

## VMware® ACE 2.5

### Unternehmensweite Bereitstellung sicherer und gemanagter virtueller Desktops

#### AUF EINEM BLICK

VMware® ACE 2.5 ermöglicht IT-Organisationen, Unternehmens-Arbeitsumgebungen als sichere, gemanagte virtuelle Maschinen für Mitarbeiter des Unternehmens auf jedem beliebigen PC bereitzustellen. Mit VMware ACE können Unternehmen Remote-Anwendern und mobilen Mitarbeitern wertvolle Ressourcen zur Verfügung stellen und sichere Unternehmens-Desktops dank Pocket ACE überall bereitstellen. Darüber hinaus ist VMware ACE eine Hilfe bei der Einhaltung wichtiger Compliance-Initiativen und bei der Kontrolle des Zugriffs auf Anwendungen, die auf gemeinsam genutzten PCs laufen.

#### VORTEILE

- Senkung der Kosten für das Desktop-Management durch Bereitstellung von unternehmenskonformen, hardwareunabhängigen virtuellen Desktops in heterogenen Umgebungen, darunter auch nicht gemanagte und Drittanbieter-PCs.
- Compliance-Optimierung durch Zertifizierung und Ausführung von Anwendungen, die vertrauliche Informationen speichern/verarbeiten, in einem sicheren, gemanagten virtuellen Desktop.
- Reduzierung von PC-Sicherheitsrisiken und zentrale Kontrolle der Endpunktsicherheit mit gesperrten, von der IT-Abteilung gemanagten virtuellen Desktops.
- Senkung der Hardware-Kosten durch Konsolidierung mehrerer Arbeitslasten auf einem einzigen PC und durch Bereitstellung „virtueller Laptops“ statt vollständig konfigurierter PCs.
- Sicherstellung der Business Continuity durch Bereitstellung von unterbrechungsfreiem Zugriff auf eine sichere Unternehmensumgebung über Wechselmedien mit Pocket ACE.

#### Wie wird VMware ACE 2.5 eingesetzt?

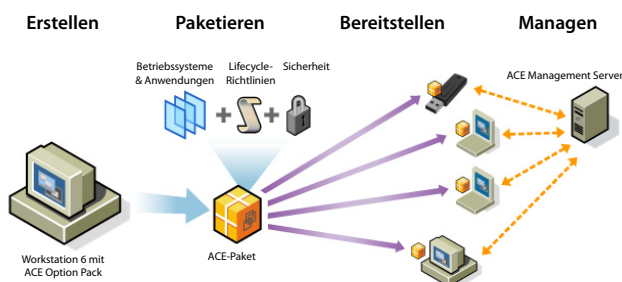
IT-Organisationen müssen viele Herausforderungen meistern, darunter steigende Kosten für Desktop-Management und -Wartung, komplexe Client-Umgebungen, PC-Sicherheitsrisiken im Zusammenhang mit Remote-Anwendern und mobilen Mitarbeitern, Einhaltung behördlicher Auflagen und Probleme mit der Betriebssystemkompatibilität bei der Systemmigration.

VMware ACE 2.5 bietet eine Lösung für diese Herausforderungen, indem das Betriebssystem mithilfe von Virtualisierungstechnologie von der Hardware entkoppelt wird. So können im Unternehmen Arbeitsumgebungen in Form von gemanagten, gesperrten virtuellen Maschinen bereitgestellt werden, die unabhängig vom Host-Betriebssystem und der zugrunde liegenden Hardware ausgeführt werden können.

Mit der Technologie „Virtual Rights Management“ (VRM) zur Anwendung von Sicherheitsrichtlinien auf virtuelle Maschinen ermöglicht ACE die Kontrolle der Endpunktsicherheit über Authentifizierung, sichere Konnektivität, Datenverschlüsselung, Geräte- und Kopierschutz sowie Ablaufzeitpunkte für virtuelle Maschinen. IT-Organisationen können so ein höheres Maß an Flexibilität, Produktivität und Kontrolle erzielen.

