



VMware ACE

Managing Guest Workers

This technical note explains how to use VMware ACE to manage personal computers for workers who routinely use their laptop computers both at work and at home to access the corporate network. These are guest workers in the sense that they do not spend all of their time inside the corporate network nor all of their time connected remotely. Although this is a fairly typical work situation, it requires flexible IT policies to manage properly.

This document contains the following topics:

- [About Guest Workers on page 1](#)
- [About VMware ACE on page 2](#)
- [Implementing a Solution with VMware ACE on page 3](#)
- [Getting Started on page 4](#)
- [Setting Multiple Network Quarantine Policies on page 5](#)
- [Verifying Network Quarantine Policies on page 14](#)
- [Updating Multiple Network Quarantine Policies on page 15](#)

About Guest Workers

Guest workers come in a number of types:

- Employees who regularly work in the office and also regularly work at home, using the same laptop computer in both environments.
- Contract employees who may primarily work off site but also bring their laptop machines to work onsite.
- Employees who generally work in the office, but take their laptops home to work at night, on weekends or while travelling.

Typically, companies use VPN or some type of terminal service to provide secure access to the corporate network for users who are working remotely. Although VPN or a terminal service provides a secure connection, any remote access situation entails security issues, such as the following:

- When the machine is outside the corporate firewall, connected through broadband, modem or wireless, it is vulnerable. Malware can be picked up and spread to the corporate network, either through the VPN connection or when the laptop machine is connected at work.
- Data on the laptop is vulnerable when the laptop sits outside the corporate firewall.
- Within the corporate network, IT policies can be enforced to restrict Web browsing and software downloading. When machines — particularly those belonging to contractors — are used outside the network, it is difficult to enforce such policies.



As a corporation, you cannot manage the operating environment of remote computers, but these computers have access to your corporate network. VMware ACE extends your control to these machines by enabling you to set host policies that prevent the machines from accessing your network. You force all sensitive data to be constrained to the virtual machine. You control the virtual machine with network policies and other policies that limit network access, and prevent data loss and malware threats.

This document shows you how to address these and other security issues by using VMware ACE to manage guest workers both when they work within the corporate network and when they access the network remotely.

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 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, 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.

Implementing a Solution with VMware ACE

This document explains how to use VMware ACE to manage a laptop machine that requires access to a corporate network from within the network as well as remotely. With VMware ACE, you create and install a virtual machine on the laptop computer. The virtual machine uses VPN to access the corporate network when the user is working remotely. The VPN server controls the user's access to other corporate resources.

Because the VPN server is not configured to accept connections from within the corporate network the virtual machine requires direct access to corporate resources when the worker uses the laptop onsite.

To manage the virtual machine (and the host on which it runs) you define policies in VMware ACE. Policies control different aspects of the virtual machine, including encryption, access to devices and network quarantine. This document focuses on setting network quarantine policies.

Ordinarily, you specify a single set of policies to define network access for the virtual machine, and if necessary, a different set of policies to define access for the host machine on which the virtual machine is running. However, to manage a laptop machine that connects both locally and remotely, you must define two network quarantine policies for the virtual machine as well as two network quarantine policies for the host computer.

You must define network quarantine policies that enforce the following restrictions:

- When the user is working remotely, the virtual machine has access to the corporate VPN server only. The host machine, on the other hand, has no restrictions other than it cannot access the VPN server.
- When the user is working onsite, the virtual machine requires access to the file server, the bug database and the company intranet. The host computer is allowed no access at all.

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-ROM 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 guest workers.



Getting Started

This document focuses on how to set network quarantine policies. 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 most cases. For network type, select bridged networking. If you select NAT, any restrictions on the host's network access also restrict network access for the virtual machine, because the NAT connection is affected by all the policies you apply to the host. Since you are going to impose host quarantine rules, you should select to use bridged networking.

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.

Creating Policies for the Virtual Machine

Policies are at the heart of managing a virtual machine. You set policies using the policy editor in VMware ACE Manager. At a minimum, you should set the following policies:



- **Encryption and authentication** 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.
- **Copy protection** ensures that the virtual machine can be run only from the location in which you install it.
- **Device policies** 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.

