



VMware ACE

The Assured Computing Environment for the Enterprise

AT A GLANCE

VMware® ACE gives security administrators the ability to lock down PC endpoints and protect critical company resources against the risks presented by unmanaged PCs. With VMware ACE, security administrators package an IT-managed PC within a secured virtual machine and deploy it to an unmanaged physical PC. Once installed, VMware ACE provides a secured and IT-compliant PC endpoint, enabling safe access to IT resources.

BENEFITS

- Provision secured, IT-managed endpoints
- Secure unmanaged PCs used by offshore workers, telecommuters, and contractors
- Secure confidential data on endpoint PCs
- Encrypt and protect sensitive enterprise intellectual property and personally identifiable information
- Run multiple secure PC environments on a single PC
- Create hardware-independent, sandboxed PC environments that run on any PC

How is VMware ACE Used in the Enterprise?

Enterprise applications and confidential data are accessed by an increasing number of unmanaged PCs used by contractors, out-sourcers, telecommuters, and partners. Unmanaged PCs are not owned or maintained by IT and therefore present increased costs and security risks.

VMware ACE offers complete control of the hardware configuration and networking capabilities of an unmanaged PC, transforming it into an IT-compliant PC endpoint. This unique capability for improving endpoint security can be used internally, remotely, connected or disconnected from the trusted network. VMware ACE increases the security and reduces the cost of enabling unmanaged PCs to access IT resources.

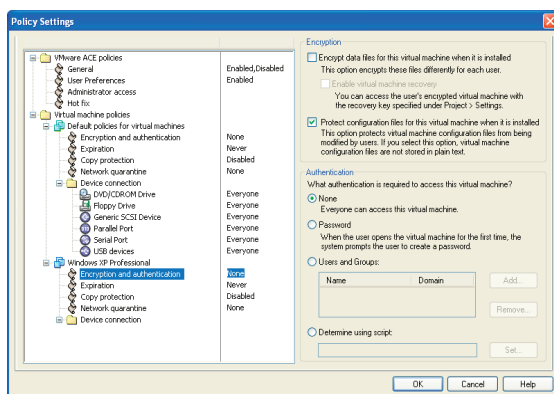
How Does VMware ACE Work?

Using VMware ACE Manager, security administrators create MSI-compliant deployment packages that are comprised of:

- One or more self-contained virtual machines with an operating system, enterprise and security applications, and data
- Security policies that control encryption, authentication, expiration, copy protection, network access, and device access for the virtual machine(s)

Security administrators then distribute the VMware ACE package to end users via direct download, provisioning tool, or DVD/CD media. End users install this package to create a secured and IT-managed endpoint.

VMware ACE Virtual Rights Management (VRM) centralizes management of security policies and access rights applied to VMware virtual machines in order to control PC environment lifecycles, and enable endpoint compliance with IT policies.



Virtual Rights Management technology built into VMware ACE Manager enables central security policy control over expiration, authentication, encryption, network access, device access, and copy protection for VMware ACE deployed on end-user PCs.

“VMware ACE will allow us to provide a home-based staff member or visiting contractor with virtual machine containing an operating system, and the software they need to do their work. The product’s Virtual Rights Management technology enables us to set up access control, image version control, image expiration, copy protection and virus control, protecting Baptist Healthcare System data.”

*Tom Taylor, senior client server analyst,
Baptist Healthcare System*

KEY FEATURES

- **Centralized security and management policies.** Virtual Rights Management (VRM) centralizes management of security policies and access rights applied to VMware ACE running on an end-user PC.
- **Secured computing environment.** Secure the entire VMware ACE environment, including data and system configuration, with authentication and seamless encryption.
- **Rules-based network access.** Enable endpoint compliance by identifying and quarantining expired, unauthorized or out-of-date VMware ACE environments.
- **Device control.** Grant or deny access to host PC devices such as printers, USB memory keys, or DVD/CD writers.
- **Digital Rights Management (DRM) capability.** Prevent end users from copying VMware ACE to a separate or removable device, network file system or another PC.
- **Expiration control.** Configure VMware ACE to expire at a pre-determined time, or after a pre-set period.
- **Design once, deploy anywhere.** Create standardized hardware-independent PC environments and deploy them to any standard PC.
- **Customizable end-user interface.** Customize the behavior and look and feel for end users.
- **Flexible computing environment.** End users can revert to a previous state within seconds. End users can work in the VMware ACE environment while connected or when disconnected from the network.

Product Specifications and System Requirements

For detailed product specifications and system requirements refer to the VMware ACE Administrator's Manual located at http://www.vmware.com/support/pubs/ace_pubs.html.