VMware ACE

Configuring a Primary Desktop Environment

This document explains how to configure VMware ACE and a host computer so the virtual machine running in VMware ACE is the primary desktop environment — so all the end user's interactions are with the virtual machine, not with the host computer and its host operating system.

Making a VMware ACE virtual machine the primary working environment provides significant advantages in a variety of use cases. Consider the following examples:

- Kiosk settings — You need to make a public-access PC available for a training course, a trade show, or a product demonstration. You give users access only to a virtual machine. Then, at the end of a working session, you can easily revert to the original state, ready to begin a new working session from a known starting point.
- Simplified configurations — The physical PCs in your environment were bought at different times or from different suppliers. To simplify software maintenance, you want a consistent environment for all users. The virtual machine, running in VMware ACE, provides this consistent environment.
- Secure workstations — You want users to work in an environment with uniform, tested security settings. The virtual machine, running in VMware ACE, gives all users this trusted environment.
- Multiple virtual machines connected to different networks — You need to provide users access to multiple networks — the Internet and a private network, for example, or a secure network and an insecure network — but you must ensure that data does not move from one of those networks to another. You can set up an appropriate number of virtual machines and configure completely independent network settings for each virtual machine.

See the following sections for details on how to configure virtual machines and the host computer for such uses:

- About VMware ACE on page 2
- Implementing a Solution with VMware ACE on page 3
- Getting Started on page 3
- Setting Policies on page 4
- Setting up the Host Machine on page 9
- Setting VMware ACE Policies on page 15

About VMware ACE

VMware ACE enables you to create and rapidly provision standardized and secure PC environments throughout the extended enterprise. You can apply corporate IT policies to a virtual machine containing an operating system, enterprise applications, and data to create a secure, isolated working environment known as an assured computing environment.

A primary of advantage of using VMware ACE is that you create a standard, self-policing working 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 in the virtual machine through encryption and control access through password and directory service authentication.
- **Life cycle control** — Control who has access to a virtual machine, what they can do with the virtual machine, and when they are authorized to use the virtual machine. For example, you can provide virtual machines for a specified group of guest workers, give them access to specified resources on the network, and set their virtual machines to expire at the endo of their contract.
- **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* —** Virtual rights management is enforced through policies that control the capabilities of a virtual machine. You set policies 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 configure VMware ACE and a host computer so the virtual machine running in VMware ACE is the primary desktop environment.

With VMware ACE Manager you create and install one or more virtual machines on the host machine. Then you use the following combination of VMware ACE policies and Windows administrative settings to secure the host machine:

- Create a VMware ACE user account on the host machine.
- Launch the virtual machine as the shell when the user logs on with the VMware ACE user account. When the virtual machine is running as the shell, a user may run applications installed in the virtual machine but cannot run any applications on the host machine.
- Use the host quarantine feature of VMware ACE Manager to specify what network access the host machine may have when the VMware ACE is logged on and the VMware ACE virtual machine is running.
- Install software and set policies for the virtual machine to give it full functionality and full network access.

Note: The solution described in this document provides several layers of protection. For example, because the virtual machine is running as the shell, a user cannot launch an Internet browser on the host computer. Therefore, it may not be strictly necessary to quarantine the network access of the host machine. However, doing so adds another level of protection in case something goes wrong.

The remainder of this document describes this solution in detail.

Getting Started

To get started, you must create a project, add a virtual machine to it, then apply policies to the virtual machine. This section provides a high-level view of how to create a project and add a virtual machine —the following sections explain how to set policies for the virtual machine and the host. This document assumes you are familiar with using VMware ACE Manager and that you have read the technical note Best Practices for Setting up VMware ACE, available at *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

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.

Setting up the Virtual Machine

After setting the policies for the virtual machine, described in detail below, you must install and configure the guest operating system and appropriate software in the virtual machine.

Setting Policies

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 securing the host machine:

- Setting Encryption and Authentication Policies on page 4 explains how to secure the data on the virtual machine through encryption and password protection.
- Creating a Recovery Key for the Password on page 5 explains how to set a recovery key that enables an administrator to unlock a virtual machine if the end user forgets the password.
- Setting Copy-Protection Policies on page 6 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 6 explains how to specify the network access for users of the virtual machine.
- Enabling Hot Fixes for the VMware ACE Application on page 8 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

With encryption and authentication policies you ensure that only authorized users have access to the virtual machine.

