CA Access Control for Virtual Environments

Enterprise Administration 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:

- [set the eACee variable for your book]
- 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.
  - [set the alternate Installation Path variable]
- *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 8: Creating Reports 171

Chapter 1: Introduction

This section contains the following topics:

About this Guide

This guide provides information about enterprise administration and reporting and the CA Access Control Enterprise Management web-based interface. Enterprise administration and reporting for CA Access Control Enterprise Management includes privileged accounts password management, reporting, and the World View enterprise viewer.

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

Who Should Use this Guide

This guide is for security, system and virtualization administrators using CA Access Control for Virtual Environments who want to use its enterprise administration, third-party programs integration and reporting capabilities:

- Enterprise policy management
- Enterprise reporting
- Web-based interface for handling your enterprise host access management.
- Privileged User Password Management (PUPM)
- Integration with third-party programs.

Enterprise Management

CA Access Control Enterprise Management is a web-based user interface that enables you to perform access-related management tasks across your enterprise. You can perform a number of management tasks. For example, you can deploy access policies through the enterprise from a central location, manage individual hosts, manage privileged accounts, generate enterprise reports and more.

Enterprise Management Interface

The CA Access Control Enterprise Management interface is your enterprise management tool that contains everything that you require to manage your enterprise. CA Access Control Enterprise Management interface contains tools for used for configuring hosts, create and assign policies, manage users, groups and administrative tasks and configure and manage access to privileged accounts throughout the enterprise. Further, you gain access to enterprise reporting and auditing capabilities.

Enterprise View

Use CA Access Control Enterprise Management to view information about and manage virtual and physical machines and PUPM endpoints from a central location. CA Access Control Enterprise Management World View displays detailed information about each managed device, when it was last updated. World View also enables you to modify the settings for a managed device and security groups.

Privileged User Password Management

Privileged User Password Management (PUPM) is the process through which an organization secures, manages and tracks all activities associated with the most powerful accounts within the organization.

CA Access Control Enterprise Management provides role based access management for privileged accounts on managed devices from a central location. CA Access Control Enterprise Management provides secure storage of privileged accounts and application ID passwords and control access to privileged accounts and passwords based on policies.

Further, CA Access Control Enterprise Management manages privileged accounts and application password life cycle and allows the removal of any passwords from configuration files and scripts.

Enterprise Reports

The CA Access Control Enterprise Management reporting options lets you view the security status of each PUPM endpoint and managed device in a central location. The collection of data from the endpoints and managed devices can be scheduled or on demand. You do not need to connect to each endpoint to find out who is authorized to access which resource.

CA Access Control for Virtual Environments reporting service, once set up, works independently to collect data from each endpoint and report it to a central server and continues to report endpoint status without the need for manual intervention. This means that each endpoint reports on its status whether the collection server is up or down.

CA Access Control Enterprise Management comes out-of-the-box with a set of pre-defined reports that displays an array of information regarding each endpoint. Further, you can both customize existing reports and create your own reports to display the information you are interested in viewing.

Chapter 2: Administering CA Access Control Enterprise Management

This section contains the following topics:

Administrative Scoping

In CA Access Control Enterprise Management, you assign privileges to users and administrators by assigning admin and privileged access roles. A role contains tasks that correspond to application functions in CA Access Control Enterprise Management.

Roles simplify privilege management. Instead of associating a user with each task that they perform, you can assign a role to the user. The user can perform all the tasks in their assigned role. You can then edit the role by adding tasks. Every user who has the role can now perform the new task. If you remove a task from a role, the user can no longer perform that task.

When a user logs in to CA Access Control Enterprise Management, they see tabs based on their role. The user can see only the tabs and tasks that are assigned to their role.

You can assign separate roles to different users to prevent one user being able to complete every task. This may help your organization comply with separation of duties requirements. However, you can assign more than one role to a user.

Admin Roles in CA Access Control Enterprise Management

Predefined admin roles in CA Access Control Enterprise Management provide a basic set of admin roles that you can assign to administrators in your enterprise according to your requirements. Out-of-the-box, CA Access Control Enterprise Management comes with the following admin roles:

- **CA Access Control Host Manager**—Defines managed devices and logical security groups.

  CA Access Control Host Managers can create managed devices and security groups, assign devices to security groups, and modify the groups. CA Access Control Host Managers cannot define policies or deploy policies but they can use World View to view policies.

- **CA Access Control Policy Deployer**—Deploys policies across the environment.

  CA Access Control Policy Deployers assign policies to hosts and host groups, upgrade and downgrade policies, and reset host configuration.CA Access Control Policy Deployers can access the deployment audit. They can view policies and hosts but cannot define either. They can access World View.

- **CA Access Control Policy Manager**—Creates policies.

  CA Access Control Policy Managers create, modify, view, and delete policies. They cannot deploy policies to hosts or host groups but they can view them and can access World View.

- **CA Access Control User Manager**—Manages users and groups in CA Access Control Enterprise Management. They can also assign CA Access Control Enterprise Management roles to users.

  Note: The CA Access Control User Manager cannot create new admin roles. Only the System Manager can create new admin roles.

- **System Manager**—Manages CA Access Control Enterprise Management.

  System Managers can perform, create, and manage all tasks in CA Access Control Enterprise Management.

  Use this role for the implementation phase to define the actual admin roles in your organization and for emergency situations. We recommend that you assign this role to a minimal number of users, ideally only one user, and closely monitor the actions of this user.

- **Reporting**—Manages English reports. A user with this role can schedule and view reports.

- **CA Enterprise Log Manager User**—Reviews CA Enterprise Log Manager reports. A user with this role can view CA Enterprise Log Manager reports.

- **CA Enterprise Log Manager Admin**—Manages CA Enterprise Log Manager reports. A user with this role can administer the CA Enterprise Log Manager reports in CA Access Control Enterprise Management and manage the connection to the CA Enterprise Log Manager server.

- **Delegation Manager**—Delegates work items. A user with this role can delegate work items to users.

- **Self Manager**—Manages their own user account. A user with this role can perform administrative actions on their account. They can change the account password, modify their user profile, view their assigned roles, submitted tasks, and the items that are waiting for their approval.

  Note: By default, every user in the system is assigned the Self Manager role.

Create an Admin Role

If the predefined admin roles in CA Access Control Enterprise Management are not suitable for your organization requirements, you can create new ones.

To create an admin role

1. In CA Access Control Enterprise Management, do as follows:
   a. Click Users and Groups.
   b. Click Roles subtab.
   c. Expand the Admin Roles tree in the task menu on the left.

      The Create Admin Role task appears in the list of available tasks.
2. Click Create Admin Role.

   The Create Admin Role: Select Admin Roles page appears.
3. (Optional) Select an existing admin role to create the new admin role as a copy of it, as follows:
   a. Select Create a copy of a role.
   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of admin roles that match the filter criteria appear.
   c. Select the object you want to use as a basis for the new admin role.
4. Click OK.

   The Create Admin Role task page appears. If you created the admin role from an existing object, the dialog fields are pre-populated with the values from the existing object.
5. Complete the following fields in the Profile tab of the dialog:

   Name

   Defines the name of the role.

   Description

   A textual description of the role.

   Enabled

   Specifies whether the role can be assigned to users and groups.

6. Add tasks to the role, as follows:
   a. Click the Tasks tab.
   b. (Optional) Select a task category from the Filter tasks drop-down list

      The tasks in this category load.

      Note: The task category matches the tab on which tasks in this category appear in CA Access Control Enterprise Management.
   c. Select a task from the Add Task drop-down list.

      The task is added to the role.
   d. Repeat steps b through c to add more tasks to the role.
7. Add Member and Scope Rules (see page 21).
8. Click Submit.

   The role is created.

Privileged Access Roles

Privileged access roles in CA Access Control Enterprise Management provide a basic set of roles that you can assign to administrators and users in your enterprise according to your requirements. Out-of-the-box, CA Access Control Enterprise Management comes with the following privileged access roles:

- **Break Glass**—A user with this role can initiate a Break Glass privileged account password check out. A Break Glass checkout lets a user gain immediate access to an endpoint to which they do not have privileged access. This role is assigned by default to all the users in CA Access Control Enterprise Management.
- **Endpoint Privileged Access Role**—A user with this role can perform privileged account tasks on the specified endpoint type. The first time that you define a new type of endpoint, CA Access Control creates a corresponding endpoint privileged access role. For example, the first time you create a Windows endpoint in CA Access Control Enterprise Management, CA Access Control creates the Windows Agentless Connection endpoint privileged access role.
- **Privileged Account Request**—A user with this role can submit or delete requests for privileged account passwords. This role is assigned by default to all the users in CA Access Control Enterprise Management.
- **PUPM Approver**—A user with this role can respond to privileged access requests that CA Access Control Enterprise Management users have submitted. This role is assigned by default to all the users in CA Access Control Enterprise Management.
- **PUPM Audit Manager**—A user with this role can audit privileged account activity and manage the CA Enterprise Log Manager audit collection parameters.
- **PUPM Policy Manager**—A user with this role can manage role members and member polices, assign role owners, and create and delete roles.

- **PUPM Target System Manager**—A user with this role can administer password policies and privileged accounts, and can execute the privileged accounts discovery wizard to discover privileged accounts on endpoints.
- **PUPM User**—A user with this role can check in and check out privileged account passwords that they are permitted to use. This role is assigned by default to all the users in CA Access Control Enterprise Management.
- **PUPM User Manager**—A user with this role can administer CA Access Control Enterprise Management users and groups and password policies, and manage the work items of users.

Note the following:

- To respond to a privileged account request, a user must have the PUPM Approver role and be the requesting user's manager.
- If a user has the Break Glass, Privileged Account Request, or PUPM User role but does not also have an endpoint privileged access role, the user cannot access any endpoints. Effectively, the user cannot perform any tasks.
- If a user has an endpoint privileged access role but does not have any other role, the user cannot perform any tasks.

Create a Privileged Access Role

A privileged access role defines the tasks that role members, administrators and owners can perform when using PUPM, for example, check-in and check-out privileged accounts. If the predefined privileged access roles in CA Access Control Enterprise Management are not suitable for your organization requirements, you can create new ones.

To create a privileged access role

1. In CA Access Control Enterprise Management, do as follows:
   a. Click Users and Groups.
   b. Click Roles subtab.
   c. Expand the Privileged Access Roles tree in the task menu on the left.

      The Create Privileged Access Role task appears in the list of available tasks.
2. Click Create Privileged Access Role.

   The Create Role: Select Privileged Access Role page appears.

3. (Optional) Select an existing privileged access role to create the new role as a copy of it, as follows:
   a. Select Create a copy of a role.
   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of privileged access roles that match the filter criteria appear.
   c. Select the object you want to use as a basis for the new privileged access role.
4. Click OK.

   The Create Admin Role task page appears. If you created the admin role from an existing object, the dialog fields are pre-populated with the values from the existing object.
5. Complete the following fields in the Profile tab of the dialog:

   Name

   Defines the name of the role.

   Description

   A textual description of the role.

   Enabled

   Specifies whether the role can be assigned to users and groups.
6. Add tasks to the role, as follows:
   a. Click the Tasks tab.
   b. (Optional) Select a task category from the Filter tasks drop-down list

      The tasks in this category load.

      Note: The task category matches the tab on which tasks in this category appear in CA Access Control Enterprise Management.
   c. Select a task from the Add Task drop-down list.

      The task is added to the role.
   d. Repeat steps b through c to add more tasks to the role.
7. Add Member and Scope Rules (see page 21).
8. Click Submit.

   The role is created.

Methods to Assign Roles to a User

You can use the following methods to assign roles to a user:

- You add or remove multiple users from a role, by using the Modify Role Members/Administrators task.
- You add or remove roles from a single user, by using the Admin Roles tab or the Privileged Access Roles tab on the Modify User task.
- You modify the member policy for the role, using the Members tab on the Modify Admin Role task or on the Modify Privileged Access Role tab.

How to Add a User to an Admin Role

Once you created the admin role you can now add members and administrators to that role. Users that are members of a role assign the privileges that are attributed to the role. The following steps are prerequisites for adding members to the role:

1. Modify the admin role members policy definition to define the members of this rule.

   Modify the role members policy allows you to add users that are members of other roles to the role that you are modifying.

   Example: *where Logon Name = "Administrator" or Admin roles = "SystemManager"*

2. Verify that administrators can add or remove members to this role.
3. Define the actions that occur when a user is added to or removed from this role.

   Example: *Add SystemManager to Admin Roles, Remove SystemManager from Admin Roles*.

4. Modify the admin policies to add a user as an administrator to this role in the admin rule and assign that user administrator privileges.

   The user that you assigned as the role administrator is authorized to add members to this role.

   You can now add members to this role.

Add Member and Scope Rules

Once you have defined the profile and tasks of the role, you add members, administrators, and owners.

To add member and scope rules

1. Click the Members tab, and do the following:
   a. Click Add.
   b. Specify a Member Rule and a Scope Rule for the member policy (see page 23), and click OK.
   c. (Optional) Select Administrators can add and remove members of this role, and specify an Add Action and Remove Action (see page 23).

   The member policy for the role is created.
2. Click the Administrators tab, and do the following:
   a. Click Add.
   b. Specify an Admin Rule and Scope Rule and specify the Administrator Privileges for the admin policy (see page 24), and click OK.
   c. (Optional) Select Administrators can add and remove administrators of this rule, and specify an Add Action and Remove Action (see page 23).

   The admin policy for the role is created.
3. Click the Owners tab, click Add, specify an owner rule (see page 24), and click OK.

   The owner rule for the policy is created.

Member Policies

A *member policy* defines the users that can carry out the tasks in a role. A member policy contains the following:

- **Member rule**—Defines the users that can perform the role
- **Scope rule**—Defines the objects the users can manage

For example, admin roles, connection, privileged accounts, and policies are all objects. You can specify many other objects in scope rules. Each member policy can have more than one member rule, and each member rule can have more than one scope rule.

Example: A Member Policy for New York CA Access Control Host Managers

Don Hailey is the IT Manager for Forward, Inc and has the System Manager admin role. Don wants to create an admin role that lets employees with the CA Access Control Host Manager admin role in New York manage hosts and host groups in Forward, Inc New York offices only. All New York employees are members of the NY employees group, and the names of all the hosts and host groups in New York begin with the letters NY.

Don creates the following member policy. The member policy contains two member rules. The first member rule contains no scope rules. The second member rule contains two scope rules:

- Member rule 1—Admin roles contains "AC Host Manager".
- Member rule 2—Users who are members of group "NY employees"; scope rules—hosts where name starts with "NY", and host groups where name starts with "NY".

Add and Remove Actions

If you specify that the administrators of an admin role can assign and unassign users from that role, you must specify an Add and Remove Action for the admin role.

An Add and Remove Action contains the following:

- **Add action**—Ensures the user meets the criteria in one of the role's member rules
- **Remove action**—Ensures the user no longer meets the criteria in one of the role's member rules

Admin Policies

An *admin policy* specifies the users that are administrators of the admin role. An admin role administrator manages an admin role's member policies, and adds and removes users and groups from the admin role.

