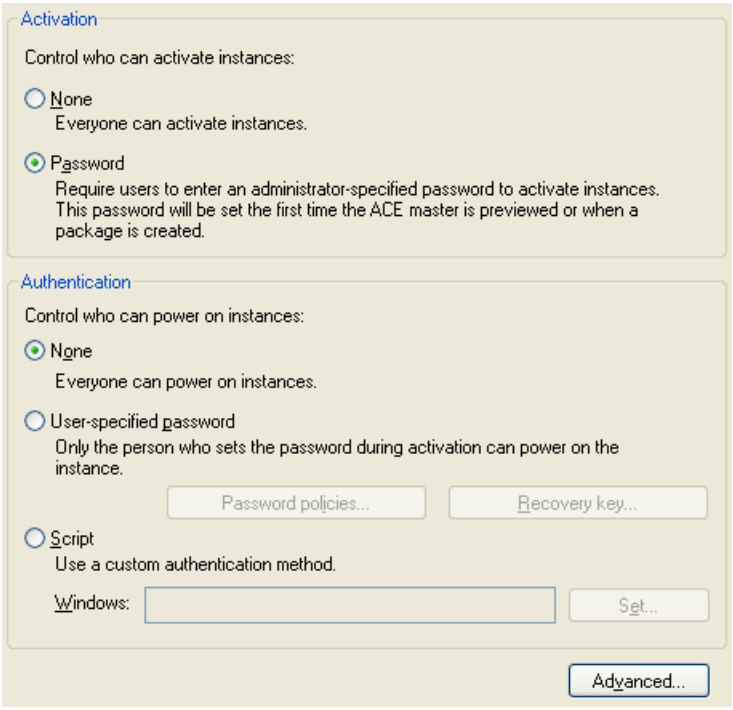
   Setting activation and authentication packages is different depending on the type of virtual machine you are creating:

   - Standalone virtual machine
   - Managed virtual machine integrated with Active Directory
   - Managed virtual machine not integrated with Active Directory

   For any type, click Help for more information.

Setting Access Control for a Standalone Virtual Machine

To set access policies for a standalone virtual machine, do the following:



- In the Activation section, select Password. A user must know the password in order to activate a virtual machine. You specify a password when you create the package. You must provide the user with the password through email or some other means.
- In the Authentication section, select User-specified password. The virtual machine cannot be run until a user enters the correct password. During activation, at first power-on, a user must set a password. Optionally, you can set policies for the password, such as length and content of the user password by clicking Set Password policies.

  Note: You may also use a script instead of setting a password to determine who can use this virtual machine. Click Help for details.

  When you require a password for activation and authentication, VMware ACE 2.0 Enterprise Edition sets the encryption policy to encrypt the package in transit and the ACE virtual machine when it is installed. It is highly recommended that you accept these encryption policy settings; see See Setting Encryption Policies on page 27.

When you require a password and encrypt the virtual machine, also set a recovery key so you are able to use a hot fix to reset the end user's password.

To set a recovery key:

1. Click Set recovery key.
2. Select Use recovery key to configure a recovery key.
   - To use an existing PEM-format key pair, click Browse for Existing Key to navigate to the public key of the pair you want to use.

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

  Enter a name and location for the key pair. Enter and confirm the password to protect the private key. Then click OK to generate the keys. 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 Public recovery key field on the Recovery Key tab.

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

  Note: You must specify a recovery key before you create the package that includes this virtual machine.

  An end user can send a hot fix request to reset the password if you have specified a hot fix policy for the VMware ACE 2.0 Enterprise Edition application that manages the user's virtual machine. See Responding to Help Requests on page 13.

Setting Access Control for a Managed Virtual Machine with Active Directory

To set access policies for a managed virtual machine integrated with Active Directory, do the following:

- Under Activation and authentication, edit the list of users and groups who can activate and authenticate (run) the virtual machine:

  Click Add to open the Active Directory users and groups dialog box. Select the users and groups who can activate and authenticate the virtual machine.

- Under Allowances, specify how many virtual machines can be activated from this package.

  In Total number of activations, select Maximum of and choose how many virtual machines can be activated from this package.

  By default, a user may activate only one virtual machine per package. Select Allow multiple activations per user to allow any individual user to activate more than one virtual machine.

You may provide additional security by using Active Directory settings, such as specifying password expiration and change requirements.

You can dynamically change the list of users who can run the virtual machine. Changes are effective at the next startup of the virtual machine.

