

SOLUTION BRIEF

Securing Virtual Environments

how can I virtualize
my mission-critical
servers while
maintaining or
improving security?

agility
made possible™





CA ControlMinder™ for Virtual Environments provides security controls that help you confidently virtualize even your most critical systems.



executive summary

Challenge

In a virtual environment, the security challenges multiply rapidly and introduce new risks. Where an organization might have had a single application server in the past, in a virtual environment they could see that quickly evolve to thirty servers. How can security, such as segregation of duties for privileged users, be enabled, not only on a physical server, but also on the virtual machines it hosts, as well as the applications running on those virtual machines? The lack of a viable security solution for virtual environments has been holding many organizations back from moving their mission-critical applications there and taking full advantage of virtualization. For organizations that are virtualizing production systems rapidly, business and regulatory requirements are demanding new security controls.

Business needs

Today's businesses are demanding that IT meet key requirements:

- Compliance for the data center for all applicable regulations (e.g., PCI, SOX)
- Clearly-understood and controlled risks
- Reduced costs for the same or improved service
- Improved responsiveness

Virtualization technology helps IT to reduce costs and improve response times, while also providing greater flexibility for service delivery. However, virtualization also adds a layer of management complexity. IT organizations have developed specific operational and technical requirements to enable compliance as well as understand and control security risks.

Solution benefits

CA ControlMinder for Virtual Environments secures privileged user access to virtual machines, hypervisors, and virtual appliances—helping organizations control privileged user actions, secure access to the virtual environment, and comply with industry mandates. It delivers key capabilities to manage privileged user passwords, harden the hypervisor, and monitor privileged user activity. CA ControlMinder also provides a centralized foundation that serves as a single portal for securing privileged user access across virtual and physical environments.

CA Technologies has been providing host-based access control solutions for distributed environments for more than fifteen years. To meet the needs of its customers, CA Technologies in partnership with HyTrust™ introduces CA ControlMinder for Virtual Environments—a scalable and extensible product that secures access to the virtual environment. CA ControlMinder is quick to deploy with extensive out-of-the-box support and easy-to-use with modern administrative interfaces and reporting dashboards—which helps to deliver a rapid TTV for customers. Other security products from CA Technologies that are integrated with CA ControlMinder include CA IdentityMinder™, CA GovernanceMinder™, CA SiteMinder®, CA DataMinder™, CA AuthMinder™, and CA RiskMinder™.

Section 1: Challenge

Security concerns often prevent virtualization of mission-critical systems

Server virtualization promotes flexible utilization of IT resources, reduced capital costs, improved energy efficiency, highly-available applications, and improved business continuity. However, virtualization brings along with it a unique set of challenges around the management and security of the virtual infrastructure. The virtualized environment is highly automated and complex, which adds to the difficulty. Regulations and the risks associated with privileged users in a virtual environment prevent many organizations from achieving the benefits of virtualization on their production and mission-critical systems and applications.

Virtual environments are subject to regulation

After an organization virtualizes its “low hanging fruit,” mission-critical applications are next. Increasingly, not just application servers but also databases, network switches and firewalls are being virtualized. As virtualization adoption matures and more critical systems and applications are moved into production virtual environments the demand will increase for security, in large part due to regulatory requirements. Already virtual environments are being included in the scope of regulations such as from the Payment Card Industry (PCI) and Sarbanes-Oxley (SOX) and formal guidance for secure virtualization has been published by the National Institute of Standards and Technology (NIST).

There is good reason that all of these standards bodies are formalizing their security frameworks for virtualization. In the physical world, servers, switches, routers and firewalls are bolted and locked into racks. Administering these systems may require physical access (probably with a keycard) into a physical datacenter (perhaps with mounted video cameras). In the virtual world, these security measures are largely bypassed. Administrative access to virtual infrastructure is equivalent to having access to every system, application, and security appliance in the datacenter. There is no keycard on the virtual door of the virtual datacenter. There are no virtual locks on the virtual racks. And it is often difficult for organization to see and understand what changes are being made and/or requested.