An admin policy contains the following:

- **Admin rule**—Defines the users who are administrators of the role
- **Scope rule**—Defines which users the administrators can manage
- **Administrator's privileges**—Specifies if the administrator can manage members and administrators of that admin role

Role Owners

A role owner adds and removes tasks from an admin role. You can define only one owner rule, but you can specify members of different groups within the owner rule.

Create an Admin Task

If the predefined admin tasks in CA Access Control Enterprise Management are not suitable for your organization requirements, you can create an admin task.

To create an admin task

1. Select the Users and Groups tab, select the Tasks link and click Create Admin Task.

   The Create Admin Task: Select Admin Task page appears.

2. Select Create a new admin task, and click OK.

   The Profile tab of the Create Admin task page appears.

   Note: To create a copy of an existing admin task, select Create a copy of an admin task, search for the admin task you want to copy, select the admin task, and click OK.

3. Enter the task name and description. Notice that the name appears in the tag field when you place the cursor in the field.
4. Select the position of the task in the tasks list from the menu.
5. Select the category that this task is part of.
6. (Optional) Select the order and category name of up to three (3) tasks.
7. Select the primary object that this task is part of. A primary object is the highest category that this task can appear in.
8. Select the action to associate with the task.
9. Select if to synchronize the user and account with the task.
10. Select either of the following options:

    Hide in menus

    Select not to display the task.

    Public task

    Select to make the task available to all users.

    Enable auditing

    Select to enable audit events logging for this task.

    Enable workflow

    Select to enable workflow.

    Enable web services

    Select to enable accessing this task using Web services.

    Workflow process

    Select the workflow process to associate with the task.

11. Select the task priority.

12. Select Submit.

    CA Access Control Enterprise Management creates the admin task.

More information:

Add Search Screens (see page 26)
Add Tabs (see page 26)
Configure Fields, Events, and Role Use (see page 27)

Add Search Screens

Select the search screen to associate with this task. In this tab, you can select to use existing search screens in this task or create a new search screen that displays information and provide search options that are specific to this task.

To add search screens

1. Select the browse button to search for an existing search screen or to create a new search screen.

   Note: To create a copy of an existing search screen, select Copy scope from another task, search for the admin task you want to copy, select the admin task, and click OK.

2. Select New to create a new search screen.
3. Select the type of search screen to create.
4. Enter the required information and click OK.

   The new search screen is added to the task.

Add Tabs

Use the tabs screen to select the tab controller to use with this task and the tabs that will appear in the task.

To add tabs

1. Select the tab controller to use in this task.

   Note: To create a copy of an existing tab definition, select Copy tabs from another task, search for the admin task you want to copy, select the admin task, and click OK.

2. Select the tabs that will appear in this task from the menu.
3. Click Submit.

   CA Access Control Enterprise Management adds the tab to the new task.

Configure Fields, Events, and Role Use

The fields, events, and role use tabs to display information regarding the fields that this task accesses, the events that the task is associated with, and the user roles that this task appears in. You cannot change the information that is displayed in these fields.

You can change the information that these tabs display by changing the settings. For example, to change the admin roles that this task appears in, modify the admin role settings to include or exclude this task.

Users, Groups, and Administrative Roles

When creating a user, you assign it one or more *admin roles* or *privileged access roles.* An admin role contains tasks that correspond to application functions in CA Access Control Enterprise Management. When you assign an admin role to a user, that user can perform the tasks contained in the admin role. Tasks enable users to perform CA Access Control functions, such as creating a policy, deploying a policy, creating a host group, and managing other users.

A privileged access role defines the tasks that correspond to privileged accounts management on the managed endpoints. When assigning a privileged access role to a user, that user can perform privileged account management task such as, checking and out privileged accounts passwords.

To make administration easier, you can create groups of users, and assign an admin role to a group. Each user in the group can then complete all the tasks in that admin role.

More information:

Create a User (see page 28)
Types of Groups (see page 31)

Active Directory Restrictions

If you use Active Directory as your user store, you cannot create and delete users and groups in CA Access Control Enterprise Management. You do not see the following tasks in the interface, and you cannot assign these tasks to an admin role or a privileged access role:

- Create User
- Delete User
- Modify Role Members/Administrators
- Create Group
- Delete Group

When you assign admin roles to an Active Directory user, CA Access Control Enterprise Management modifies the user profile and notes the admin roles that are assigned to this user in the registered address field.

Note: You can choose to define a user with read-only privileges in the User DN: parameter. However, if you define a user with read-only privileges, you cannot assign admin roles or privileged access roles to users in CA Access Control Enterprise Management. Instead, you modify the member policy for each role to point to an Active Directory group.)

Create a User

Users perform tasks in CA Access Control Enterprise Management. You create a user with the System Manager role when you install CA Access Control Enterprise Management. Create additional users when you start CA Access Control Enterprise Management to enforce separation of duties.

Note: If you use Active Directory as your user store, you cannot create a user in CA Access Control Enterprise Management.

To create a user

1. In CA Access Control Enterprise Management, click Users and Groups.

   The Create User task appears in the list of available tasks.

2. Click Create User.

   The Create User: Select User window appears.

3. (Optional) Select an existing user to create the new user as a copy of it, as follows:
   a. Select Create a copy of a user.
   b. Select an attribute for the search, type in the filter value, and click Search.

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

   The Create User task page appears. If you created a user from an existing object, the dialog fields are pre-populated with the values from the existing object.
5. Complete the fields in the Profile tab. The following fields are not self-explanatory:

   User ID

   Defines the string that identifies the user to CA Access Control Enterprise Management. This is the name the user used to log in.

   Password Must Change

   Specifies to force the user to change the password on first login.

   Enabled

   Specifies whether the user can log in to CA Access Control Enterprise Management.
6. (Optional) Click the Admin Roles tab to assign admin roles to the user, as follows:
   a. Click Add an admin role.

      The Select Admin Roles section appears.
   b. Type a filter value and Click Search.

      A list of roles that match the filter criteria appears.
   c. Select the admin roles that you want to assign to the user, and click Select.

   The admin roles are assigned to the user.
7. (Optional) Click the Privileged Access Roles tab to assign privileged access roles to the user, as follows:
   a. Click Add a privileged access role.

      The Select Privileged Access Roles section appears.
   b. Type a filter value and Click Search.

      A list of roles that match the filter criteria appears.
   c. Select the privileged access roles that you want to assign to the user, and click Select.

   The privileged access roles are assigned to the user.

8. (Optional) Click the Groups tab to add the user to groups, as follows:
   a. Click Add a group.

      The Select Group section appears.

   b. Type a filter value and Click Search.

      A list of groups that match the filter criteria appears.

   c. Select the groups that you want to assign to the user, and click Select.

   The user is added to the groups.
9. Click Submit.

   The user is created.

Reset a User Password

Reset a user password when a user account was locked after several failed login attempts, or when the user has lost or forgot the password.

To reset a user password

1. In CA Access Control Enterprise Management, click Users and Groups.

   The Reset User Password appears in the list of available tasks.
2. Click Reset User Password.

   The Reset User Password search page opens.
3. Type in the search query and click Search.

   The query displays the results according to the search criteria.
4. Select the user account and click Select.

   The reset password window opens.
5. Type in the account password in the Confirm Password field.
6. (Optional) Select the Password Must Change option.
7. Click Submit.

   CA Access Control Enterprise Management resets the user password.

Enable or Disable a User

Enable a user account so that a user can use the account credentials to log in to CA Access Control Enterprise Management. Disable a user account to prevent that user from accessing CA Access Control Enterprise Management, and to keep the user profile in the system.

To enable or disable a user

1. In CA Access Control Enterprise Management, click Users and Groups.

   The Enable/Disable User task appears in the list of available tasks.

2. Click Enable/Disable User.

   The Enable/Disable User page appears.

3. Define a search query and click Search.

   The list of users that matches the search query displays.

4. Specify the user accounts to disable and enable, as follows:

   - Clear a user to disable that account.
   - Select a user to enable that account.

5. Click Select.

   A screen summarizing the changes you specified appears.

6. Click Yes to confirm the modifications you made.

   CA Access Control Enterprise Management submits the task to make the requested changes.

Types of Groups

You can create several types of groups, or a combination of these types:

- **Static groups**

  A list of users that are added interactively.

- **Dynamic groups**

  Users belong to the group if they meet an LDAP query. (Requires an LDAP directory as the user store).

  Note: To view the dynamic group query field, you must include it in the task by editing the associated profile screen.

- **Nested groups**

  Groups containing other groups. (Requires an LDAP directory as the user store).

  Note: To view static, dynamic and nested groups to which a user belongs, use the Groups tab for the User object. The tab appears in the View and Modify User tasks.

Create a Static or a Dynamic Group

You can associate a collection of users in a static group. You manage the group by adding or removing users from the group membership list. To view the members of a group, use the Membership tab in the View or Modify Group tasks.

You create a dynamic group by defining an LDAP filter query using the CA Access Control Enterprise Management to determine group membership at runtime.

Note: The Membership tab displays only the members that are explicitly added to the group. If you use Active Directory as your user store, you cannot create a group in CA Access Control Enterprise Management.

To create a static or dynamic group

1. Log into CA Access Control Enterprise Management as a user with group management privileges.
2. Select Groups, Create Group.

   The create group search screen appears.
3. Select to create a group and click OK.

   The group profile tab appears.
4. Enter the group name and description.
5. Navigate to the Membership tab.

   Note: Only an administrator with the Modify Group task can change a group dynamic membership.
6. Click Add a User.

   The select user search window opens.
7. Enter the search query and click Search.

   The query returns the results according to the search criteria.
8. Select a user and click Select.

   Navigate to the Administrators tab.
9. Click Submit.

   A message appears informing you that the process completed successfully.

   Note: When you assign a user as a group administrator, verify that the administrator has a role with appropriate scope for managing the group.

LDAP Filter Query—Define Dynamic Group Query Parameters

You create a dynamic group by defining an LDAP filter query using the CA Access Control Enterprise Management to determine group membership at runtime.

This filter query has the following format:

LDAP:///*search_base_DN*??*search_scope*?*searchfilter*

search_base_DN

Defines the point from where you begin the search in the LDAP directory. If you do not specify the base DN in the query, then the group organization is the default base DN.

search_scope

Specifies the extent of the search and includes:

- **sub**—Returns entries at the base DN level and below.
- **one**—Returns entries one level below the base DN you specify in the URL.
- **base**—Uses one instead, ignoring base as a search option.

Using *one* or *base* obtains only the users in the Base DN organization.

Using *sub* obtains all users under the Base DN organization and all sub-organizations in the tree.

searchfilter

Defines the filter that you want to apply to entries within the scope of the search. When you enter a search filter, use the standard LDAP query syntax as follows:

`([logical_operator]Comparison)`

logical operator

Defines a logical operator. Can be one of:

- **|**—Logical OR
- **&**—Logical AND
- **!**—Logical NOT

Comparison

Defines *AttributeOperatorValue*

- *Attribute*—Defines the name of the LDAP attribute.
- *Operator*—Specifies the comparison operator. Can be one of: **=** (equals), **<=** (less than or equals), **>=** (greater than or equals), or **~=** (approximately equals).
- *Value*—Defines the value for the attribute data.

Example: (&(city=Boston)(state=Massachusetts))

Default: (objectclass=*)

Note the following when creating a dynamic query:

- The "LDAP" prefix must be lowercase, for example:

  `ldap:///o=MyCorporation??sub?(title=Manger)`

- You cannot specify the LDAP server host name or port number. All searches occur within the LDAP directory that you configured for your environment.

Example: Sample LDAP Queries

The following are sample LDAP queries:

Description	Query
All users who are managers.	ldap:///o=MyCorporation??sub?(title=Manger)
All managers in the New York West branch office	ldap:///o=MyCorporation??one?(&(title=Manager) (office=NYWest))
All technicians with a cell phones	ldap:///o=MyCorporation??one? (&(employeetype=technician) (mobile=*))

Description	Query
All employees with employee numbers from 1000 through 2000	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
All help desk administrators who have been employed at the company for more than six months	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) **Note:** This query requires that you create a DOH attribute for the user date of hire.

Note: The > and < (greater than and less than) comparisons are lexicographic, not arithmetic. For details on their use, see the documentation for your LDAP directory server.

Modify Group Members

Use this option to add or remove members and groups. Use the procedure to modify the group list of members.

To modify group members

1. Log into CA Access Control Enterprise Management as a user with group management privileges.
2. Select Groups, Modify Group Members.

   The modify group members screen appears.
3. Select a group and click Select.

   The group members list opens.
4. To remove a member, clear the check box next to the member name.
5. To add a member click Add a User.
   a. Type in the search query and click Search.

      The search query displays the results according to the search criteria.
   b. Select the user and click Select.

      The user is added as a group member.
6. To add a group click the Add a Group button.
   a. Type in the search query and click Search.

      The search query displays the results according to the search criteria.
   b. Select the group and click Select.

      The group is added.

7. Click Submit.

   A confirmation message appears informing you that the task completed successfully.

Audit Data

Audit data provides a historical record of operations that occur in a CA Access Control Enterprise Management environment. Some examples of audit data include the following:

- System activity for a specified period.
- A list of objects that were modified during a specific period.
- The roles assigned to a user
- The operations performed for a particular user account

Audit data is generated for *events*. An event is an operation that is generated by a CA Access Control Enterprise Management task. For example, the Create User task can include an AssignAccessRoleEvent event.

CA Access Control Enterprise Management stores audit data in the central database. You can configure an audit collector to route audit data to CA Enterprise Log Manager.

Note: For more information about integrating with CA Enterprise Log Manager, see the *Implementation Guide*.

More information:

Search for Submitted Tasks (see page 37)
View Task Details (see page 40)
View Event Details (see page 40)
Clean Up Submitted Tasks (see page 41)
Route Message Queue Audit Messages to Windows Event Log (see page 43)
Route Message Queue Audit Messages to UNIX Syslog (see page 45)
Configure an Audit Collector (see page 169)

Search for Submitted Tasks

Submitted tasks provide information about tasks in a CA Access Control Enterprise Management environment. You can search for and view high-level details about actions that CA Access Control Enterprise Management performs. Detail screens provide additional information about each task and event.

Depending on the status of the task, you can cancel or resubmit a task.

Submitted tasks let you track the processing of a task from beginning to end.

To search for submitted tasks

1. In CA Access Control Enterprise Management, click System, Audit subtab.

   The View Submitted Tasks task appears in the list of available tasks.

2. Click View Submitted Tasks.

   The View Submitted Tasks page appears.

3. Specify search criteria (see page 37), enter the number of rows to display, and click Search.

   The tasks that satisfy your search criteria are displayed.

Search Attributes for Viewing Submitted Tasks

To review tasks that have been submitted for processing, you can use the search feature in View Submitted Tasks. You can search for tasks based on the following criteria:

Initiated By

Identifies the name of the user who has initiated a task as the search criteria. Searches are based on the user name. To ensure that you entered a valid user name, use the Validate button.