You can set other policies as well, such as an expiration date when the virtual machine can no longer be used. But the policies just described ensure that the virtual machine is secure and isolated from the host on which it runs.

See the technical papers, "VMware ACE: Best Practices Setup" and "VMware ACE: Managing Remote Access," at http://www.vmware.com/support/resources/ace_resources.html for detailed information about why and how to set these policies. The remainder of this document describes in detail how to set multiple network quarantine policies.

Setting Multiple Network Quarantine Policies

The following sections step you through the process of setting network quarantine policies for multiple zones.

Note: To complete some of the step-by-step procedures that follow, you use VMware ACE Manager. For others, you must manually edit VMware ACE policy files using a text editor such as Notepad.

- [About Zones on page 6](#) describes zones and how you use them to apply multiple network quarantine policies for a virtual machine and host.
- [Working in Files on page 6](#) provides guidelines for editing VMware ACE policy files.
- [Setting Network Quarantine Policies to be Used for the Corporate Zone on page 6](#) explains how to create a set of policies using the Network Quarantine Wizard in VMware ACE Manager. After creating the policies, you set them aside. Later, after creating a zone for the corporate network, you associate the policies to this zone.
- [Defining the Corporate Network Zone on page 8](#) explains how to create a network zone by editing the `app.vmp1` file in the project's main folder. The zone defines your corporate network.
- [Setting Host Policies for the Corporate and Default Zones on page 11](#) explains how to set host network quarantine policies by editing the `app.vmp1` file in the project's main folder. You create two sets of policies for the host: one when the user is within the corporate network and one when the user is connected remotely.
- [Associating Guest Policies to the Corporate Zone on page 12](#) explains how to edit the virtual machine policy file (`<vmname>.vmp1`) to associate the network quarantine policies created earlier to the corporate zone.
- [Setting Default Policies for the Virtual Machine on page 13](#) explains how to create a new, default set of policies for the virtual machine when it is connected remotely.



About Zones

Network zones are the mechanism VMware ACE uses to support the application of multiple network quarantine policies on a single virtual machine. A network zone is essentially a set of characteristics, such as IP addresses for a subnet and DNS names for machines or networks that you specify to define a network. For each zone you define, you can create a separate network quarantine policy.

When you deploy a virtual machine and the VMware ACE application, a service application is also installed on the host machine. The service application examines the network or networks directly connected to the network adapters on the host computer to see if there is a match for all the criteria in any of the zone definitions. If there is a match, the policies you have defined for that zone are enforced.

By default, a virtual machine (and its host) are not zone aware. You must turn on zone awareness to enable the VMware ACE application to check for network connections. Every virtual machine is deployed with a set of network quarantine policies: either the default policies from VMware ACE Manager or the policies that you create with the Network Quarantine Wizard. These policies are not associated with any zone. If zone awareness is turned off, these policies are applied to the virtual machine regardless of the network to which the virtual machine is connected. Likewise, if zone awareness is turned on but VMware ACE finds no networks that match the zone definitions for the virtual machine, the default policies are applied. In effect, policies that are not associated to any zone are the policies for a default zone.

Working in Files

In most of the procedures in this section, you must manually edit VMware ACE policy files. Be careful when working in these files. Keep the following guidelines in mind:

- Make a copy of the `.vmp1` file before you begin editing.
- Be careful of typographical errors. For example, if you define a zone and misspell the name when you refer to the zone, the policies do not work.
- Do not edit anything in the file other than what you are instructed to edit. VMware ACE Manager writes policies and other information to `<vmname>.vmp1`. If you change anything in this file inadvertently, the virtual machine may not work correctly when you deploy it.
- When editing files, be certain that no instances of VMware ACE Manager are running. Otherwise, you may lose some of your changes and the virtual machine does not behave correctly when deployed.

If you want to create a log file to help with debugging potential problems with the virtual machine, place the following lines in the `config.ini` file in the project directory:

```
vmauthd.logEnabled="TRUE"
log.vmauthdFileName="<logfile>"
```

Setting Network Quarantine Policies to be Used for the Corporate Zone

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 procedure, you create the network quarantine policy that is applied to the virtual machine when it is in the corporate zone. These policies allow access to the file server, the bug database and the company intranet. All other access is denied.

