CA Access Control for Virtual Environments

Product Guide

r2.0

Third-Party Notices

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

Sample Scripts and Sample SDK Code

The Sample Scripts and Sample SDK code included with the CA Access Control product are provided "as is", for informational purposes only. They may need to be adjusted in specific environments and should not be used in production without testing and validating them before deploying them on a production system.

CA Technologies does not provide support for these samples and cannot be responsible for any errors that these scripts may cause.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Access Control Enterprise Edition
- CA Access Control
- CA User Activity Reporting Module
- CA Identity Manager

Documentation Conventions

The CA Access Control documentation uses the following conventions:

Format	Meaning
`Mono-spaced font`	Code or program output
Italic	Emphasis or a new term
Bold	Text that you must type exactly as shown
A forward slash (/)	Platform independent directory separator used to describe UNIX and Windows paths

The documentation also uses the following special conventions when explaining command syntax and user input (in a mono-spaced font):

Format	Meaning
Italic	Information that you must supply
Between square brackets ([])	Optional operands
Between braces ({})	Set of mandatory operands
Choices separated by pipe (|).	Separates alternative operands (choose one). For example, the following means *either* a user name *or* a group name: {*username*|*groupname*}
...	Indicates that the preceding item or group of items can be repeated
Underline	Default values

Format	Meaning
A backslash at end of line preceded by a space (\)	Sometimes a command does not fit on a single line in this guide. In these cases, a space followed by a backslash (\) at the end of a line indicates that the command continues on the following line. **Note:** Avoid copying the backslash character and omit the line break. These are not part of the actual command syntax.

Example: Command Notation Conventions

The following code illustrates how command conventions are used in this guide:

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

In this example:

- The command name (ruler) is shown in regular mono-spaced font as it must be typed as shown.
- The *className* option is in italic as it is a placeholder for a class name (for example, USER).
- You can run the command without the second part enclosed in square brackets, which signifies optional operands.
- When using the optional parameter (props), you can choose the keyword *all* or, specify one or more property names separated by a comma.

File Location Conventions

The CA Access Control documentation uses the following file location conventions:

- *ACVEInstallDir*—The default CA Access Control for Virtual Environments installation directory:
  - /opt/CA/AccessControlServer/VirtualAppliance
- *ACInstallDir*—The default CA Access Control installation directory.
  - /opt/CA/AccessControl
- *ACSharedDir*—A default directory used by CA Access Control for UNIX.
  - /opt/CA/SharedComponents
- *ACServerInstallDir*—The default CA Access Control Enterprise Management installation directory.
  - /opt/CA/AccessControlServer

- *JBoss_HOME*—The default JBoss installation directory.
  - /opt/jboss-4.2.3.GA

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA Technologies product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This section contains the following topics:

About this Guide

This guide provides information about how to plan, deploy, configure and manage CA Access Control for Virtual Environments in a VMware vCenter environment.

This guide was written for system, security and VMware administrators that are tasked with managing and securing the VMware-based virtualization environment in their organizations.

Review this guide before you begin to deploy and configure CA Access Control for Virtual Environments in your environment.

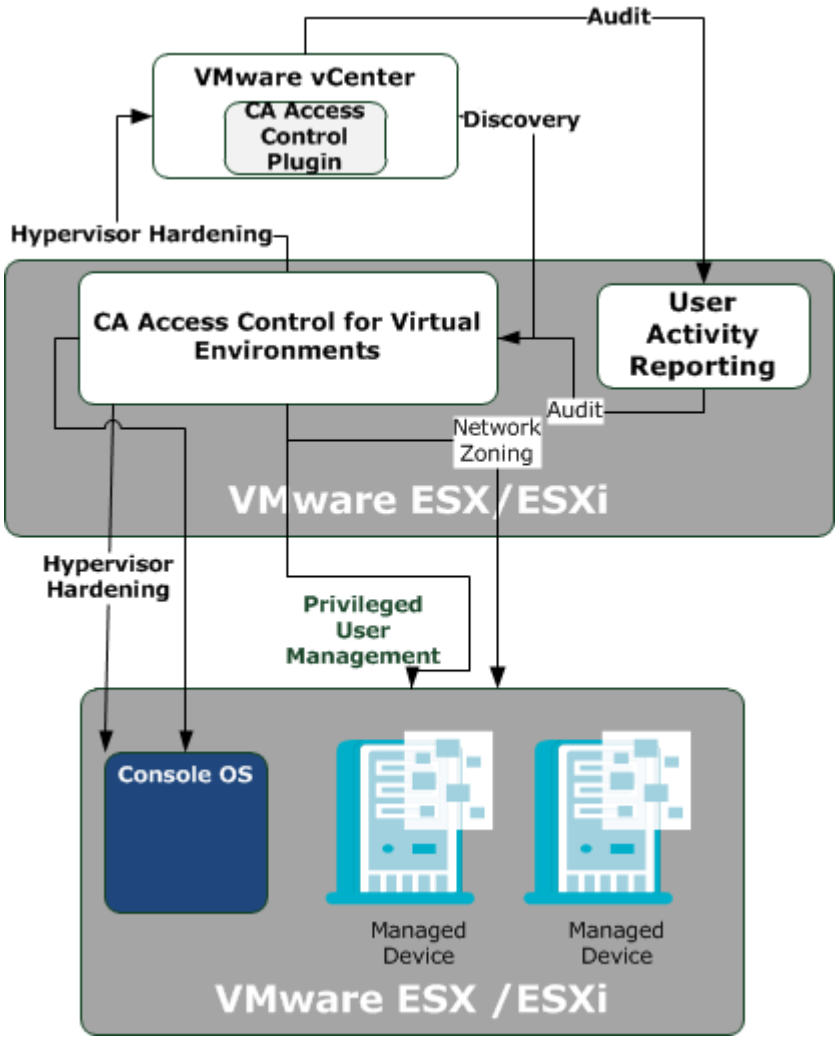
To simplify terminology, we refer to the product as CA Access Control throughout the guide.

About CA Access Control for Virtual Environments

CA Access Control for Virtual Environments (CA VE) is a standalone solution to secure privileged user access to the virtual environment that can scale as your virtual environment expands. CA Access Control for Virtual Environments integrates with VMware vCenter to offer a management interface that allows you to control managed devices, security groups, network zones and policies. Using tags, tag rules, and policies, CA Access Control for Virtual Environments can help you manage your virtual environment by automating much of your administrative tasks.

CA Access Control for Virtual Environments Environment Architecture

The following diagram displays the CA Access Control for Virtual Environments environment architecture:

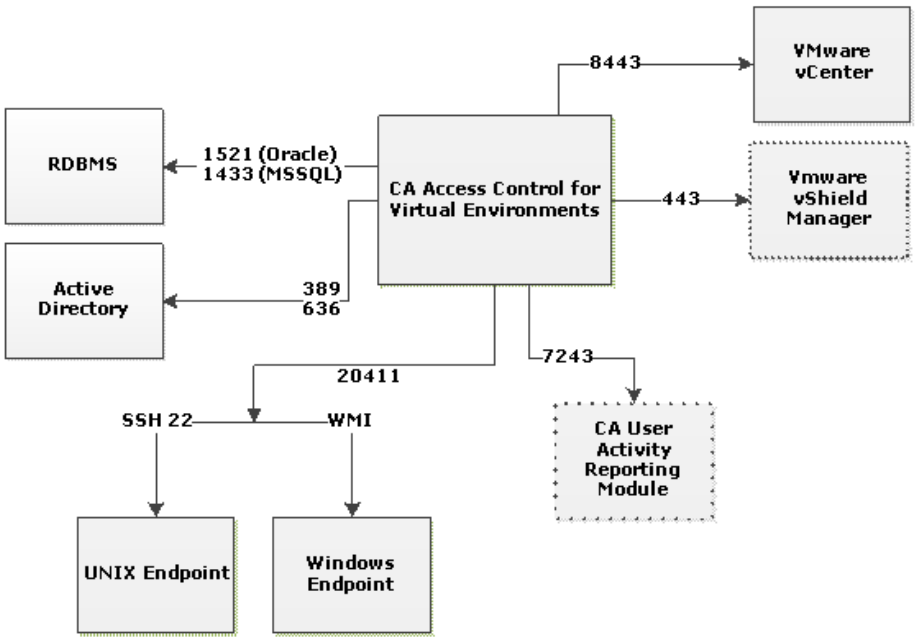


As illustrated in the preceding diagram, CA Access Control for Virtual Environments does the following:

- Privileged user password management on the managed devices in the virtual environment
- Hypervisor hardening on VMware ESX/ESXi servers
- Network zoning
- Audit events collection from managed devices for CA User Activity Reporting Module reports generation

CA Access Control for Virtual Environments Network Protocol and Ports

The following diagram displays the network protocol and ports used by CA Access Control for Virtual Environments:



Note: The dashed lines represent optional components

What Is Protected?