Setting Access Control for a Managed Virtual Machine Without Active Directory

To set access policies for a managed virtual machine that is not integrated with Active Directory, do the following:

- In the Activation section, select one of the following:
  - Administrator-specified password and enter and confirm the password. The user must specify this password to activate the virtual machine when it is installed. Send the password to the user via email or some other means.
  - Activation key and click Set key list to add or import a key. To activate the virtual machine when it is installed, a user must enter a key from the key list.

  Do not select None unless you want to allow anyone to activate the virtual machine when it is installed.

- In the Authentication section, select User-specified password. The virtual machine cannot be run until a user enters the correct password. During activation, at first power-on, a user must set a password. Optionally, you can set policies for the password, such as length and content of the user password by clicking Set Password policies.

  Note: You may also use a script instead of setting a password to determine who can use this virtual machine. Click Help for details.

- In the Allowances section, specify how many virtual machines can be activated from this package.

  In Total number of activations, select Maximum of and choose how many virtual machines can be activated from this package.

  By default, a user may activate only one virtual machine per package. Select Allow multiple activations per user to allow any individual user to activate more than one virtual machine.

The activation and authentication policies for a managed virtual machine (without Active Directory) are dynamic. You can edit the policy, then publish it. When a new virtual machine from the package is installed and activated, the changes to the policy take effect.

Setting Removable Devices Policies

In the section, Adding Devices on page 12, you add devices to the virtual machine.

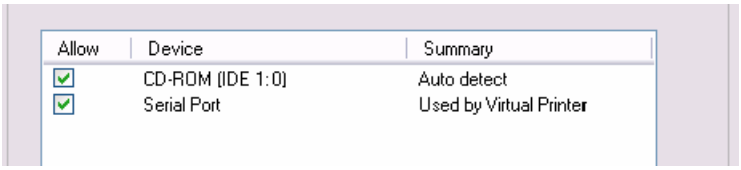
The current section explains how to deny access to any particular device or to all devices. You may want to do this as an added security feature. For example, to prevent data on the virtual machine from being exposed if the host machine is used outside the corporate network.

If you want to restore a device at a later time, you can update the policy to allow a particular user, or any user, to connect the device. A user can connect a device by using the VMware ACE 2.0 Enterprise Edition instance installed on the host.

To remove access to devices, take these steps in VMware Workstation ACE Edition with the ACE master powered off. Note that VMware Workstation ACE Edition provides separate policies for general devices, such as CD-ROMs and Floppy disks, and for USB devices:

1. Start the policy editor (select the ACE master and click ACE > Policies; or under Policies, click Edit policies). Then click Removable Devices.

   A list of devices appears in the Removable devices panel.



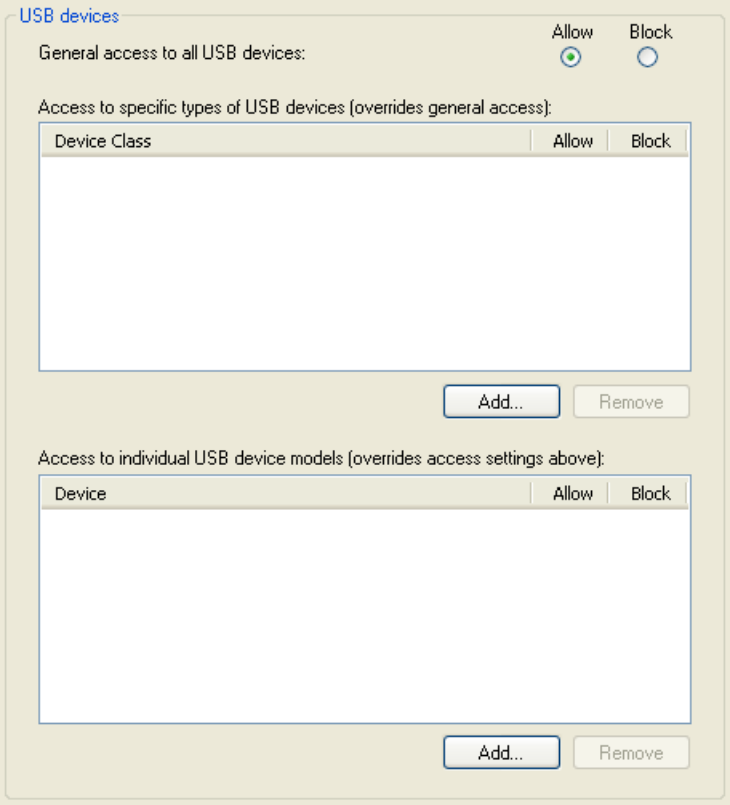
2. Select each device in turn and clear the Allow box to remove access to the device from virtual machines created from this ACE master.
3. In the left pane, select USB Devices, which is a sub-policy of Removable Devices.

