Pocket ACE Guide

VMware ACE 2

This technical note describes the VMware ACE 2 Pocket ACE feature and contains the following sections:

About This Guide

The purpose of this technical note is to provide an in-depth view of Pocket ACE, a feature of VMware ACE 2 Enterprise Edition. This guide is intended for architects or administrators looking for more information about Pocket ACE and how it might be used in their environments. This guide covers the steps required to create an ACE master, policy, and package for deploying Pocket ACE instances.

Overview of ACE 2 Enterprise Edition

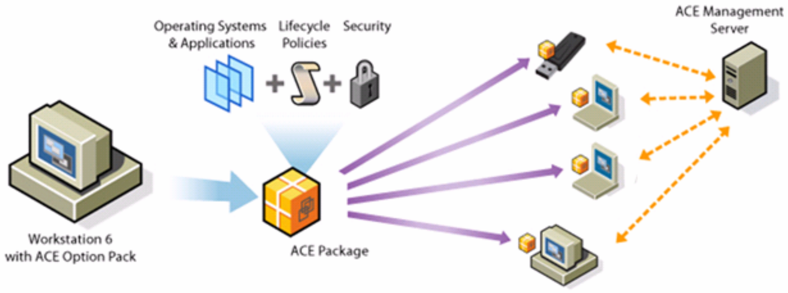
VMware ACE 2 Enterprise Edition is a software solution that delivers enhanced management, security, and usability to standard desktop virtualization products. Using ACE 2, an organization can rapidly provision a standardized, secure PC environment—an ACE virtual machine—to any device end point in the enterprise, whether or not it is managed by the ACE administrator. An ACE is a policy-protected virtual machine containing an operating system, applications, and data. Using virtual rights management technology, ACE 2 enables desktop administrators to control ACE life cycles, protect data, and ensure compliance with IT policies, including software life cycle management and access to data and applications.

The creation tool for an ACE instance is VMware Workstation 6 with the ACE Option Pack. Using this tool, system administrators can easily create, package, deploy, and manage virtual desktop instances for a wide array of use cases across the enterprise. System administrators create an ACE Master for distribution to users that includes:

- A virtual machine with an operating system, applications, and data.
- An application to run the virtual machines.
- A set of policies to control the life cycle and capabilities of the virtual machine.

From the ACE Master, administrators create an ACE package that is distributed to end users using download, DVD, CD, USB Flash drive, or other media. See Figure 1 for a diagram of ACE package distribution.

Figure 1. ACE Package Distribution


Operating Systems & Applications
Lifecycle Policies
Security
ACE Management Server
Workstation 6 with ACE Option Pack
ACE Package

ACE 2 Enterprise Edition is used across the enterprise to:

- Ensure secure controlled access to enterprise resources from a standardized PC environment running an ACE virtual desktop.
- Provide a simplified end-user interface designed for non-technical users.
- Provide policy-based controls including access, network, and device rights.
- Provision time-limited locked-down ACE virtual desktops on unmanaged guest PCs.
- Encrypt and protect sensitive enterprise information for safe deployment to mobile users.

Introduction to Pocket ACE

Reducing risk and providing more secure desktop solutions continue to be top priorities for IT organizations. Workplace trends such as flexible schedules, work from home, and real estate consolidation lead to increased user mobility. Even as user mobility increases, there is still a need for providing access to enterprise resources, while at the same time reducing the risk of losing sensitive data and suffering network attacks from unknown or unmanaged systems.

The increase in user mobility has spawned new approaches to addressing the ability of mobile users to leverage portable media devices. IT organizations have a number of solutions they can choose from including desktop virtualization, application virtualization, and solutions that attempt to blend the two. Consider the following when selecting a mobile solution for the enterprise:

- Preventing lost or stolen data.
- Isolating your instance from unknown or untrusted hosts.
- Application compatibility.
- Effort required to repackage applications.
- Remotely disabling and managing instances.
- Provisioning an easy-to-use and understandable solution for users.

Pocket ACE enables an ACE Administrator to deploy ACE instances using portable media devices such as USB keys (flash memory drives), Apple iPod mobile digital devices, or portable hard drives. When an ACE instance is deployed, you can attach the portable device to any x86-based host computer to run the ACE instance. When you finish using an ACE instance, you can shut down, detach the media, take it with you, and restart your session by attaching the portable media device to another host.

Because Pocket ACE is a feature of ACE 2, it includes several benefits that differentiate it from other solutions that target portable media devices, including:

- Fully isolated virtual machine based desktops that work connected or disconnected.
- The broadest combination of operating system (Windows and Linux) support.