CA Access Control for Virtual Environments protects and enhances the following entities:

- **Hypervisor**—CA Access Control for Virtual Environments supports several hardening levels. The hardening policies can restrict user login to the VMware vCenter Server, control remote audit collection, remote management and SNMP trap collection.
- **Managed devices**—CA Access Control for Virtual Environments protects managed devices by enabling you to deploy password lockdown policies to manage privileged account passwords. You can also assign managed devices to network zones and collect audit records through audit collection policies.

Privileged Account Passwords Management

CA Access Control for Virtual Environments discovers privileged account passwords on the managed devices in your environment and stores the passwords in its database. CA Access Control for Virtual Environments provides secure storage of privileged accounts and application ID passwords and controls access to privileged accounts and passwords based on policies you define.

Network Traffic Segregation

CA Access Control for Virtual Environments controls network traffic and access by assigning managed devices to *security groups*. Security groups are logical groups of managed devices that enforce security controls on the group members. Each member of a security group can communicate with every other member inside the network zone.

CA Access Control for Virtual Environments integrates with the VMware vShield Manager to enforce network access rules using the native firewall capabilities.

Virtual Environment Tools and Interfaces Enhancement

CA Access Control for Virtual Environments enhances the native VMware virtual management tools. CA Access Control for Virtual Environments plugs in to the VMware vSphere Client that enriches the native environment by adding privileged passwords management capabilities.

Further, CA Access Control for Virtual Environments integrates with the VMWare vShield App to enforce network access rules. VMware vShield Manager is a vNIC-level firewall that enforces access control policies.

Asset Tagging

Asset tagging allows you to assign logical tags to managed devices and security groups. When assigned a tag, the managed device becomes a member of a security group that the tag applies to.

You can manually assign tags to managed devices and add the device to a security group. You can define tag rules and set rule criteria to associate managed devices to security groups according to the tags you assigned to managed devices.

Chapter 2: Preparing Your Implementation

This section contains the following topics:

Sizing Your Implementation

Before you implement CA Access Control for Virtual Environments, determine the size of your implementation and allocate resources accordingly. Use the following information to help you assess the scope of your implementation.

The following table describes the supported configuration for CA Access Control for Virtual Environments:

Component	Limits
Virtual machines per host	320
Hosts per vCenter Server	3200
Registered virtual machines per vCenter Server	15000
Virtual machines per datacenter	5000
Power-on virtual machines per vCenter Server	10000

Components of CA Access Control for Virtual Environments

CA Access Control for Virtual Environments consists of the following software components:

CA Access Control Server

The CA Access Control Server is installed as part of the CA Access Control for Virtual Environments deployment and resides on the VMware ESX/ESXi Server. The CA Access Control Server manages the following:

- Network traffic management
- Network zones management
- Privileged passwords management
- Hypervisor hardening

CA Access Control Enterprise Management

CA Access Control Enterprise Management is the user-interface through which you manage your enterprise. We recommend that you familiarize yourself with the user-interface after you have completed the initial installation of the product.

The Enterprise Management lets you do the following:

- View your implementation of CA Access Control for Virtual Environments throughout the enterprise
- Configure hosts and host groups and assign policies to security groups and PUPM endpoints
- Check out and check in privileged account passwords
- Configure privileged accounts, endpoints, password policies and password consumers
- Display reports, manage snapshot definitions and capture snapshot data
- Manage users, groups, roles and tasks
- Manage systemwide connection settings
- Manage tags and tag rules
- View audit records

Note: For more information about completing tasks in CA Access Control Enterprise Management, see the *Online Help*

CA Access Control Plug-in

The CA Access Control plug-in helps to manage the virtual environment. The plug-in is embedded into the VMware vCenter Server and lets you do the following from the VMware vSphere Client:

- Discover PUPM endpoints and privileged passwords
- Manage privileged account passwords
- Assign tags to managed devices
- Display CA User Activity Reporting Module reports

Central RDBMS

The central RDBMS stores the following:

- Endpoint data that is used in reports
- Privileged accounts passwords
- Session data for the web-based applications
- User data for the web-based applications (if you do not use Active Directory as a user store)

User Store

You can configure CA Access Control for Virtual Environments to use the groups and users that are defined in Active Directory or a database. Therefore, you can use a single data store for all your users.

Chapter 3: Implementing CA Access Control for Virtual Environments

This section contains the following topics:

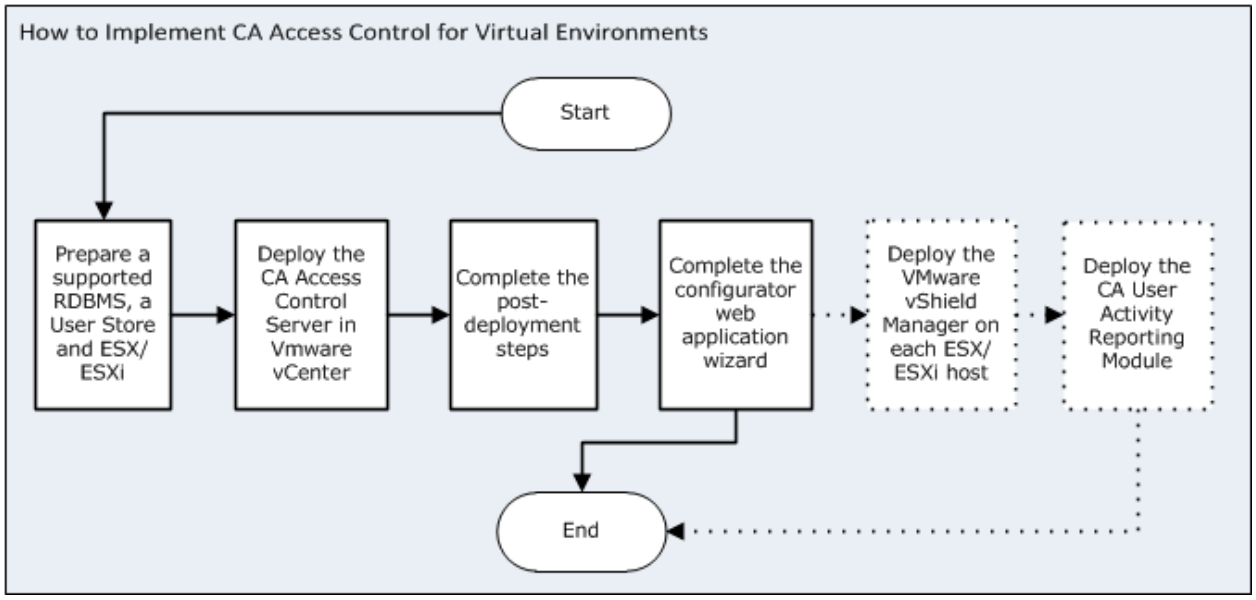
About the CA Access Control for Virtual Environments Virtual Appliance

CA Access Control for Virtual Environments is distributed as a Virtual Appliance. A *Virtual Appliance* is a virtual machine with preinstalled and preconfigured operating system and applications package.

How to Implement CA Access Control for Virtual Environments

CA Access Control for Virtual Environments enables you to manage privileged accounts, configure network zoning, manage privileged accounts, write hypervisor and audit collection policies, and assign tags to assets.

