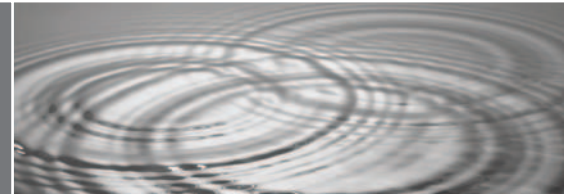


VMware ACE

The Assured Computing Environment for the Enterprise



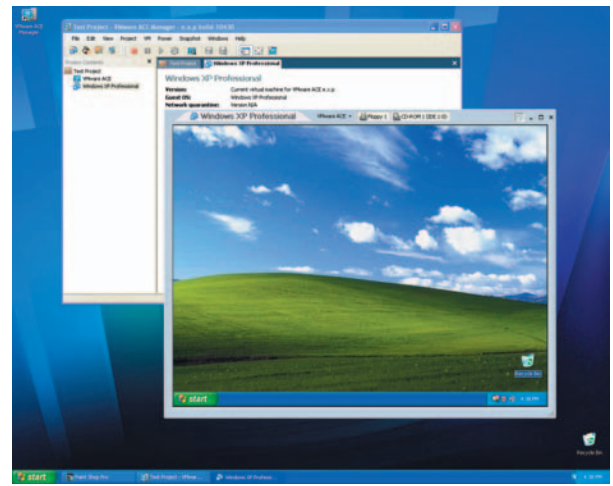
What Is VMware ACE?

VMware® ACE™ is an enterprise solution for IT desktop managers who want to rapidly provision standardized and secure PC environments throughout the extended enterprise. VMware ACE installs easily, improving the manageability, security and cost-effectiveness of any industry standard PC. VMware ACE enables IT desktop managers to apply enterprise IT policies to a virtual machine containing an operating system, enterprise applications, and data to create an isolated PC environment known as an “assured computing environment”. VMware® assured computing environments are self-policing, protect enterprise data, and enable safe access to enterprise resources.

How Is VMware ACE Used in the Enterprise?

VMware ACE is used across the enterprise to:

- Provision enterprise-standard PC environments on unmanaged remote PCs
- Provision time-limited, locked-down PC environments on unmanaged guest PCs
- Encrypt and protect sensitive enterprise and personally identifiable information on mobile PCs
- Provision standardized, hardware-independent PC environments on any enterprise PC



How Does VMware ACE Work?

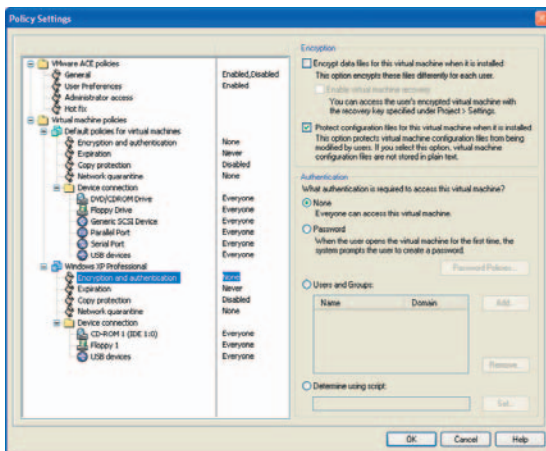
VMware ACE leverages VMware virtual machine technology to provide an isolated PC environment known as an “assured computing environment”. Using VMware ACE Manager, IT desktop managers create projects that include:

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

From this project, PC managers create a VMware ACE package that is distributed to end users via download, DVD, or CD media. VMware ACE enables end-users to run an “assured computing environment” on their desktop or laptop PC. The VMware virtualization layer maps the physical hardware resources to the VMware ACE virtual machine resources, providing the full equivalent of a standard x86 machine within the assured computing environment.

“This new solution from VMware installs and runs like an application on the students’ PC--it’s easy for students to use and much easier for us to manage. This product will save us time and money. It is going to decrease development time on my part, and because we can set everything up for the students, they need less training and have fewer problems. They just click it and it works.”

Scott Worthington
Technology Support Analyst, Arizona State University



Virtual Rights Management technology built into VMware ACE enables IT desktop managers to control assured computing environment lifecycles, secure enterprise information on PCs, and ensure compliance with IT policies.

