vmware®

VMware® ACE

Managing Remote Access

This technical note explains how to use VMware ACE to manage remote access through VPN to a corporate network.

This document contains the following topics:

This document provides a brief overview of VMware technology in general and of VMware ACE in particular. It assumes that you have some familiarity with virtual technology. Keep the *VMware ACE Administrator's Manual* available for reference.

About Remote Access

Companies are finding that they must provide remote access to corporate resources for a number of different people:

- Employees who work from home on a regular basis
- Employees who require access to resources — such as email and enterprise applications — after regular hours, on weekends or while travelling
- Business partners who need access to specific data, applications or other resources
- Outsourced and off-shore workers

Typically, companies today give employees a laptop computer for home use, and use a virtual private network (VPN) or some type of terminal service to provide those employees with remote access to the corporate network. Laptop machines provide the flexibility of working onsite or remotely, and VPNs provide a secure connection between remote users and the corporate network. However, there are cost and security issues associated with this solution to remote access.

To begin with, laptop machines are expensive, particularly if they are required in addition to desktop machines. Remote machines are also an inherent security risk because the company does not own or manage every computer that has access to the corporate network.

For example, consider the following scenarios:

- A trusted individual logs onto the corporate LAN through VPN using an unmanaged computer that is infected with a virus or other malicious code. The malicious code infects the corporate network after the user connects through VPN.
- A user, connected through VPN, downloads files to a home computer or other unmanaged PC, leaving sensitive data outside the protection of the corporate network. Or a user copies files onto a CD, floppy or USB drive, putting sensitive data at risk outside the corporate network.
- A user, connected to the corporate network through VPN, browses to different Web sites and downloads software. Within the corporate network, browsing and downloading may be restricted, but the remote machine, although connected through VPN, is free to browse without restriction.
- A remote user is using system software without the most up-to-date patches, even though company policy requires that users install the latest operating system patches. It is challenging to enforce policies on machines controlled by the company and impossible to do so on machines outside the company.

With VMware ACE, IT organizations can reduce the cost, and improve manageability and security when providing access to IT resources for remote, unmanaged PCs.

About VMware ACE

VMware ACE extends virtual machine technology to address security issues in a networked computing environment. VMware ACE 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 "assured computing environment".

A primary of advantage of using VMware ACE is that you create a standard, self-policing PC environment for your user. 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 users are not connected, IT policies, such as authentication and access to devices and networks, are still enforced.

With VMware ACE, you create a virtual machine and apply a set of Virtual Rights Management policies to it. Policies include:

- **Encryption and authentication** — Protect data on the virtual machine through encryption and control access through password and directory service authentication.
- **Life cycle control** — Set an expiration date, after which the virtual machine is disabled. For example, you can limit guest workers to the length of a contract, or reclaim licenses that have expired.
- **Network quarantine** — Restrict the networks that the virtual machine or host can access. For example, you can require that the virtual machine connect to the corporate network through a VPN server only and restrict the host machine from any access to the corporate network.
- **Device access** — Restrict the virtual machine access 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 a virtual machine, set desired policies and install any software on the virtual machine, you create an installable package. You can easily supply the newly created virtual machine to employees, contractors or business partners as needed.

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 a virtual machine.

Host computer (or machine) — The physical computer on which the VMware ACE software is installed. It hosts VMware 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 a virtual machine. You set policies by using the policy editor in VMware ACE Manager.

Network quarantine policy — A policy that controls the access of a virtual machine to networks and machines. Network quarantine policies can be either static or dynamic. A static policy is installed with the 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 virtual machine.

Update or patch server — A server containing update patches that you set up and manage with patch management software. Virtual machines can access this server to update their operating environments.

Implementing a Solution with VMware ACE

This document explains how to use VMware ACE to enhance the security of an existing remote access solution that uses VPN. VMware ACE doesn't replace VPN but supplements it by securing resources on the remote machine.

With VMware ACE you create and install a virtual machine on the remote computer; and you install or set up VPN on the virtual machine. It is the virtual machine — which you control with policies — rather than the user's remote machine, that accesses the corporate VPN server. The VPN server still controls the user's access to other corporate resources.

To manage the virtual machine you define policies in VMware ACE. Policies control different aspects of the virtual machine, including network quarantine, encryption, and access to devices.

The network quarantine policy restricts the access of the virtual machine to the corporate VPN server only. The host machine, on the other hand, has no restrictions.

You must also isolate the virtual machine from the host machine by setting policies that:

- Secure data in the virtual machine with encryption, authentication requirements and copy protection.
- Prevent data from being copied to and from the virtual machine (except through the authenticated VPN connection) by removing access to USB drives, CD and DVD drives, floppy disk drives and the host machine itself.