The following diagram illustrates how to implement CA Access Control for Virtual Environments:



Note the following:

- For information about supported RDBMS and user stores, refer to the *Release Notes*.
- The dotted lines indicate an optional step.

Deploy the CA Access Control Server

Deploying the CA Access Control for Virtual Environments virtual appliance, installs the operating system, the CA Access Control Server and creates a virtual machine in the ESX/ESXi Server.

Follow these steps:

1. Open the VMware vSphere Client, go to File, Deploy OVF Template.

   The Deploy OVF Template wizard opens.

2. Click the Deploy from File button, then click Browse to locate the CA Access Control for Virtual Environments OVF template.

3. Click Next.

   The OVF Template details screen appears. Do the following:

   a. Review the details and click Next to continue.

      The End User License Agreement screen opens.

   b. Review the license agreement, select Accept and click Next.

      The Name and Location screen appears.

   c. Specify the virtual machine name and select the folder where you want to deploy the virtual appliance. Click Next.

      The Host/Cluster screen opens.

      Note: This screen appears only if you did not select the resource pool before you began deploying the OVF template.

   d. Select the data center to host the virtual appliance. Click Next.

      The Resource Pool screen opens.

   e. Select the resource pool that you want to deploy the template to. Click Next.

      The Datastore screen opens.

   f. Select a datastore that will store the virtual appliance. Click Next.

      The network mapping screen opens.

   g. Select a network to use. Click Next.

      Note: You can map the networks that the OVF template uses to networks defined in your environment.

      The networking properties screen appears.

h. Complete the following fields:

Domain Names

Specifies the search path for a host name look up. You can specify more than one search path.

Host Name

Specifies the fully qualified name of the virtual machine

Time zone

Specifies the time zone where the CA Access Control Server is located

Default gateway

Specifies the default gateway IP address. Leave this field empty if DHCP is used.

DNS

Specifies the DNS server for this virtual machine. Leave this field empty if DHCP is used.

Network IP Address

Specifies the virtual machine IP address. Leave this field empty if DHCP is used.

Network Netmask

Specifies the netmask or prefix for the network card you selected. Leave this field empty if DHCP is used.

i. Click Next.

j. Review the deployment settings and click Finish.

The VMware vSphere Client deploys the template and adds a virtual machine in the location you specified. The process can take several minutes to complete. A message appears indicating that the templates were successfully deployed.

4. Power on the CA Access Control for Virtual Environments machine from the VMware vSphere Client.

The CA Access Control for Virtual Environments installation process begins. This may take a few minutes to complete.

5. Go to the Console tab.
6. Define the passwords of the root and superadminuser user accounts.

   Note the following:

   - Remote root login is blocked by default. You can use the root account to log into the CA Access Control for Virtual Environments machine console only.
   - You can use the superadminuser account to administer the virtual machine remotely. For example, using SSH.
   - By default, the superadminuser is assigned the same password as the root account. Run passwd superadminuser command from the CA Access Control for Virtual Environments console to change the default password.
7. (Optional) Define the network settings and host name, if not automatically detected. Enter N to change settings or Y to accept the settings
8. Enter Y to complete the installation.

   CA Access Control for Virtual Environments installation is finalized. This process can take several minutes to complete.
9. Enter the root user account password to log in to CA Access Control for Virtual Environments.

   You have successfully deployed CA Access Control for Virtual Environments. You now need to complete the post deployment tasks.

Post-Deployment Tasks

After you deploy the CA Access Control for Virtual Environments virtual appliance in your environment, complete the following procedures to configure the user store and database connection information.

How to Prepate the Central Database

CA Access Control for Virtual Environments requires a relational database management system (RDBMS). You must prepare the database before you configure CA Access Control for Virtual Environments:

1. If you do not already have one, install a supported RDBMS as the central database.

   Note the following before installing an RDBMS:

   - For a list of supported RDBMS software, see the Release Notes.
   - You do not have to install the central database on the CA Access Control for Virtual Environments virtual machine. For information about system requirements for your RDBMS, see the documentation for your product.

2. Configure the RDBMS for CA Access Control Enterprise Management:

   Verify that the database can be accessed locally and from a remote client.

   - For SQL Server, do the following:
     - Create a new case-*insensitive* database.
     - Set the sort order to SQL_Latin1_General_CP1_CI_AS.
     - Create a new user, make the new database the default database of the user, and assign the user the following privileges: DBCREATOR, SYSADMIN
   - For Oracle, do the following:
     - Create a new user for the central database and assign the following privileges:

       CONNECT (granting the following system privileges: ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW)

       RESOURCE (granting the following system privileges: CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE)
     - Grant the user additional privileges on the CA Access Control for Virtual Environments database using the following query:

       grant adminiser database trigger to <*DB_USER*>;
     - Set unlimited quota on the tablespace that hosts CA Access Control for Virtual Environments

Configure the Database Connection Information

CA Access Control for Virtual Environments requires a relational database management system (RDBMS).

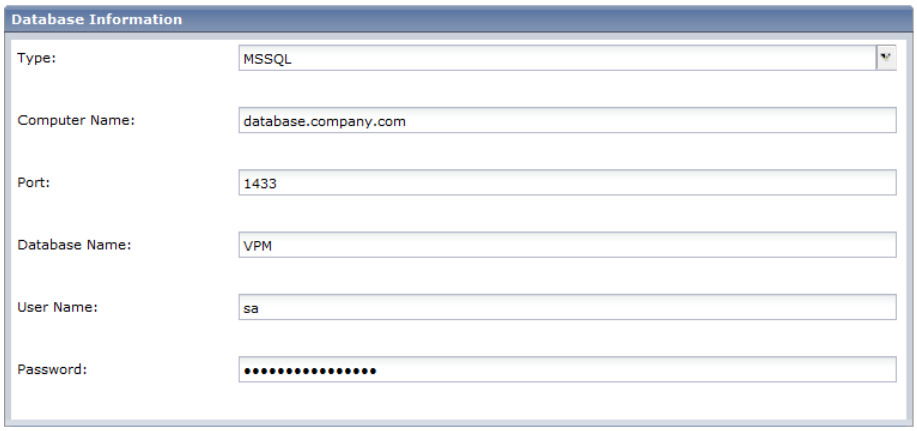
Follow these steps:

1. Open a web browser and enter the following URL for your host:

   `https://enterprise_host:18443/iam/ac`

   Example: https://192.168.1.1:18443/iam/ac

   The CA Virtual Appliance Configuration wizard appears, displaying the database information table:



2. Complete the following fields:

   Database Type—Specifies a supported RDBMS.

   Computer Name—Specifies the name of the host where the RDBMS is installed.

   Port Number—Defines the port used by the RDBMS.

   - **Oracle**—1521
   - **SQL**—1433

   Database Name—Defines the name of the database you created.

   User Name—Defines the user name that CA Access Control for Virtual Environments uses to connect to the database. Specify the user name you created when you prepared the database.

3. Click Next.

   The server name configuration screen opens.

4. Define the fully qualified name of the Enterprise Management Server.

5. Click Next.

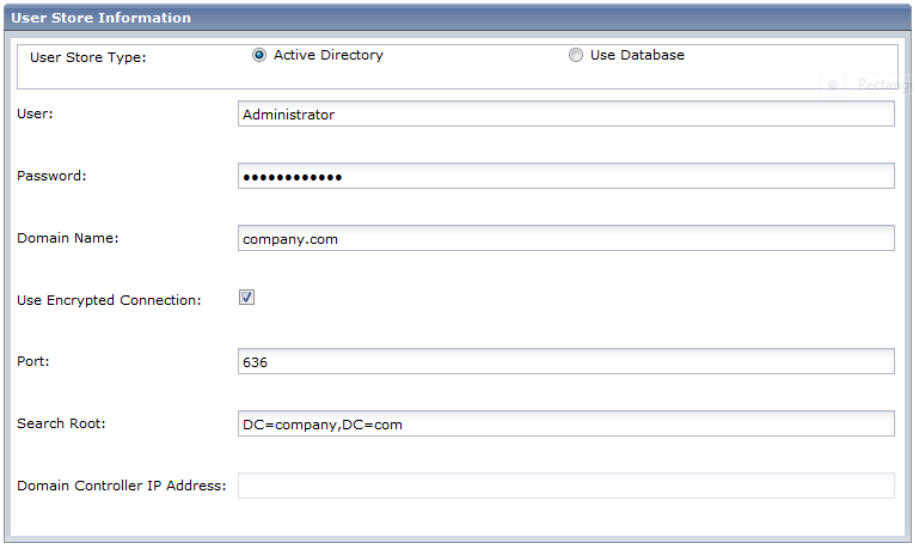
   The installation program verifies the connection to the database before it continues. Now configure the user store connection information.