Approval By

Identifies the name of the task approver as the search criteria. Searches are based on the user name. To ensure that you entered a valid user name, use the Validate button.

Note: If you select Approval Tasks Performed By criteria to filter the tasks, the Show approval tasks criteria is also enabled by default.

Task Name

Identifies the task name as the search criteria. You can refine the search by specifying conditions such as equals, contains, starts with, or ends with the value of the Where Task Name field. For example, you can specify the search criteria "task name equals Create User" by selecting the equals condition, and entering Create User in the text field.

Task Status

Identifies task status (see page 39) as the search criteria. You can select the task status by enabling Where task status equals, and selecting the condition. You can further refine the search based on the following conditions:

- Completed
- In Progress
- Failed
- Rejected
- Partially Completed
- Cancelled
- Scheduled

Task Priority

Identifies task priority as the search criteria. You can select the task priority by enabling Where task priority equals, and selecting the condition. You can further refine the search based on the following conditions:

Low

Specifies that you can search for tasks that have a low priority.

Medium

Specifies that you can search for tasks that have a medium priority.

High

Specifies that you can search for tasks that have a high priority.

Performed On

Identifies tasks that are performed on the selected instance of the object. If you do not select an instance of the object, the tasks that were performed on all the instances of that object will be displayed.

Note: This field appears only when the Configure Performed On field is populated in the Configure Submitted Tasks screen. You use this screen to configure the Submitted Tasks tab.

Date range

Identifies the dates between which you want to search submitted tasks. You must provide the From and To dates.

Show unsubmitted tasks

Identifies the tasks in the Audited state. Identifies the tasks that have initiated other tasks or tasks that have not been submitted. All such tasks will be audited and displayed if you select this tab.

Show approval tasks

Identifies the tasks that have to be approved as part of a workflow.

More information:

Task Status Description (see page 39)

Task Status Description

A submitted task exists in one of the states described below. Based on the state of the task, you can perform actions such as cancelling or resubmitting a task.

Note: To cancel or resubmit a task, you must configure View Submitted Tasks to display the cancel and resubmit buttons based on the task status.

In progress

Displayed when any of the following occurs:

- Workflow is initiated but not yet completed
- Tasks, which are initiated before the current tasks, are in progress
- Nested tasks are initiated but not yet completed
- The primary event is initiated but not yet completed
- Secondary events are initiated but not yet completed

You can cancel a task in this state.

Note: Cancelling a task will cancel all the incomplete nested tasks and events for the current task.

Cancelled

Displayed when you cancel any of the tasks or events in progress.

Rejected

Displayed when CA Access Control Enterprise Management rejects an event or task that is part of a workflow process. You can resubmit a rejected task.

Note: When you resubmit a task, CA Access Control Enterprise Management will resubmit all the failed or rejected nested tasks and events.

Partially Completed

Displayed when you cancel some of the events or nested tasks. You can resubmit a partially completed event or nested task.

Completed

Displayed when a task is completed. A task is completed when the nested tasks and nested events of the current task are completed.

Failed

Displayed when a task, nested task, or event nested in the current task are invalid. This status is displayed when the task fails. You can resubmit a failed task.

Scheduled

Displayed when the task is scheduled to execute at a later date. You can cancel a task in this state.

View Task Details

CA Access Control Enterprise Management provides task details, such as the status of a submitted task, nested tasks, and events associated with a task.

To view details of a submitted task

1. Click the right arrow icon next to the selected task in the View Submitted Tasks page.

   The task details appear.

   Note: Events and nested tasks (if any) are displayed in the Task Details page. You can view the task details for each of the tasks and events.

2. Click Close.

   The Task Details tab closes and CA Access Control Enterprise Management displays the View Submitted Tasks tab with the tasks list.

View Event Details

CA Access Control Enterprise Management provides events details, such as the status of a submitted event, event attributes, and any additional information about the events.

To view details of a submitted event

1. Click the right arrow icon next to an event in the View Task Details page.

   The event details appear.

2. Click Close.

   The Event Details page is closed.

Clean Up Submitted Tasks

CA Access Control Enterprise Management stores audit data, including PUPM audit data, in the central database. However, database performance may be affected if you store a large amount of audit data in the central database. To improve database performance, you can use the Cleanup Submitted Tasks wizard to remove submitted tasks from the central database.

Important! Cleaning up submitted tasks deletes audit data from the database. To avoid data loss, we recommend that you route audit events to CA Enterprise Log Manager before you run the cleanup task.

You can schedule the cleanup task to run immediately or at recurring intervals. Cleaning up submitted tasks may consume a large amount of system resources. We recommend that you schedule this task outside business hours.

To clean up submitted tasks

1. In CA Access Control Enterprise Management, do as follows:
   a. Click System.
   b. Click the Tasks subtab.
   c. Click Cleanup Submitted Tasks.

      The Cleanup Submitted Tasks: Recurrence page appears.
2. Do *one* of the following:
   - To run the task immediately, select Execute now and click Next.

     The Cleanup Submitted Tasks: Cleanup Submitted Tasks page appears.
   - To create a recurring schedule, select Schedule new job and complete the fields that appear. The following fields are not self-explanatory:

     Time Zone

     Specifies the time zone of the Enterprise Management Server.

     If you are in a different time zone to the server, you can select either your time zone or the server time zone when you schedule a new job. You cannot change the time zone when you modify an existing job.

Weekly Schedule

Specifies that the task runs at a specific time on a specific day or days of the week.

Specify the time in 24-hour format, for example, 17:15.

Advanced Schedule

Lets you use a cron expression to specify the times at which the task runs.

Click Next.

The Cleanup Submitted Tasks: Cleanup Submitted Tasks page appears.

3. Complete the following fields:

Minimum Age

Specifies the minimum age of tasks in a final state (Completed, Failed, Rejected, Cancelled, or Aborted) that CA Access Control Enterprise Management removes from the central database.

Audit Timeout

(Optional) Specifies the minimum age of tasks in the audit state that CA Access Control Enterprise Management removes from the central database.

Note: Tasks in the audit state have not been submitted.

Time Limit

(Optional) Specifies the maximum length of time that CA Access Control Enterprise Management takes to perform the cleanup operation.

Task Limit

(Optional) Specifies the maximum number of tasks that CA Access Control Enterprise Management removes from the central database.

Click Finish.

CA Access Control Enterprise Management removes submitted tasks from the central database at the time that you specified.

Route Message Queue Audit Messages to Windows Event Log

Valid on Windows

You can configure the Enterprise Management Server to route message queue audit messages to the Windows event log. Each time the Enterprise Management Server writes an audit message to the audit log, a corresponding event is sent to the event log.

To route message queue audit messages to Windows event log

1. Stop the JBoss application server,If running.
2. Navigate to the following directory, where *JBOSS_HOME* indicates the directory where you installed JBoss:

   JBOSS_HOME\server\default\conf\
3. Open the jboss-log4j.xml file.
4. Add an appender named "ENTM_NTEventLog" in the class.

   The appender specifies the class to use for auditing and how to display the data.
5. Create a logger named "EventLog".

   You specify the logger that the appender binds to as a input channel for the audit messages.
6. Save and close the file.
7. Copy the NTEventLogAppender.dll file to the Windows System32 directory.

   Note: You can find the NTEventLogAppender.dll file in the Apache log4j 1.2.16 bundle. You can download the Apache log4j 1.2.16 from the Apache Logging Services website.
8. Start the JBoss application server.

   The Enterprise Management Server now route message queue audit message to the Windows event log.

Example: Modify the jboss-log4j.xml file to send message queue audit messages to Windows Event Log

The following snippet shows the jboss-log4j.xml file that is configured to route message queue audit messages to the Windows Event Log::

```
 <appender name="ENTM_NTEventLog"
                        class="org.apache.log4j.nt.NTEventLogAppender">
    <param name="Source" value="CA Access Control Enterprise Management"/>
    <layout class="org.apache.log4j.SimpleLayout"/>
</appender>

<logger name="EventLog">
    <appender-ref ref="ENTM_NTEventLog"/>
</logger>
```

In this example,you did the following changes:

- Added a new appender by the name "ENTM_NTEventLog"
- Added class by the name "org.apache.log4j.nt.NTEventLogAppender"
- Defined the param name: "Source"
- Defined the value: "CA Access Control Enterprise Management"
- Defined the layout class:"org.apache.log4j.SimpleLayout"
- Defined the logger name: "EventLog"
- Defined the appender-ref ref : "ENTM_NTEventLog"

Route Message Queue Audit Messages to UNIX Syslog

Valid on UNIX

You can configure the Enterprise Management Server to route message queue audit messages to the UNIX syslog. Each time the Enterprise Management Server writes an audit message to the audit log, a corresponding event is sent to the syslog.

To route message queue audit messages to UNIX syslog

1. Stop the JBoss application server, if running.
2. Navigate to the following directory, where *JBOSS_HOME* indicates the directory where you installed JBoss:

   JBOSS_HOME\server\default\conf\
3. Open the jboss-log4j.xml file.
4. Add an appender named "ENTM_UNIXEventLog" in the class.

   The appender specifies the class to use for auditing and how to display the data.
5. Create a logger named "EventLog".

   You specify the logger that the appender binds to as a input channel for the audit messages.
6. Save and close the file.
7. Open the /etc/syslog.conf file and verify that the syslog routes the messages to the /var/log/messages file.
8. Open the /etc/sysconfig/syslog parameters file and verify that the remote mode option appears in the following entry:

   ```
   SYSLOGD_OPTIONS="-m 0-r"
   ```
9. Restart the syslog daemon. Run the following command:

   ```
   /etc/rc.d/init.d/syslog restart
   ```

   The syslog daemon starts.
10. Start the JBoss application server.

    The Enterprise Management Server will now route message queue audit message to the UNIX syslog

Example: Modify the jboss-log4j.xml file to send message queue audit messages to UNIX SysLog

The following snippet shows the jboss-log4j.xml file after a LogAppender object was created:

```
<appender name="ENTM_UNIXSysLog"
                        class="org.apache.log4j.net.SyslogAppender">
    <param name="Facility" value="USER"/>
    <param name="FacilityPrinting" value="false"/>
    <param name="SyslogHost" value="localhost"/>
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%p - [CA AC ENTM]: %m%n"/>
    </layout>
</appender>

<logger name="EventLog">
    <appender-ref ref="ENTM_UNIXSysLog"/>
</logger>
```

In this example, you did the following:

- Added the appender:"ENTM_UNIXSysLog"
- Created a class: "org.apache.log4j.net.SyslogAppender"
- Defined the param name: "Facility" and the value "USER"
- Defined the param name: "FacilityPrinting" with the value "false"
- Defined a param name: "SyslogHost" with the value "localhost"
- Defined a layout class: "org.apache.log4j.PatternLayout"
- Defined a param name: "ConversionPattern" with the value: "%p - [CA AC ENTM]: %m%n"
- Defined the logger name: "EventLog"
- Defined an appender-ref: ref="ENTM_UNIXSysLog"

Email Notifications

Email notifications inform CA Access Control Enterprise Management users of events in the system, and are generated from email templates. If you enable email notifications, CA Access Control Enterprise Management can generate email notifications when one of the following occurs:

- An event that requires approval or rejection is pending.
- An approver approves an event.
- An approver rejects an event.
- An event starts, fails, or completes.
- A CA Access Control Enterprise Management user is created or modified.

Note: For more information about how to enable email notifications, see the *Implementation Guide*.

Email Templates

CA Access Control Enterprise Management generates email notifications from email templates. Each email template contains the following information:

- **Delivery information**—A list of email recipients.
- **Subject**—The text used in the subject line of the email.
- **Content**—The email body. The body typically includes both static text and variables, which CA Access Control Enterprise Management resolves based on the task or event that triggers the email.

The email templates are located in the following directory, where *JBoss_home* is the directory in which you installed JBoss:

JBoss_home/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default

The emailTemplates directory contains five subdirectories. Each folder is associated with an event state. The following table lists the purpose of the email templates in each subdirectory:

Subdirectory	Contents
Approved	■ CertifyRoleEvent.tmpl—Obsolete. ■ CheckOutAccountPasswordEvent.tmpl—Informs recipients that a privileged account password request was approved. ■ CreatePrivilegedAccountExceptionEvent.tmpl—Informs recipients that a privileged account password request was approved for a set period of time (this template corresponds to the Privileged Account Request task). ■ defaultEvent.tmpl—Informs recipients that an event was approved. ■ defaultTask.tmpl—Informs recipients that a task was approved. ■ ForgottenPasswordEvent.tmpl—Obsolete. ■ SelfRegisterUserEvent.tmpl—Obsolete.

Subdirectory	Contents
Completed	■ AccumulatedProvisioningRolesEvent.tmpl—Obsolete. ■ CertificationNonCertifiedActionCompletedNotificationEvent.tmpl—Obsolete. ■ CertificationNonCertifiedActionPendingNotificationEvent.tmpl—Obsolete. ■ CertificationRequiredFinalReminderNotificationEvent.tmpl—Obsolete. ■ CertificationRequiredNotificationEvent.tmpl—Obsolete. ■ CertificationRequiredReminderNotificationEvent.tmpl—Obsolete. ■ CheckOutAccountPasswordEvent.tmpl—Informs recipients of the password for the privileged account that they checked out. ■ CreateProvisioningUserNotificationEvent.tmpl—Obsolete. ■ defaultEvent.tmpl—Informs recipients that CA Access Control Enterprise Management completed an event. ■ defaultTask.tmpl—Informs recipients that CA Access Control Enterprise Management completed a task. ■ ForgottenPassword.tmpl—Obsolete. ■ ForgottenUserID.tmpl—Obsolete. ■ Self Registration.tmpl—Obsolete.
Invalid	■ AssignProvisioningRoleEvent.tmpl—Obsolete. ■ DefaultEvent.tmpl—Informs recipients that an event failed. ■ DefaultTask.tmpl—Informs recipients that a task failed.
Pending	■ BreakGlassCheckOutAccountEvent.tmpl—Informs approvers that a break glass checkout was performed. ■ CertifyRoleEvent.tmpl—Obsolete. ■ CheckOutAccountPassswordEvent.tmpl—Informs approvers that a privileged account check-out request requires attention. ■ defaultEvent.tmpl—Informs approvers that a work list item requires attention. ■ defaultTask.tmpl—Informs approvers that a task requires attention. ■ ModifyUserEvent.tmpl—Obsolete.

Subdirectory	Contents
Rejected	■ CertifyRoleEvent.tmpl—Obsolete. ■ CheckOutPasswordEvent.tmpl—Informs recipients that a privileged account password request was rejected. ■ CreatePrivilegedAccountExceptionEvent.tmpl—Informs recipients that a user request to access a privileged account for a set period of time was rejected (this template corresponds to the Privileged Account Request task). ■ defaultEvent.tmpl—Informs recipients that an event was rejected. ■ defaultTask.tmpl—Informs recipients that a task was rejected. ■ ForgottenPasswordEvent.tmpl—Obsolete. ■ SelfRegisterUserEvent—Obsolete.