- Hardware independence.
- Native application compatibility. Applications install just as they do on a PC.
- FIPS 1402-compliant data and configuration encryption. Data is fully encrypted at all times.
- The ability to suspend, resume, and snapshot.
- Robust policy management including access, network, and device rights.
- Ability to deploy instances to PCs and laptops, not just portable media drives.
- Robust management tools for creating, packaging, deploying, and managing ACE instances.

Examples Use Cases for Pocket ACE

The following sections describe example uses for Pocket ACEs.

Providing Secure Remote Access for Users Working Remotely Using Untrusted Hosts

Providing remote access for employees who work from home in today's enterprise is not uncommon. It is also not uncommon for the user to use a personally owned computer for accessing enterprise resources remotely. Typically, this is handled on a laptop or desktop PC using a web-based SSL VPN solution or a locally installed VPN client. Providing remote access from untrusted or unmanaged clients introduces inherent risk to the enterprise. Unmanaged clients can be infected by malware or spyware. In addition, there is a risk of lost data if a remote user were to download sensitive data to a personal computer. There is also the added burden of deploying and managing the software needed by remote users.

Using Pocket ACE, IT administrators can deploy a trusted, managed, and more secure virtual desktop instance to remote users needing access from untrusted clients. The virtual disk of the Pocket ACE can be encrypted to minimize the risk of lost data. By setting specific network quarantine policies, administrators can strictly control traffic between the untrusted client and Pocket ACE instance, protecting the enterprise from creating a compromised host.

Increasing the Security and Mobility of Mobile Users

Mobile users in the enterprise introduce the highest risk of losing sensitive data. Mobile users often access or carry sensitive data outside the enterprise using laptops or other mobile devices. The question for IT organizations is not if, but when, a mobile user's laptop will be lost or stolen, leading to the loss of sensitive or confidential data.

Using Pocket ACE to deploy a desktop environment to mobile users, IT administrators can reduce the risk of lost data while also increasing users' mobility. A desktop instance with an encrypted disk can be deployed to mobile users, reducing the risk of data being lost or stolen. Using the ACE Management Server, a lost or stolen Pocket ACE can be disabled remotely. In addition, the Pocket ACE instance can be used with any supported x86 system by mobile users, further increasing their mobility.

Providing Temporary Access to Contract Workers Using Untrusted Hosts

More and more often, contractors or business partners are connecting to the enterprise network from unknown or untrusted clients. Pocket ACE can be used to provide a standardized, trusted, and managed environment to these users while enabling safe connectivity to enterprise resources. For contractors, the Pocket ACE instance can be configured to be available only during the length of the contract. When the expiration time is reached, the contractor can no longer use the Pocket ACE instance.

Providing Access to Offshore Outsource Partners

Typically, offshore partners manage and own the desktop systems they use. Because these resources are owned by an outside organization, they do not fall under standard IT policy. In some cases, desktop systems are purchased, imaged, and shipped to an offshore partner for accessing the enterprise. This is often a lengthy and costly process.

With Pocket ACE, IT administrators can easily deploy a trusted, managed, and more secure virtual desktop instance to offshore partners. The virtual desktop instances can be distributed using portable media or download. The virtual disk of the Pocket ACE can be encrypted to reduce the risk of lost data. By setting specific network quarantine policies, traffic between offshore partners can be limited, allowing only communication between the Pocket ACE instance and the enterprise network.

Providing Disaster Recovery

Using Pocket ACE, organizations can easily package desktop instances with all the necessary enterprise applications for use in the case of a disaster. These instances can be deployed to portable media devices and stored safely in a secure offsite facility. If a disaster occurs, the Pocket ACE instances can be quickly distributed and used.

Distributing Beta or Trial Software

Using Pocket ACE, ISVs can distribute software preinstalled as a virtual appliance either by download or on a portable media device. An ISV can provide a complete working environment, ensuring no compatibility issues. Custom EULAs can be created and used to ensure that a user agrees to prior to using an ACE instance. In addition, an expiration period can be set that disables an ACE instance after an allotted period of time.

Choosing a Portable Media Device

Before deploying Pocket ACE instances to end users, administrators must decide which portable media devices to use. Pocket ACE supports a wide array of devices that include:

- Flash memory drives (USB Keys)
- Flash-based Apple iPod mobile digital devices
- Hard Drive based Apple iPod mobile digital devices
- Portable hard drives

How a portable media device will be used and transported are important considerations. In addition, the performance of the device and the target host are both important considerations. In all cases, use a high speed USB 2.0 compliant device. Flash-based portable media devices that offer the fastest read/write speed typically offer the best performance. Table 1 provides posted performance specifications collected from leading manufacturers of different devices.