Configure the User Store Connection Information

CA Access Control for Virtual Environments supports Active Directory and the database you previously specified as user stores.

Follow these steps:

1. From the CA Virtual Appliance Configuration screen, select the user store type.



Select *one* of the following:

Active Directory—you specify the connection information details

Database—stores user information in the RDBMS

2. (Active Directory) Complete the following fields:

User

Defines the Active Directory user account name that is used to manage CA Access Control for Virtual Environments.

Note: You can define a user with read-only privileges for this parameter.

Password

Defines the password of the Active Directory user account that is used to manage CA Access Control for Virtual Environments.

Domain Name

Defines the Active Directory DNS domain name.

Use Encrypted Connection

Specifies the use of an encrypted connection with Active Directory

Port

Defines the port used by default for LDAP queries against Active Directory, for example, 636.

Search Root

Defines the search root, for example, ou=DomainName, DC=com.

Note: Set the Search Root at least one node higher in the directory tree than the container where users are defined. Otherwise, CA Access Control for Virtual Environments can launch without displaying any tabs.

Domain Controller Address

Defines the domain controller IP address.

The installation program verifies the connection to Active Directory before continuing.

3. (Database) Define the RDBMS password of the user that you created when you prepared the database.
4. Click Next.

   The system user screen opens.
5. Complete the following fields:

   System User

   (Active Directory only) Defines the DN of the Active Directory user who is assigned the System Manager admin role in CA Access Control for Virtual Environments.

   Note: By default, a user with the System Manager admin role can perform, create, and manage all tasks in CA Access Control for Virtual Environments. For more information about the System Manager admin role, see the *Enterprise Administration Guide*.

   Password

   (Database only) Defines the password of *superadmin*, the CA Access Control for Virtual Environments administrator. Make a note of the password so you can log in to CA Access Control for Virtual Environments when the installation is complete.

   Note: In this step, you create the superadmin user in the database. The superadmin user is assigned the System Manager admin role in CA Access Control Enterprise Management. You log in as superadmin the first-time you log in to CA Access Control for Virtual Environments. For more information about the System Manager admin role, see the *Enterprise Administration Guide*.
6. Click Next.

   You have defined the database and user store connections information. Configure the connection to the VMware vCenter.

Configure the Connection to the VMware vCenter Server

Configure the connection to VMware vCenter to integrate CA Access Control security features with the managed devices in VMware vCenter Server.

Follow these steps:

1. From the CA Virtual Appliance Configuration wizard, move to vCenter Connection Configuration.
2. Complete the fields in the dialog:

   Name

   Defines the name you want to use for the VMware vCenter Connection

   Description

   (Optional) Defines a description for this VMware vCenter Connection

   Server Name

   Defines the DNS name of the VMware vCenter Server you want to manage

   Example: vcenter.company.com

   Username

   Defines the name of a user account with VMware vCenter Server administrative privileges

   Password

   Defines the password of a user account with VMware vCenter Server administrative privileges

3. Click Next.

   CA Access Control for Virtual Environments validates the settings and continues to the shared secret screen.

4. Complete the following field:

   Communication Password

   Defines the password used for CA Access Control Enterprise Management Server inter-component communication.

5. Click Next.

   A summary screen opens.

6. Review the information and click Finish to complete the wizard.

CA Access Control for Virtual Environments configures the database and user store for use.

CA Access Control for Virtual Environments uses the information you specified to try to connect to the VMware vCenter Server. If the information is correct, the connection is set and you can now use VMware vSphere Client to manage your enterprise deployment of CA Access Control for Virtual Environments. If the information is incorrect and CA Access Control for Virtual Environments cannot connect to the VMware vCenter and an error message appears. The message describes the reason the connection could not be established.

How You Configure CA Access Control for Virtual Environments for SSL Communication

By default, CA Access Control for Virtual Environments is installed with SSL support using a self-signed certificate. To configure SSL support with a different certificate, configure CA Access Control for Virtual Environments to use SSL when working with Active Directory.

Follow these steps:

1. Obtain the users directory certificate in a DER, CRT, or CERT format.
2. Add the certificate to the keystore.

More information:

Adding the Users Directory Certificate to the Keystore (see page 30)

Adding the Users Directory Certificate to the Keystore

Before you can configure CA Access Control for Virtual Environments to use SSL communication, add the users directory certificate to the keystore.

Note: For more information about how to configure SSL for Active Directory or CA Directory, see the Active Directory and CA Directory documentation.

Example: Adding the Active Directory Certificate to the Keystore

Important! This example shows you how to configure CA Access Control for Virtual Environments to use SSL for secure communication with Active Directory. You must obtain the Active Directory certificate in a DER, CER, or CERT encoded binary format before you begin this procedure.

1. On the CA Access Control Server, stop JBoss if it is running. Do the following:
   - From the JBoss job windows, interrupt (Ctrl+C) the process.
2. Navigate to the following directory, where *JBOSS_HOME* is the directory where JBoss is installed:

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore
3. Enter the following command:

   keytool -import -keystore ssl.keystore -*alias ad* -file <*activedirecoty.cert*>

   A password prompt appears.

   -import

   Specifies that the utility reads the certificates and stores it in the keystore.

   -alias

   Specifies the alias to use for adding an entry to the keystore.

   -file

   Specifies the full pathname of the Active Directory certificate file.
4. Enter the password *secret*.
5. Navigate to the JBoss bin directory. By default this directory is found in:

   JbossInstallDir/bin
6. Open the run.bat file and set the java_ops parameter with the trusted user store data. For example:

   ```
   set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m
   -Djavax.net.ssl.trustStore=C:\jboss-4.2.3.GA\server\default\deploy\IdentityMi
   nder.ear\custom\ppm\truststore\ssl.keystore
   ```
7. Save the file and start JBoss.

   You have added the users store certificate to the keystore.

Chapter 4: Administering CA Access Control for Virtual Environments

This section contains the following topics:

Open CA Access Control for Virtual Environments

Once you install and start the CA Access Control Server, you can start the web-based interface from a remote computer using the URL for CA Access Control for Virtual Environments.

Follow these steps:

1. Open a web browser and enter the following URL, for your host:

   `https://enterprise_host:18443/iam/ac`

2. Use the credentials you specified when you installed the CA Access Control Server to log in.

   The CA Access Control for Virtual Environments home page appears.

Example: Open CA Access Control for Virtual Environments

Enter the following URL into your web browser to open CA Access Control for Virtual Environments from any computer on the network:

```
https://appserver123:18443/iam/ac
```

The URL suggests that CA Access Control for Virtual Environments is installed on a host named appserver123 and uses the default CA Access Control for Virtual Environments SSL port 18443.

World View

The World View in CA Access Control for Virtual Environments lets you view the enterprise implementation of CA Access Control for Virtual Environments that you are managing.

Using World View you can do the following:

- Identify the managed devices and security groups managed by CA Access Control for Virtual Environments
- Navigate the VMware vCenter hierarchy
- View details about the managed devices and security groups. Details include which policies are deployed, the total number of groups and managed devices and compliance status of each device
- Administer managed devices or security groups
- Manage security groups to assign or remove policies, members, tags and tag rules.

Manage Your Enterprise Implementation

Using CA Access Control Enterprise Management you can view and manage your enterprise implementation of CA Access Control for Virtual Environments. Enterprise "World View" is a snapshot of your PUPM endpoints and managed devices, their logical security groups, the deployed policies, and the policy tags.