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 an option to authenticate the virtual machine:

   - **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.

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

   - **Users and Groups** — Allow access by individuals and groups defined in an Active Directory domain.

   - **Determine using script** —Use your own custom plug-in to determine the settings that are applied. Click **Set** to open a dialog box that allows you to locate the plug-in script file and specify the command line for running the script. For more information, see VMware ACE: Writing a Simple Authentication Script, available at *www.vmware.com/support/resources/ace_resources.html*.

When you are finished setting encryption and authentication policies, go to the next section to enable a recovery key for the virtual machine.

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 8.

When you are finished setting a recovery key, 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.

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.

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.

VMware ACE Manager allows you to set different network quarantine policies for the virtual machine and for the host machine. You are going to set open policies for the virtual machine and restrictive polices for the host.

Setting Network Quarantine Policies for the Virtual Machine

By default, a virtual machine has unrestricted network access. The assumption in this document is that the virtual machine has unlimited access, therefore you do not need to change anything. However, if you want to impose some restrictions, such as allowing general access but denying access to specific networks or machines, you can use the Network Quarantine Wizard to do so.

To set specific network quarantine policies complete the following steps:

1. With VMware ACE Manager running and the policy editor open, 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. The Network Quarantine Options panel appears.

   Select the type of quarantine to apply.

- **Static quarantine** — Stores the list with the virtual machine and distributes it 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.
- **Dynamic quarantine** — Stores the list on a server. The virtual machine checks the server periodically to retrieve the list. If you need to make changes in the future you update the list on the server.
- **Version-based quarantine** — Allows you to set two different policies, normal or restricted, depending on whether the most up-to-date version of the virtual machine is running. The technical note, "VMware ACE: Enforcing Patch Management," which is available at *www.vmware.com/support/resources/ace_resources.html*, explains how to use version-based network quarantine policies to enforce patch management strategies.
- **Custom quarantine using script** — Allows you to set two different policies, normal or restricted, depending on the patch state of the virtual machine. The technical note, "VMware ACE: Enforcing Patch Management Using Custom Quarantine," which is available at *www.vmware.com/support/resources/ace_resources.html*, explains how to use custom network quarantine policies to enforce patch management strategies.

  Version-based quarantine and custom quarantine are specialized uses of network quarantine and require some effort to implement. See the technical notes if you are interested in using them to support your patch management strategy. This document assumes you choose **Static quarantine**. If you choose **Dynamic quarantine**, the wizard displays a panel in which you choose the server on which to store the policy. It can be a Web server or an Active Directory server.

3. The Access panel appears.

   Select **Deny access to selected networks and machines** to specify a blacklist of networks and machines with which the virtual machine may not communicate.

4. The Networks and Machines panel appears.

   Enter the IP address or the fully qualified host name of any machine to which you want to deny access. Click **Add**. You may add as many exceptions as you like.

   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 machine is moved to a new address.

   Click **Next** after entering the list is complete.

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.

Setting Network Quarantine Policies for the Host Machine

You can use advanced network quarantine policies to control the network access of the host machine. By default, the host computer has unrestricted network access. To restrict the access of the host machine to a proxy server use a text editor to change the default host quarantine policies, which are defined in the `app.vmpl` file in the main folder for the project.

Keep the following guidelines in mind when editing `app.vmpl`:

- Make a copy of `app.vmpl` file before you begin editing.
- Be careful of typographical errors.
- Do not edit anything in the file other than what you are instructed to edit. VMware ACE Manager writes information to this file. 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.

To edit the host quarantine settings, open `app.vmpl` and locate the following two lines:

```
host.default.blockIPv4 = "0"
host.default.exceptions.IPv4 = ""
```

The default host policies you define may establish either whitelists (`blockIPv4="1"`) — networks and machines to which connections are allowed — or blacklists (`blockIPv4="0"`) — networks and machines to which connections are prohibited. The current settings establish a blacklist with an empty exceptions list, which effectively means unrestricted access.