Privileged identity management is more important than ever

Privileged Identity Management is an important element of every security best practice. According to a CA Technologies sponsored research report, “maintaining security and access control” is the number one challenge organizations face in virtual server management, which has kept many organizations from moving mission-critical applications into a virtual environment. As virtual server use continues to grow, organizations run the risk of losing control of their environments and the potential for malicious activity increases dramatically.

This was dramatically borne out during an incident in 2011 at a global pharmaceutical company. A former IT staffer who had been terminated used his credentials to illegally gain access to fifteen VMware host systems and deleted 88 virtual machines that were running e-mail, order entry, payroll and other services. This action froze the company’s operations for a number of days, leaving employees unable to ship product, to cut checks, or even to communicate via e-mail or Blackberry, with an estimated recovery cost of \$800,000.

Section 2: Business needs

Virtualization meets key business needs, but security requirements must be met

In today’s business environment, organizations are demanding that IT meet key business requirements:

- Compliance for the data center for all applicable regulations (e.g., PCI, SOX)
- Clearly-understood and controlled risks
- Reduced costs for the same or improved service
- Improved responsiveness

Virtualization addresses business concerns by reducing costs and improving responsiveness, but also adds a management layer that leads to compliance and risk reduction challenges. To address these challenges, IT organizations are developing operational and technical requirements before virtualization is considered for production systems. Requirements typically include:

- Control over privileged users and access to enterprise data
- Reduced administrative cost and complexity through automation of password changes without installing agents
- Central control of application IDs
- Enhanced security with automatic logins by preventing ‘over the shoulder’ password theft
- Regulatory compliance through proactively reporting on the status of key compliance policies
- Quickly-generate privileged user reports from secure activity logs

Meeting in-depth security requirements benefits IT

The ability to control access to the virtual infrastructure can significantly reduce the risk of compromise, which in turn means that IT organizations can virtualize applications that were once considered off-limits.

Being able to assess the integrity of the hypervisor configuration and validate the security of the hardware not only reduces the risk of compromise but also automates tedious maintenance activities and eliminates configuration drift.

Defining and then automatically enforcing security policies prevents administrators from making costly mistakes, like moving a virtual machine with sensitive data to an untrusted hypervisor or network.

Automating controls and providing clear visibility in the form of audit-quality logs enables organizations to confidently virtualize in the face of security demands and auditor scrutiny.

Section 3: Solution benefits

CA ControlMinder for Virtual Environments extends security from physical to virtual environments

CA ControlMinder secures privileged user access to virtual machines, hypervisors, and virtual appliances—helping organizations control privileged user actions, secure access to the virtual environment, and comply with industry mandates. It delivers key capabilities to manage privileged user passwords, harden the hypervisor, and monitor privileged user activity. CA ControlMinder also provides a centralized foundation that serves as a single portal for securing privileged user access across virtual and physical environments.

CA ControlMinder provides a proactive approach to securing sensitive information and critical systems without impacting normal business and IT activities. It helps to mitigate both internal and external risk by controlling how business or privileged users access and use enterprise data. This can result in a higher level of security, lower administrative costs, easier audit/compliance processes and a better user experience.

Key product capabilities

CA ControlMinder hardens the hypervisor and centrally controls and audits privileged users, as well as provides temporary privileged access across virtual and physical servers, applications, and devices—all from a single, central management console. Key capabilities of the product include:

Privileged user password management

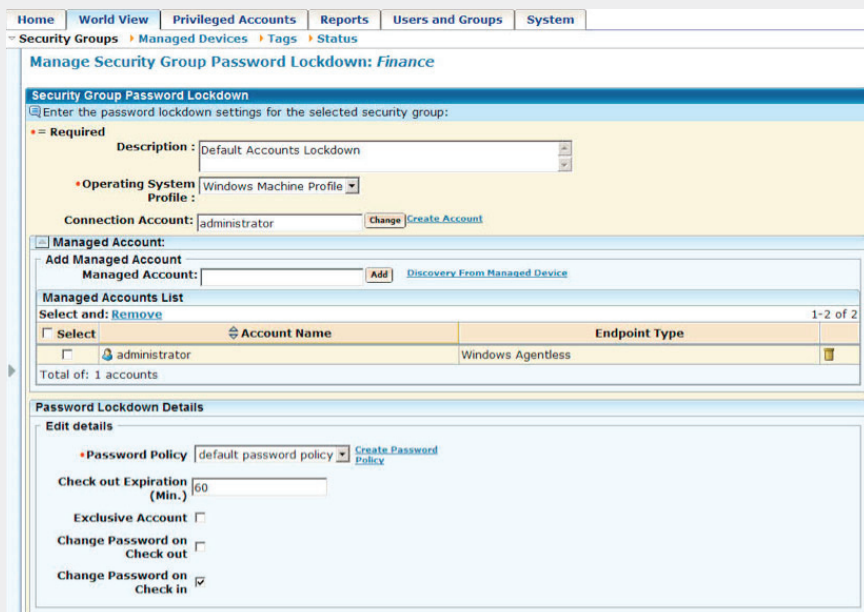
Privileged users have extensive access and capabilities to critical IT resources in a virtualized environment. In addition to the malicious activity outlined above, a privileged user (hypervisor) could start/stop virtual machines, revert a VM to an earlier version, or copy a VM (with its accompanying

data) to an external storage device. CA ControlMinder provides secure access to privileged accounts and helps maintain the accountability of privileged users. It enables the issuance of passwords on a temporary, one-time use basis, or as necessary, while providing accountability of privileged user actions through secure auditing. A simple workflow for requesting and checking out a system-generated, one-time use password facilitates password checkout and eliminates the need to share passwords. Users can check in the password once their task is completed, or CA ControlMinder can be configured to automatically check in the password after a specific time period.

Figure A.

Configuring default password policy.

Setting the default password policy for a security group allows an administrator to do this once, from a central location.



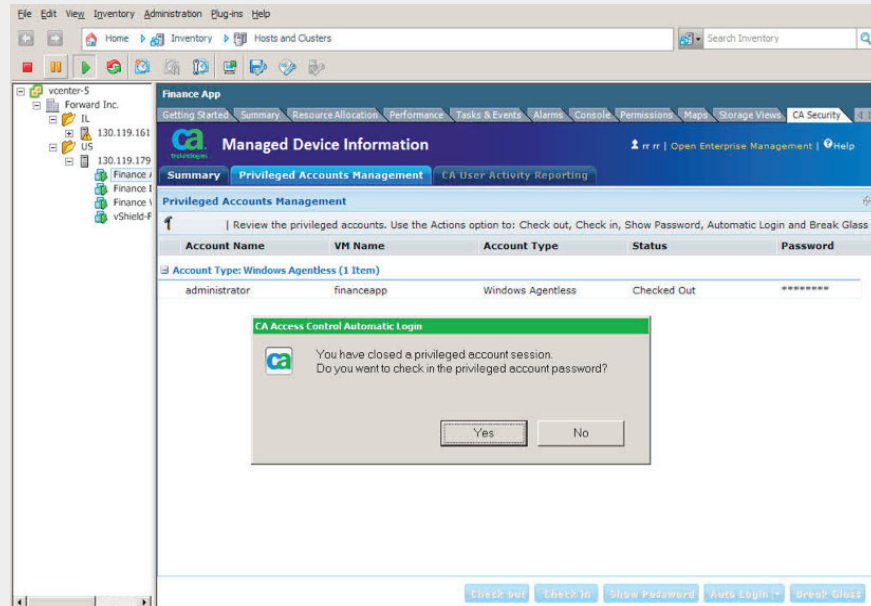
The screenshot shows the 'Manage Security Group Password Lockdown' configuration page for the 'Finance' group. The interface includes a navigation menu at the top with options like Home, World View, Privileged Accounts, Reports, Users and Groups, and System. Below the navigation, there are tabs for Security Groups, Managed Devices, Tags, and Status. The main content area is divided into several sections:

- Required:** This section contains a 'Description' dropdown menu set to 'Default Accounts Lockdown', an 'Operating System Profile' dropdown menu set to 'Windows Machine Profile', and a 'Connection Account' text field set to 'administrator'. There are 'Change' and 'Create Account' buttons next to the connection account field.
- Managed Account:** This section includes an 'Add Managed Account' form with an 'Add' button and a 'Discovery From Managed Device' link. Below this is a 'Managed Accounts List' table with columns for 'Select', 'Account Name', and 'Endpoint Type'. The table shows one account: 'administrator' with 'Windows Agentless' as the endpoint type. There are 'Select' and 'Remove' buttons for each row. A 'Total of: 1 accounts' summary is shown at the bottom of the table.
- Password Lockdown Details:** This section has an 'Edit details' sub-section. It includes a 'Password Policy' dropdown menu set to 'default password policy' with a 'Create Password Policy' button. Below this are several checkboxes: 'Check out Expiration (Min.)' with a value of '60', 'Exclusive Account' (unchecked), 'Change Password on Check out' (unchecked), and 'Change Password on Check in' (checked).

CA ControlMinder comes with fully functional and customizable workflows that enable common out-of-the-box use cases—examples include “break glass” and password request scenarios. A “break glass” scenario occurs when privileged users need immediate access to accounts that they are not authorized to manage. It allows users to obtain an account password immediately without approval, eliminating the possibility of delay in case of emergency, but securely logs all transactions for audit purposes. In contrast, a password request scenario allows the organization to only authorize passwords per request for a limited period of time. In this scenario, user requests go to their managers for approval, and can include a time-period required for accessing the privileged account. Once the request is approved, users can check out the password and have access to the requested systems only for the approved time period.

Figure B.
Privileged account check in.

After closing a privileged user session, CA ControlMinder asks the user to confirm they wish to check the password in so it can be used again.



CA ControlMinder is also designed to provide third-party applications with programmatic access to passwords—removing the need to hard code passwords in scripts. It supports a multitude of servers, applications (including databases) and devices (like routers) in a physical or virtual environment.

User activity monitoring

CA ControlMinder audits activity performed on the hypervisor and keeps track of privileged account usage based on the original user ID. In addition, the integration with CA User Activity Reporting allows customers to extend auditing capabilities beyond CA ControlMinder events—thus providing a holistic view of privileged activity performed in the IT environment.

For visual user activity recording, CA Session Recording is available separately. This allows an organization to create a secure visual record of a privileged user’s session. This is especially applicable for browser-based sessions that are entirely mouse-driven and thus, cannot be recorded by traditional keyloggers.

Segregation of duties

CA ControlMinder makes it possible to enforce industry-standard segregation of duties rules on the hypervisor. For example, it can prevent the hypervisor administrator from accessing virtual machine configurations via the hypervisor—thus forcing all virtual environment changes to be governed through the management consoles only.