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 **Initial Setup to enter the** Network Quarantine Wizard and set quarantine policies. The wizard guides you through the settings. You may rerun the wizard at any time to change the settings.

Note: This example shows you how to set access to specific machines and networks. If you want unrestricted access when in the corporate zone, you do not set any network quarantine policies. Select **None — allow access to all machines and networks**. Then click **OK** to exit the wizard.

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

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

3. The Access panel appears.

You may specify either a whitelist of machines and networks with which virtual machine may communicate or a blacklist of machines and networks with which the virtual machine may not communicate.

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 following information:

- The name of your file server (for example, `p-fps1.MyCompany.com`). Click **Add**.
- The name of your bug database (for example, `bugzilla.MyCompany.com`). Click **Add**.
- The name of the company intranet (for example, `<MC>web.MyCompany.com`). 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 host names are resolved to an address, if any of the servers is moved to a new address, the connection does not work.

Click **Next** after entering the information.

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.

For now, these policies apply to the default zone. You can set these policies aside temporarily. Later, after you create a zone for the corporate network, you are going to edit these policies in



the virtual machine policy file, `<vmname>.vmp1`, and associate them to the corporate zone. See [Associating Guest Policies to the Corporate Zone on page 12](#).

Defining the Corporate Network Zone

You are going to use two zones to manage network access for the virtual machine and host:

- The corporate zone is defined by the company domain name, `MyCompany.com`. The policies for this zone take effect when the host is connected within the corporate network.
- The other zone does not need to be explicitly defined. It is the default zone that is in effect when the host is not connected to the corporate zone. Policies for this zone take effect whenever the user is connected from outside the corporate network.

In this section, you create a zone, called `Corporate`, which is defined by a connection to the `MyCompany.com` domain. To create a zone description you must manually edit the project's policy file (`app.vmp1`).

Note: To avoid conflicts, be certain to close all copies of VMware ACE Manager before editing this file.

To create a zone description for the company network:

1. In the project directory (`My Documents\VMware ACE Projects\<projectName>\`), open the policy file `app.vmp1`.
2. To define the company zone, type the following parameters and values in the file:

```
zoneDescription.0.present="1"
zoneDescription.0.key="0"
zoneDescription.0.name="Corporate"
zoneDescription.0.domainName="MyCompany.com"
```

These lines define a zone as follows.

```
zoneDescription.0.present="1"
```

This is the required first parameter for a zone description.

```
zoneDescription.0.key="0"
```

This parameter specifies 0 as the key. Note that the key matches the number in each zone description parameter name.

```
zoneDescription.0.name="<zoneName>"
```

This parameter specifies `<zoneName>` as the name of the zone. You can name the zone whatever you wish, but this example uses the name `Corporate`. Later, when you specify policies to apply to this zone, you identify the zone with the name you specify here. See [Associating Guest Policies to the Corporate Zone on page 12](#) and [Setting Host Policies for the Corporate and Default Zones on page 11](#).

```
zoneDescription.0.domainName="<domain_name>"
```

This parameter specifies the domain name as the defining characteristic of the zone. This example uses the domain `MyCompany.com`.

When the virtual machine is deployed, if the host machine has any network connections whose connection-specific DNS suffix matches `MyCompany.com`, the zone comes back as a match and triggers the specific host and guest policies that you are going to define for this zone.

You may specify only one entry for the `domainName` parameter. The behavior of this parameter is governed by the value of `domainNameExactMatch`. If you set this



parameter to 1, as follows, the domain name of the network must match the value of `<domain_name>` exactly:

```
zoneDescription.0.domainNameExactMatch = "1"
```

For example, if you set the value to 1, the domain `corp.MyCompany.com` is not considered a match for `MyCompany.com`. On the other hand, if you set the value of this parameter to 0 (the default), then the domain `corp.MyCompany.com` is considered a match for `MyCompany.com`.

There are a number of issues regarding how to specify the defining characteristics of a zone. For example:

- You can use parameters other than `domainName` to define the characteristics of the network zone.
- You can use multiple parameters to define the characteristics of the network. There are benefits and disadvantages to using longer or shorter lists of parameters.