Table 1. Portable Media Device Specifications

Manufacturer	**Device Type**	**Read**	**Write**
Manufacturer 1	4GB USB Flash	30MB/sec	18MB/sec
Manufacturer 2	4GB USB Flash	24MB/sec	10MB/sec
Manufacturer 3	4GB USB Flash	30MB/sec	21MB/sec
Manufacturer 4	4GB USB Flash	15MB/sec	9MB/sec
Manufacturer 5	8GB USB Flash	30MB/sec	25MB/sec
Manufacturer 6	16GB USB Flash	9MB/sec	5.3MB/sec
Manufacturer	**Device Type**	**RPM**	**Avg. Seek**
Manufacturer 7	USB 8GB Pocket Drive	4600	11.0 ms
Manufacturer 8	USB 6GB Pocket Drive	3600	
Manufacturer 9	USB 8GB Pocket Drive	3600	

External USB hard drives and pocket drives offer higher capacities, typically at lower cost. Although these devices usually post slower read/write speeds than USB flash drives, they handle sequential and random writes better. Overall, they offer better performance. Pocket flash drives are likely found to be more portable by end users than portable hard drives, which offer greater capacity. Typically, these media types are not built to withstand a high degree of shock from being dropped or tossed around, although some protection is offered.

Currently, USB flash drives are very common in 4GB and 6GB capacities at increasingly higher read/write speeds. In addition, they are much more resistant to being dropped and tossed around. Some manufacturers also offer features such as rugged designs and waterproofing.

Creating the Pocket ACE Master

Before getting started with deploying Pocket ACE instances, you must create an ACE master that includes a virtual machine, policy settings, and package settings. An ACE master can be created in a number of ways including:

- From scratch
- By cloning an existing virtual machine
- By cloning an existing ACE master

When planning the configuration of virtual machine settings for a Pocket ACE, take the following into consideration:

- The size of the virtual disk needed
- Memory settings
- Hardware configuration of the target hosts
- Size of the portable media used for storing the Pocket ACE instance

Before creating the Pocket ACE master make sure you consider the size of the portable media that will be used for storing the Pocket ACE. This is important to properly configure the size of the virtual disk before you install the operating system and applications, regardless of whether you intend to use an existing virtual machine or create an ACE master from scratch. When creating an ACE master from scratch, the New ACE Master Wizard notifies you about the portable media requirements required for supporting your Pocket ACE instances.

Reducing Pocket ACE Storage Requirements

When planning the initial configuration of a Pocket ACE master, administrators can take a few steps to reduce the storage requirements for storing a Pocket ACE instance. Some things you can do to reduce the required storage are:

- Disable suspend and sync.
- Package only a Windows- or Linux-based player.
- Do not include a Linux 64-bit player.
- Streamline your operating system installation and required applications.

The New ACE Master Wizard assumes you will allow users to suspend and sync. When using suspend and resume, you need enough extra storage space for saving the suspend file. In the case of a virtual machine that is configured for 512 MB of RAM, you will also need 512 MB of storage. When using the Pocket ACE feature, VMware recommendeds that you do not enable suspend and resume for Pocket ACE users.

Combined, all three VMware ACE player installers require approximately 222 MB of storage. If you expect end users will never need to run a Pocket ACE from a Linux-based host, deploying only the Windows player can save 98 MB of storage.

Most importantly, removing unneeded applications and features from the base operating system instance contribute greatly to reducing the overall storage required. It is easy to fit Windows XP SP2 plus Office 2003 and additional applications on a 4GB USB flash stick.

Creating the ACE Master Policy

Before you begin defining the policy for your ACE Master, consider the target users who will use the Pocket ACE instances. Some factors include how secure or restrictive the environment should be, how remote users will get assistance if there is an issue, and whether any restrictions should be placed on accessing peripherals.

The following example shows a policy that can be used by an ACE administrator who is deploying Pocket ACE-enabled devices to users as a secure remote access solution. In this case, the users will be accessing the enterprise network using an unmanaged Personal Computer from their home or other remote location.

Use the following requirements to define the ACE policy:

- Provide an ACE instance for secure remote access to enterprise resources.
- Distribute a secure remote access solution with preinstalled applications ensuring software compliance.
- Restrict access to communication between the enterprise network and the ACE virtual desktop.
- Restrict access to who can initialize the Pocket ACE instance.
- Prevent the Pocket ACE instance from being copied or moved when deployed.
- Ensure the Pocket ACE regularly checks for policy updates.