   You can set USB device policies to restrict the ACE user's access to USB devices to protect the integrity of ACE virtual machines and your network. The policies are dynamic, so you can allow and then block access to USB devices at will.

   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.

4. In Device Class, click Add.



The USB Device Classes panel appears with a list of device classes.

5. Select the following classes — use the Ctrl key to select multiple classes:

   - Mass Storage
   - Other
   - Unknown

   Then click OK.

   For each device, select Block.

6. For Default for other device classes, select Allow.

Setting Network Access Policies

Network access policies give you fine-grained control over the network access you provide to users of your virtual machines.

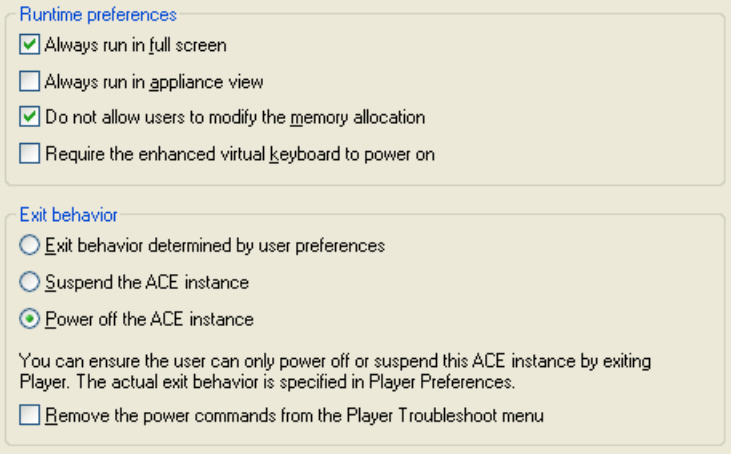
The network access feature of VMware ACE 2.0 Enterprise Edition, which uses a bi-directional packet filtering firewall, lets you specify exactly which machines or subnets a virtual machine may access. The current document does not describe how to use network quarantine polices.

Network quarantine has a number of specific uses, which are described in the following VMware ACE 2.0 Enterprise Edition white papers, available at *http://www.vmware.com/support/resources/ace_resources.html*:

- "VMware ACE: Managing Remote Access," explains how to use network quarantine and other policies to manage remote access through VPN to a corporate network.
- "VMware ACE: Managing Guest Workers" explains how to use network quarantine and other policies to manage workers who at different times access the corporate network remotely and from within the network.
- "VMware ACE: Enforcing Patch Management" explains how to use version-based network quarantine policies to enforce patch management strategies.

Setting Runtime Preferences Policies

Use the Runtime Preferences policies to provide a user experience that is as close to that of a physical computer as possible.



Set the following policies:

- Full screen — Always run in full screen. The virtual machine runs in full-screen mode and masks the fact that it is running inside a host computer.
- Memory allocation — Do not allow users to modify the memory allocation. This setting prevents users from changing the memory allocation and compromising operation of the ACE virtual machine, or of the host computer.
- Exit behavior — Power off the ACE virtual machine. If you quit VMware Player, the ACE virtual machine powers off — much like a PC that shuts down when you turn off the power. If you do not enable this policy setting, the user has a choice when exiting VMware Player of suspending the virtual machine or running it in the background. The 'Power off' setting more closely emulates the behavior of a physical machine.

Setting Other Policies

You can leave the default option for Snapshots policies.

Caution: The Snapshots option, Revert to the reimage snapshot, enables a powerful feature: the ability of an end user to restore the virtual machine to the state in which it was installed. This destroys any changes the user made to the virtual machine since installation, including data and installed applications. It is recommended that you not select this option unless you provide end users with training in how and when to use the feature.

Packaging an ACE Master

This section describes considerations you need to keep in mind when doing any of the following:

- Previewing an ACE Master
- Preparing an ACE Master for Packaging
- Creating a Package
- Creating an Update Packages

Setting Encryption Policies

A virtual machine that may contain sensitive data is particularly vulnerable on a laptop computer that is used outside the corporate offices. If you know that some end users host virtual machines on laptop computers, it is a good idea to encrypt the virtual machine. By encrypting the virtual machine, you protect the data files even if the computer is lost or stolen.