The remainder of this document explains in detail how to use VMware ACE to implement this solution for managing access for remote workers.

Getting Started

This document focuses primarily on how to set network quarantine policies, and other policies, to manage remote workers. However, before you can do that, you must create a project, add a virtual machine to it, and apply other policies to the virtual machine. This section provides a high-level view of that process. It assumes you are familiar with using VMware ACE Manager and that you have read the technical note, *VMware ACE: Best Practices Setup*, available at: *http://www.vmware.com/support/resources/ace_resources.html*. That document describes in detail the process that this section covers at a high level.

What You Need

To complete the procedures in this document requires the following:

- VMware ACE Manager
- System software to install on the virtual machine
- Any software applications required by end users of the virtual machine
- IPSec or SSL VPN

Before starting the step-by-step procedures in this document, make certain you have the *VMware ACE Administrator's Manual* available. You should also photocopy and fill out the two checklists in that manual:

- Checklist: Creating a Project
- Checklist: Adding a Virtual Machine

Creating a Project and Adding a Virtual Machine

A project contains one or more virtual machines and the VMware ACE application to run the virtual machines. In the project you create a package to install a virtual machine and the application on a user's machine.

To create a project, run VMware ACE Manager and click the New Project icon or click **File** > **New Project** to start the New Project Wizard. Enter a name for the project and a location in which to store project files. When you are finished, select **Open the Add Virtual Machine Wizard** to go directly to the wizard for adding a virtual machine to the project.

Note: When you create a project, the New Project Wizard automatically adds the VMware ACE application to the project. End users use this application to run and manage the virtual machine. You can set preferences for this application if you wish, although this document does not show you how to do so.

To add a virtual machine, enter information in the Add Virtual Machine Wizard. You can accept the default values in all cases.

When you are ready to finish the Add Virtual Machine Wizard, select **Set policies after the wizard closes** to go directly to the policy settings editor after the wizard creates the virtual machine.

Setting Policies to Support Remote Access

VMware ACE enables you to extend control to computers you do not own and control, but that have access to your corporate network. You do so by providing users with a virtual machine that they can use to access the company network. Then you isolate the virtual machine from everything except the corporate VPN server, by doing the following:

- Provide network access for the virtual machine to the VPN server only.
- Secure data in the virtual machine with encryption, authentication requirements and copy protection.
- Prevent data from being copied to and from the virtual machine (except through the authenticated VPN connection) by removing access to USB devices, CD and DVD drives, floppy disk drives and the host machine itself.

Policies are the means for managing virtual machines. They give you control over many aspects of your end users' experiences, including security and authentication, and network access. The following sections guide you through the steps to set policies for your virtual machine that are important from the standpoint of remote access:

- Setting Encryption and Authentication Policies on page 5 explains how to secure the data on the virtual machine through encryption and password protection.
- Creating a Recovery Key for the Password on page 6 explains how to set a recovery key that enables an administrator to unlock a virtual machine if the end user forgets the password.
- Setting Expiration Policies on page 6 explains how to set an expiration date for guest workers or business partners when the virtual machine can no longer be used.
- Setting Copy-Protection Policies on page 7 explains how to ensure that the virtual machine can be run only from the location where you install it.
- Setting Network Quarantine Policies on page 7 explains how to specify the network access for users of the virtual machine.
- Restricting Access to Devices on page 8 explains how to specify who can use peripheral devices such as CD and DVD drives, floppy drives and USB devices on the virtual machine.
- Enabling Hot Fixes for the VMware ACE Application on page 9 explains how to enable hot fixes, which let an end user recover the password, request an extension to an expiration date or use a copy-protected virtual machine from a different location.

Setting Encryption and Authentication Policies

A virtual machine that may contain sensitive data is particularly vulnerable on a laptop computer that will be used outside the corporate offices. By encrypting the virtual machine, you protect the data files even if the computer is lost or stolen.

When you specify that the virtual machine should be encrypted, the VMware ACE installer encrypts the virtual machine's files, including the configuration file and the virtual disk files, when it installs VMware ACE on the end user's computer. The encryption key is different on each computer.

Encryption is transparent so the end user of the virtual machine does not have to think about it. With authentication policies, you require that the end user create a password to be used to run the virtual machine. The VMware 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 and authentication policies:

1. Start the policy editor (click **Project** > **Policies**; or from the project summary page, select the **Edit virtual machine policies** icon).

   Click the + sign beside the name of the virtual machine. The list of policy categories appears below the virtual machine name.