Creating the Pocket ACE Policy

To start the policy editor, right click the ACE master you created and select **Policies**.

Access Control

To configure access control

1 Select Access Control.

2 Under Activation select **Password**.

3 Under Authentication select **User-specific password**.

By configuring the activation policy to use either a password or activation key, you can protect the Pocket ACE instance while it is in transit to the user. The activation password or key is known only to the Pocket ACE administrator and end user. Setting an authentication policy ensures that a Pocket ACE instance will prompt the user for a new authentication password after the Pocket ACE has been initialized. This password is always used to power on the Pocket ACE instance, and is known only by the end user. If the user forgets the authentication password, it can be reset by an administrator from the ACE management server.

Expiration

Set an expiration time period if you want the Pocket ACE instance to expire after a certain period of time.

Copy Protection

Under Copy Protection, select **Do not allow moving or copying the instance files**.

Configuring the copy protection policy for the Pocket ACE instances allows you to minimize the risk of lost or stolen media devices. This prevents a Pocket ACE instance that has been moved or copied from running.

Resource Signing

Under Resource Signing, select **Verify the integrity of all files in the ACE** resource directory.

Configuring resource signing ensures the configuration and ACE resources files that accompany the Pocket ACE instance have not been modified or changed. If someone attempts to modify or tamper with the configuration files, the Pocket ACE becomes unusable. By default all Pocket ACE files are encrypted.

Removable Devices

To configure removable devices

1 Under Removable Devices, ensure that the boxes for **CD-ROM** and **Serial** are selected**.**

2 Under **Removable Devices, USB Devices,** accept the default setting, **Allow.**

The removable device policy enables you to configure user access for the devices that are connected to the host system. Each use case and organization policies will vary. For a more secure Pocket ACE instance, disable all access to all devices.

Virtual Printer

Accept the default, **Enable Virtual Printer** for instances.

ACE 2 includes the ThinPrint universal print driver and management tools. Enabling the virtual printer will add the necessary serial device to the virtual machine configuration. When the Pocket ACE instance is running, it inherits the printers configured on the local host automatically.

Runtime Preferences

To configure runtime preferences

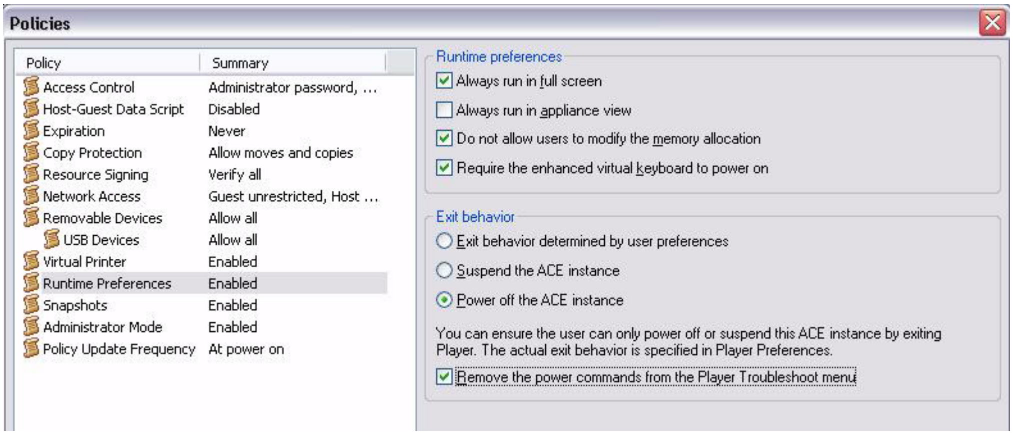
1 Under Runtime Preferences select **Always run in full screen**.

2 Select **Do not allow the users to modify the memory allocation**.

3 Select **Require the enhanced virtual keyboard to power on**.

4 Select **Power off the ACE instance**.

5 Select **Remove the power commands** from the Player Troubleshoot menu.



Policies

Policy	Summary
Access Control	Administrator password, ...
Host-Guest Data Script	Disabled
Expiration	Never
Copy Protection	Allow moves and copies
Resource Signing	Verify all
Network Access	Guest unrestricted, Host ...
Removable Devices	Allow all
USB Devices	Allow all
Virtual Printer	Enabled
Runtime Preferences	Enabled
Snapshots	Enabled
Administrator Mode	Enabled
Policy Update Frequency	At power on

Runtime preferences

☑ Always run in full screen

□ Always run in appliance view

☑ Do not allow users to modify the memory allocation

☑ Require the enhanced virtual keyboard to power on

Exit behavior

○ Exit behavior determined by user preferences

○ Suspend the ACE instance

● Power off the ACE instance

You can ensure the user can only power off or suspend this ACE instance by exiting Player. The actual exit behavior is specified in Player Preferences.