The enterprise deployment snapshot is based on the managed devices and groups hierarchy that you configured in the VMware vCenter Server. Any change you make to the hierarchy in VMware vCenter, is displayed also in the World View.

Follow these steps:

1. Go to the World View tab, Security Groups, Security Groups Management

   The Security Groups Management page appears displaying the security groups on the VMware vCenter Server and the logical groups, defined by the CA Access Control Server.

   Note: You can configure, modify, or change the hierarchy for CA Access Control for Virtual Environments managed devices only.

2. (Optional) You can define additional managed devices, security groups, tags and tag rules in the CA Access Control Server. Select the following from the Actions menu:

   - Create Security Groups (see page 36)
   - Create Tags (see page 45)
   - Create Tag Rules (see page 46)
   - View Policy Status

3. From the Security Groups section, select a security group.

   CA Access Control Enterprise Management displays the security group details, assigned policies, group members and compliance status of each member.

4. Select Add Policy to manage the security group policies.

   Following are the available policies:

   - Network zone (see page 42)—configure network segregation policies
   - Audit Collection (see page 53)—configure CA User Activity Reporting Module audit collection policies
   - Hypervisor Hardening (see page 50)—configure hypervisor hardening policies
   - Password Lockdown (see page 39)—configure privileged account password lockdown policies

5. (Optional) Select Configure to modify an existing policy or Remove to remove a policy.

Create Security Groups

You manage the security groups in your environment to add or remove members and assign or remove tags.

Follow these steps:

1. Go to World View tab, Security Groups, Security Groups Management

   The Security Groups Management page appears displaying the security groups on the VMware vCenter Server and the CA Access Control Server details.

2. Select create or modify to access the security group configuration

   The General tab opens.

3. Complete the following fields:

   Name

   Displays the name of the security group

   Description

   Specifies a description of the security group

   Owner

   Specify the name of the owner of the security group

   Organization Unit

   Specifies the departmental unit of the security group

4. Select the Managed Devices Selection tab

   The host selection tab open.

5. Click Add to add managed devices to the group

6. Select the Security Group Members tab

   The group groups tab opens, displaying the security groups that are members of the group.

7. Click Add to add security groups as members of the group

8. Select the Tags tab

   The tags tab opens, displaying the assigned tags

9. Click Add to assign tags to the computer groups

10. Select the Membership By Tags tab

    The membership by tag tab opens.

11. Click AND to add a tag to the membership criteria. Click ADD to add the tag to the criteria list.

    The membership criteria is added to the list.

    Note: You can add up to three (3) tags in a single membership criteria

12. Click Submit

    CA Access Control Enterprise Management commits the changes to the security group.

About Tags Membership Criteria

To help you automate and facilitate managed devices administration, you can use the tag membership criteria. Using tags membership criteria, you define security groups whose members comply with the criteria rules that you define. CA Access Control for Virtual Environments automatically adds each managed device that the criteria rules apply to the security group.

The tags membership criteria uses the following syntax:

```
[tag1] AND | OR [tag2] AND | OR [tag3]
```

Example: Create the tag membership criteria

In this example, you configure the tags membership criteria to assign managed devices that are assigned one of the following tags: Development, Accounting, Marketing.

```
Development OR Accounting OR Marketing
```

In this example, you configure the tags membership criteria to automatically assign managed devices that are assigned the Accounts and Marketing tags only.

```
Accounts AND Marketing
```

View the Managed Devices Status

The status view enables you to review error and warning messages that relate to managed devices. The alerts display information about the deployed policies that you assign to the security groups.

Follow these steps:

1. Select World View, View, Status

   The status window opens, displaying the most recent alerts.

2. Select to view all messages or error and warning messages only.
3. Click Refresh to refresh the list of alerts.

Privileged Account Passwords Management

The privileged account passwords lockdown policy enables you to configure and assign a unified policy to all the privileged accounts in a security group.

How CA Access Control for Virtual Environments Create Endpoints and Accounts

CA Access Control for Virtual Environments automatically creates PUPM endpoints, discovers the privileged account and assigns a password policy to the account passwords.

The following process describes how CA Access Control for Virtual Environments configures PUPM endpoints and accounts:

1. A virtualization administrator adds a PUPM endpoint to a security group.
2. The administrator creates a disconnected privileged account with administrative privileges in CA Access Control Enterprise Management for each endpoint type in the security group.

   CA Access Control for Virtual Environments uses the disconnected accounts to connect to each endpoint and discover the privileged account passwords.
3. In CA Access Control Enterprise Management, an administrator configures the password lockdown policy and assign it to a security group.
4. CA Access Control for Virtual Environments discovers the endpoint and automatically configures the endpoint connection settings and attempts to configure the privileged accounts on that endpoint.
5. If successful, CA Access Control for Virtual Environments creates an endpoint privileged access role for using privileged accounts on that endpoint type.

   For example, the first-time you discover privileged accounts on a Windows Agentless endpoint, CA Access Control for Virtual Environments automatically creates the Windows Agentless Connection endpoint privileged access role.
6. CA Access Control for Virtual Environments automatically assigns the privileged account passwords policy to the privileged accounts on each member of the security group.

Configure Account Passwords Lockdown Policy

You configure the account passwords lockdown policy for each security group that CA Access Control for Virtual Environments manages. CA Access Control for Virtual Environments enforces the privileged password lockdown policy on each managed device that you add to the group.

Important! Before you complete this procedure, create a privileged account with administrative privileges for each endpoint type you want CA Access Control for Virtual Environments to create and manage.

Follow these steps:

1. Go to World View, Security Groups, Security Groups Management.

   The Security Groups Management page appears displaying the security groups on the VMware vCenter and the CA Access Control Server details.

2. Select a security group.

   CA Access Control Enterprise Management displays the security group details and members.

3. Select Add Account Password Policy from the Actions menu.

   The manage password lockdown: *host name* window opens.

4. Select an operating system profile from the drop-down menu. Options:

   - Windows Machine Profile
   - Linux Machine Profile
   - Solaris Machine Profile

   You can configure a specific password lockdown policy for each operating system profile.

5. Complete the following fields:

Description

Specify a description for the password lockdown policy

Operating System Profile

Displays the operating system profile you previously selected

Connection Account

Defines an administrator user account that CA Access Control for Virtual Environments uses to connect to each managed device. Select Create Account to create an administrator account.

Lockdown Connection Account

Specifies that the connection account is a connected account.

Managed Account

Defines the privileged accounts that CA Access Control for Virtual Environments creates on each managed device.

Password Policy

Specifies the password policy you want to apply to the privileged or service account. Select Create Password Policy to create a password policy.

Check out Expiration

Defines the duration, in minutes, before the checked out account expires.

Exclusive Account

Specifies whether only a single user can use the account at any one time. An *exclusive account* is a restriction imposed on a privileged account that limits use of the account to a single user at a time.

Change Password on Check Out

Specifies whether you want CA Access Control Enterprise Management to change the password of the privileged account every time it is checked out.

Change Password on Check In

Specifies whether you want CA Access Control Enterprise Management to change the password of the privileged account every time it is checked in by a user or a program, or when the checkout period expires.

Note: If the account is not exclusive, CA Access Control Enterprise Management generates a new privileged account password only when *all* users have checked in the account.

Note: This option does not apply to service accounts.

Login Applications

Specifies the login applications to assign to this endpoint.

Note: Create a login application before you can assign it to an endpoint. You can assign multiple login applications to the same endpoint.

6. Click Submit.

   CA Access Control Enterprise Management submits the privileged account passwords lockdown policy to the group.

Network Segregation

Network segregation is the process through which a security or a virtualization administrator defines groups of managed devices in network zones, based on a common criteria, for example, physical location of hosts or tags.

Members in the network zone can communicate with other members within that zone only, and cannot access other network zones or hosts on the network. You can assign network services to the security group to enable members to access the network.