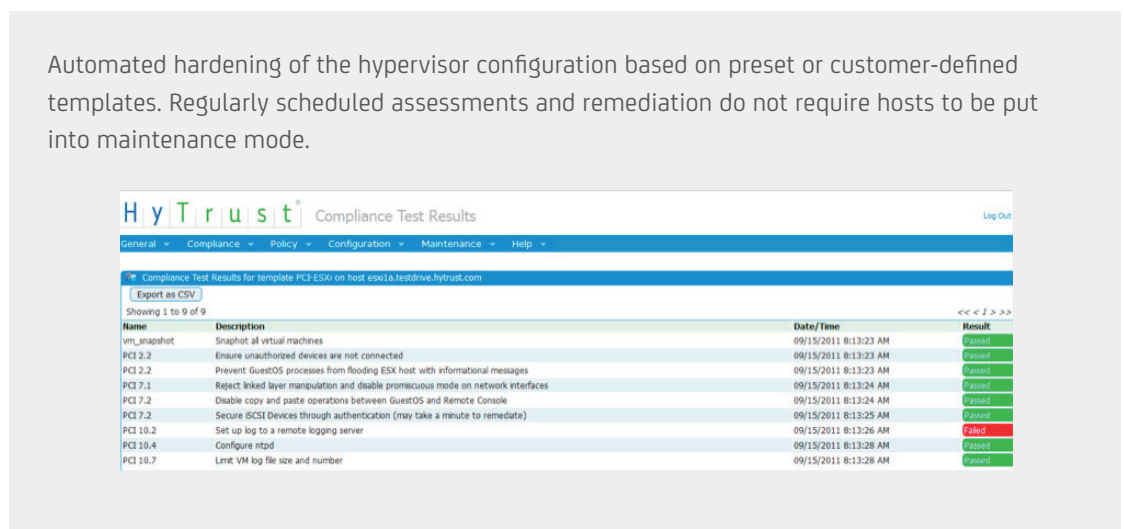
Secure multi-tenancy

CA ControlMinder extends traditional physical network segmentation to virtual environments. It can provide improved tenant isolation for better compliance and MSP enablement, inter-VM traffic control over policy-based framework and higher VM density on physical hardware by enabling guests with various trust-levels to share a common host with least privileged access between members of different zones.

Hypervisor hardening

CA ControlMinder, which includes the HyTrust® Appliance, provides a broad range of capabilities to harden the hypervisor. It controls access to the system resources, programs, files, and processes through a stringent series of criteria that includes time, login method, network attributes and access program. It is possible to configure newly developed VMware servers to one of the predefined security configurations in order to consistently monitor VMware vSphere hosts to identify configuration errors using pre-built assessment frameworks and actively remediate problems with minimal service interruption.

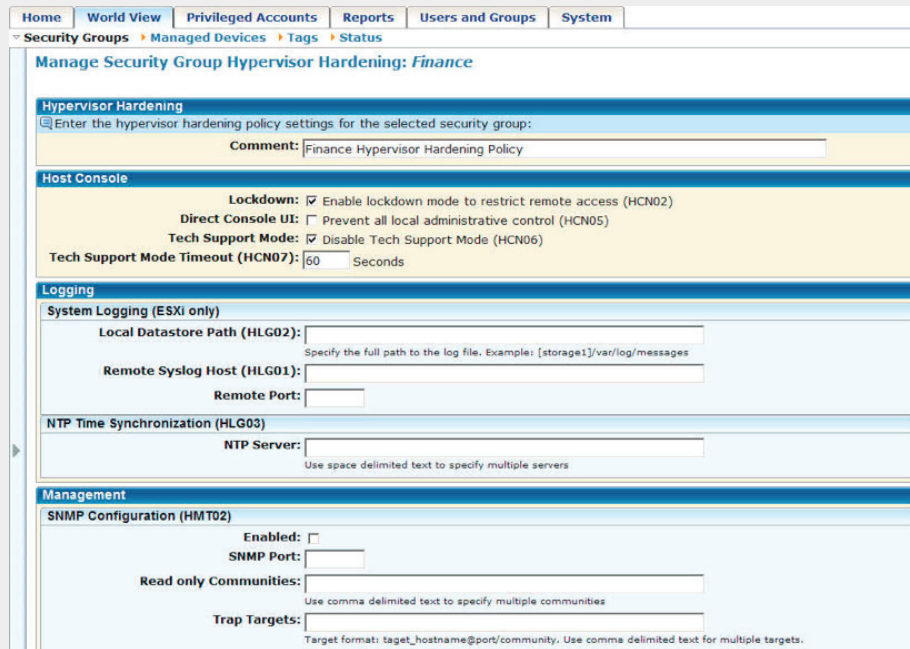
Figure C.
Compliance reporting.