☑ Remove the power commands from the Player Troubleshoot menu

Runtime preferences allow you to configure how the Pocket ACE instance will run when started by the end user. Typically, most administrators configure the ACE instances to run in full screen mode. This can help minimize end user confusion between what is on the host operating system and what is on the ACE instance. Selecting **Power off the ACE instance** disables suspend and sync. This reduces the overall storage needed for storing the Pocket ACE instance.

Snapshots

Snapshots for Pocket ACE are always disabled.

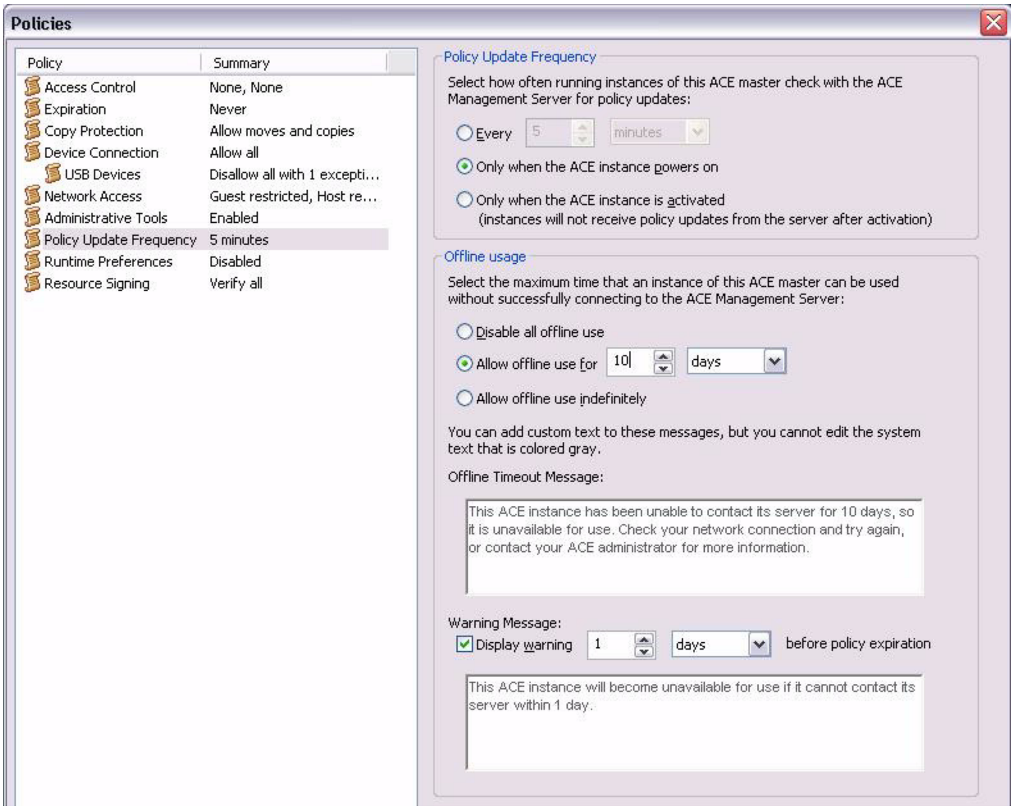
Administrative Mode

Under Administrative Mode select **Enable administrative mode**. Enter a password that can be given to end users. This password enables users to access administrator functions for resolving problems.

Enabling Administrator Mode allows an ACE administrator to remotely help a user who has limited or no connectivity to solve common problems such as password resets and expired ACE instances. The administrator can give the user the administrator mode password and enable utilities for solving common problems. Afterwards, the administrator mode password can be reset from the ACE management server.

Policy Update Frequency

Select **Policy Update Frequency**, under policy update frequency, and click **Only when the ACE instance powers on**. Under offline usage, click **Allow offline use**, and configure it for **10 days**.



Policies

Policy	Summary
Access Control	None, None
Expiration	Never
Copy Protection	Allow moves and copies
Device Connection	Allow all
USB Devices	Disallow all with 1 excepti...
Network Access	Guest restricted, Host re...
Administrative Tools	Enabled
Policy Update Frequency	5 minutes
Runtime Preferences	Disabled
Resource Signing	Verify all

Policy Update Frequency

Select how often running instances of this ACE master check with the ACE Management Server for policy updates:

○ Every 5 minutes

● Only when the ACE instance powers on

○ Only when the ACE instance is activated
(instances will not receive policy updates from the server after activation)

Offline usage

Select the maximum time that an instance of this ACE master can be used without successfully connecting to the ACE Management Server:

○ Disable all offline use

● Allow offline use for 10 days

○ Allow offline use indefinitely

You can add custom text to these messages, but you cannot edit the system text that is colored gray.