Configure a Network Zone Policy in CA Access Control Enterprise Management

The network segregation rules that you define specify the network zone and apply to security groups. When applied, members can communicate within the zone only. You can define security groups and assign members to the groups or use the automatically created security groups.

Note: Define the network services to use before you configure the network zone policy.

Follow these steps:

1. Go to World View, Security Groups, Security Groups Management.

   The Security Groups Management page appears displaying the security groups on the VMware vCenter and the CA Access Control Server details.

2. Select a security group.

   CA Access Control Enterprise Management displays the security group details and members.

3. From the Actions menu, select Add Network Zone Policy.

   The manage network rules window opens.

4. Complete the following:

   Description

   Specifies a description for the network zone policy

   Service

   Defines the network services to assign to the network zone policy. Click Add to search for the network service to assign.

   Directional

   Defines the network traffic direction that the network service is permitted to use.

   Options: Inbound, Outbound, Bidirectional

5. Click Submit.

   CA Access Control Enterprise Management submits the network segregation rule. A confirmation message appears informing you that the task successfully completed.

   You successfully applied the network zone policy to the security group.

Configure Network Services

Configure network services for a security group to enable members in the network zone to access services and resources located outside of the network zone.

Follow these steps:

1. In CA Access Control Enterprise Management, do as follows:
   a. Click System
   b. Click Network Services
   c. Select Configure Network Services

   The Configure Network Services:Configure Network Search screen opens.
2. (Optional) Select existing Network Services to create a copy, as follows:
   a. Select Create an object of type Network Services.
   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of Network Services that match the filter criteria appears.
   c. Select the object you want to use as a basis for the new Network Services.
3. Click OK.

   The Create Network Service task page appears. If you created a Network Service from an existing object, the dialog fields are prepopulated with the values from the existing object.
4. Complete the following fields. The following fields are not self-explanatory:

   Network Address

   Defines the host name or IP address of the server that provides the network service.

   Service

   Defines the network service properties:

   - Protocol— UDP, TCP
   - Port number
   - Service
5. Click Add.

   CA Access Control Enterprise Management adds the network services.

   Note: You can define more than one network service for each security group.
6. Click Submit

   CA Access Control Enterprise Management submits the task and assigns the network services to the security group.

Assets Tagging

Assets tagging is the process through which a system, security, or a virtualization environment administrator associates tags to managed devices and security groups. By assigning tags the administrator can manage individual assets as groups to automate policy distribution and define administrative scoping.

To automate administration, each managed device inherits the tags that you add to the security group. You can define tagging rules based on the asset attributes, such as IP addresses range. You can also define tagging policies, which CA Access Control for Virtual Environments automatically distributes to all the members in the group.

How You Use Tags To Administer Security Groups

Using tags and tag rules can facilitate security groups management. Based on the tags and tag rules you define, CA Access Control Enterprise Management can automatically add managed devices to security groups and apply policies to the managed devices.

Follow these steps:

1. You create a tag in CA Access Control Enterprise Management.
2. You do *one* of the following:
   - Assign the tag to managed devices manually

     The managed devices are added to the security group. The policies assigned to the security group are applied to the managed devices.
   - Create tag rules
3. You define a tag rule, associate a tag with the rule you create and define the rule criteria.
4. CA Access Control Enterprise Management does the following:
   a. Applies the rule to the security group that the tag is associated with
   b. Assigns the tag to each managed device that complies with the tag rule
   c. Adds the managed devices that comply with the tag rule to the security group
   d. Applies the policies you configured for the security group to the managed devices

   You can now administer the managed devices from the security group.

   Note: If you delete the tag rule, CA Access Control Enterprise Management removes the managed devices from the security group

Configure Tags in CA Access Control Enterprise Management

CA Access Control Enterprise Management maps managed devices, for example, folders, datacenters and resource pools, to host groups. Assigning tags to security groups simplifies management of the assets in your virtualized environment. You can easily perform administrative scoping based on the tags you assign.

Follow these steps:

1. Go to World View, Tags, Create Tag.

   The Create Tag: Tag Search window opens.

2. (Optional) Select an existing tag to create the tag as a copy of it, as follows:

   a. Select Create a copy of a new object of type Tag.

   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of tags that match the filter criteria appears.

   c. Select the object you want to use as a basis for the new tag.

3. Click OK.

   The Create Tag window appears.

4. Type in the name of the tag.

5. Click Submit.

   CA Access Control Enterprise Management creates the tag. You can now assign the tags to the managed devices or create a tag rule.

Create Tag Rules in CA Access Control Enterprise Management

Create a tag rule to assign managed devices to security groups based on properties that you define. When CA Access Control for Virtual Environments discovers a managed device with an IP address that matches a tag rule, the device is tagged and associated with a security group.

Follow these steps:

1. Go to World View, Tags, Create Tag Rule.

   The Create Tag Rule: Tag Rule Search window opens.

2. (Optional) Select an existing tag rule to create the tag as a copy of it, as follows:

   a. Select Create a copy of a new object of type Tag Rule.

   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of tag rules that match the filter criteria appears.

   c. Select the object you want to use as a basis for the new tag.

3. Click OK.

   The Create Tag Rule window appears.

4. Complete the following fields:

   Name

   Specify the name of the tag rule

   Description

   Specify a description for the tag rule

   Applied Tag

   Select the tag to associate with the tagging rule

   Matching Object Type

   Displays the object type that the tag rule applies

   Criteria

   Specifies the tag rule criteria as follows:

   Name|*IP Address*|*Host*[equal|not equal] *managed_device*

   Name

   Specifies the managed device DNS name

   IP

   Specifies the managed device IP address

   OS Information

   Specifies the managed device operating system, as defined in the VMware vCenter

   VM Network

   Specifies the name of the virtual network that the managed device uses

   Annotation

   Specifies the annotation key and value, as defined in the VMware vCenter.

   Example: "Owner=John"

   Note: Use wildcards (*) to apply the tag rule to more than a single managed device

5. Click Submit.

   CA Access Control Enterprise Management creates and applies the tag rule to the managed devices

Assign Tags to Managed Devices in VMware vSphere Client

You can assign tags to each managed device that CA Access Control for Virtual Environments manages from the VMware vSphere Client.

Follow these steps:

1. Select a managed device from the left pane, then select the CA Security tab.

   The CA Security tab opens, displaying the content of the summary tab.

2. Click the Add Tag button.
3. Select a tag from the pull-down menu, then click OK.

   The tag is assigned to the managed device.

Hypervisor Hardening

The VMware hypervisor, the vSphere Client console and the managed devices are susceptible to malicious attacks and unintended damage by users. Hardening the hypervisor and vSphere Client Console, helps ensure that your VMware environment is secured and less pronged to attacks.

CA Access Control for Virtual Environments helps system, security, or VMware administrators to configure policies. The policies harden the hypervisor and VMware vSphere Client Console from CA Access Control Enterprise Management and deploy the policies to host groups.

Note: For more information about VMware hypervisor and vSphere Client console hardening, see to the *VMware vSphere Hardening Guide* on the VMware website.

Hypervisor Hardening Policies

Before you decide what level of hardening to apply, review the following supported hypervisor hardening policies:

- **Remote Access**—(ESXi Only) Restrict remote access by enabling lockdown mode to disable all remote access to ESXi server. When enabled, lockdown mode forces administrators to perform tasks from a central location only and reduces the risk of performing tasks that are not audited.
- **Remote Syslog**—Logging events to a central location increases administration capabilities and enables you to monitor all devices from a central location. Further, storing events in to a central location help prevent log tampering.
- **Persistent Logging**—Configure persistent logging to a database to keep server logs for an extended period. Persistent logging makes it easy to monitor events and diagnose server issues.
- **NTP Time Synchronization**—Incorrect time settings can prevent you from identifying and tracking attacks. Configure NTP time synchronization to help ensure all systems use the same time source to help track and correlate attacks.
- **SNMP Configuration**—(ESXi Only) If the SNMP agent is not properly configured, attackers can redirect the traps to malicious hosts and use the information for malicious purposes.
- **Direct Console User Interface** (ESXi Only)—the Direct Console User Interface (DCUI) is the ESXi management console that enables administrators to perform host configuration and maintenance tasks. A user with local administrative privileges can perform actions directory in the DCUI that are not audited in the VMware vCenter Server. Disable the DCUI to prevent users from performing administrative tasks directly on the ESXi server.
- **Tech Support Mode** (ESXi Only)—Tech support mode is an interactive command line available on the server console or through an SSH console. When enabled, you can perform troubleshooting and support related tasks directly on the ESXi Server. Disable tech support mode to prevent unauthorized access to the server.
- **VMSafe Network API**—The VMSafe Network API provides a security architecture for virtualized environments. Disable the VMSafe Network API if you are not using the VMSafe Network API.