How Email Notifications Work

Email notifications inform CA Access Control Enterprise Management users of events in the system. The following process describes how email notifications work:

1. When an event occurs, CA Access Control Enterprise Management checks if an email notification is enabled for the event.
2. If an email notification is enabled, CA Access Control Enterprise Management looks in the appropriate subdirectory for the event type.

   For example, if an email is to be sent for the approval of a privileged account request, CA Access Control Enterprise Management looks in the Approved subdirectory.
3. CA Access Control Enterprise Management checks the subdirectory for an email template with the same name as the event, and does one of the following:
   - If an email template exists with the same name as the event, CA Access Control Enterprise Management sends that email template to the recipients.
   - If an email template does not exist with the same name as the event, CA Access Control Enterprise Management sends the defaultEvent.tmpl email template to the recipients.

Note: For more information about how to configure email notification settings, see the *Implementation Guide*.

Customize Email Templates

CA Access Control Enterprise Management generates email notifications from email templates. You can customize the email templates to suit your enterprise requirements.

To customize an email template

1. Open the template in an editable form.
2. Edit the email template by doing one or both of the following:
   - Type static text in the body of the template.
   - Use the variables in the Email Template API to specify dynamic content in the template.
3. Save and close the template.

Note: For more information about the Email Template API, see the *CA Identity Manager Administration Guide*.

Chapter 3: Planning Your PUPM Implementation

This section contains the following topics:

Privileged User Password Management

Privileged User Password Management (PUPM) is the process through which an organization secures, manages, and tracks all activities associated with the most powerful accounts within the organization.

PUPM provides role-based access management for privileged accounts on target endpoints from a central location. PUPM provides secure storage of privileged accounts and application ID passwords and controls access to privileged accounts and passwords based on policies you define. Further, PUPM manages privileged accounts and application password lifecycle and lets you remove passwords from configuration files and scripts.

What Are Privileged Accounts?

Privileged accounts are accounts that are not assigned to individuals accounts and have access to mission critical data and processes. System Administrators use privileged accounts to perform administrative tasks on target endpoints and privileged accounts are also embedded in service files, scripts, and configuration files to facilitate unattended processing.

Privileged accounts are difficult to control because they are not assigned to an identifiable user, which renders auditing and tracing difficult. This is a vulnerability that exposes mission critical systems to accidental harm and malicious activities. Organizations must reduce the number of these privileged accounts to a minimum that satisfies operational needs.

Administrators can bypass most internal controls to access restricted information and cause denial of service (DOS) attacks by deleting or rendering applications inaccessible. Further, the activities performed using privileged accounts are difficult to correlate to an identifiable user account.

Privileged Access Roles and Privileged Accounts

You use privileged access roles to specify the PUPM tasks that each user can perform in CA Access Control Enterprise Management and the privileged accounts that each user can check in and check out. CA Access Control Enterprise Management comes with predefined privileged access roles. You can modify the predefined roles to suit your enterprise, or create new roles entirely.

When a user logs in to CA Access Control Enterprise Management, they see only the tasks and privileged accounts that correspond to their role.

Using Privileged Access Roles

You should consider the following points before you set up PUPM for your enterprise:

- We recommend that you use Active Directory as your user store and modify the member policy for each role to point to a group in Active Directory. To add or remove users from a role that you set up in this manner, you add or remove users from the Active Directory group. This simplifies administrative overhead.
- If you use Active Directory as your user store, you cannot use CA Access Control Enterprise Management to create or delete users or groups. You can only create and delete users and groups in Active Directory.
- If a role has a member policy defined for it, and a PUPM User Manager assigns that specific role to a user but the user does not fit the scope of the member policy, then CA Access Control does not assign the role to the user. The rules defined in the member policy override the PUPM User Manager assignment.
- To respond to a privileged account request, a user must have the PUPM Approver role and be the requesting user's manager. If you use the embedded user store, you can specify a user's manager in the Create User and Modify User tasks in CA Access Control Enterprise Management.
- Out-of-the-box, CA Access Control assigns the Break Glass, PUPM Approver, Privileged Account Request, and PUPM User roles to all users. To change this behavior, modify the member policy for each role.
- You can modify scope rules for a role to define the specific endpoints and privileged accounts that the role can access. Scope rules let you implement fine-grained access to privileged accounts across your enterprise. The scope rules are defined in the member policy of a role.

More information:

Member Policies (see page 23)

How Privileged Access Roles Affect Check Out and Check In Tasks

You check out privileged accounts to perform administrative tasks on endpoints, and check in privileged accounts when you have finished working on the endpoint.

Important! A user must have an endpoint privileged access role to perform tasks on an endpoint type. Endpoint privileged access roles specify the types of endpoints on which a user can perform tasks using a privileged access account.

For example, if you assign the Windows endpoint privileged access role to a user, the user can perform endpoint tasks on Windows endpoints that use privileged accounts. If you assign the Break Glass, Privileged Account Request, or PUPM User role to a user, assign the user an endpoint privileged access role, or the user is not able to complete any tasks.

The following process describes how privileged access roles affect the check-out and check-in tasks that users perform:

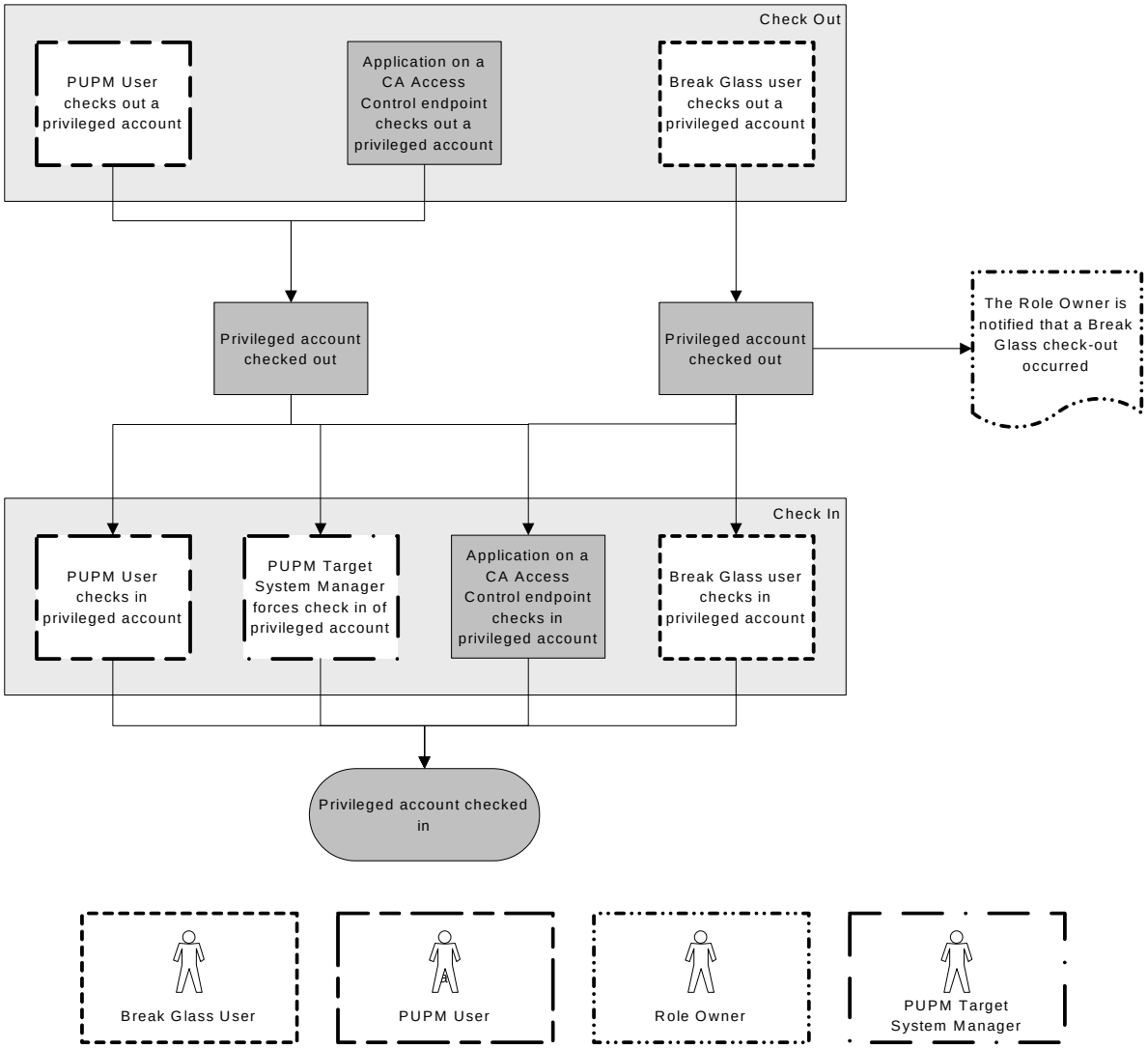
1. A user checks out a privileged account, using one of the following methods:
   - A user with the PUPM User role checks out a privileged account.
   - A user with the Break Glass role performs a break glass checkout.
   - An application, for example a CLI password consumer, on a CA Access Control endpoint checks out a privileged account.

   The privileged account is checked out.

   Note: If a user performs a break glass checkout, CA Access Control notifies the role owner. The role owner can choose to add information to this message for auditing purposes.
2. A user checks in a privileged account, using one of the following methods:
   - The user with the PUPM User role checks in the privileged account.
   - The user with the Break Glass role checks in the privileged account.
   - The application on the CA Access Control endpoint checks in the privileged account.
   - A user with the PUPM Target System Manager role forces the check-in of the privileged account.

   The privileged account is checked in.

The following diagram illustrates how privileged access roles affect the check in and check out tasks that users perform:



Example: Check Out a Privileged Account

You have the System Manager role. You assign Joe the PUPM User role and the Windows Agentless Connection endpoint privileged access role. Joe logs in to CA Access Control Enterprise Management, and sees only the tasks that let him check out and check in privileged accounts on Windows endpoints.

Example: Break Glass for a Privileged Account

You have the System Manager role. You assign Fiona the Break Glass role and the Oracle Server Connection endpoint privileged access role. Fiona needs immediate access to an Oracle endpoint. She logs in to CA Access Control Enterprise Management and sees only the tasks that let her perform a break glass check out for accounts on Oracle endpoints. Fiona performs a break glass check out for an Oracle privileged account, and CA Access Control sends a notification message to the Break Glass role owner.

Note: By default, the Break Glass role owner is the System Manager admin role.

How Privileged Access Roles Affect Privileged Account Request Tasks

If a user cannot check out a privileged account and does not need immediate access to the account, the user can submit a privileged account request. The manager can approve or reject the privileged account request. This topic explains what privileged access roles a user needs to perform privileged account request tasks.

Important! A user must have an endpoint privileged access role to perform tasks on an endpoint type. Endpoint privileged access roles specify the types of endpoints on which a user can perform tasks using a privileged access account.

For example, if you assign the Windows endpoint privileged access role to a user, the user can perform endpoint tasks on Windows endpoints that use privileged accounts. If you assign the Break Glass, Privileged Account Request, or PUPM User role to a user,also assign the user an endpoint privileged access role, or the user will not be able to complete any tasks.

The following process describes how privileged access roles affect the privileged account request tasks that a user can perform:

1. A user with the Privileged Account Request role requests access to a privileged account.
2. CA Access Control sends the privileged account request to the user's manager, who also has the PUPM Approver role.

   Note: A user must have the PUPM Approver role and must be the user's manager to receive the privileged account request.

3. The user with the PUPM Approver role responds to the privileged account request, and does *one* of the following:

   - Rejects the privileged account request.

     The user with the Privileged Account Request role cannot check out the privileged account.

   - Reserves the privileged account request.

     No other user can approve or reject the privileged account request. The user with the Privileged Account Request role cannot check out the privileged account until the PUPM Approver chooses to approve the request.

   - Approves the privileged account request.

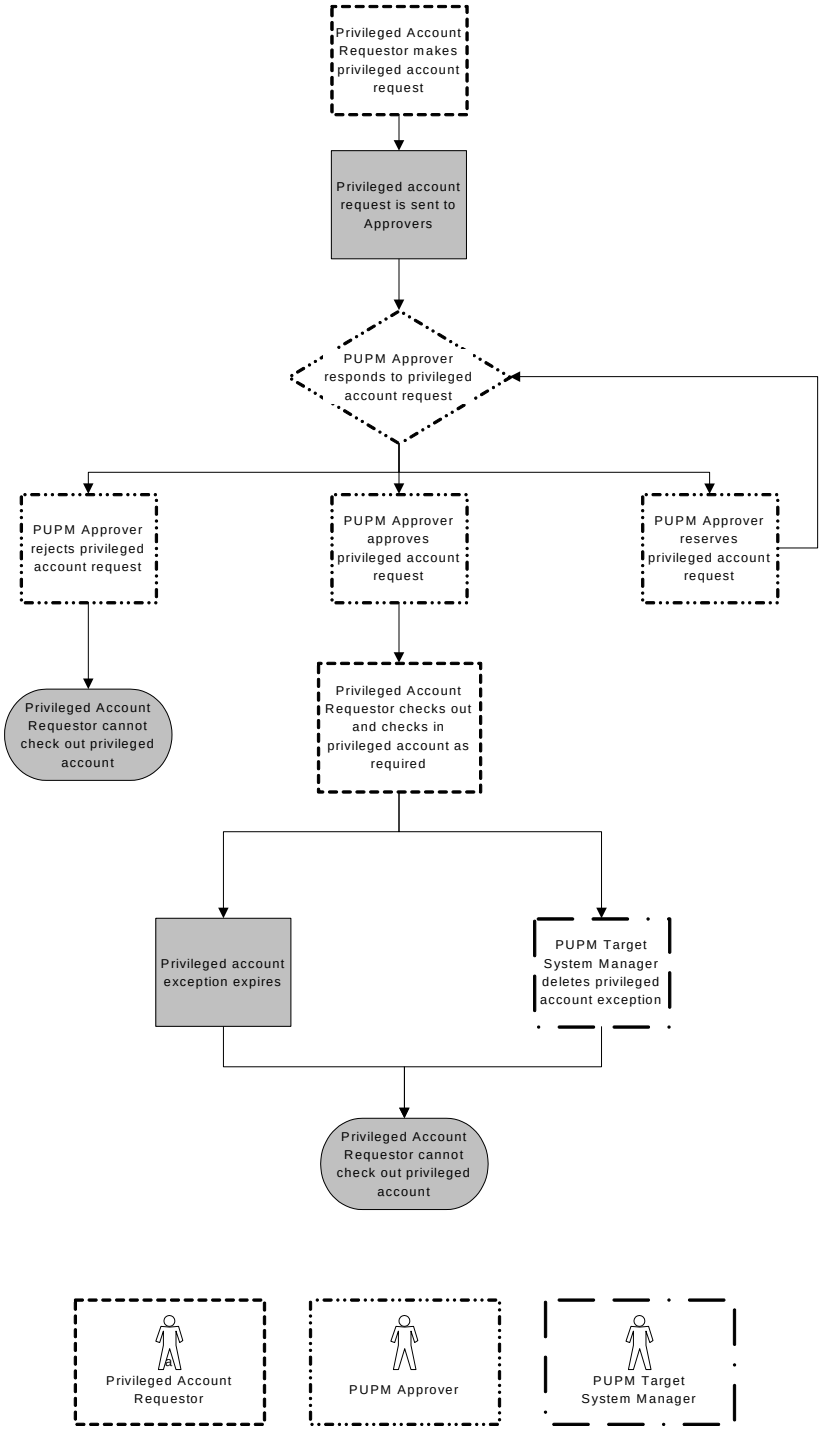
     The user with the Privileged Account Request role is granted a privileged account exception, and can check out and check in the privileged account.