Offline Timeout Message:

This ACE instance has been unable to contact its server for 10 days, so it is unavailable for use. Check your network connection and try again, or contact your ACE administrator for more information.

Warning Message:

☑ Display warning 1 days before policy expiration

This ACE instance will become unavailable for use if it cannot contact its server within 1 day.

How you configure the update frequency policy might vary from organization to organization. It might also vary between groups across the enterprise. The policy update frequency configures how often the ACE instances checks with the ACE Management server for updates. There is no significant impact to setting the policy update checking to a more regular interval such as one minute. VMware recommends that this setting be set to a low interval. Doing so ensures that an ACE instance that has been revoked from the ACE Management Server is disabled in a shorter time period. The offline usage policy controls how long an ACE instance can be used without checking in with the ACE management server for updates.

The policy that is created will be applied to future Pocket ACE packages created from this ACE master. Now that the ACE master policy has been created, the operating system and applications for the Pocket ACE instances can be installed. For more information on installing guest operating systems for the ACE master, refer to the *VMware Guest Operating System Installation Guide*.

Creating the Pocket ACE Deployment Package

After the ACE master for a Pocket ACE instance has been created and the policies configured, a package for deploying Pocket ACE instances must be created. In addition to full deployment packages, policy update packages and server update packages can be created. Update packages can be created for updating existing Pocket ACE instances after they have been deployed.

Configuring the Pocket ACE Package Settings

To configure the Pocket ACE package settings

1 Start the package settings editor from the tab workspace of the ACE master you created for your Pocket ACE instances by selecting **Edit Package Settings**.

2 Under **Encryption** in the Package protection section, select **Encrypted.**

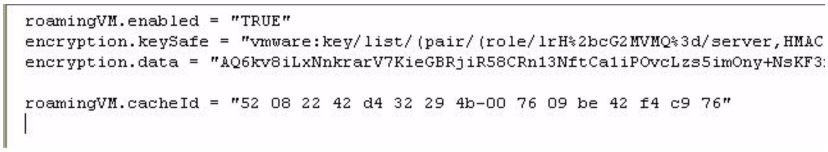
3 Under Instance protection, select **Encrypted**.

Encryption for a package encrypts the configuration files to prevent tampering if a deployment package were to be compromised. In addition, a Pocket ACE instance and configuration files can be encrypted. This means when a Pocket ACE instance is deployed, the configuration files as well as the virtual disk are encrypted. This protects the data inside the virtual disk as well as encrypting the Pocket ACE instance configuration files to prevent tampering. Below is an example of an encrypted Pocket ACE configuration file.

Package Lifetime

Under Package lifetime, select **Up to 30 days from package creation**.

Package lifetime determines how long a package can be used for deploying new Pocket ACE instances after it is created. It is not intended as a way to secure packages, but rather to set a the lifetime of a package.



```
roamingVM.enabled = "TRUE"
encryption.keySafe = "vmware:key/list/(pair/(role/lrH%2bcG2MVMQ%3d/server,HMAC
encryption.data = "AQ6kv8iLxNnkrarV7KieGBRjiR58CRn13NftCa1iPOvcLzs5imOny+NsKF3

roamingVM.cacheId = "52 08 22 42 d4 32 29 4b-00 76 09 be 42 f4 c9 76"
```

Instance Customization

Instance customization allows an ACE administrator to customize each Pocket ACE instance leveraging the Microsoft Sysprep tools. This is unique in that you do not need to load the sysprep tools inside the operating system. Using the Package Setting GUI you can configure all the options needed for individual operating system customization. For instructions on setting up VMware ACE 2 and how to use the instance customization feature, refer to the *VMware ACE Administrator's Manual*.

Deployment Platform

To configure the deployment platform

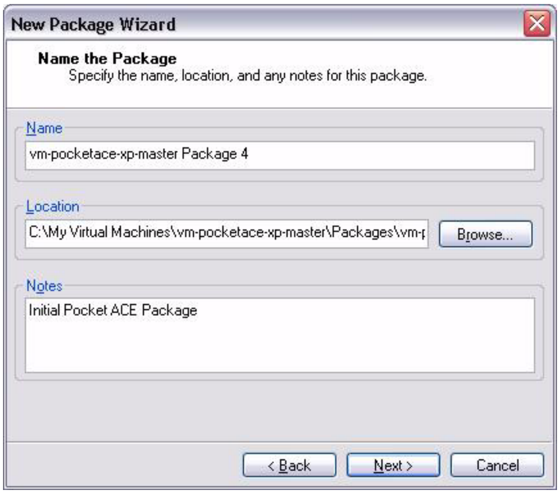
1 Select the target deployment platform that the Pocket ACE instances will be run from.