Configure a Hypervisor Hardening Policy in CA Access Control Enterprise Management

The hypervisor hardening policy helps you to limit users access to the hypervisor, configure remote system logging, time synchronization and configure the SNMP agent settings.

Note: You must have the System Manager role assigned to manage virtual machines access permissions.

Important! Verify that you configure the connection to the VMware vCenter Server before you complete this procedure. Also, create a PUPM endpoint for each hypervisor that you want to apply the hardening policies to.

Follow these steps:

1. Go to WorldView, Security Groups, Security Groups Management.

   The Security Groups Management page appears displaying the security groups on the VMware vCenter Server and the CA Access Control Server details.

2. Select a security group.

   CA Access Control Enterprise Management displays the security group details and members.

   Important! Verify that the security group you select has at least one ESX server as a member of the group.

3. From the Actions menu, select Add Hypervisor Hardening Policy.

   The Manage Security Group Hypervisor Hardening *host group name* page opens.

4. Complete the following fields:

   Comment

   Specifies a description of the hardening policy.

   Lockdown

   Specifies to block remote access to the hypervisor.

   Direct Console UI

   Specifies that the local administrative control is disabled.

Tech Support Mode

Specifies that the tech support mode is disabled.

Tech Support Mode Timeout

Specifies the interval, in seconds, after which to disable the tech support mode.

Local Datastore Path

(ESXi Only) Specifies the full pathname of the datastore where syslog logs messages.

Example: [storage1]/var/log/messages

Remote Syslog Host

Defines the remote syslog host name.

Remote Port

Defines the remote syslog host port number.

NTP Server

Specifies the NTP (Network Time Protocol) server name.

Enabled

Specifies that SNMP configuration is enabled.

SNMP Port

Defines the SNMP listening port number.

Read-only Communities

Specifies the name of the communities that has read-only access.

Example: snmp-server community public RO

Trap Targets

Defines the SNMP traps target hostname, port and community.

Format: *target_hostname@port/community*

Example: SNMP_host@55222/comm

VMSafe Network API

Specifies to disable the use of VMSafe Network API.

Hypervisor Administrator

Defines the name of a hypervisor administrator account. CA Access Control for Virtual Environments uses this account to connect to the hypervisor.

5. Click Submit.

CA Access Control Enterprise Management deploys the hardening policies to the group.

Audit Collection

CA User Activity Reporting Module lets you collect, normalize, aggregate, and report on IT activity, and generate alerts requiring action when possible compliance violations occur.

The CA User Activity Reporting Module audit collection policy lets you assign a policy for each virtual machines group according to the audit collection profile you assign to the group.

Note: For more information about CA Access Control for Virtual Environments and CA User Activity Reporting Module integration, see the *Enterprise Administration Guide.*

Configure an Audit Collection Policy in CA Access Control Enterprise Management

You configure the audit collection policy and for each security group that CA Access Control for Virtual Environments manages. CA Access Control for Virtual Environments enforces the audit collection policy on each virtual machine that you add to the group.

Follow these steps:

1. Go to WorldView, Security Groups, Security Groups Management

   The Security Groups Management page appears displaying the computer groups on the VMware vCenter and the CA Access Control Server details

2. From the Security Groups section, select a group

   CA Access Control Enterprise Management displays the group details and members.

3. From the Action menu, select Add Audit Collection Policy

   The manage security group audit collection: *security group name* window opens.

4. Complete the following fields:

   Description

   Specify a description for the audit collection policy.

   Enabled

   Select to enable events collection from the managed devices.

   Operating System Profile

   Select the operating system profile that you want to apply the audit collection policy to.

   Audit Collection Profile

   Specify the audit collection profile that you defined in CA User Activity Reporting Module.

   Profile Description

   Specify a description from the audit collection profile.

   Authentication Account

   Define the user account used to connect to CA User Activity Reporting Module.

   Note: This field is enabled or disabled according to the audit collection profile you selected.

5. Select Submit

   CA Access Control Enterprise Management creates the audit collection policy and assigns the policy to the security group. CA User Activity Reporting Module can now collect audit events directly from the managed devices.

View CA User Activity Reporting Module Reports in VMware vSphere Client

If CA User Activity Reporting Module is configured to collect audit records from the managed devices, you can view CA User Activity Reporting Module reports from the VMware vSphere Client.

Follow these steps:

1. Select a managed device from the left pane, then select the CA Security tab.

   The CA Security tab opens, displaying the content of the summary tab.

2. Select the User Activity Reporting Module tab.
3. Select a report from the pull-down menu.

   The report is displayed.

Privileged Account Passwords Discovery

Privileged account passwords discovery is the process through which CA Access Control for Virtual Environments discovers, vaults, and manages privileged accounts and application ID passwords. Once discovered, you can use CA Access Control for Virtual Environments to control access to privileged accounts and passwords based on policies you define.

Manually Discover Privileged Account Passwords in VMware vSphere Client

To control access to privileged account passwords, first identify the privileged accounts on the managed devices and then store the privileged account passwords in CA Access Control for Virtual Environments.

Follow these steps:

1. Select a managed device from the left pane, then select the CA Security tab.

   The CA Security tab opens, displaying the content of the summary tab.

2. From the Services field, select Configure if PUPM is disabled to launch the account discovery wizard.

   The account discovery and vaulting wizard starts.

3. Complete the following fields in the dialog:

   Name

   Identifies the name of the managed device that you configure.

   Description

   Specifies a description for the endpoint.

   Endpoint Type

   Defines the endpoint type.

   Note: When you select the endpoint type, an additional dialog opens. Use that dialog to supply the credentials required to manage privileged accounts on that type of endpoint. The endpoint type you select affects the connection information you have to supply.

4. Select Validate.

   CA Access Control for Virtual Environments attempts to validate the endpoint connection settings.

5. Click Next.

6. Select an attribute for the search, type in the filter value, and click Search.

   A list of privileged accounts that match the filter criteria appears.

7. Select the privileged accounts you want to manage and click Next.

   The lockdown properties screen opens.

8. Complete the fields in the dialog. The following fields are not self-explanatory:

   Disconnected System

   Specifies whether the account originates from a disconnected system.

If you select this option, PUPM does not manage the account. Instead, it acts only as a password vault for privileged accounts of the disconnected system. Every time you change the password, you also must manually change the account password on the managed endpoint.

Password Policy

Specifies the password policy you want to apply to the privileged or service account.

Check out Expiration

Defines the duration, in minutes, before the checked out account expires.

Exclusive Account

Specifies whether only a single user can use the account at any one time. An *exclusive account* is a restriction imposed on a privileged account that limits use of the account to a single user at a time.

Change Password on Check Out

Specifies whether you want PUPM to change the password of the privileged account every time it is checked out.

Change Password on Check In

Specifies whether you want PUPM to change the password of the privileged account every time it is checked in by a user or a program, or when the checkout period expires.

Note: If the account is not exclusive, PUPM generates a new privileged account password only when *all* users have checked in the account.

9. Click Next.

   The Summary screen opens.

10. Review the details and click Finish.

    CA Access Control for Virtual Environments submit the task and creates the selected privileged accounts if there are no errors.

More information:

Windows Agentless Connection Information (see page 57)
SSH Device Connection Information (see page 58)
VMware ESX/ESXi Connection Information (see page 59)

Windows Agentless Connection Information

The Windows Agentless endpoint type lets you manage privileged Windows accounts.