4. The privileged account exception expires, for one of the following reasons:

   - The expiration time specified in the privileged account exception is reached.
   - A user with the PUPM Target System Manager role deletes the privileged account exception.

   The user with the Privileged Account Request role can no longer check out the privileged account.

The following diagram illustrates how privileged access roles affect the privileged account request tasks that a user can perform:



Example: Make and Respond to a Privileged Account Request

You have the System Manager role. You assign Alice the Privileged Account Request role and the SSH Device Connection endpoint privileged access role. Bob is Alice's manager, and you assign Bob the PUPM Approver role.

Alice logs in to CA Access Control Enterprise Management, and sees only the tasks that let her submit a privileged account request for accounts on UNIX endpoints. Alice submits a privileged account request for the example_ux account on a UNIX endpoint.

Bob logs in to CA Access Control Enterprise Management, and sees only the tasks that let him respond to privileged account requests. Bob approves Alice's privileged access request and specifies that the privileged account exception is valid until 6pm. Alice can now check in and check out the example_ux privileged account. At 6pm, the privileged account exception expires and Alice can no longer check out the example_ux privileged account.

What Happens During the Break Glass Process

A user performs a break glass check out 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 if the need arises.

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 nor stop the process.

The checked out Break Glass account is added to the user's 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.

PUPM Audit Records

CA Access Control Enterprise Management records audit data for events, for example, when a user checks in a privileged account password. CA Access Control Enterprise Management also records audit data for failed events. For example, if you choose automatic login when you check out a privileged account password but do not accept the ActiveX download, CA Access Control Enterprise Management records the reason that the automatic login failed. CA Access Control Enterprise Management stores PUPM audit data in the central database.

More information:

Audit Data (see page 36)
Audit Privileged Accounts (see page 139)

PUPM Feeder Audit Records

The PUPM feeder performs the following tasks. CA Access Control Enterprise Management creates an audit record for each action that the PUPM feeder performs:

- Feeder Folder Polling—Specifies whether the PUPM feeder successfully uploaded the CSV files in the polling folder to CA Access Control Enterprise Management.
- Feeder Process csv File—Specifies whether CA Access Control Enterprise Management successfully processed the uploaded CSV file, and provides a progress indicator that tracks the number of lines CA Access Control Enterprise Management has processed in the CSV file.

In addition, CA Access Control Enterprise Management creates an audit record for each line in the imported CSV file. Each line represents a task to create or modify a PUPM endpoint or privileged account. The audit records track the status of each task. These tasks can have the following statuses:

- **Completed**—CA Access Control Enterprise Management completed the task, for example, created a privileged account.
- **Failed**—CA Access Control Enterprise Management processed the task but did not complete it, for example, could not create a privileged account on an endpoint that does not exist.
- **Audited**—CA Access Control Enterprise Management did not process or complete the task, for example, could not create a privileged account because the ACCOUNT_NAME attribute is not specified.

A user with the System Manager role can use the View Submitted Tasks task to view the status of each task.

Auditing Events on PUPM Endpoints

CA Access Control Enterprise Management records audit data for events that occur on the Enterprise Management Server. If you integrate your PUPM endpoints with CA Enterprise Log Manager, you can also record audit events on the endpoints for each privileged account session.

After a user checks out a privileged account and uses the account to log in to an endpoint, the integration lets you track the actions that the privileged account performs on the endpoint. These actions are recorded in audit events, which are collected in CA Enterprise Log Manager reports. You can view these CA Enterprise Log Manager reports in CA Access Control Enterprise Management.

For example, you want to review the actions that a user performed after they checked out an account named privileged1. You use the Audit Privileged Accounts task in CA Access Control Enterprise Management to find the audit record for the privileged1 account checkout. You then drill down from this audit record and view a CA Enterprise Log Manager report of the activities that the privileged1 account performed on the endpoint, for example, opening and closing programs.

More information:

View Audit Events on a PUPM Endpoint (see page 142)

How to Integrate PUPM Endpoints with CA User Activity Reporting Module

Integrating your PUPM endpoints with CA User Activity Reporting Module lets you record audit events on endpoints for each privileged account session. The integration also lets you view CA Enterprise Log Manager reports of privileged account audit events on PUPM endpoints in CA Access Control Enterprise Management.

Follow these steps::

1. In CA Access Control Enterprise Management:
   a. Configure the connection to CA User Activity Reporting Module.
   b. Specify the CA User Activity Reporting Module Host Name and Event Log Name for each PUPM endpoint.

      To specify the Host Name and Event Log Name, use the CA User Activity Reporting Module tab of the Create Endpoint or Modify Endpoint task.
2. Configure CA User Activity Reporting Module to continuously collect information from the PUPM endpoints.

Note: For more information about how to configure CA User Activity Reporting Module, see the CA User Activity Reporting Module documentation.

More information:

View Audit Events on a PUPM Endpoint (see page 142)

Implementation Considerations

The following topics list items you should consider before you implement PUPM.

Email Notification of Privileged Account Passwords

Occasionally, CA Access Control Enterprise Management may hang for longer than 20 seconds when a user tries to check out a password, for example, if the network is slow. If CA Access Control Enterprise Management hangs for longer than 20 seconds, the screen times out and the password is not displayed to the user. CA Access Control Enterprise Management emails the password to the user instead.

To help ensure that the user receives the password, do the following:

- Configure email notification settings for CA Access Control Enterprise Management.
- Verify that a valid email address is recorded in the user store for each PUPM user.

Note: For more information about configuring email notifications, see the *Implementation Guide*.

Restrictions on Domain Users on Windows Agentless Endpoints

If you configure a domain user on a local computer, PUPM cannot change the password of the domain user. This limitation is due to Windows behavior.

Connector Servers

CA Access Control Enterprise Management communicates with the Connector Server to search for and manage privileged accounts on the PUPM endpoints. CA Access Control Enterprise Management uses a Java Connector Server (JCS) to communicate with CA Access Control for PUPM endpoints. By default, a JCS is installed as part of the Distribution Server when you install CA Access Control Enterprise Management.

To use PUPM to manage CA Identity Manager Provisioning endpoints, you must create an Identity Manager Provisioning type Connector Server in CA Access Control Enterprise Management.

Note: For more information about creating Connector Servers, see the *Online Help*.

Connector Xpress Overview

Connector Xpress is a CA Identity Manager utility for managing dynamic connectors, mapping dynamic connectors to endpoints, and establishing routing rules for endpoints. You can use it to configure dynamic connectors to provision and manage of SQL databases.

Connector Xpress lets you create and deploy custom connectors without the technical expertise required when creating connectors managed by the Provisioning Manager.

You can also set up, edit, and remove a connector server configuration (both Java and C++) using Connector Xpress.

The primary input into Connector Xpress is the native schema of an endpoint system. For example, you can use Connector Xpress to connect to an RDBMS and retrieve the SQL schema of the database. You can then use Connector Xpress to construct mappings from those parts of the native schema that are relevant to identity management and provisioning. A mapping describes how the provisioning layer represents an element of the native schema.

Note: For more information about the Connector Xpress, see the *Connector Xpress Guide*.

How to Implement Connector Xpress for PUPM

To manage endpoints that are not default PUPM endpoint type, you can use Connector Xpress to create new endpoint types and manage privileged account passwords. For example, create an endpoint of type SQL when you want to manage privileged account passwords that are located in a Microsoft SQL Server database. The default PUPM SQL endpoint type was designed to manage privileged accounts on the SQL Server and not to manage individual tables within a database.

Follow these steps:

1. Install Connector Xpress.

   Note: For more information about how to install Connector Xpress, see the *Connector Xpress Guide* available in the CA Identity Manager bookshelf on CA Support.

2. Configure the new endpoint type in Connector Xpress.

3. Register the new endpoint type with the Java Connector Server.

   You register the new endpoint type to enable the Java Connector Server to manage the endpoint type.

4. Load the new endpoint type to the Enterprise Management Server.

   You load the endpoint type to make it available in CA Access Control Enterprise Management.

5. Create PUPM endpoints for the new endpoint type in CA Access Control Enterprise Management.
6. Discover privileged account passwords on the new endpoints.

Connector Xpress Example: Configure a JDBC Endpoint

In this example, the system administrator Steve creates a JDBC endpoint type in Connector Xpress to connect to a Microsoft SQL Server.

Steve has installed Connector Xpress on the Enterprise Management Server host. Steve does the following:

1. From the Start menu, selects Programs, CA, Identity Manager, Connector Xpress.

   The Identity Manager Connector Xpress main menu appears.
2. Clicks Setup Data Sources.

   The Setup Data Sources window opens.
3. Clicks Add.

   The Source Types window opens, displaying the available sources.
4. Selects JDBC and clicks OK.

   The Edit Source window opens.
5. Enters the following details:
   - Data source name—SQL Server
   - Database type—Microsoft SQL Server
   - Username—sa
   - Server Name—mysql
   - Port—1433
   - Database—users
6. Clicks Test to verify the connection settings.

   The Enter password for data source window opens.
7. Enters the sa user account password and clicks OK.

   A confirmation message appears, if no errors were discovered. The new data source is created. Steve now configures the new endpoint type.

8. Returns to the Identity Manager Connector Xpress main menu, and selects New Project.

   The Select Data Source for New Project window appears.

9. Selects the data source he created and clicks OK.

   The Endpoint Type Details window opens.

10. Enters the endpoint name and description, double clicks the Classes icon and selects the User Details option.

    The Map Class and Attributes window opens.

11. In the Select Schema and Table section, selects the following:

    - For Schema, selects dbo
    - For Table, selects sqlConnector table.

    The mapped columns are displayed.

12. In the Map Columns section, enters the following values in the Name columns:

    - In the uname row,enters Account ID
    - In the upassword row, enters Password

13. Selects Project, Save to save the endpoint type definitions.

Steve has configured a new JDBC endpoint type in Connector Xpress. Steve now registers the endpoint type with the Java Connector Server.

Connector Xpress Example: Register the JDBC Endpoint in the Java Connector Server

In this example, the system administrator Steve registers the endpoint type that he created in Connector Xpress in the Java Connector Server. Steve registers the new endpoint type to display it in CA Access Control Enterprise Management. Steve does the following:

1. From the Identity Manager Connector Xpress project window, right clicks the Connector Server option and selects Add Server.

   The Connector Server Details window opens.

2. Specifies the Java Connector Server host name, and clicks OK.

   Note: The Java Connector Server is part of the Distribution Server. The Enterprise Management Server installs the Distribution Server on this server by default. The connector Server Password Required window opens

3. Enters the Enterprise Management Server communication password.

   You specified the communication password when you installed the Enterprise Management Server. A list of existing endpoint types is displayed.

4. Right clicks Endpoint Types and selects Create New Endpoint type.

   The Create New Endpoint Type window opens.

5. Enters the endpoint type name, and clicks OK.

   Connector Xpress creates the new endpoint type if no errors are found.

Steve has registered the new endpoint with the Java Connector Server. Steve now loads the new endpoint type to the Enterprise Management Server.

Connector Xpress Example: Load the Endpoint Type to the Enterprise Management Server

In this example, the system administrator Steve loads the new endpoint type that was created to the Enterprise Management Server. After Steve loads the new endpoint type, Steve is able to configure and manage the endpoint from CA Access Control Enterprise Management. Steve does the following:

1. Stops the JBoss application server.
2. Does *one* of the following:
   - (JDBC) Edits the file conXpressnamespace_config.xml.template.
   - (SUN One) Edits the iplanetnamespace_config.xml

   You can find the files in the following directory, where *JBOSS_HOME* indicates the directory where you installed JBoss:

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/namespaceConfigs/
3. Locates the <endpointType> parameter and removes the default value: 'REPLACE_WITH_ENDPOINT_TYPE'.
4. Enters the endpoint type name as specified in Connector Xpress.
5. Saves the file under the name conXpress_*Endpoint_Type*_namespace_config.xml in the following directory:

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/namespaceConfigs/
6. Starts the JBoss application server.

Steve has loaded the new endpoint type to the Enterprise Management Server. Steve can now define endpoints of this type in CA Access Control Enterprise Management and discovers the privileged accounts on the endpoint.

Connector Xpress Limitations

You should consider the following before you run the Discover Privileged Accounts wizard on the endpoint type you created in Connector Xpress:

- Define an endpoint of the same type that you created in Connector Xpress, for example, a SQL Server endpoint, and provide the endpoint administrator account credentials. When CA Access Control Enterprise Management creates the endpoint, it also creates a disconnected privileged account.
- Specify the endpoint type you created in Connector Xpress from the endpoint type menu. In the URL field, specify the database name as in the example below.
- Leave the user login and password fields empty. Check Use the following privileged account and select a privileged account with privileges to connect to the endpoint. Use the disconnected privileged account that CA Access Control Enterprise Management created for the endpoint you previously defined.

Example: SQL Server database name in the endpoint URL field

The following example shows you the URL field that contains the SQL Server database name:

```
jdbc:sqlserver://server.company.com:1433;database=database_name
```

The PUPM SDK

The PUPM SDK lets you write applications that check out and check in privileged account passwords. There are two types of PUPM SDK, password consumer SDKs and the Web Services SDK.

The following table summarizes the differences between the two types of SDK:

Feature	Password Consumer SDK	Web Services SDK
Programming languages	Java .NET	Java
User authentication	Yes	No
Password caching	Yes	No
Requires CA Access Control on endpoint	Yes	No

Use Case: The PUPM SDK

The PUPM SDK lets you automate the management of privileged account passwords in scripts. If you do not want to modify scripts that contain hard-coded passwords, you can write an application that regularly replaces the passwords in the scripts.

For example, you have ten scripts on an endpoint that contain hard-coded passwords for the same privileged account. You do not want to modify the scripts. You can use the PUPM SDK to write an application that checks out the privileged account password at a suitable downtime, updates the password in each script, and then checks in the password. Regularly changing the passwords helps increase the security of your privileged accounts.

If you create an application to perform this task, verify that CA Access Control Enterprise Management does not change the privileged account password on check out or check in. You can use the View Privileged Account task to verify this information.