KEY FEATURES

Manageability

- **Design once, deploy anywhere.** Create and deploy standardized hardware-independent PC environments to any PC throughout the extended enterprise.
- **Virtual Rights Management interface.** Control VMware ACE lifecycle, system configuration, security settings, network settings, and user interface capabilities.

Security

- **Rules-based network access.** Identify and quarantine unauthorized or out-of-date VMware ACE environments. Enable access to the network once the VMware ACE environment complies with IT policies.

- **Tamper resistant.** Protect the entire VMware ACE environment, including data and system configuration, with seamless encryption.
- **Copy protected.** Prevent end users from copying enterprise information.

Usability

- **Customizable interface.** Customize the behavior and look and feel for end users.
- **Flexible computing environment.** End users can revert to a previous state within seconds and work online or when disconnected from the enterprise network.

Why Use VMware ACE?

USAGE SCENARIOS	BENEFITS
<p>Provision assured computing environments to unmanaged remote PCs Provision enterprise-standard PC environments to remote PCs used by telecommuters, remote employees or offshore workers</p>	<ul style="list-style-type: none"> • Reduce security risk from unmanaged and unsecured PCs • Simplify management and support of employee-owned PCs • Protect company assets in secure, encrypted, and copy-protected PC environments
<p>Provision assured computing environments to unmanaged guest PCs Provision time-limited, locked-down PC environments to guest PCs used by consultants, contractors, auditors, and other temporary workers</p>	<ul style="list-style-type: none"> • Reduce security risk from unmanaged and unsecured PCs connecting to the enterprise network • Simplify management and support of guest worker-owned PCs • Protect company assets in secure, encrypted, and copy-protected PC environments
<p>Secure data on enterprise PCs Encrypt and protect sensitive enterprise and personally identifiable information on mobile PCs</p>	<ul style="list-style-type: none"> • Centralize copy protection and encryption policies with Virtual Rights Management (VRM) technology • Reduce theft and unauthorized copying of enterprise and personally identifiable information
<p>Standardize PC environments Provision hardware-independent PC environments to any PC and control PC environment lifecycle, configuration, and compliance with IT policies</p>	<ul style="list-style-type: none"> • Simplify and streamline the management and support of enterprise PCs • Reduce the cost of creating, testing, provisioning and migrating PC images • Lockdown PCs with Virtual Rights Management (VRM) technology while preserving end user freedom • Reduce costs by eliminating hardware dependent PC images • Improve flexibility of PC purchasing and lease cycles

SPECIFICATIONS

Host System Requirements for End Users

PC Hardware

- Standard PC
- 500MHz or faster compatible x86 processor (recommended; 400MHz minimum)

Compatible processors include

- Intel®: Celeron®, Pentium® II, Pentium III, Pentium 4, Pentium M, Xeon
- AMD: Athlon, Athlon MP, Athlon XP, Duron, Opteron
- Multiprocessor systems supported
- Experimental support for AMD64 Opteron, Athlon 64 or Intel IA-32e CPU

Memory

- 256MB recommended, 128MB minimum

Display

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

Disk Drives

- 80MB free space required for basic installation
- At least 1GB free disk space recommended for the guest operating system and applications
- IDE or SCSI hard drives, CD-ROM and DVD-ROM drives supported

Windows Host Operating Systems

- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
- Windows XP Professional and Windows XP Home Edition with Service Pack 1 or 2

- Windows 2000 Professional Service Pack 3 or 4, Windows 2000 Server Service Pack 3 or 4, Windows 2000 Advanced Server Service Pack 3 or 4

Host System Requirements for ACE Manager

Windows Host Operating Systems

- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
- Windows XP Professional and Windows XP Home Edition with Service Pack 1 or 2
- Windows 2000 Professional Service Pack 3 or 4, Windows 2000 Server Service Pack 3 or 4, Windows 2000 Advanced Server Service Pack 3 or 4

SYSTEM REQUIREMENTS

Please see http://www.vmware.com/support/ace/doc/intro_sysreqs_ace.html for a complete listing of current system requirements.