These controls are essential to help enforce industry-standard segregation of duties rules on the hypervisor. For example, CA ControlMinder can prevent the virtualization administrator from accessing virtual machine configurations via the hypervisor—thus forcing all virtualization environment changes to be governed through the management consoles.

Figure D.
Managing the
hypervisor hardening.

Controlling access to the Hypervisor is critical to enable security of the virtual environment as well as meeting regulations.



The screenshot shows the configuration page for 'Manage Security Group Hypervisor Hardening: Finance'. The interface includes a navigation menu at the top with options like Home, World View, Privileged Accounts, Reports, Users and Groups, and System. Below the navigation, there are breadcrumb links for Security Groups, Managed Devices, Tags, and Status. The main content area is divided into several sections:

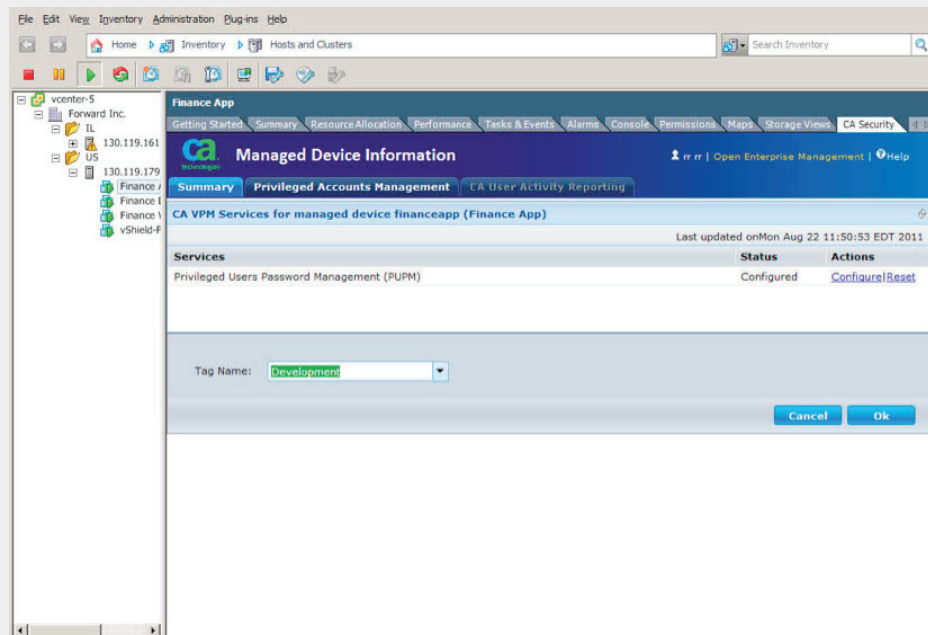
- Hypervisor Hardening:** Includes a search icon and a text field for 'Enter the hypervisor hardening policy settings for the selected security group:'. A 'Comment' field contains 'Finance Hypervisor Hardening Policy'.
- Host Console:** Contains several checkboxes: 'Lockdown' (checked), 'Direct Console UI' (unchecked), and 'Tech Support Mode' (checked). A 'Tech Support Mode Timeout (HCN07)' field is set to '60' seconds.
- Logging:**
 - System Logging (ESXi only):** Includes fields for 'Local Datastore Path (HLG02)', 'Remote Syslog Host (HLG01)', and 'Remote Port'.
 - NTP Time Synchronization (HLG03):** Includes a field for 'NTP Server'.
- Management:**
 - SNMP Configuration (HMT02):** Includes an 'Enabled' checkbox (unchecked), 'SNMP Port' field, 'Read only Communities' field, and 'Trap Targets' field.