Note: You can also use a CLI password consumer to replace hard-coded passwords in scripts. For example, use a CLI password consumer if you want to manually update a hard-coded password in a file.

How a Password Consumer SDK Application Gets a Password

The password consumer SDKs let you write applications that get, check in, and check out privileged account passwords. To use a password consumer SDK, you must do the following:

- Install CA Access Control on the endpoint on which the application runs
- Define a password consumer for the application in CA Access Control Enterprise Management

There are two types of password consumer SDK:

- Java PUPM SDK
- .NET PUPM SDK

Password consumer SDK applications communicate with the PUPM Agent, which then uses the Message Queue to communicate with CA Access Control Enterprise Management. The PUPM Agent uses SSL communication and port 7243 to communicate with the Message Queue.

The following process describes how a password consumer SDK application gets a password:

1. The application sends a password request to the PUPM Agent.
2. The PUPM Agent receives the password request. CA Access Control verifies the identity of the user running the application, and checks the cache. *One* of the following happens:
   - If the password request is cached, the PUPM Agent sends the privileged account password to the application. The process ends at this step. CA Access Control Enterprise Management does not write an audit record for the password request.
   - If the password request is not cached, the PUPM Agent sends the password request and the name of the user running the application to CA Access Control Enterprise Management.
3. CA Access Control Enterprise Management receives the request, and checks that a password consumer exists that authorizes the application to obtain the privileged account password.

   The password consumer specifies the path of the application, the privileged accounts that the application can request, the users that can run the application, and the hosts on which the application can be run.

4. *One* of the following happens:
   - If the application is authorized to obtain the password, CA Access Control Enterprise Management sends the privileged account password to the PUPM Agent.
   - If the application is not authorized to obtain the password, CA Access Control Enterprise Management sends an error message to the PUPM Agent.

   In both cases, CA Access Control Enterprise Management writes an audit record for the event.
5. The PUPM Agent sends the privileged account password or error message to the application.

   If the application has obtained the privileged account password for the first time, the PUPM Agent caches the password.

Note: When the password for a privileged account changes, CA Access Control Enterprise Management broadcasts the password change event to the endpoints. When an endpoint receives the broadcast message, the PUPM Agent removes the privileged account password from the cache.

The Java PUPM SDK

The Java PUPM SDK is a password consumer SDK that lets you write Java applications that get, check out, and check in privileged account passwords. You can use the Java PUPM SDK on Windows and UNIX endpoints on which CA Access Control is installed. The Java application that you write must use JRE 1.5 or later.

The Java PUPM SDK is located in the following directory:

ACInstallDir/SDK/JAVA

This directory contains the following:

- PupmJavaSDK.jar—The SDK library that you include in your Java application.
- CAPUPMCLientCommons.jar—A supporting library that you must include in the classpath when you run the application.
- jsafeFIPS.jar—A supporting library that you must include in the classpath when you run the application.

- CAPUPM.properties.SAMPLE—A sample file that you can edit to change the default application properties.

  If you edit this file, you must name the new file CAPUPM.properties and include the file name in the classpath when you run the application.

  Note: We recommend that you contact CA Support before you modify this file. For assistance, contact CA Support at http://ca.com/support.

- Samples—A folder that contains a sample Java application that checks out and checks in privileged account passwords.

If you want the application to log runtime events and information, you must also include a log4j library in the classpath. You must create a Software Development Kit (SDK/CLI) password consumer for the application in CA Access Control Enterprise Management before it can get, check out, and check in privileged account passwords.

The .NET PUPM SDK

Valid on Windows

The .NET PUPM SDK is a password consumer SDK that lets you write C# applications that get, check out, and check in privileged account passwords. You can use the .NET PUPM SDK only on Windows endpoints where CA Access Control is installed, although you can get, check out, and check in passwords for privileged accounts that reside on any operating system. You must install the .NET Framework 2.0 or later on the endpoint to use the .NET PUPM SDK.

The .NET PUPM SDK is located in the following directory:

ACInstallDir\SDK\DOTNET

This directory contains the following:

- Pupmcsharpsdk.dll—The SDK library that you include in your C# application.
- Examples—A folder that contains sample applications that check out and check in privileged account passwords.

  Each sample application contains an uncompiled sample (.cs file) and a compiled sample (.exe file).

You must create a Software Development Kit (SDK/CLI) password consumer for the application in CA Access Control Enterprise Management before it can get, check out, and check in privileged account passwords.

The Web Services PUPM SDK

The Web Services PUPM SDK lets you write Java applications that check in and check out privileged account passwords. You can use the Web Services PUPM SDK on endpoints on which CA Access Control is not installed, for example, on mainframe endpoints.

Before you can use a Web Services PUPM SDK application to check out or check in a privileged account password, you must create a user that represents the application in CA Access Control Enterprise Management and assign the user the appropriate privileged access role.

You must install the following components on the endpoint to use the Web Services PUPM SDK:

- Apache Ant 1.7
- Apache Axis 1.4
- Java SDK 1.4.2
- (Optional) An integrated development environment (IDE), for example, Eclipse

The Web Services PUPM SDK is located in the following directory:

ACServerInstallDir`/IAM Suite/Access Control/tools/samples/webservice/Axis`

This directory contains the following components for the Web Services PUPM SDK:

- Readme.txt—A file that contains instructions on how to configure the environment, build the Java samples, and run the Java samples.
- build.xml—The Apache Ant build script.
- build.properties—A file that sets properties in build.xml.
- CheckInPrivilegedAccount.java—A sample Java application that checks in privileged account passwords.
- CheckOutPrivilegedAccount.java—A sample Java application that checks out privileged account passwords.
- client-config.wsdd—A file that configures Axis to save all incoming and outgoing XML messages to a file named axis.log.

  Note: The directory also contains sample Java applications that let you perform other administrative tasks, for example, creating or deleting privileged accounts.

How a Web Services SDK Application Gets a Password

The Web Services PUPM SDK lets you write Java applications that check in and check out privileged account passwords. You do not need to install CA Access Control on the endpoint on which the Web Services PUPM SDK application runs. However, unlike password consumer SDKs, the Web Services PUPM SDK does not cache passwords or authenticate users.

Web Services PUPM SDK applications use SOAP (Simple Object Access Protocol) and port 18080 to communicate directly with the Enterprise Management Server.

Important! We recommend that you use a strong authentication protocol such as NTLM to authenticate the connection between the application and the Enterprise Management Server.

The following process describes how a Web Services PUPM SDK application gets a password:

1. The application logs in to CA Access Control Enterprise Management.

   The user name and password with which the application logs in are defined in the application.

2. The application requests the password for a privileged account.

3. CA Access Control Enterprise Management checks the privileged access role assigned to the user that represents the application.

4. *One* of the following happens:

   - If users with that privileged access role can obtain the privileged account password, CA Access Control Enterprise Management sends the password to the application.
   - If users with that privileged access role cannot obtain the privileged account password, CA Access Control Enterprise Management sends an error message to the application.

5. The application logs out of CA Access Control Enterprise Management.

Chapter 4: Implementing Privileged Accounts

This section contains the following topics:

How to Set Up Privileged Accounts

Privileged User Password Management (PUPM) is the process through which an organization secures, manages, and tracks all activities associated with the most powerful accounts within the organization. Before you can begin using privileged account passwords, you complete several steps that set up CA Access Control Enterprise Management for PUPM. Users can then start working with the privileged accounts that you define.

The following process explains the tasks that users in your enterprise must complete to set up privileged accounts. Users must have the specified role to complete each process step. A user with the System Manager admin role can perform every CA Access Control Enterprise Management task in this process.

Note: Before you begin this process, verify that email notification is enabled in CA Access Control Enterprise Management. If CA Access Control Enterprise Management cannot display a password to a user, it emails the password to the user instead.

To set up privileged accounts, users do the following:

1. The PUPM Target System Manager creates password policies. Password policies set password rules and limitations for privileged accounts.
2. The PUPM Target System Manager creates endpoints in CA Access Control Enterprise Management. Endpoints are devices that are managed by privileged accounts. You can create endpoints in CA Access Control Enterprise Management or use the PUPM feeder to import endpoints.
3. The PUPM Target System Manager creates privileged accounts for each endpoint. Creating privileged accounts lets CA Access Control Enterprise Management manage the accounts. You can create privileged accounts in CA Access Control Enterprise Management or use the PUPM feeder to import privileged accounts.

4. (Optional) The System Manager creates login applications, and the PUPM Target System Manager modifies PUPM endpoints to use the login applications. Login applications let users log in to a privileged account from CA Access Control Enterprise Management.

5. The PUPM Policy Manager modifies the member policies of privileged access roles. Member policies define the users that can carry out the tasks in a role.

   Note: If you use Active Directory as your user store, we recommend that you modify each member policy to point to a corresponding Active Directory group. You can then add or remove users from a role by adding or removing them from the corresponding Active Directory group. This greatly simplifies administrative overhead.

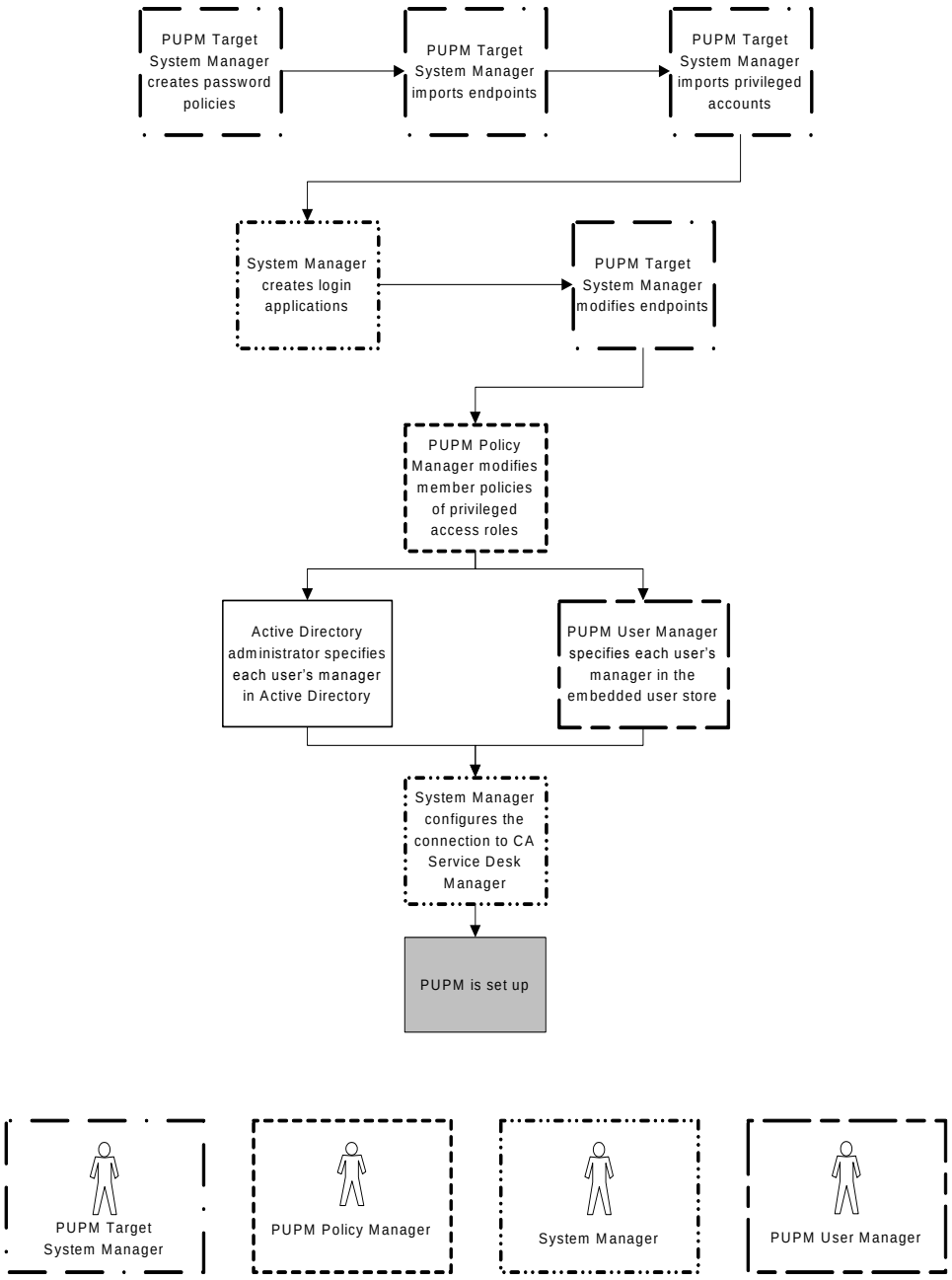
6. (Embedded user store) The PUPM User Manager specifies the manager of each user.

   Note: Only a manager can approve privileged account requests that the user makes. If you use Active Directory as your user store, verify that each user's manager is specified in Active Directory.

7. (Optional) The System Manager configures the connection to Unicenter Service Desk.

   Integrating with Unicenter Service Desk lets you create multiple approval processes for privileged account requests.

The following diagram illustrates the privileged access role that performs each process step:



Discover Privileged Accounts

We recommend that you run the privileged accounts discovery process at fixed intervals to scan for new privileged accounts on the endpoints. Discovering privileged accounts lets you create multiple privileged accounts at the same time. CA Access Control Enterprise Management presents the accounts it discovers in a table, so that you can easily tell which accounts you already manage with PUPM.

The first time you discover privileged accounts on an endpoint type, CA Access Control Enterprise Management automatically 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 Enterprise Management automatically creates the Windows Agentless Connection endpoint privileged access role.

Follow these steps:

1. In CA Access Control Enterprise Management, click Privileged Accounts, Accounts, Discover Privileged Accounts Wizard.

   The Discover Privileged Accounts Wizard: Select Privileged Accounts page appears.

2. Select the Endpoint Type from the list.

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

   A list of endpoints that match the filter criteria appears.

4. Select the privileged accounts you want to manage.

   The following table column headings are not self-explanatory:

   Discovered Account

   Specifies whether the account is already known to CA Access Control Enterprise Management. Known accounts include ones that CA Access Control Enterprise Management already manages and the administrator account CA Access Control Enterprise Management uses to manage the endpoint.

   Is Endpoint Administrator

   Specifies whether CA Access Control Enterprise Management uses the account to manage the endpoint.

   Important! Be cautious when selecting the endpoint administrator account. CA Access Control Enterprise Management can automatically change the password of privileged accounts it manages. If you select the endpoint administrator account, you may lose the ability to log in and manage privileged accounts on the endpoint.

   Click Next.

   The Discover Privileged Accounts Wizard: General Account Details page appears.

5. 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 need to 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 CA Access Control Enterprise Management to change the password of the privileged account every time it is checked out.

   Note: This option does not apply to service accounts.

   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.

6. Click Finish.

   CA Access Control Enterprise Management submit the task and creates the selected privileged accounts if there are no errors.

Create a Privileged Account

You create privileged accounts to manage account passwords on managed and disconnected systems. You use privileged accounts to let users check out and check in privileged account passwords, create a privileged account.