If you want to learn more about how to define the characteristics of a zone, see [About Defining Zone Characteristics on page 9](#).

If you are satisfied with using the domain name to define the zone, go to step 3.

3. Save `app.vmp1`.

Leave the file open and go to [Setting Host Policies for the Corporate and Default Zones on page 11](#).

About Defining Zone Characteristics

VMware ACE provides a number of parameters that enable you to identify the company network by any of the following:

- Domain name
- IP address with a subnet range
- DHCP server
- DNS or WINS server address
- Gateway address

You can use multiple parameters to identify a network. When you do so, all the criteria must match or the network is not considered a match.

There are benefits and disadvantages to using a longer or shorter list of parameters.

If you use a longer list of parameters to define the network, you minimize the chances of a false positive or a misidentification. This can be important because you are providing a VMware ACE package to someone who connects a host computer to multiple networks at different times. If one of the other networks matches the characteristics you define in the zone definition, the host policies are applied — even if the host is not connected to your network.

In some cases, however, using a longer list increases the likelihood that the policies you set for the corporate network do not work. For example, if the host is configured to access the corporate network with a subset of the characteristics that you defined for your zone, the network quarantine policies are not applied when the host laptop computer is connected to the corporate network, because all characteristics must be matched.

Another point to consider is that the addresses or names of certain servers may change over time. Such changes may also introduce detection issues. Using a smaller set of information in a zone description — for example, using only the IP address and netmask — lessens the chance



that the detection mechanism fails to restrict a host or guest that should be restricted, but it also increases the chance that a false positive or misidentification occurs. Such false positives are especially likely if your network is using a common netblock, such as 10/8, 172.16/12 or 192.168/16, that is also used by other networks.

The following is a list of the parameters that you can use to specify network zone characteristics.

`zoneDescription.<zone_number>.subnets = "<IP_address>/<subnet>"`

This parameter specifies an IP address or subnet range that is used by the network. The value may be a comma-separated list of IP addresses and subnets. The value of `<subnet>` if you include it, must be the number of bits in the netmask. Do not use any spaces in the comma-separated list. A network adapter matches this condition if it is using an IP address that lies within any of the specified ranges.

For example, if the network has a static IP address and no domain specific DNS suffix, using a parameter such as the domain name to characterize the network does not work. In this case, using an IP address with a subnet range, as in this example, works better:

```
zoneDescription.0.subnets="10.17.0.0\19"
```

`zoneDescription.<zone_number>.domainName = "<domain_name>"`

This parameter specifies the domain name of the network — for example, `MyCompany.com`. This parameter is discussed in detail in [Defining the Corporate Network Zone on page 8](#).

`zoneDescription.<zone_number>.dhcpServers = "<IP_address>"`

This parameter specifies one or more IP addresses for DHCP servers on the network, using a comma-separated list with no spaces. A network adapter matches this condition if it is using at least one of these servers.

`zoneDescription.<zone_number>.gateways = "<IP_address>"`

This parameter specifies one or more IP addresses for default gateways on the network, using a comma-separated list with no spaces. A network adapter matches this condition if it is using at least one of these gateways.

`zoneDescription.<zone_number>.dnsServers = "<IP_address>"`

This parameter specifies one or more IP addresses for DNS servers on the network, using a comma-separated list with no spaces. A network adapter matches this condition if it is using at least one of these servers.

`zoneDescription.<zone_number>.minDnsServersToMatch = "<number>"`

This parameter modifies the `dnsServers` parameter (above). A network may have multiple DNS servers, and a host may be configured to use more than one DNS server. If the value of this option is greater than 1, the host must be using the specified number of DNS servers on the list before a network adapter is considered to be on the defined network.

`zoneDescription.<zone_number>.winsServers = "<IP_address>"`

This parameter specifies one or more IP addresses for WINS servers on the network, using a comma-separated list with no spaces. A network adapter matches this condition if it is using at least one of these servers.

`zoneDescription.<zone_number>.minWinsServersToMatch = "<number>"`

This parameter modifies the `winsServers` parameter (above). A network may have multiple WINS servers, and a host may be configured to use more than one WINS server. If the value of this option is greater than 1, the host must be using the specified number of WINS servers on the list before a network adapter is considered to be on the defined network.