2 If you expect your end users to only run from a Windows host, select **Windows** only.

Creating the Pocket ACE Deployment Package

The actual creation of the package for deploying your Pocket ACE instances is done using the Pocket ACE Package Wizard. You can start the Pocket ACE Package Wizard from the workspace tab of the ACE master you created for your Pocket ACE instances by selecting Create Pocket ACE Package.

You must provide a name for the Pocket ACE package and a location for storing the package and its accompanying configuration files. This will typically be the ACE management station where VMware ACE 2 is running and it should be backed up regularly.



New Package Wizard

Name the Package

Specify the name, location, and any notes for this package.

Name: vm-pocketace-xp-master Package 4

Location: C:\My Virtual Machines\vm-pocketace-xp-master\Packages\vm-p

Notes: Initial Pocket ACE Package

Player Selection

Selecting both Windows and Linux creates a package with the necessary files needed for deployment to both platforms. However, it also increases the total amount of storage needed on the portable media. If you expect end users to connect only from Windows-based hosts, you can package only the Windows player.

Deployment Password

Enter a password that will be used when the Pocket ACE deploy utility is run.

Configuring a deployment password ensures that only someone who knows the password can deploy a Pocket ACE instance using the deploy utility.

Package Summary

After it has been completed, a package summary is displayed that lets you review your entries before creating the package.

Deploying the Pocket ACE package

There are a few ways to deploy Pocket ACE packages. One is to run the deploy utility from the directory where the ACE master is stored. Another way to deploy a Pocket ACE package is by using the tabbed workspace. When deploying from the tabbed workspace, the Pocket ACE deploy utility can be accessed by right clicking on the Pocket ACE package from the package history and selecting **Properties**.

After selecting the package a summary of the Pocket ACE package will appear. From there, you can launch the Pocket ACE deploy utility by clicking the **Deploy Pocket ACE** button.

When deploying the Pocket ACE instance, your portable media should be plugged in and available. After launching the Pocket ACE deploy utility, the Pocket ACE deploy wizard will appear.

To deploy a Pocket ACE

1 Select the portable media device listed and click **Deploy**.

2 When the password dialog box appears, enter the password for deploying the Pocket ACE package.

As the Pocket ACE is deployed, a progress dialog box appears. When completed, a success dialog box appears.

After the Pocket ACE instance is deployed to the portable media, it can be distributed to the end user. For Pocket ACE instances that have an initialization password set, the end user needs the password. The first time a Pocket ACE is used on a system, VMware Player will be installed, if it is not already.

Conclusion

The Pocket ACE feature of ACE 2 Enterprise Edition allows administrators to bundle and deploy ACE packages directly on portable USB media devices such as flash memory sticks, portable hard drives or even Apple iPods. End users can operate their ACE client machines directly from the USB device for unparalleled mobility and flexibility.

References

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

http://technet.microsoft.com/en-us/default.aspx

http://www.usbflashdrive.org/

http://www.usb.org

Glossary

ACE instance

Virtual machine configuration – the specification of what virtual devices (disks, memory size, and so on) are present in a virtual machine (an ACE instance) and how they are mapped to host files and devices.

authentication

A step in ACE instance setup that includes instance protection. The successful completion of the authentication step allows the user to run the instance.

bridged networking

A type of network connection with an ACE instance. Using bridged networking, an ACE instance appears as an additional computer on the same physical Ethernet network as the host. See also host-only networking.

configuration

See virtual machine configuration file.

full screen mode

A display mode in which the ACE instance's display fills the entire screen.

guest operating system

An operating system that runs inside an ACE instance. See also host operating system.

host computer

The physical computer on which the VMware Player software is installed. It hosts the ACE instances.

host-only networking

A type of network connection between an ACE instance and the host. Under host-only networking, an ACE instance is connected to the host on a private network, which normally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the same network. See also bridged networking and network address translation.

host operating system

An operating system that runs on the host machine. See also guest operating system.

instance customization

The act of customizing an ACE instance, thus making it unique from all other instances. The instance customization process automates the actions of the Microsoft sysprep utility. It also provides the ACE administrator with features needed to set up an automated remote domain join process of the ACE instance to a company VPN network.

live copy of policies

The currently deployed policy set. The active ACE instances on the ACE end users' machines use this set.

managed ACE instance

An ACE instance that is managed by an ACE Management Server.