To create multiple accounts, use the Discover Privileged Accounts wizard to search for privileged on the endpoints. If you want to create a single account, provide the privileged or service account details in this window.

Follow these steps:

1. In CA Access Control Enterprise Management, click Privileged Accounts, Accounts, Create Privileged Account.

   The Create Privileged Account: Select Privileged Account page appears.

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

   a. Select Create a copy of an object of type Privileged Account.

   b. 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.

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

3. Click OK.

   The General tab of the Create Privileged Account task page appears. If you created the privileged account from an existing object, the dialog fields are prepopulated with the values from the existing object.

4. Complete the following fields in the General tab:

   Account Name

   Defines the name you want to refer to this privileged account by.

   Note: Mainframe systems such as RACF, ACF, and Top Secret, use case-sensitive user names. Enter the account name in capital letters.

Disconnected Account

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, also change the account password on the managed endpoint manually.

Account Type

Specifies whether the account is a shared (privileged) account or a service account.

Note: When you create a service account, PUPM does not attempt to change the account password.

Endpoint Name

Specifies the name of a defined endpoint where your privileged accounts reside. CA Access Control Enterprise Management lists only those endpoints that are of the type you specified.

Endpoint Type

Specifies the type of endpoint where your privileged or service accounts reside.

Container

Specifies the name of the container for the privileged or service account. A *container* is a class whose instances are collections of other objects. Containers are used to store objects in an organized way following specific access rules.

Password Policy

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

Password

Defines and verifies the password to use with the new privileged account.

Note: The new password must comply with the password policy you specify.

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.

Note: This option does not apply to service accounts.

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 Application Check Out Only

Specifies whether to allow password check out only if a login application is defined for the endpoint.

Note: When this option is enabled, the user cannot display or copy the password to a clipboard.

Click Submit.

CA Access Control Enterprise Management creates the new privileged account.

Create a Password Policy

A password policy for privileged accounts is a set of rules and restrictions that determine permissible privileged account passwords. For example, you can configure the policy to mandate passwords that are at least eight characters long and contain a number and a letter. Password policies also determine an interval at which CA Access Control Enterprise Management automatically creates a new password for the account.

Note: CA Access Control Enterprise Management comes with a predefined password policy that you can use. We recommend that you define password policies that are appropriate for each of your endpoints and adhere to your security requirements.

To create a password policy

1. In CA Access Control Enterprise Management, click Privileged Accounts, Password Policy, Create Password Policy.

   The Create Password Policy: Configure Standard Search Screen page appears.

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

   a. Select Create a copy of an object of type Privileged Account Password Policy, and click Search.

      The list of password policies appears.

   b. Select the object you want to use as a basis for the new password policy.

3. Click OK.

   The Create Password Policy task page appears. If you created the password policy from an existing object, the dialog fields are pre-populated with the values from the existing object.

4. Type a name and an optional description for the password policy.

5. (Optional) Clear Enabled.

   By default, new password policies are enabled. If the policy you are creating is not approved yet, you can choose to clear this checkbox and leave the policy disabled.

6. Define the password composition rules.

7. (Optional) Define a password expiration interval.

   This is a regular interval at which CA Access Control Enterprise Management changes passwords automatically. By default, the expiration interval is disabled (set to zero).

8. (Optional) Define the times, in 24-hour time format, at which CA Access Control Enterprise Management can change the password.

   For example, if you create a password policy for a service account, you can specify that CA Access Control Enterprise Management can change the password of the account only between 10:00 p.m. and 11:59 p.m. (22:00–23:59) on Sundays.

9. Click Submit.

   CA Access Control Enterprise Management creates the password policy.

More Information:

Password Composition Rules (see page 84)

Password Composition Rules

When you create a password policy, you can define the content requirements for new passwords.

Important! When you configure password composition rules, consider the maximum password length when you set the requirements. If the total number of required characters exceeds the maximum password length then all passwords are rejected.

CA Access Control Enterprise Management provides the following password composition rules for privileged accounts:

Minimum password length

Defines the minimum number of characters that passwords must contain.

Maximum password length

Defines the maximum number of characters that passwords can contain.

Maximum repeating characters

Defines the maximum number of repeating characters passwords can contain.

For example, if you set this value to 3, the string “aaa” cannot appear in the password but “aa” can.

Upper case letters (u for pattern)

Specifies whether passwords can contain uppercase letters and, if so, defines the minimum number of those that passwords must contain.

Lower case letters (c for pattern)

Specifies whether passwords can contain lowercase letters and, if so, defines the minimum number of those that passwords must contain.

Letters (l for pattern)

Specifies whether passwords can contain alphabetic characters and, if so, defines the minimum number of those that passwords must contain.

Digits (d for pattern)

Specifies whether passwords can contain digits and, if so, defines the minimum number of those that passwords must contain.

Letters or digits (a for pattern)

Specifies whether passwords can contain alphanumeric characters and, if so, defines the minimum number of those that passwords must contain.

Punctuation (p for pattern)

Specifies whether passwords can contain punctuation or special (non-alphanumeric) characters and, if so, defines the minimum number of those that passwords must contain.

Any (* for pattern)

Specifies that passwords can contain any characters. If you select this option, CA Access Control Enterprise Management automatically selects all other character content definitions.

Use Pattern

Specifies that, instead of defining the character content definitions, you define a pattern that the password must use.

Examples:

- **uuuuu**—matches ASDKF or IUTYE
- **ucdddp**—matches Rv671* or Uc194^
- **********—matches lkI&5Jj@ or sffIU*&1
- **lllaaaa**—matches yuUI1Uo3 or qWcV1Er6

Prohibited Characters

Defines the characters that cannot be used when creating or modifying a privileged account password.

PUPM Endpoint and Privileged Account Creation

The following topics explain how to create endpoints, create and discover privileged accounts, and create login applications in CA Access Control Enterprise Management.

If you want to create or modify multiple PUPM endpoints or privileged accounts, consider using the PUPM feeder. The PUPM feeder lets you import many endpoints or privileged accounts in a single step, and lets you automate the management of PUPM endpoints and privileged accounts.

Create an Endpoint

Creating endpoint definitions in CA Access Control Enterprise Management lets you manage endpoints and discover the privileged and service accounts on that endpoint.

Follow these steps:

1. In CA Access Control Enterprise Management, click Privileged Accounts, Endpoints, Create Endpoint.

   The Create Endpoint: Select Endpoint page appears.

2. (Optional) Select an existing endpoint to create the endpoint as a copy of it, as follows:
   a. Select Create a copy of an object of type Endpoint.
   b. Select an attribute for the search, type in the filter value, and click Search.

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

   The General tab of the Create Endpoint task page appears. If you created the endpoint from an existing object, the dialog fields are prepopulated with the values from the existing object.
4. Complete the fields in the tab. The following fields are not self-explanatory:

   Name

   Defines the logical name of the endpoint.

   Note: This field defines how the name of the endpoint appears in CA Access Control Enterprise Management. You specify connection information when you select the endpoint type.

   Description

   (Optional) Defines the information you want to record for this endpoint (free text).

   Endpoint Type

   Specifies the type of endpoint where your privileged or service accounts reside.

   Note: When you select the endpoint type, you are asked to supply the credentials PUPM requires to manage privileged accounts on that endpoint. The endpoint type you select affects the connection information you have to supply.

   Managed Device

   (Optional) Specifies whether to associate the PUPM endpoint with a CA Access Control for Virtual Environments managed device
5. (Optional) Click the Login Applications tab and complete the field in the tab.

   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. (Optional) Click the Information tab and complete the fields in the tab.

   This tab lets you specify endpoint-specific attributes and use the attributes when you define or modify privileged access roles.

   When a member of the access-privileged role logs in to CA Access Control Enterprise Management, the user gains access to the privileged access accounts according to the attributes defined in the privileged access role.

   Owner

   Specify the name of the endpoint owner.

   Department

   Specify a name of a department.

   Example: Development

   Custom 1...5

   Specify up to five custom endpoint-specific attributes.

   Note: Specify the custom attributes in the privileged access role Members tab, Member Policy section, Member Rule window.

7. Click Submit.

   CA Access Control Enterprise Management tries to connect to the endpoint using the credentials you provide. If the connection succeeds, the endpoint is created. Otherwise, you receive a connection error.

Related Topics:

Access Control for PUPM Connection Information (see page 88)
VMware ESX/ESXi Connection Information (see page 89)
Windows Agentless Connection Information (see page 93)
CA Identity Manager Provisioning Connection Information (see page 108)
Disconnected Endpoint Connection Information (see page 111)

Access Control for PUPM Connection Information

The Access Control for PUPM endpoint type lets you manage privileged Access Control accounts.

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

User Login

Defines the name of an administrative user of the endpoint. PUPM 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.

Host Domain

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

Example: Domain.com

Use Enhanced Functionality

Specifies to use CA Access Control on the endpoint to manage privileged and services accounts.

Note: Supported on CA Access Control r12.6.01 and above only.

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.

Disable Exclusive Sessions

Specifies whether to disable the exclusive sessions check on this endpoint. When selected, PUPM does not check for open sessions on the endpoint.

Deny Exclusive Break-Glass

Specifies to block break-glass check-out action on exclusive accounts.

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.

MS SQL Server Connection Information

The MS SQL Server endpoint type lets you manage privileged Microsoft SQL Server accounts.

The administrative user that you specify for an MS SQL Server endpoint must:

- Have the securityadmin server role

Note: A user with the securityadmin server role cannot modify serveradmin and sysadmin server roles.

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

User Login

Defines the name of an administrative user of the endpoint. PUPM 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.

URL

Defines the URL that CA Access Control Enterprise Management can use to connect to the endpoint. The URL specifies a particular type of database server.

Format: jdbc:sqlserver://*servername*:*port*

Example: jdbc:sqlserver://localhost:1433

Note: For more information on the format of the URL, see your endpoint documentation.

Host

Defines the host name of the endpoint.

Note: If CA Access Control is installed on the endpoint, we recommend that you specify the CA Access Control host name for this attribute. You can use World View to view the CA Access Control host name of the endpoint.

Port

(Optional) Specifies the server listening port number. The port number that you specify must match the port number that you specify in the URL.

Example: 1433

Instance Name

(Optional) Specifies the database instance name.

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.

Oracle Server Connection Information

The Oracle Server endpoint type lets you manage privileged Oracle database accounts.

The administrative user that you specify for an Oracle Server endpoint must have the ALTER USER and SELECT ANY DIRECTORY system privileges.

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

User Login

Defines the name of an administrative user of the endpoint. PUPM 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.

URL

Defines the URL that CA Access Control Enterprise Management can use to connect to the endpoint. The URL specifies a particular type of database server.

Format: jdbc:oracle:*drivertype*:@*hostname*:*port:service*

Example: jdbc:oracle:thin:@ora.comp.com:1521:orcl

Note: For more information on the format of the URL, see your endpoint documentation.

Host

Defines the host name of the endpoint. This is the fully-qualified host name.

Note: If CA Access Control is installed on the endpoint, we recommend that you specify the CA Access Control host name for this attribute. You can use World View to view the CA Access Control 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.

Sybase Server Connection Information

The Sybase Server endpoint type lets you manage privileged Sybase Server accounts.

Important! Verify that the database is properly configured and that port 2638 is open for connections.

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

User Login

Defines the name of an administrative user of the endpoint. PUPM 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.

URL

Defines the URL that CA Access Control Enterprise Management can use to connect to the endpoint. The URL specifies a particular type of database server.

Format: jdbc:sybase:Tds:*servername*:*port*

Example*:* jdbc:sybase:Tds:localhost:2638

Note: For more information on the format of the URL, see your endpoint documentation.

Host

Defines the host name of the endpoint.

Note: If CA Access Control is installed on the endpoint, we recommend that you specify the CA Access Control host name for this attribute. You can use World View to view the CA Access Control 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.

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, PUPM 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 so that CA Access Control Enterprise Management can connect to the endpoint:

User Login

Defines the name of an administrative user of the endpoint. PUPM 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.

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 specify 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.

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.

Disable Exclusive Sessions

Specifies whether to disable the exclusive sessions check on this endpoint. When selected, PUPM does not check for open sessions on the endpoint.

Configure Windows Agentless Endpoints for PUPM

The following topics describe additional configuration steps that you may need to perform on your Windows Agentless endpoints before you can implement PUPM.

More information:

Restrictions on Domain Users on Windows Agentless Endpoints (see page 63)

Firewall Configuration on Windows Agentless Endpoints

Valid on Windows Server 2008 and Windows 7 Enterprise

The PUPM Windows Agentless connector uses port 135 (the DCOM port) to connect to Windows Agentless endpoints. The PUPM Windows Agentless connector is part of the JCS. After the connector connects to the endpoint, it uses a dynamic port (above 1000) for communication with the WMI (Windows Management Instrumentation) service.

If the Windows firewall is enabled on a Windows Agentless endpoint, the firewall can block both the connection to port 135 and the dynamic port. If the Windows firewall blocks these connections, the Enterprise Management Server cannot communicate with the endpoint. Therefore, you cannot create Windows Agentless endpoints or discover service accounts and scheduled tasks on the endpoint.

If the Windows firewall is enabled, configure the firewall so that the PUPM Windows Agentless connector can connect to the endpoint. When you configure the firewall, open port 135 and specify that the firewall permits any traffic arriving to the WMI service from dynamic RPC ports.

More information:

How to Configure a Windows Firewall for PUPM (see page 95)

How to Configure a Windows Firewall for PUPM

Valid on Windows Agentless endpoints

The PUPM Windows Agentless connector uses port 135 (the DCOM port) to connect to Windows Agentless endpoints. After the connector connects to the endpoint, it uses a dynamic port (above 1000) for communication with the WMI (Windows Management Instrumentation) service.

If the Windows firewall is enabled, you must configure the firewall so that the PUPM Windows Agentless connector can connect to the endpoint. If you do not configure the firewall, the Enterprise Management Server cannot communicate with the endpoint.

To configure a Windows firewall for PUPM, do as follows:

1. Open port 135.
2. Create a firewall rule so that the firewall permits any traffic arriving to the WMI service from dynamic RPC ports.

   Use the information in the following examples to help you configure the Windows firewall.

Example: Open Port 135

The following example shows you how to open port 135 on a Windows Server 2008 computer.

1. Click Start, Control Panel, Windows Firewall.

   The Windows Firewall dialog appears.
2. Click Change Settings.

   The Windows Firewall Settings dialog appears.
3. Click the Exceptions tab, and click Add port.

   The Add a Port dialog appears.
4. Complete the dialog, as follows:
   - In the Name field, type **DCOM_TCP135**
   - In the Port number field, type **135**
   - In the Protocol section, select TCP

   Click OK.

   The DCOM_TCP135 rule appears in the Exceptions tab.
5. Click OK.

   The Windows Firewall Settings dialog closes. You have opened port 135.