Integration with vCenter

By installing itself in the vCenter, CA ControlMinder adopts this user interface as its own, which helps vCenter administrators reduce their learning curve and quickly adapt to it. Administrators can now view the available/appropriate security services including, if applicable, exact versions so they can manage them (Install, Uninstall, Enable, Disable, Upgrade, etc.).

Figure E.
Integration with
VMware vCenter.

CA ControlMinder for Virtual Environments is delivered as a soft appliance and installs itself into the VMware vCenter, which allows administrators to quickly get up-to-speed.

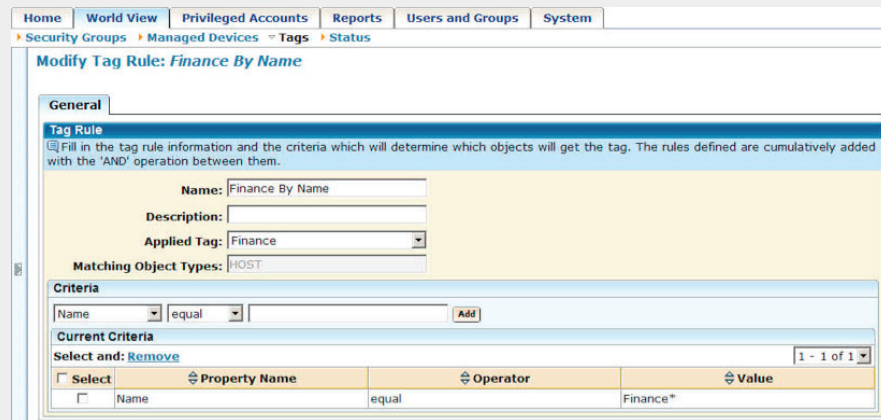


Automatic policy deployment

CA ControlMinder can track infrastructure configuration changes as well as software asset inventory, all in real-time. It also has the ability to leverage asset properties, tagging, and policies (corporate/regulatory compliance, best practices, and security hardening rules) to automatically enable and configure relevant security services in the environment.

Figure F.
Asset tagging allows security automation.

The virtual environment is extremely fast-moving. Virtual machines are often mounted and unmounted, several times an hour. Tagging allows CA ControlMinder to keep up with these changes and automatically apply a security policy.



The screenshot shows the 'Modify Tag Rule: Finance By Name' configuration page in the CA ControlMinder interface. The page is divided into several sections:

- General:** Contains the 'Tag Rule' section with the following fields:
 - Name:** Finance By Name
 - Description:** (empty)
 - Applied Tag:** Finance
 - Matching Object Types:** HOST
- Criteria:** A section for defining the rule logic. It includes a 'Name' dropdown, an 'equal' operator dropdown, and an 'Add' button.
- Current Criteria:** A table showing the current criteria for the rule. It has columns for 'Select', 'Property Name', 'Operator', and 'Value'.

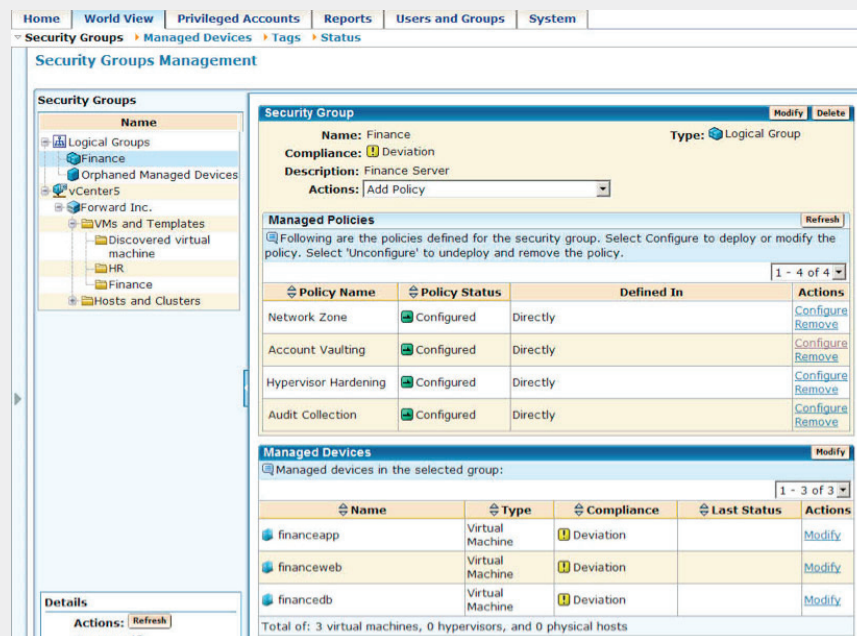
Select	Property Name	Operator	Value
<input type="checkbox"/>	Name	equal	Finance*