To use these parameters to define network characteristics, see [Defining the Corporate Network Zone on page 8](#).

Setting Host Policies for the Corporate and Default Zones

In [Defining the Corporate Network Zone on page 8](#), you created a zone that is defined by the `MyCompany.com` domain. In this section you create a network quarantine policy for the host machine and associate it to this zone. The policy for the host, when connected to this zone, is to restrict all network access.

You also create a default policy for when the host is connected to any network but your corporate network. The policy for the default zone is to allow all access except to the corporate VPN server, which is how the virtual machine on the host is remotely connected to the corporate network.

To create host policies and associate them to a zone, edit `app.vmp1`. If you still have this file open, proceed to step 1. If the file is closed, open it with a text editor. The file is located in the project directory (`My Documents\VMware ACE Projects\<<projectName>\`).

1. To make the host aware of the zone, find the line that begins with `host.useZones="0"` and change it to:
`host.useZones="1"`
2. Define a quarantine policy for the host machine while it is connected to the corporate network. The policy is to restrict all network traffic while the host machine is connected to the corporate zone.

Type the following lines in `app.vmp1`:

```
host.zone.0.present="1"
host.zone.0.key="0"
host.zone.0.descriptionName="Corporate"
host.zone.0.blockIPv4="1"
host.zone.0.exceptions.IPv4=""
```

The first three lines identify the policy. The key for this policy is 0. Although the key for the network zone defined earlier is also 0, this is simply a coincidence. Each time you create a new zone, you must increment the key — key numbers must be contiguous. Network policy numbers must also be contiguous. In addition, for a policy, the key specifies the order in which VMware ACE searches to find a network policy that matches the network to which the host is connected.

The `descriptionName` parameter associates this policy to the `Corporate` network zone that you defined previously.

The last two lines specify the network traffic. By default, all traffic is allowed. Setting `blockIPv4="1"` restricts traffic to a whitelist (1 specifies a whitelist; 0 specifies a blacklist). The `exceptions.IPv4` parameter lists exceptions to the restriction, and since the parameter list is empty, there are no exceptions. In effect, this policy restricts all network access for the host when connected to the `Corporate` zone.

3. Restrict the host machine from the corporate VPN server when outside the company network. This prevents the user from accessing your network through VPN except by using the virtual machine.

By default, the host machine has no network restrictions. It specifies a blacklist (`blockIPv4="0"`) with no exceptions. To restrict access to the company VPN server,



find the line, `host.default.exceptions.IPv4 = ""`, and change it to include the host name (or IP address) of the VPN server, as follows:

```
host.default.exceptions.IPv4 = "<vpn.company.com>"
```

4. Save and close `app.vmp1`.

Associating Guest Policies to the Corporate Zone

In this section you associate the network quarantine policy that you already created to the `Corporate` zone. The policy file, `<vmname>.vmp1`, defines the policies for a virtual machine. The policy file is contained in the virtual machine's folder within the project folder; for example, look in:

```
My Documents\VMware ACE Projects\MyProject\win2kPro\win2kpro.vmp1
```

When you set policies for the virtual machine using the Network Quarantine Wizard, VMware ACE Manager writes the policies — in the form of quarantine statements — to `<vmname>.vmp1`. VMware ACE Manager writes one set of policies only. These are the default policies for the virtual machine.

You cannot use the Network Quarantine Wizard to write policies for multiple zones. If you use the Network Quarantine Wizard multiple times, you can change the default policies each time but you cannot create additional sets of policies. To do so, you must manually edit `<vmname>.vmp1`, create a zone policy, then associate each network quarantine statement to that policy. The step-by-step instructions in this section show you how to edit `<vmname>.vmp1` and modify the network quarantine policies so they apply to the `Corporate` zone.

Before beginning this procedure, be certain you have created policies for the virtual machine as described in [Setting Network Quarantine Policies to be Used for the Corporate Zone on page 6](#).

Note: To avoid conflicts, be certain to close all copies of VMware ACE Manager before editing the virtual machine policy file.