2. Select **Encryption and authentication**.

   To protect the contents of the virtual machine, select **Encrypt data files when this virtual machine** is installed. Each installation of the virtual machine is encrypted differently.

3. Select **Password**.

   The virtual machine is password-protected and does not run until the user enters the correct password. Each user must set a password the first time that user's installation of this virtual machine is opened.

4. Optionally, you can set policies for the password, such as length and content of the user password. Click **Help** for more information.

When you are finished setting encryption and authentication policies, go to the next section.

Creating a Recovery Key for the Password

A recovery key enables you to access and reset the password for an encrypted virtual machine that has been deployed.

To create a recovery key:

1. If you are in the Encryption panel, select **Enable virtual machine recovery**. The Recovery Key dialog box appears. Click **Yes** and the Recovery Key panel appears.

   If you are not in the Encryption panel, select **Project** > **Settings**. Then click the **Recovery** tab.

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

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

2. 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: 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 application that manages the user's virtual machine. See Enabling Hot Fixes for the VMware ACE Application on page 9.

When you are finished setting a recovery key, go to the next section.

Setting Expiration Policies

You can 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.

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 installation** — The virtual machine runs for the specified number of days after the package is installed, then cannot be used. Consider this option for such uses as time-limited demonstrations.
- **On this date** — The virtual machine runs until and on the specified date. It cannot be used after the specified date. Consider this option for such uses as computing environments for contractors.

You can extend the life of a virtual machine in a number of ways:

- You may specify a script used to renew the virtual machine by selecting **This virtual machine is renewable using script**. Click **Set** to open a dialog box that allows you to find the plug-in script and set a command line for running the script. You may also specify a timeout interval in case the script does not run to completion.

  For example, the plug-in script could query a server on your network and, based on the results of that query, do one of the following:

  - Make no change.
  - Renew the virtual machine for a specified number of days.
  - Renew the virtual machine until a specific date.
  - Set the virtual machine so it never expires.
  - Expire the virtual machine.

  For information on writing scripts, consult the *VMware ACE Administrator's Manual*.
- If the user sends a hot fix requesting an extension, you can respond to the hot fix. See "Responding to Hot Fix Requests" in the *VMware ACE Administrator's Manual*.
- You can send an update package to the end users before they reach the expiration date. To do so, change the expiration date in the policy editor as just described. Then create an update package. In the package information, specify **Virtual machine policies only**. Send the update package to the affected end users, who can install the new polices to update their machines accordingly.

When you are finished setting expiration policies, go to the next section.

Setting Copy-Protection Policies

A virtual machine is software, implemented in a set of files. This makes it easy to package and install a virtual machine on multiple physical machines. It also makes it easy for an unauthorized person to copy the virtual machine to a different location. Copy-protection policies ensure that a virtual machine can run only from the location where the VMware ACE installer placed it.

To apply copy protection:

1. Select **Copy Protection** from the Policy list.
2. Select **Copy protect this virtual machine** as the copy-protection policy in the policy editor.

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

When you are finished setting copy-protection policies, go to the next section.

Setting Network Quarantine Policies

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

The network quarantine feature of VMware ACE, which uses a bi-directional packet filtering firewall, lets you specify exactly which machines or subnets a virtual machine may access. In this example, you configure the virtual machine so it is allowed to connect only to your VPN server, which then controls access to other resources.

You set and modify network quarantine policies with a wizard. This section steps you through the process of setting a quarantine policy that limits the virtual machine to a connection to the VPN server.

To set network quarantine policies, complete the following steps:

1. Select **Network quarantine** from the Policy list.

   Select **Quarantined access to specific networks and machines**, then click **Network Quarantine Wizard** to set quarantine policies. The wizard guides you through the settings. You may rerun the wizard at any time to change the settings.

2. When you click **Network Quarantine Wizard**, the Network Quarantine Options panel appears.

   Select **Static quarantine** to specify a single list of approved networks and machines, or of networks and machines that are off-limits. The list is stored with the virtual machine and distributed as part of the package. If you need to make any changes in the future, you must update the package and distribute the update to your users.

3. The Access panel appears.

   Select **Allow access to selected networks and machines** to specify a whitelist of networks and machines with which the virtual machine may communicate.

4. The Networks and Machines panel appears.

   Enter the IP address or the fully qualified host name for your VPN server, and click **Add**.

   If you enter a host name, the wizard resolves the name and displays both the host name and the IP address in the list. The wizard can resolve the host name only if you are connected to the network on which the host resides.

   Note: Because the host name is resolved to an address, the connection does not work, if the VPN server is moved to a new address.