Encryption is of two types:

- Package encryption — Protects a package from being copied or altered while in transit.
- ACE virtual machine encryption — Protects ACE virtual machine files from being copied or altered. The VMware ACE 2.0 Enterprise Edition installer encrypts the virtual machine's files — including the configuration file and the virtual disk files — when it installs ACE virtual machines on the end user's computer.

The encryption key is different for each package and for each computer.

Encryption is transparent so the end user of the virtual machine does not have to think about it. With access control policies, you require that the end user create a password to be used to run the virtual machine. The Workstation ACE application handles the details of encrypting and decrypting the virtual machine as needed. With every disk access, the virtual machine files are automatically encrypted.

To set encryption policies, select the ACE master and under Package Settings, click Edit package settings. Then click Encryption.

The settings for Package protection and ACE virtual machine protection are automatically set based on the activation and authentication policies you set (see Setting Access Control Policies on page 20). If you specified password protection with the access control policies, the recommended setting defaults to encrypted for package and virtual machine protection. If you change the setting, you can click Restore Recommended Setting to return to the recommended setting.

Previewing an ACE Master

Preview mode allows you to run the ACE virtual machine as it will run on the end user's machine. You can see the effects of changed policies as they will appear on the ACE user's machine as well as 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.

Click the Preview in Player icon in the toolbar to create a preview virtual machine. 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 virtual machine events are the same as those for a standard ACE package deployment: activation of the ACE virtual machine; virtual machine customization (if any); encryption. You can then run the virtual machine, checking for the effects of any changes you made to the ACE master.

Preparing an ACE Master for Packaging

When you wish to preview the policies you have set for an ACE master, you can run it in VMware Workstation ACE Edition to see the virtual machine as end users see it. Click VM > Run in VMware ACE or under Commands, click Run in VMware ACE.

When you are preparing to package a virtual machine by installing an operating system, VMware Tools and application software, it is best not to run the virtual machine in VMware ACE 2.0 Enterprise Edition. Rather, start the virtual machine by clicking Power > Power on, or under Commands by clicking Start this virtual machine.

To prepare the virtual machine for end users:

- Install your standard supported operating system and any updates or service packs. See the "Guest Operating System Installation Guide" at *http://www.vmware.com/support/resources/ace_resources.html*.
- Install VMware Tools in the virtual machine. Installation varies between operating systems. To prepare VMware Tools for installation, in VMware Workstation ACE Edition, power on the virtual machine and click VM < Install VMware Tools. See the *VMware ACE Administrator's Manual* for detailed instructions on the rest of the steps to take.
- As a local administrator, install the applications your end users require. Customize the desktop and applications as necessary. For example, map network directories such as the update server for patches.

  Note: You want to install the standard applications that you know all end users require. Over time, end users may install any additional applications or application updates that they need.
- Use VMware Tools to shrink the size of the disk, which decreases the size of the package you deploy. In a Windows guest, double-click the VMware Tools icon in the system tray. In a Linux or FreeBSD guest, run `vmware-toolbox`. Click the Shrink tab. Select the virtual disks you want to shrink, then click Prepare to Shrink.

  Shrinking disks may take considerable time.
- If you are deploying a Windows virtual machine to multiple users, set up Sysprep or NewSID in the guest operating system just as you would on a physical computer you intend to clone for a large deployment. Sysprep and NewSID generate a new security identifier (SID) and host name for each virtual machine when it is installed on an end user's machine.
- If you are preparing a virtual machine that needs to join your company domain, take the following additional steps:

  a. Create a list of host names and user names, and add them to the domain.

  b. Use the `sysprep.inf` file to specify the domain to join for the guest operating system.

  c. Provide users the host name and user names to specify when using Sysprep.

  End users must install the package on a host machine in your company network. They must be able to locate the domain controller.

Creating a Package

To create a package you use the New Package Wizard (ACE > New Package), which guides you through the process. For detailed instructions, see the *VMware ACE Administrator's Manual*. This section provides information to keep in mind when creating a package.

You can create and store packages locally or on a network share. In either case, be certain you have adequate free space. VMware Workstation ACE Edition requires several gigabytes of free space when creating a package.

Note: The New Package Wizard displays the amount of space required to create a package and verifies that the specified location has adequate space.

The name of the package is the name that appears in the Add/Remove program list after the end user installs the package. Use a descriptive name that is obviously a VMware ACE 2.0 Enterprise Edition package, such as ACE_WinXP.