To completely restrict network traffic, edit the two parameters to establish a whitelist with no entries, as follows:

```
host.default.blockIPv4 = "1"
host.default.exceptions.IPv4 = ""
```

Alternately, you may not want to completely restrict network traffic. For example, to restrict network traffic to a proxy server only, edit the two parameters to establish a whitelist and specify the proxy server, as follows:

```
host.default.blockIPv4 = "1"
host.default.exceptions.IPv4 = "<proxy_server@company.com>"
```

Do not change the other host default settings, such as:

```
host.default.restrictDHCP = "0"
host.default.restrictDNS = "0"
```

Even when the host is otherwise blocked from all access to the network, it is allowed to communicate with DNS and DHCP servers.

Save `app.vmpl` and exit the text editor.

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 5.

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

Packaging the Virtual Machine

When you are satisfied with the policies you have set and with other aspects of the project, you can use the package creation wizard in VMware ACE Manager to create a package.

Note: Be certain that you have installed an operating system and any applications for end users on the virtual machine.

For details on creating packages, including information about installing an operating system, see the *VMware ACE Administrator's Manual* or the technical note "Best Practices for Setting Up VMware ACE," available at *www.vmware.com/support/resources/ace_resources.html*.

Setting up the Host Machine

After you create a virtual machine package, you must set up the host machine by following the guidelines in the following sections:

- Installing the Virtual Machine Package on page 10 explains how to install the package you created.
- Creating a User Account for Running the Virtual Machine on page 10 explains how to create a user account with settings customized for running the VMware ACE virtual

machine. Users who log in to this account are not able to remove or install software, which prevents them from removing the virtual machines installed on the host machine.

- Launching the Virtual Machine as the Shell and Disabling Windows Features on page 11 explains how to set up the virtual machine as the shell that Windows launches when it starts.

Installing the Virtual Machine Package

You install a virtual machine package the same way you do any other application package.

You may install a VMware ACE package from a location on the network or from one or more CDs or DVDs. In either case, take the following steps:

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

   Caution: Do not install VMware ACE on a Windows NT Server 4.0 system that is configured as a primary or backup domain controller.

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

   Note: Although you must be logged in as an administrator to install VMware ACE, a user with normal user privileges can run the program after it is installed.

2. If installing from CDs or DVDs, insert the first disc into the computer's drive. If installing from the network, navigate to the location of the installer.

3. Find the `setup.exe` file and double-click to start the installer.

4. Follow the instructions in the installation wizard.

   The installer installs the VMware ACE application in `<ProgramFiles>\VMware\VMware ACE`.

   The installer asks where you want to place the virtual machine files. The default location is `<CommonAppData>\VMware\VMware ACE\<project_name>`. If you want to place the files in a different location, you may enter the path to the new location or click **Browse** and navigate to the new location. Be sure the location you specify has enough space to hold the virtual machine files. If it does not, the installer prompts you to specify a different location.

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

6. Click **Finish** to complete the installation. The wizard closes and a VMware ACE icon is visible on the desktop.

Creating a User Account for Running the Virtual Machine

The VMware ACE user account described in this section is customized for uses in which the end user should be able to run a virtual machine and not have access to the host operating system. You may want to tailor the settings for this user account in other ways, depending on your specific needs. For example, you may want to use the access control features of the NTS file system to restrict the VMware ACE user's access to particular folders.

To assign security policies to individual users in Windows, you create a user and assign the user to a group. The group contains the privileges and the user obtains privileges from the group.

To create a user account and assign privileges:

1. Open **Users and Groups** in Control Panel.

   The Users and Passwords dialog box appears.

2. Click **Add**.

   Enter a name and optional description for the user. Click **Next**.

3. Enter and confirm a password for the user. Click **Next**.

4. Assign the user to the standard users group.

   With standard user privileges, users of this account can run the virtual machine but do not have administrative privileges to change any of the registry settings that you make for this account.

5. Click **Finish** to create the user and assign the user to the standard users group.

6. With the name of the new user highlighted, click the **Advanced** tab then click the **Advanced** button.

   Open the **Users** folder. Double-click the name of the new user to open the Properties dialog box.

7. Select **User cannot change password**.

   Click OK to save the settings for the new user.

After creating the VMware ACE user account, log out as administrator and log back in as the VMware ACE user to verify that you can run the virtual machine from this account. If you can run the virtual machine, go on to the next section. If not, fix any problems now before going on to make changes to the VMware ACE user account.