   Click **Next** after entering a valid address.

5. The Network Traffic panel appears.

   Accept all defaults and click **Next**.

6. The Summary panel appears. Click **Finish** to close the Network Quarantine Wizard.

7. Click **OK** to exit the policy editor and create the policies you have specified.

Restricting Access to Devices

One weakness of a VPN setup is that the hard drive of the remote machine and its peripheral devices such as CD and DVD drives sit outside the protection of the corporate firewall. The virtual machine itself is secure, but it has access to the same CD/DVD drives, floppy disk drives and USB devices as the host machine.

This section explains how to deny access to host devices. 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 application installed on the host.

To remove access to devices, take these steps in VMware ACE Manager with the virtual machine powered off:

1. Start the policy editor (click **Project** > **Policies**; or from the project summary page, select the **Edit virtual machine policies** icon).

   Click the + sign beside the name of the virtual machine. The list of policy categories appears below the virtual machine name

2. Select the + sign beside **Device connection** to see a list of devices.

   Select each device in turn and select **No one** in the Device Connection panel.

3. When you have specified no connection for each device, click **OK** to close the policy editor.

Note: You may be familiar with the drag-and-drop feature of VMware Workstation that allows you to copy and paste files between a host machine and the virtual machine. For security reasons, this feature is disabled in VMware ACE. If you enable drag and drop in the settings editor, drag and drop works when you run the virtual machine in VMware ACE Manager. However, when you deploy the virtual machine to a host machine, drag and drop does not work.

Enabling Hot Fixes for the VMware ACE Application

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 VMware ACE application that runs on a user's host machine.

To enable hot fixes:

1. In VMware ACE Manager, click **Projects** > **Policies**.

   The Virtual machine policies panel appears. Click the + sign next to VMware ACE policies to expand it, if it is not already expanded. Then select **Hot fixes**.

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 resetting the virtual machine passwords. See Creating a Recovery Key for the Password on page 6.

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

Extending Policies to the Host

The policies described above, including the network quarantine policies, restrict the network access of the virtual machine and isolate the virtual machine from the host machine. In general, these steps are sufficient to protect your network when you grant VPN access. However, in different situations, such as when remote workers use a laptop onsite as well as remotely, different issues arise. For these kinds of situations, VMware ACE provides advanced network quarantine features that allow you to control the network access of the host machine.

For example, you may want to prevent an end user from connecting to your VPN server from the host machine. Advanced network quarantine features also let you define different access for the virtual machine depending on whether the host machine is inside or outside the corporate network.

Advanced network quarantine features are outside the scope of this document but are covered in the document: *VMware ACE: Managing Guest Workers* available at: *http://www.vmware.com/support/resources/ace_resources.html*.

Installing an Operating System and VMware Tools for the Virtual Machine

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

If you created a new virtual machine and added it to the project, you must install a guest operating system in the virtual machine. This sections describes general considerations and general steps for installing an operating system For instructions on how to install a Windows XP guest operating system from an installation CD, see the *VMware ACE Administrator's Manual* available from the VMware Web site. For notes on installing all supported guest operating systems, see the *Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

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

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

Installing a Guest Operating System

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

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

1. Start VMware ACE.

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

   Note: In some host configurations, the virtual machine is not able to boot from the installation CD-ROM. You can work around that problem by creating an ISO image file from the installation CD-ROM. Use the Virtual Machine Control Panel to connect the virtual machine's CD drive to the ISO image file, then power on the virtual machine.

3. Power on your virtual machine by clicking the Power On button.
4. Follow the instructions provided by the operating system vendor.
5. Install VMware Tools in the guest operating system.

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

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

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

Installing VMware Tools in a Guest Operating System

The detailed steps for installing VMware Tools depend on the operating system, and for Windows, on the version of Windows you are running. The steps that follow are the general steps for any operating system.

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

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

   Choose VM > Install VMware Tools.

The remaining steps take place inside the virtual machine. For details on installing to a particular operating system, see the *VMware ACE Administrator's Manual*.

Installing VPN and Application Software

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

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

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

If you are using IPSec VPN for this virtual machine, you need to install the client software on the virtual machine. If you are using SSL VPN, you can create a shortcut to your VPN server.

Creating Packages to Deploy to Users

After you have created a project and applied policies to the virtual machines in the project, you create packages to deploy those virtual machines to end users. A package includes an installer

and the additional files needed to install a virtual machine and the VMware ACE application that runs the virtual machine.

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

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

For details on creating packages, see the *VMware ACE Administrator's Manual*.

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

Revision 20050207 Item: ACE-ENG-Q105-061