Put packages on a network share directory with adequate free space. You may distribute ACE packages in a number of ways, including direct download, through deployment software, or on CDs or DVDs. If you are using deployment software, such as Microsoft® Systems Management Server (SMS), be certain it can browse to the directory where your VMware ACE 2.0 Enterprise Edition packages are saved.

If you plan to use a CD or DVD, make certain the CD/DVD burner can browse to the package directory. If your package spans multiple CDs or DVDs, be sure you label the disks in the correct install order.

Before creating a package, be certain that debugging is turned off. In VMware Workstation ACE Edition, click VM > Settings > Options > Advanced. In Settings, verify that the option Gather debugging information is set to None.

Also, be certain the virtual machine is powered off, not simply suspended. To verify that the virtual machine is off, click Power. If the machine is off, the Power On option is available. If Resume is available, it means the virtual machine is suspended. Click Resume, then shut down the guest operating system, which powers off the virtual machine.

Creating an Update Packages

When creating an update package, you use the New Package Wizard just as you do when you create the original package. However, on the Package Contents panel, select just those items you want to update. For example, if you have updated policies for a virtual machine in the project, select Virtual machine policies for that virtual machine, and unselect everything else. The New Package Wizard creates an update package that contains the policies for the specified virtual machine and nothing else.

Save update packages in the same directory as the original package.

For updates, provide descriptive names with the following types of information:

```
<Company>ACE_<ProjectName>_<Version>_<Date>
```

For example,

```
AcmeACE_Contract1_v2_011505vm
```

Appendix — Requirements for VMware Workstation ACE Edition

This section discusses hardware and operating system guidelines to keep in mind for VMware Workstation ACE Edition, VMware Player, and ACE Management Server.

System Requirements for VMware Workstation ACE Edition

System requirements change over time so be certain to refer to the *VMware ACE Administrator's Manual* for up-to-date and detailed system requirements for installing VMware Workstation ACE Edition.

PC Hardware

- Standard PC

- 1000MHz or faster compatible x86 and x86-64 architecture processor (recommended; 600MHz minimum)

Memory

- Enough memory to run the host operating system, plus memory required for each guest operating system and for applications on the host and guest; see your guest operating system and application documentation for their memory requirements.
- 1GB recommended, 512MB minimum.

Display

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

Disk Drives

- 150MB free space required for basic installation
- At least 1GB free disk space recommended for each guest operating system and the application software used with it; if you use a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer.
- Additional disk space for building packages; temporary files require about as much space as those of the virtual machine included in the package.

Windows Host Operating (Systems 32-bit)

- Windows Server 2003 Web Edition SP1, Windows Server 2003 Standard Edition SP1, Windows Server 2003 Enterprise Edition SP1, Windows Server 2003 Small Business Edition SP1, Windows Server 2003 R2 (Listed versions are also supported with no service pack.)
- Windows XP Professional and Windows XP Home Edition with Service Pack 1 or 2 (Listed versions are also supported with no service pack.)
- Windows 2000 Professional Service Pack 3 or 4, Windows 2000 Server Service Pack 3 or 4, Windows 2000 Advanced Server Service Pack 3 or 4
- Windows Vista

Windows Host Operating (Systems 64-bit)

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

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

System Requirements for VMware Player (end-user client devices)

Hardware Requirements

- Processor speed – 400MHz or faster (500MHz or faster recommended)
- Memory – 512MB recommended, 256MB minimum. 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 – 70MB required for basic installation. At least 1GB free disk space for each guest operating system.

Supported Host Operating Systems
VMware Player is available for both Windows and Linux host operating systems. The requirements for Windows are the same as those for VMware Workstation ACE Edition; see Windows Host Operating (Systems 32-bit) on page 30 and Windows Host Operating (Systems 64-bit) on page 30.

For supported Linux platforms, see the *VMware ACE Administrator's Manual*.

System Requirements for ACE Management Server

Hardware Requirements

- Processor speed – 1200MHz or faster compatible x86 and x86-64 architecture processor (recommended; 800MHz minimum)
- Memory – 1024MB recommended, 256MB minimum
- Hard disk – 40MB free space required for basic installation; at least 10GB free disk space recommended
- Display – 16-bit display adapter recommended; 8-bit display adapter required

Windows Host Operating 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 Management Server running under a Windows 2000 operating system cannot be configured for Active Directory integration.

Linux Host 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 Management Server. In addition, you can use external databases, through ODBC connectivity:

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

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

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

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

Revision 20050207 Item: ACE-ENG-Q105-058