#### VMware ACE 2.5 ermöglicht Folgendes:

- **Sichere mobile Datenverarbeitung** – Paketieren Sie sichere, gemanagte virtuelle Desktops, die Unternehmensstandards und Sicherheitsrichtlinien erfüllen. Stellen Sie die vollständig isolierten Pakete für Remote- und mobile Anwender auf jedem beliebigen PC bereit, einschließlich nicht gemanagter PCs und PCs von Drittanbietern.
- **Mitarbeitereigene Computerausrüstung** – Senken Sie die Kosten mit einer sicheren, gesperrten Unternehmens-Arbeitsumgebung, die auf jedem beliebigen PC ausgeführt werden kann.
- **Compliance in einer Sandbox-Umgebung** – Managen und erhalten Sie die Compliance mit aktuellen Regeln und Standards, indem Sie den Zugriff auf vertrauliche Daten über streng kontrollierte Images von Unternehmens-Desktops absichern.
- **Unterstützung von Legacy-Betriebssystemen** – Minimieren Sie Probleme mit der Anwendungs- und Betriebssystemkompatibilität bei der Systemmigration, indem Sie Legacy-Anwendungen und -Betriebssysteme in isolierten virtuellen Maschinen neu hosten.
- **Business Continuity für Desktops** – Bieten Sie Organisationen mittels Pocket ACE unterbrechungsfreien Zugriff auf sichere Unternehmens-Arbeitsumgebungen, die auf USB-Sticks gespeichert sind.
- **Kioske/gemeinsam genutzte PCs** – Stellen Sie sicheren und kontrollierten Zugriff auf Anwendungen bereit, die auf gemeinsam genutzten physischen PCs ausgeführt werden.



Erstellen hardwareunabhängiger, von der IT-Abteilung gemanagter PCs mit virtuellen Maschinen und Bereitstellen auf physischen PCs oder mobilen Geräten.

## HAUPTMERKMALE

## VMware ACE 2.5 – Lösungsumfang

### VMware Workstation 6.5

Mit VMware Workstation 6.5 können Sie hardwareunabhängige, sichere, von der IT-Abteilung gemanagte virtuelle Desktops, die aus einem Betriebssystem, Anwendungen und Konfigurationen bestehen, einfach erstellen, konfigurieren und paketieren. Virtuelle ACE-Maschinen können über CD/DVD, ein gemeinsames Netzlaufwerk und mobile Geräte wie USB-Flash-Laufwerke oder iPods auf einem ordnungsgemäß lizenzierten PC bereitgestellt werden.

### VMware ACE Management Server 2.5

Die optionale Komponente ACE Management Server bietet über eine webbasierte Konsole zentrales Management von und zentrale Kontrolle über im Einsatz befindliche virtuelle ACE-Maschinen. Mit ACE Management Server können Sie dynamische Richtlinien-Updates konfigurieren und per Push-Verfahren auf bereitgestellte virtuelle ACE-Maschinen anwenden. Sie können virtuelle Desktops kontrollieren und jederzeit aktivieren bzw. deaktivieren und die Integration in Active Directory für rollenbasierte Zugriffsauthentifizierung nutzen.

### VMware Player 2.5

VMware Player ist im Lieferumfang von VMware ACE enthalten und stellt die Laufzeit-Virtualisierungs-Engine zur Ausführung entsprechend lizenzierter virtueller ACE-Maschinen auf Linux- und Windows-Hosts bereit.

## Hauptmerkmale

### Sicherheit am Unternehmens-Desktop

- **Granulare Sicherheitsrichtlinien:** Nutzen Sie die VRM-Technologie, um Sicherheitsrichtlinien und Zugriffsrechte für virtuelle VMware ACE-Maschinen auf Anwender-PCs anzuwenden und zu managen.
- **Sicherer Zugriff:** Sichern Sie die gesamte VMware ACE-Umgebung ab mit Authentifizierung und Verschlüsselung der virtuellen Festplatte, einschließlich Daten und Systemkonfiguration.
- **Geräte-Kontrolle:** Sperren Sie PCs durch Gewähren oder Verweigern des Zugriffs auf Host-PC-Geräte wie Drucker, USB-Sticks oder DVD/CD-Laufwerke auf Basis von Gerätetyp oder ID.
- **Ablaufkontrolle:** Konfigurieren Sie den Ablauf virtueller VMware ACE-Maschinen an einem vordefinierten Datum oder nach einem eingestellten Zeitraum.
- **Sichere Netzwerkkonnektivität:** Ermöglichen Sie die Endpunkt-Compliance mit regelbasiertem Netzwerkzugriff durch Identifizieren und Isolieren nicht autorisierter und abgelaufener VMware ACE-Umgebungen nach Port- oder Verkehrstyp.
- **Kiosk-Modus:** Stellen Sie sicheren und kontrollierten Zugriff auf Anwendungen bereit, die auf gemeinsam genutzten physischen PCs laufen.
- **Eingebauter Schutz vor Keyloggern:** Vermeiden Sie Identitätsdiebstahl, indem Sie die Laufzeiteinstellungen virtueller ACE-Maschinen zum Schutz vor Keyloggern konfigurieren.