Note: If you configure a domain user on a local computer, CA Access Control for Virtual Environments cannot change the password of the domain user. This limitation is due to Windows behavior.

When you create endpoints of this type, provide the following information:

User Name

Defines the name of an administrative user of the endpoint. CA Access Control Enterprise Management uses this account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords.

Password

Defines the password of the administrative user of the endpoint.

Host

Defines the host name of the endpoint.

Example: myhost-ac-1

Host Domain

Specifies the domain name that this host is a member of.

Note: Specify the host domain name with only the prefix. For example, if the full domain name is company.com, you enter only the prefix company.

Is Active Directory

Specifies whether the user account is an Active Directory account.

User Domain

Specifies the domain name that the user is a member of.

Note: Specify the user domain name with only the prefix. For example, if the full domain name is company.com, you enter only the prefix company.

Important! Verify that you specified the host domain name if you want to log in to the endpoint using PUPM Automatic Login. If the endpoint is a member of workgroup, specify the host name and not the workgroup name.

Note: For more information regarding additional steps required to configure Windows Agentless endpoints. refer to the *Enterprise Administration Guide*.

SSH Device Connection Information

The SSH Device type lets you manage privileged UNIX accounts.

Important! Before you configure a PUPM SSH endpoint, disable tunneled clear text passwords on the endpoint before you configure the endpoint settings.

When you create devices of this type, provide the following information so that CA Access Control Enterprise Management can connect to the device:

User Name

Defines the name of an administrative user of the endpoint. CA Access Control Enterprise Management uses this account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords. If you specify an operation administrator account, PUPM uses that account to perform administrative tasks on the endpoint.

Password

Defines the password of the administrative user of the endpoint.

Host

Defines the host name of the endpoint.

Operation Administrator User Login

(Optional) Defines the name of an operation administrator user of the endpoint. PUPM uses this account to perform administrative tasks on the endpoint, for example, discovering and changing the password of privileged accounts. If you do not specify an operation administrator user, PUPM uses the User Login account to perform administrative tasks on the endpoint.

If you specify an operation administrator user for an SSH endpoint that uses a Check Point firewall, specify the expert user. However, you cannot use PUPM to change the password for the expert account on the endpoint. This restriction means that the expert account must be a disconnected account in PUPM.

Operation Administrator Password

(Optional) Defines the password of the operation administrator user.

Configuration File

Specifies the name of the SSH Device XML configuration file. You can customize the XML files according to your needs.

Note: If you do not specify a value for this field, CA Access Control Enterprise Management uses the ssh_connector_conf.xml file.

Note: For more information about additional steps required to configure SSH Device endpoints. see the *Enterprise Administration Guide*.

VMware ESX/ESXi Connection Information

The VMware ESX/ESXi endpoint type lets you manage privileged VMware ESX/ESXi accounts

When you create endpoints of this type, provide the following information so that CA Access Control for Virtual Environments can connect to the endpoint:

User Name

Defines the name of an administrative user of the endpoint. CA Access Control Enterprise Management uses this account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords.

Note: If you specify the Advanced option, PUPM does not use the User Login account to perform administrative tasks. Instead, PUPM uses the specified privileged account to perform administrative tasks on the endpoint.

Password

Defines the password of the administrative user of the endpoint.

Host

Defines the host name of the endpoint.

Advanced

Specifies whether you want to use a privileged administrative account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords. For example, you can specify a privileged domain account that can perform administrative tasks on multiple endpoints.

If you specify this option, PUPM does not use the User Login account to perform administrative tasks.

Check Out a Privileged Account Password from VMware vSphere Client

You check out a privileged account password to log in to a managed device that the account belongs to. When you check out a privileged account, you can display the password, copy the password to a clipboard, or log in to the managed device.

Follow these steps:

1. Select a managed device from the left pane of the VMware vSphere Client window, then select the CA Security tab.

   The CA Security tab opens, displaying the content of the summary tab.

2. Navigate to the Privileged Accounts Management tab.

   The Privileged Accounts Management tab opens, displaying the accounts available for you to check out.

3. Select the account that you want to check out and the managed device, then select *one* of the following options from the Actions menu:

   - Select Checkout to check out the password
   - Select Auto Login to log in to the managed device
   - Select Show Password to display the password

   VMware vSphere Client processes the task and proceeds according to the option you selected.

   If you have selected to log in to the managed device, a window on the managed device opens and logs you in.

   Note: The first-time that you log in to the managed device, you are asked to confirm the action before you can connect to the managed device.

   Important! On Microsoft Windows 2008 Server, enable the "Automatic prompting of ActiveX controls" in the Microsoft Internet Explorer browser security settings. If disabled, the browser blocks the ActiveX file required to run the Remote Desktop application.

Check In a Privileged Account Password from VMware vSphere Client

You check in a privileged account password after log out of the managed device. After you check in the privileged account password, CA Access Control for Virtual Environments can change the password based on the setting of a configuration option.

Follow these steps:

1. Select a managed device from the left pane of the VMware vSphere Client window, then select the CA Security tab.

   The CA Security tab opens, displaying the content of the summary tab.

2. Navigate to the Privileged Accounts Management tab.

   The Privileged Accounts Management tab opens, displaying the accounts available for you to check in.

3. Select the account passwords that you want to check in and select Check-in from the menu.

   CA Access Control for Virtual Environments checks the account in.

What Happens During the Break Glass Process

A user performs a break glass checkout when they need immediate access to an account that they are not authorized to manage.

Break Glass accounts are privileged accounts that are not assigned to the user according to the user role. However, the user can obtain the account password.

In a Break Glass check-out process, a notification message is sent to the role administrator, informing the administrator that a Break Glass check-out process occurred. However, the administrator cannot approve or stop the process.

The checked-out Break Glass account is added to the user My Checked-out Privileged Accounts tab in the Break Glass option of the Home tab.

Note: Only users with the break glass privileged access role can perform the break glass process.

Break Glass from CA Access Control Enterprise Management

Use the Break Glass task to gain *immediate* access to an endpoint that you do not have privileged access to.

Note: If you do not require immediate access to the endpoint, you can request access to the privileged account. And then wait for and administrator to approve the request.

Follow these steps:

1. In CA Access Control Enterprise Management ,click Home, My Accounts, My Privileged Accounts.

   The My Accounts page appears, displaying the accounts available for you to check out.

2. In the Select Accounts field, select Advanced.

   The advanced search options appear.

3. Select to include break glass accounts, and select Search.

   A refined list of privileged accounts that match the filter criteria appears.

4. Select the privileged account to check out from the Actions menu.

5. Fill in the justification and click Check Out.

   CA Access Control Enterprise Management submits the task and, if successful, displays the account password in the confirmation message.

Note: After you check out the password, the following options are also displayed in the Actions menu: Check in, Login Application, and Show Password.

Break Glass from VMware vSphere Client

Use the Break Glass task to gain *immediate* access to an endpoint that you do not have privileged access to.

Follow these steps:

1. From the Host Information screen, select Privileged Accounts Management.

   The Privileged Accounts Management tab opens, displaying the privileged accounts available for you to break glass.

2. Select the privileged account to check out and select Break Glass.

3. Fill in the justification and click Check Out.

   CA Access Control for Virtual Environments submits the task and, if successful, displays the account password in the confirmation message.

Note: After you check out the password, the following options are also displayed in the Actions menu: Check in, Login Application, and Show Password.

Check In a Break Glass Privileged Account Password in CA Access Control Enterprise Management

You check in a Break Glass privileged account password once you have logged out of the managed endpoint.

Follow these steps:

1. Click Home, My Accounts, My Privileged Accounts.

   The My Accounts page appears, displaying the accounts available for you to check in.

2. In the Select Accounts field, select Advanced.

   The advanced search options appear.

3. Select to include break glass accounts, and select Search.

   A refined list of privileged accounts that match the filter criteria appears.

4. Select the accounts that you want to check in and click Check-in from the Actions menus.

   CA Access Control Enterprise Management submits the task to check in the account.