Common policy management

CA ControlMinder is designed to streamline the management of privileged user entitlements. It centralizes management policies that govern access to virtual servers across a large and heterogeneous virtual environment. The governing criteria include access to the hypervisor’s resources within the virtual environment, network access to and from the consoles, access to virtual machine configuration, etc. These policy management capabilities help clarify complex, cross-platform policy environments and simplify administrative tasks—providing a reliable common policy management process.

Figure G.
Security groups management.

In order to facilitate managing access rights, CA ControlMinder allows an administrator to define groups and their associated virtual machines.



Section 4

The CA Technologies advantage

CA Technologies and HyTrust combine to provide a broad range of capabilities that enable you to control the virtualization environment. HyTrust delivers significant domain expertise as an acknowledged leader in policy management and access control specifically for virtual infrastructure. HyTrust empowers organizations to virtualize more—including servers and applications that are subject to compliance—by delivering enterprise-class controls for access, accountability, and visibility to an organization's existing virtualization infrastructure.

With over 30 years of expertise delivering robust, reliable, secure enterprise-class IT management software CA Technologies offers:

- A demonstrated commitment to emerging technologies and IT delivery paradigms such as virtualization, SaaS, and cloud
- Cutting-edge best-of-breed security management technologies

CA Technologies is also uniquely positioned to help make your virtualization security a success with additional implementation and training services, including:

On-ramp to enterprise solutions

CA ControlMinder for Virtual Environments not only helps secure virtual-only deployments, but also provides an on-ramp to enterprise class solutions for securing virtual and physical environments—protecting virtualization security investments in the long run.

CA Services

CA Services forms an integral part of the overall solution, providing assessment, implementation, health check, and other pre- and post-deployment services. This enables organizations to accelerate time-to-value for their virtualization investment, mitigate implementation risks, and improve the alignment between IT and business processes.

CA Services also provides Rapid Implementation services delivered through our internal staff and a network of established partners chosen to help customers achieve a successful deployment and get the desired business results as quickly as possible. Through our proven nine-stage methodology, best practices and expertise, we help customers achieve a faster time-to-value for their CA ControlMinder implementation.

CA Education

CA Education also contributes exceptional value to our offerings, providing skills training and best practices education through classrooms, virtual instructor-led training, and web-based training. This enables organizations to rapidly build expertise in virtualization and virtualization management, overcome many barriers to deployment, reduce or eliminate deployment errors, and gain fast time-to-value with a high-quality solution.

Section 5

Next steps

There is no doubt that virtualization can provide exceptional benefits for IT and business. However, almost every organization faces substantial problems delivering these benefits in a broad virtualization deployment. Security problems such as controlling identities, controlling access, and controlling information threaten to derail deployments as VM sprawl create security problems such as compliance failure, and undermine the gains in agility, efficiency, and cost control.

Fortunately, CA Technologies can help with sophisticated, robust, and innovative solutions that help to solve the difficult identity and access management security issues. If you need better ways to control identities, access, and information for your existing virtual environments as well as future enterprise-wide virtualization, and drive immediate and long-term business results; then you need to take a look at CA ControlMinder for Virtual Environments.

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.