- **Kopierschutz und Ressourcensignaturen:** Kopierschutz- und Ressourcensignatur-Richtlinien bieten Schutz vor Missbrauch.

### Robustes Management virtueller Desktops

- **Zentrale Managementkonsole:** Sie können Tausende im Einsatz befindliche virtuelle ACE-Maschinen von einem zentralen Standort aus anzeigen, verfolgen und managen.
- **Erzwingung von Richtlinien für Endpunkte:** Sie können dynamische Richtlinien-Updates konfigurieren und per Push-Verfahren auf im Einsatz befindliche virtuelle ACE-Maschinen anwenden, um die Aktivierung, Deaktivierung und Authentifizierung gemanagter virtueller ACE-Maschinen zu kontrollieren.
- **Integration von Active Directory:** Mit der Active Directory-Infrastruktur können Sie rollenbasierten Zugriff auf virtuelle ACE-Maschinen konfigurieren und authentifizieren.

### Schnelle Desktop-Bereitstellung

- **Einmal erstellt – überall verwendet:** Erstellen Sie mit VMware Workstation standardisierte, hardwareunabhängige Unternehmens-Desktop-Umgebungen mit sicheren, gemanagten virtuellen Desktops, die sich einfach auf beliebigen PCs oder mobilen Geräten wie Flash-Laufwerken bereitstellen lassen.
- **Schnelle Wiederherstellung mit Snapshots:** Mit vorab erfassten Snapshots fehlerfreier Desktop-Zustände erstellen Sie Systeme im Handumdrehen neu.

### Nahtlose Anwendererfahrung mit virtuellen Desktops

- **Umfassender virtueller Desktop:** In einer sicheren virtuellen ACE-Maschine gespeicherte Anwendungen lassen sich direkt über das Host-Startmenü ausführen, wobei die Kontrolle durch die VRM-Technologie sichergestellt wird.
- **Anwendermobilität:** Mobile Mitarbeiter können dank Pocket ACE jederzeit und an jedem Ort mit sicheren virtuellen Unternehmens-Desktops arbeiten, die auf Wechselmedien gespeichert sind.
- **Integrierte Desktop-Erfahrung im „Unity“-Modus:** Anwender können auf Anwendungen innerhalb von virtuellen ACE-Maschinen zugreifen, als würden sie auf ihrem normalen Standard-Desktop laufen.

### Business Continuity

- **Sicherer Unternehmens-Desktop überall:** Bieten Sie mittels Pocket ACE unterbrechungsfreien Zugriff auf sichere Unternehmens-Arbeitsumgebungen, die auf USB-Sticks gespeichert sind.

## Produktspezifikationen und Systemanforderungen

Eine breite Palette von Plattformen und Geräten werden unterstützt, einschließlich Windows und Linux auf Desktops, Laptops und mobilen Geräten. Ausführliche Produktspezifikationen und Systemanforderungen finden Sie unter <http://www.vmware.com/go/ace>.

Für VMware ACE 2.5 stehen verschiedene Support-Optionen zur Verfügung, einschließlich globaler Abonnementprogramme für Support und Software-Upgrades der Stufen „Platin“ und „Gold“ mit Laufzeiten von einem oder mehreren Jahren sowie Support-Pakete für einen, drei und fünf Fälle.

## Weitere Informationen

Wenn Sie ein VMware-Produkt kaufen möchten oder weitere Informationen benötigen, setzen Sie sich unter der folgenden Telefonnummer direkt mit VMware in Verbindung: +49 (0)89 370 617 000. Sie können auch unsere Website unter [www.vmware.com/de/products](http://www.vmware.com/de/products) besuchen oder online nach einem autorisierten Händler suchen.