Network Address Translation (NAT)

A type of network connection that enables you to connect ACE instances to an external network when you have only one network IP address, and that address is used by the host computer. If you use NAT, your ACE instance does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your ACE instance gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more ACE instances and the external network. It identifies incoming data packets intended for each ACE instance and sends them to the correct destination.

network access

Policies that give you fine-grained and flexible control over the network access you provide to users of your ACE instances. Using a packet filtering firewall, the network access feature of ACE 2 lets you specify exactly which machines or subnets an ACE instance or its host system may access.

New ACE Master wizard

A point-and-click interface for convenient, easy creation of an ACE master configuration. To launch it, choose **File > New ACE Master**. You are prompted for information, suggesting default values in most cases. It creates files that define the ACE master. See also virtual machine settings editor.

package

An installable bundle for distribution to end users. A full package includes an ACE master configuration file, virtual disk files, and policies; package installer; and VMware ACE Administrator's Manual

package settings

A set of rules and settings associated with a package, such as Revert to Installed and Instance Customization settings. These settings cannot be changed after packaging. The only way to change package settings is to create a new package.

Pocket ACE

An ACE feature that allows the ACE administrator to distribute an ACE instance on a removable device such as a USB key, Apple iPod mobile digital device, or portable hard drive. The user of a Pocket ACE instance can plug the device into a host computer, run the instance, save data from the session and close it, and then unplug the device. The user can then take the instance to another host computer and use it in that new location.

policy

A policy controls the capabilities of an ACE instance. Policies are set in the policy editor. See also live copy of policies, working copy of policies, and publish.

preview

An operating and viewing mode that an administrator can use to preview the ACE instance as it will run on the end user's machine. The administrator can use this feature to see the effects of policy and configuration settings without having to go through the packaging and deployment steps. The preview mode displays the working copy of the policies. See also working copy of policies.

publish

To publish policies (applies only to managed ACE instances) is to make those policies part of the live copy of the policy set. Publishing copies the working copy of the policies over to the live copy. See also policy, live copy of policies, and working copy of policies.

resume

To return an ACE instance to operation from its suspended state. When you resume a suspended instance, all applications are in the same state they were when the instance was suspended.

snapshot

A snapshot preserves an ACE instance (or ACE master) as it was when you took the snapshot— the state of the data on all the ACE instance's disks and whether the instance was powered on, powered off or suspended.

standalone ACE instance

An ACE instance that is not managed by an ACE Management Server. Any changes to its policies or other settings are made by the administrator's distribution of updates to the end user.

suspend

To save the current state of a running ACE instance. To return a suspended ACE instance to operation, use the resume feature. See also resume.

virtual disk

A file or set of files, usually on the host file system, that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. When you configure an ACE master with a virtual disk, you can install a new operating system into the disk file without the need to repartition a physical disk or reboot the host.

virtual machine

A virtualized x86 PC environment in which a guest operating system and associated application software can run. The managed virtual machine that has policies and other settings associated with it is known as an ACE instance. See also ACE instance.

virtual machine configuration file

A file, with file extension.vmx, containing an ACE instance configuration. It is used by VMware Player to identify and run a specific ACE instance. An ACE master's configuration file has the file extension.vmxa. See also ACE instance; ACE master.

Virtual Machine Settings Editor

A point and click editor used to view and modify the virtual machine settings of an ACE master. You can launch it from the VM menu. See also New ACE Master wizard.

.vmxa

The file extension for an ACE master configuration file.

VMware Player

An application that allows an end user to run an ACE instance.

Workstation ACE Edition

The program used by the administrator to create and deploy ACE packages and manage ACE instances. Formerly named “VMware ACE Manager.”

VMware Tools

A suite of utilities and drivers that enhance the performance and functionality of your guest operating system. Key features of VMware Tools include some or all of the following, depending on your guest operating system: an SVGA driver, a mouse driver, the VMware Tools control page, and support for such features as shared folders, shrinking virtual disks, time synchronization with the host, VMware Tools scripts, and connecting and disconnecting devices while the ACE instance is running.

working copy of policies

The policy that the ACE administrator uses to make and try out policy changes. For managed ACE masters, the working copy contains “unpublished” policies. For standaloneACE masters, the working copy contains policies that have not yet been packaged or distributed. Manipulating the working copy for a managed ACE master does not affect any existing instances associated with that master.

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

Revision 20070806 Item: TBD