To associate guest quarantine policies to the `Corporate` zone:

1. Open the policy file, `<vmname>.vmp1`, with a text editor.

To make the virtual machine zone aware, find the line, `guest.useZones="0"` and change it to:

```
guest.useZones="1"
```

To create a guest zone policy, add the following lines:

```
guest.zone.0.present="1"
guest.zone.0.key="0"
guest.zone.0.descriptionName="Corporate"
```

The key for this policy is 0. Although the key for the network zone defined earlier is also 0, this is simply a coincidence. Each time you create a new zone, you must increment the key — key numbers must be contiguous. Network policy numbers must also be contiguous. In addition, for a policy, the key specifies the order in which VMware ACE searches to find a network policy that matches the network to which the host is connected.

The `descriptionName` parameter associates this policy to the `Corporate` network zone that you defined previously.

2. When you created guest quarantine policies with the Network Quarantine Wizard, VMware ACE Manager wrote the following lines in `<vmname>.vmp1`:



```

quarantine.configurationBlock = "explicit"
quarantine.configurationBlock.explicit.value = <very long line>
quarantine.descriptor.custom.script = ""
quarantine.descriptor.type = "nonversion"
quarantine.httpRoot = ""
quarantine.networkSettings = <very long line>
quarantine.showUpdatesAvailMsg = "1"
quarantine.webFile = ""

```

Note: You might find it easier to read and edit `<vmname>.vmp1` if you turn off the word wrap feature in your text editor. In Notepad you can turn off word wrap by deselecting **Word Wrap** in the **Format** menu. With word wrap turned off, each of the `quarantine.` statements begins on a new line. Otherwise, the `<very long line>` wraps over multiple lines and can be visually confusing.

Copy each of these lines — which all begin with `quarantine` — and paste them into another part of the file. At the start of each line, paste `guest.zone.0`. The result should look like this:

```

guest.zone.0.quarantine.configurationBlock = "explicit"
guest.zone.0.quarantine.configurationBlock.explicit.value = <very
long line>
guest.zone.0.quarantine.descriptor.custom.script = ""
guest.zone.0.quarantine.descriptor.type = "nonversion"
guest.zone.0.quarantine.httpRoot = ""
guest.zone.0.quarantine.networkSettings = <very long line>
guest.zone.0.quarantine.showUpdatesAvailMsg = "1"
guest.zone.0.quarantine.webFile = ""

```

3. Save and close `<vmname>.vmp1`.

Setting Default Policies for the Virtual Machine

The virtual machine can be used in two locations: at work and remotely. You defined one zone for corporate access. VMware ACE always defines one set of default network policies. You do not need to define an additional zone but can use the default policies for remote access.

For the virtual machine, the only access allowed is to the company VPN server.

To set default network quarantine policies, run VMware ACE Manager and complete the following steps:

Be certain that you have saved and closed `<vmname>.vmp1` and `app.vmp1`.

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 **Network quarantine** from the Policy list.
Select **Quarantined access to specific networks and machines**, then click **Initial Setup** to set quarantine policies. The wizard guides you through the settings. You may rerun the wizard at any time to change the settings.
3. When you click **Initial Setup**, 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.

4. 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.

5. The Networks and Machines panel appears.

Enter the name of your VPN server; for example, enter `vpn.<company.com>` 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 host names are resolved to an address, if the VPN server is moved to a new address, the connection does not work.

Click **Next** after entering the information.

6. The Network Traffic panel appears.

Accept all defaults and click **Next**.

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

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

Verifying Network Quarantine Policies

VMware ACE provides a number of status indicators and logs to track and verify network quarantine policies. Before deploying the virtual machine, you can verify that the policies are working as expected.

To run the virtual machine and check status indicators, run VMware ACE Manager and complete the following steps:

Note: The same status indicators and logs are available to end users from the VMware ACE environment running on their host machines.

1. Select the project and the virtual machine.
2. From the **Commands** list on the virtual machine details page click **Run in VMware Ace**.

After the operating system boots, the network quarantine icon (a shield-shaped icon) appears in the status icon tray in the lower right corner of the window. Click this icon to see the Network Quarantine Info panel, which lists the network quarantine settings for this virtual machine.

This panel lists the zone that the machine is in and also indicates if any network packets are being dropped.