Launching the Virtual Machine as the Shell and Disabling Windows Features

This section explains how to configure the host operating system to start the virtual machine and nothing else when someone logs in with the VMware ACE user account. You also disable any Windows features that allow the user to start processes other than the virtual machine.

Normally, when you start Windows, it launches Windows Explorer as the shell application. Windows Explorer allows users to locate files and documents to work on and it gives them a variety of ways to execute applications.

By editing registry keys, you can designate any application as the startup shell. This section explains how to make a virtual machine the shell that Windows launches when it starts. This section also describes registry settings needed to prevent users who log in with the VMware ACE user account from running other applications on the host. Taken together, these changes limit their activity to the virtual machine.

Windows 2000 and later operating systems provide an interface called Group Policy to control user and system restrictions. You can see the policies that are set for the current user by running the `gpedit.msc` utility.

This document describes a different process for making the necessary registry settings — loggin in as Administrator and using `regedit` to edit the settings.

One important reason for showing how to make the registry changes from the Administrator account, rather than the VMware User account, is that some of the necessary changes impose restrictions that make it impossible to go back and make further changes while logged in as the VMware ACE user. In other words, you would have only one chance to make all the changes correctly. If you are making the changes from the Administrator login, you have access to make additional changes after testing the initial settings.

Editing the Registry

You are going to edit the registry settings for the VMware ACE user you just created.

Note: You must log in with administrative privileges to edit the registry. In the procedure described here, you log in using the Administrator account.

Users are listed by SID, not by name. To get the SID for a user, you can use a utility such as `psgetsid`, available for download at *www.sysinternals.com*.

In the registry the SID for the user is listed under `HKEY_USERS`. If you do not see the SID for the user, click **Start > Run** and enter the following command to create a login session for the user and load their registry hive.

```
runas /profile /user:<ace_user> notepad
```

Leave the Notepad window open until you have finished editing registry entries for the user.

Caution: Before editing the registry, be certain to back up any valuable data on your system. Mistakes in the registry settings can damage the your system or make it unusable and you may need to reinstall the operating system.

If you plan to make these modifications on more than one machine, you can speed up the process byusing a registry merge file that includes all these changes. Be sure the registry merge file uses the correct SID number in the paths for each machine.

A sample registry merge file is available at *www.vmware.com/support/resources/ace_resources.html*.

You must customize the registry merge file for the host computer where you run it. To do so, take the following steps:

1. Log on to the host computer as a user with administrator privileges.
2. Copy the registry merge file to the user's host computer.
3. Determine the SID for the user — for example, using `psgetsid`.
4. Open the registry merge file in Notepad.
5. In all paths under `HKEY_USERS`, substitute the user's SID in the appropriate location.
6. In the `Shell` line, substitute the correct path to the `.vmx` file of the virtual machine and the correct path to vmplayer.exe if it is not in the default location (for example, if the location of the `Program Files` folder is not `C:\Program Files\`).
7. Save the registry merge file and close Notepad.
8. Double-click the registry merge file and follow the on-screen instructions to merge its content into the host computer's registry.

Policies to Edit

This section lists the policies to edit in the registry.

The items listed below represent new keys you must add to the registry. Follow the steps listed in the help for the Registry Editor.

In the registry, most of the entries you need to change are under the following path:

```
HKEY_USERS\<SID_number>\Software\
```

Except as noted in the list, the paths for items shown below are relative to this path.

Note: Most of the policies are under `Microsoft\Windows`, but the login shell is under `Microsoft\Windows NT`, many of the settings for Internet Explorer are under `Policies\Microsoft\Internet Explorer`.

Edit the following policies:

- **Startup Shell** — The application to run the virtual machine is `vmplayer.exe`. To make it start the virtual machine when the user logs on, change the following setting:

  ```
  Microsoft\WindowsNT\CurrentVersion\Winlogon: Shell (REG_SZ
  "vmplayer.exe" "<config_name>.vmx")
  ```

- **Autorun** — If autorun is enabled, a user can insert a CD-ROM disk and launch explorer or some other application. To disable autorun, set the following value:

  ```
  Microsoft\Windows\CurrentVersion\Policies\Explorer:
  NoDriveTypeAutoRun (REG_DWORD, value 255)
  ```

- **New Task in Task Manager** — A user can use **File > New** in Task Manager to launch a new process. To disable this feature, set the following value:

  ```
  Microsoft\Windows\CurrentVersion\Policies\Explorer: NoRun
  (REG_DWORD, value 1)
  ```

- **Common file dialogs** — A user can browse the file system by using right-click context menus. File dialogs enable a user to launch the application for a file by opening the file in the file dialog box. To disable context menus, set the following value:

  ```
  Microsoft\Windows\CurrentVersion\Policies\Explorer:
  NoViewContextMenu (REG_DWORD, value 1)
  ```

- **Windows key combinations** — The Windows key can be used to launch Windows Explorer (Windows-E) and the Run dialog (Windows-R). These combinations are disabled entirely when Windows Explorer is not running, but it is a good idea to use Group Policy to disable all Windows key combinations.

  ```
  Microsoft\Windows\CurrentVersion\Policies\Explorer: NoWinKeys
  (REG_DWORD, value 1)
  ```

- **Task Manager** — A user can access Task Manager even when it is not running by using Ctrl-Shift-Esc or by clicking the Task Manager button on the Windows Security dialog that appears by using Ctrl-Alt-Del. Task Manager allows a user to launch other applications. To disable Task Manager completely, set the following value:

  ```
  Microsoft\Windows\CurrentVersion\Policies\System:
  DisableTaskMgr (REG_DWORD, value 1)
  ```

- **Print dialog box** — From the print dialog box with the default configuration, a user may be able to launch program files on the host computer. To disable addition and removal pf printers through the print dialog box, set the following two values:

  ```
  Microsoft\Windows\CurrentVersion\Policies\Explorer:
  NoAddPrinter (REG_DWORD, value 1)
  ```

  ```
  Microsoft\Windows\CurrentVersion\Policies\Explorer:
  NoDeletePrinter (REG_DWORD, value 1)
  ```

  Note: You must also be sure the host computer has at least one printer set up, even if that printer is only a placeholder. If no printers are set up, Windows offers to let the user add one.

- **Network drive mapping** — To disable mapping and unmapping of network drives on the host computer, set the following value:

```
Microsoft\Windows\CurrentVersion\Policies\Explorer:
NoNetConnectDisconnect (REG_DWORD, value 1)
```

- **Internet Explorer context menus** — Using the context menus in Internet Explorer, a user can launch a text editor by choosing View Source. To disable context menus in Internet Exolorer, set the following value:

```
Policies\Microsoft\Internet Explorer\Restrictions:
NoBrowserContextMenu (REG_DWORD, value 1)
```

- **Internet Explorer reconfiguration** — From the Internet Options dialog box with the default configuration, a user may be able to launch program files on the host computer. To disable all the tabs in the Internet Options dialog box, set the following seven values:

```
Policies\Microsoft\Internet Explorer\Control Panel: AdvancedTab
(REG_DWORD, value 1)
Policies\Microsoft\Internet Explorer\Control Panel:
ConnectionsTab (REG_DWORD, value 1)
Policies\Microsoft\Internet Explorer\Control Panel: ContentTab
(REG_DWORD, value 1)
Policies\Microsoft\Internet Explorer\Control Panel: GeneralTab
(REG_DWORD, value 1)
Policies\Microsoft\Internet Explorer\Control Panel: PrivacyTab
(REG_DWORD, value 1)
Policies\Microsoft\Internet Explorer\Control Panel: ProgramsTab
(REG_DWORD, value 1)
Policies\Microsoft\Internet Explorer\Control Panel: SecurityTab
(REG_DWORD, value 1)
```

- **Internet explorer file browsing** — A user can launch programs on the host computer using file browsing features in Internet Explorer and direct commands entered into the Internet Explorer address bat. To prevent Internet Explorer from browsing the local file system and prevent it from launching programs using paths typed into the address bar, set the following value:

```
Microsoft\Windows\CurrentVersion\Policies\Explorer: NoFileUrl
(REG_DWORD, value 1)
```

  Note: This setting is effective only if you also set the NoRun value described earlier in this list.