Because you have turned on host quarantine, a similar network quarantine icon appears in the system tray of the host computer's Windows operating system. You can click this icon to see the zone that the host machine is in and if any network packets are being dropped because of network quarantine policies.

3. From the Network Quarantine Info panel (for the virtual machine or the host), you can control the level of the network quarantine log file.



In **Network quarantine log level**, you can set one of the following levels to specify the amount of data to display:

- **Terse** — Messages are brief.
- **Normal** — The default level, provides additional details.
- **Verbose** — Lists every packet that is dropped from the virtual machine (or host). When **verbose** is set, the log file grows very quickly. It is recommended that you set **verbose** only while debugging your network quarantine policies.

The Network Quarantine Info panel shows the location of the log file.

If you are having trouble connecting to specific networks, or the host or virtual machine is operating sluggishly, check the log files to see if network traffic is being impeded. You can also check the `aut.hd` log file you enabled earlier. [See Working in Files on page 6](#). By seeing which machines and networks your operating systems are trying to reach, you can adjust your network quarantine policies accordingly.

Be certain to turn off debugging before packaging the virtual machine. Click **VM > Settings > Options > Advanced** and make certain the option **Run with debugging information** is not selected.

4. When you are satisfied that the virtual machine is operating correctly, shut down the virtual machine by clicking **Start > Shut down** in the virtual machine. This closes the VMware ACE window and returns you to VMware ACE Manager.

Note: Be sure to shut down and not simply suspend the virtual machine. If you close the VMware ACE window by clicking the close icon (✕), the virtual machine is suspended, not powered off. You cannot package a suspended virtual machine.

Updating Multiple Network Quarantine Policies

If you need to manage access to an additional network, you can easily create another zone, then distribute an update package to the end user. For example, suppose you have defined network access for a contract worker as described in this paper. Now the contractor needs to work onsite not only at your company, but also at the parent company.

To manage this situation, you need to create a zone for the parent company and assign a set of network quarantine policies, for the host and the virtual machine, to this zone.

Creating an Additional Zone and Host Policy

You create an additional zone in exactly the same way you created the original zone description — by editing `app.vmp1` with a text editor. The file is located in the project directory (`My Documents\VMware ACE Projects\\`).

1. In the project directory (`My Documents\VMware ACE Projects\\`), open the policy file, `app.vmp1`.
2. To define the parent company zone, type the following parameters and values in the file:

```
zoneDescription.1.present="1"
zoneDescription.1.key="1"
zoneDescription.1.name="Parent"
zoneDescription.1.domainName="MyParentCompany.com"
```



Note: This is the second network zone you have defined in the file, so the key has been incremented from 0 to 1. Zone numbers must be contiguous.

The name of the zone is whatever you want (`Parent` in this example). This example uses the `domainName` parameter to identify the network (`MyParentCompany.com`). You can use domain name or a different method if you wish. [See About Defining Zone Characteristics on page 9.](#)

3. Define a quarantine policy for the host machine while it is connected to the parent company network. The policy is to restrict all network traffic while the host machine is connected to the `Parent` zone. The policy is implemented with a whitelist (`blockIPv4="1"`) with no exceptions (`exceptions.IPv4=""`).

Type the following lines in `app.vmp1`:

```
host.zone.1.present="1"
host.zone.1.key="1"
host.zone.1.descriptionName="Parent"
host.zone.1.blockIPv4="1"
host.zone.1.exceptions.IPv4=""
```

This is the second network zone policy in the file, so the key has been incremented from 0 to 1. This is actually the same policies that are applied to the `Corporate` zone.

Creating an Update Package

To deploy the new zone and policies, create an update package to distribute to end users.

To create an update package:

1. Start VMware ACE Manager and open the appropriate project.
2. Under **Commands**, click **Create package for distribution to end users**. This starts the New Package Wizard.
3. Click **Next** to enter the wizard. The Name the Package panel appears.

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

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

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

Click **Next**.

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

Click the + sign to expand the tree. Select **Policies** and deselect all other items.

Click **Next**.

5. The Package Files Panel appears.

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

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

6. The Ready to Complete panel appears.

Click **Next** if the summary information is correct.



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

If you created one or more files for distribution on CD or DVD, the files are now ready to be copied to a disk. Use the software of your choice to copy the files to disks.