- **Help viewer** — The Windows help viewer can launch programs on the host computer. To prevent the help viewer from launching external programs, set the following value:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System:
HelpQualifiedRootDir (REG_SZ value empty)
```

  Note: Unlike most of the settings in the list, this setting is under `HKEY_LOCAL_MACHINE`. The registry path shown above lists the full path to this setting.

  Note: This setting is available only on systems running Internet Explorer 6 Service Pack 1 or a more recent version.

- **Accessibility feature keyboard shortcuts** — When the accessibility keyboard shortcuts are turned on, certain key presses can take the user to the Accessibility control panel. To turn off the keyboard shortcuts for accessibility features, set the following values:

```
HKEY_CURRENT_USER\Control Panel\Accessibility\StickyKeys: Flags
(REG_SZ value "506")
```

```
HKEY_CURRENT_USER\Control Panel\Accessibility\Keyboard
Response: Flags (REG_SZ value "122")
```

```
HKEY_CURRENT_USER\Control Panel\Accessibility\ToggleKeys: Flags
(REG_SZ value "58")
```

- **Screen saver** — Disable the host screen saver. If it starts, it steals focus away from the virtual machine, which can lead to user confusion. If you want a screen saver, you can still run one in the guest operating system:

  ```
  HKEY_CURRENT_USER\Control Panel\Desktop: ScreenSaveActive
  (REG_DWORD, value 0).
  ```

Making Additional Host System Changes

This section lists changes you must make that cannot be made by setting registry values.

- **Windows Explorer, Internet Explorer, Outlook Express** — To prevent users from running Windows Explorer, Internet Explorer, or Outlook Express, you must use the NTFS file system on the host computer's system disk, then use the file system's access controls to deny access to the following three files:`%SYSTEMROOT%\explorer.exe` , `Program Files\Internet Explorer\iexplore.exe`, and `Program Files\Outlook Express\msimn.exe`. Right-click each of these files in turn, choose **Properties**, click the **Security** tab, select your VMware ACE user's account, and change the setting for **Read & Execute** to **Deny**.
- **Utility Manager** — On Windows 2000 hosts only, use the Services control panel to disable the Utility Manager service

Setting VMware ACE Policies

This section has some suggestions for policies to set that are particularly helpful if you are using virtual machines in a training situation.

Starting the Virtual Machine in Full Screen Mode

You can set the virtual machine to start in full screen mode. If you configure the host machine to run the VMware ACE application as the shell when a user logs on, the user never sees the host operating system's desktop — only the desktop of the guest operating system.

Note: Launching the virtual machine in full screen mode focuses users' attention on the virtual machine environment. However, it does not, by itself, deny them access to the host machine. The additional steps described in previous sections of this document are required to restrict access to the host.

To set the virtual machine to start in full screen mode, complete the following steps in VMware ACE Manager:

1. Click the tab for the project and click **Edit policies for application and virtual machines**.
2. The policy settings editor appears.

   Expand **VMware ACE policies** if it is not already expanded, and click VMware ACE window.
3. The VMware ACE window panel appears.

   Select **Always run maximized**.

4. Leave the editor open and go to the next section to set troubleshooting policies, or click OK to save the setting you made and close the policy editor.

Setting Troubleshooting Options

VMware ACE provides a feature that enables a user to restore a virtual machine to its initial state. You enable this feature by setting a troubleshooting option for the VMware ACE application.

Consider this option carefully. It can be very useful in a situation like a training lab or a trade show demonstration because it allows you, with the click of a button, to return a virtual machine to its original state at the end of the day or at the end of each session.

On the other hand, since all changes to the virtual machine are lost, if you enable and use this option, you cannot make any persistent changes to an installed virtual machine, including installing or upgrading software. If you need to make persistent changes to a virtual machine that is configured to use this feature, you must use VMware ACE Manager to create a new installable virtual machine package that includes the software updates.

To enable the revert to installed image feature, complete the following steps in VMware ACE Manager:

1. If you have the policy editor open, click Troubleshooting. If it is not open, select the tab for the project and click Edit policies for application and virtual machines. Make sure VMware ACE policies is expanded. Then click Troubleshooting.
2. In Reimage virtual machine, select Enable revert to installed virtual machine image.
3. Click OK to save the setting and close the policy editor.

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

The virtual machine image is similar to a snapshot. It includes the state of the virtual machine's disks., the contents of the virtual machine's memory and the virtual machine settings.

If an end user chooses Revert to the Installed <vmname> Environment, a warning message appears. It cautions that all changes to the virtual machine will be lost and urges the user to take this action only if advised to do so by a system administrator.

Caution: If you enable this option, be certain to warn users not to use it before the end of the working session.