Example: Create a Firewall Rule That Permits Traffic Arriving to the WMI Service from Dynamic RPC Ports

The following example shows you how to create a firewall rule on a Windows Server 2008 computer. The firewall rule permits traffic arriving to the WMI service from dynamic RPC ports.

1. Click Start, Administrative Tools, Windows Firewall with Advanced Security.

   The Windows Firewall with Advanced Security dialog opens.

2. Right-click Inbound Rules in the left pane and click New Rule.

   The New Inbound Rule Wizard appears.

3. Complete the New Inbound Rule Wizard. Accept the default settings on all pages *except* the following:

   a. On the Rule Type page, select Custom.

   b. On the Program page, do as follows:

      - Select All programs.
      - Click Customize.

        The Customize Service Settings dialog opens.

      - Select Apply to this Service, select Windows Management Instrumentation, and click OK.

   c. On the Scope page, do as follows in the Which remote IP addresses does this rule match section:

      - Select These IP addresses and click Add.

        The IP Address dialog appears.

      - Enter the IP address of the Distribution Server in the This IP address or subnet, and click OK.

   d. On the Name page, type a name for the new rule in the Name field.

   After complete the wizard, you have created a firewall rule so that the firewall permits any traffic arriving to the WMI service from dynamic RPC ports.

More information:

Firewall Configuration on Windows Agentless Endpoints (see page 94)

Configure a Windows Server 2008 R2 x64 Endpoint for PUPM

Valid on Windows Server 2008

To use PUPM on a Windows Server 2008 R2 x64 endpoint, perform additional configuration steps on the endpoint.

Follow these steps:

1. Open the Windows registry.
2. Navigate to the following registry keys and do steps 3-6 for each key:

   `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

   `HKEY_CLASSES_ROOT\CLSID\{233664b0-0367-11cf-abc4-02608c9e7553}`

   Note: You can use the Find option in the Edit menu to search for these registry keys.
3. Right-click each key and select Permissions.

   The Permissions dialog appears.
4. Click Advanced.

   The Advanced Security Settings dialog appears.
5. Click the Owner tab, click Administrators in the Change Owner to: field, click Apply, and click OK.

   The Advanced Security Settings dialog closes.
6. Select Administrators in the Group or User Names window of the Permissions dialog, and select the Full Control checkbox in the Allow column of the Permissions for Administrators window.
7. Click OK.
8. Click Start, Administrative Tools, Local Security Policy.

   The Local Security Policy management console opens.
9. Select Local Policies, Security Options.

   A list of available security options appears.
10. Locate the following security policies:
    - Network Security: minimum session security for NTLM SSP based (including secure RPC) clients
    - Network Security: minimum session security for NTLM SSP based (including secure RPC) clients

11. Right click each policy and select Properties.

    The local security settings tab opens.

12. Verify that the Require 128 bit encryption option is not selected.

13. Click OK and exit.

    You have configured the Windows Server 2008 R2 x64 endpoint for PUPM. You may also need to configure the firewall and add permission to the DCOM.

Modify Windows Server 2008 Endpoints to Use a Login Application

Valid on Windows Server 2008

On Windows Server 2008 computers, Microsoft changed the default value of the Automatic prompting for ActiveX controls option. On Windows Server 2008 computers, the default value of this option is Disabled. On previous versions of Windows, the default value of this option is Enabled. This option affects the security settings for the local intranet and trusted site zones.

To modify Windows Server 2008 endpoints to use a login application, change the value of the Automatic prompting for ActiveX controls option to Enabled for the local intranet and trusted sites zones.

Note: If you do not change the value of this option, you cannot use automatic login on Windows Server 2008 computers.

Configure a Windows 7 Enterprise Endpoint for PUPM

Valid on Windows 7 Enterprise

If you want to use PUPM on a Windows 7 endpoint, you perform additional configuration steps on the endpoint.

Follow these steps:

1. Open the Windows registry.

2. Navigate to the following registry keys and do steps 3-6 for each key:

   `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

   `HKEY_CLASSES_ROOT\CLSID\{233664b0-0367-11cf-abc4-02608c9e7553}`

   Note: You can use the Find option in the Edit menu to search for these registry keys.

3. Right-click the key and select Permissions.

   The Permissions dialog appears.

4. Click Advanced.

   The Advanced Security Settings dialog appears.

5. Click the Owner tab, click Administrators in the Change Owner to: field, click Apply, and click OK.

   The Advanced Security Settings dialog closes.

6. Select Administrators in the Group or User Names window of the Permissions dialog, and select the Full Control checkbox in the Allow column of the Permissions for Administrators window.

7. Click OK and close the Windows registry

8. Open the Windows Control Panel, Administrative Tools, Services.

   The Windows Services console opens.

9. Right-click the Remote Registry service and select Properties.

   The Properties dialog opens.

10. Change the Startup type to Automatic and select Start.

    The Remote Registry service starts.

11. Run the DCOMCNFG command from the Run command line window.

    The Components Services window opens.

12. Select Console Root, Component Services, Computers.

13. Right-click My Computer and Select Properties.

    The Properties dialog opens.

14. Click the COM Security tab and under the Access Permissions section, click Edit Default.

    The Default Security dialog opens.

15. Select Administrators in the Group or User Names window and select the Local Access and Remote Access Allow checkboxes.

16. Click OK and repeat steps 14 and 15 in the Launch and Activation Permissions section.

17. Click OK and close the Component Services console.

    You have configured the Windows 7 Enterprise endpoint for PUPM. You might also need to configure the firewall

Challenge and Response Authentication Protocol Restrictions

Valid on Windows Agentless endpoints

Challenge/response authentication protocols for network login affect the level of authentication protocol and the session security that endpoints use for client/server communication. There are three types of Windows challenge/response authentication protocols for network login:

- LM—LAN Manager challenge/response
- NTLM—Windows NT challenge/response
- NTLMv2—A second version of NTLM

The LAN Manager authentication level setting controls the challenge/response authentication protocol that the endpoint uses. The default value for this setting is Send LM & NTML responses. The Enterprise Management Server can communicate with Windows endpoints only when the value of the LAN Manager authentication level setting is Send LM & NTML responses. For example, the Enterprise Management Server cannot communicate with a Windows endpoint when the value of this setting is Send NTLMv2 response only\refuse LM & NTLM.

You can create a Windows Agentless endpoint only if the LAN Manager authentication level setting on the endpoint is Send LM & NTML responses. If you cannot create a Windows Agentless endpoint, you may need to change the challenge and response authentication protocol on the endpoint.

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 Login

Defines the name of an administrative user of the endpoint. PUPM 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. 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.

Use Telnet

Specifies to use Telnet rather than SSH to connect to the SSH device.

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.

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.

How PUPM Connects to UNIX Endpoints

When you create an endpoint, you specify the administrator account that PUPM uses to connect to the endpoint and perform administrative tasks, such as discovering and changing the password of privileged accounts. For UNIX accounts, the most suitable administrator account is often root. However, PUPM uses SSH to connect to UNIX endpoints, and some organizations prohibit users and applications from making SSH connections as the root user.

To overcome this problem, you can specify both a connection account and an operation administrator account when you create an SSH Device endpoint. (PUPM uses SSH Device as the endpoint type for UNIX endpoints.) Using two accounts also lets you use a connection account that has fewer privileges than the operation administrator account.

The following process explains how PUPM uses these accounts to connect to an SSH Device endpoint:

1. PUPM uses the credentials of the connection account to connect to the endpoint.
2. PUPM uses the credentials of the operation administrator account to su to that account.

   For example, if the operation administrator account is root, PUPM uses the root credentials to su to root.
3. PUPM performs administrative tasks as the operation administrator.

   For example, if the operation administrator account is root, PUPM performs administrative tasks as root.

When you view the privileged accounts on an SSH Device endpoint, both the connection and the operator administrator account are listed as endpoint administrator accounts.

How to Create a Customized SSH Device Endpoint

If the default settings that PUPM uses to discover privileged accounts do not apply to an SSH Device endpoint, you can create a customized SSH Device endpoint.

To create a customized SSH Device endpoint, do the following:

1. Customize the SSH Device XML file.
2. Create an SSH Device endpoint in CA Access Control Enterprise Management (see page 85). In the Configuration File field, enter the name of the XML file that you created.

   The SSH Device endpoint is created using the custom settings.
3. Run the privileged accounts discovery wizard (see page 78)on the endpoint you created.

   CA Access Control Enterprise Management searches the endpoint for privileged accounts using the parameters you defined in the XML file.
4. Review the JCS connector log file (jcs_stdout.log) and JCS connector error file (jcs_sterr.log). The files are located under:

   ACServerInstallDir`/Connector Server/logs`
5. If needed, modify the XML file to resolve the errors that appear in the log files.

Types of SSH Device XML Configuration File

CA Access Control provides the following SSH Device XML configuration files. You customize these files to suit your enterprise requirements:

- **aix_connector_conf.xml**—Defines configuration settings for an SSH device that is an AIX endpoint.
- **checkpoint_connector_conf.xml**—Defines configuration settings for an SSH device that uses a Check Point firewall.
- **Cisco-UCS_connector_conf.xml**—Defines configuration settings for an SSH device that is a Cisco UCS endpoint.
- **device_connector_conf.xml**—Defines configuration settings for a device, for example, a router.
- **nis_connector_conf.xml**—Defines configuration settings for an SSH device that works with a NIS server.

  Note: Use the local root account as the connected user. Do the following:

  a. Create a NIS endpoint (nis_endpoint_1) and define the root account using the default XML file. (ssh_connector_conf.xml)

  b. Create another NIS endpoint (nis_endpoint_2) and use the Advanced option to define the root account of the first NIS endpoint.

- **netdevice_connector_conf.xml—**Defines configuration settings for a network device that is a Cisco 2600 network device.
- **ssh_connector_conf.xml**—Use this file when you configure an SSH device that uses the passwd command to change account passwords.

  Note: Specify a local user, for example, root, as the connected user.
- **sudo_connector_conf.xml**—Use this file when you configure an SSH device that uses the sudo and passwd commands.

Customize an SSH Device XML File

The SSH Device XML file defines how PUPM connects to an SSH Device endpoint, discovers user accounts, and changes privileged account passwords on the endpoint.CA Access Control provides several different SSH Device XML files. These files contain the default settings that PUPM uses to connect to the various types of SSH Device endpoints.

If an SSH Device endpoint uses an alternate t method to change privileged account passwords on the endpoint, customize the SSH Device XML file to specify the nondefault settings. For example, customize the SSH Device XML file to create an endpoint for a router, switch, or firewall that uses a nonstandard method to discover user accounts and change privileged account passwords.

Follow these steps:

1. On CA Access Control Enterprise Management, locate the XML file that you want to customize. The files are located in the following directory:

   ACServerInstallDir/Connector Server/conf/override/sshdyn
2. Duplicate the file that you want to customize and open the new file for editing.

   Note: Save the new file in the same directory.
3. Modify the parameters in the file to suit your enterprise requirements.

   Each <item> element in the file defines the parameters for a specific command. PUPM uses these commands to get users and change passwords on the endpoint. You modify the <item> elements to define the commands that PUPM sends to the endpoint. You can also modify the settings that PUPM uses to connect to the endpoint.
4. Save and close the file.

   You have customized the SSH Device XML file for the endpoint.

Note: If you are customizing the file with Chinese, Japanese, or Korean characters, save the file using UTF-8 encoding.

Example: How an SSH Device XML File Defines PUPM Commands

This example explains how a section of the SSH Device XML file defines the commands that PUPM executes on an SSH Device endpoint. Each <item> element in the section defines the parameters for a specific action. Together, all the <item> elements create a script that defines how PUPM interacts with the endpoint.

Each <item> element begins with the sCommand parameter. The sCommand parameter defines a command that PUPM executes on the endpoint. The parameters after the sCommand parameter define any other actions that PUPM performs after that command.

This example shows you how a section of the Cisco-UCS_connector_conf.xml file defines the commands that PUPM uses to change privileged account passwords on a Cisco switch. The Cisco-UCS_connector_conf.xml file is located in the following directory:

ACServerInstallDir/Connector Server/conf/override/sshdyn

This example shows only a section of the Cisco-UCS_connector_conf.xml file. Additional elements in the file configure the connection to the Cisco switch and specify the commands that PUPM executes to get users.

Note: For more information about the format of the SSH Device XML file, see the *Reference Guide*.

The following process shows you the commands that PUPM executes to change privileged account passwords on a Cisco switch. To demonstrate how <item> elements configure the commands that PUPM executes, the corresponding <item> element is given at the end of each step.

1. PUPM specifies to change the password for the privileged account. PUPM performs the following actions to complete this step:
   a. PUPM issues the following command:

      ```
      set password
      ```

   b. PUPM waits 500 milliseconds.
   c. PUPM waits to receive the **word:** text string. When it receives this string, it proceeds to the next step.

   The following <item> element specifies the actions that PUPM takes in this step:

   ```
   <item>
   <param name="sCommand" value="set password" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="word:" />
   </item>
   ```

2. PUPM specifies the new password for the privileged account. PUPM performs the following actions to complete this step:

   a. PUPM sends the new password to the endpoint.

      PUPM does not write the new password to the log file.

   b. PUPM waits 500 milliseconds.

   c. PUPM waits to receive the **word:** text string. When it receives this string, it proceeds to the next step.

   The following <item> element specifies the parameters for this command:

```
<item>
<param name="sCommand" value="[%%password%%]" />
<param name="bHideSentLog" value="true" />
<param name="iWait" value="500" />
<param name="sWaitForText" value="word:" />
</item>
```

3. PUPM confirms the new password for the privileged account. PUPM performs the following actions to complete this step:

   a. PUPM resends the new password to the endpoint.

      PUPM does not write the new password to the log file.

   b. PUPM waits 500 milliseconds.

   c. PUPM waits to receive the **local-user* #** text string. When it receives this string, it proceeds to the next step.

      If PUPM receives a **failure**, **invalid**, or **error** text string, the password change failed.

   The following <item> element specifies the parameters for this command:

   ```
   <item>
   <param name="sCommand" value="[%%password%%]" />
   <param name="bHideSentLog" value="true" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="local-user* #" />
   <param name="sFailureResult" value="failure;invalid;error" />
   </item>
   ```

4. PUPM commits the new password for the privileged account. PUPM performs the following actions to complete this step:

   a. PUPM issues the following command:

      ```
      commit-buffer
      ```

      PUPM does not write this command to the log file.

   b. PUPM waits 500 milliseconds.

   c. PUPM waits to receive the **local-user #** text string. When it receives this string, the password change is complete.

      If PUPM receives the **Error: Update failed:** text string, the password change failed.

   The following <item> element specifies the parameters for this command:

   ```
   <item>
   <param name="sCommand" value="commit-buffer" />
   <param name="bHideSentLog" value="true" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="local-user #" />
   <param name="sFailureResult" value="Error: Update failed:" />
   </item>
   ```

   The password change is complete.

CA Identity Manager Provisioning Connection Information

The CA Identity Manager provisioning connectors let you manage the CA Identity Manager endpoints you defined in your Provisioning Server. Before you create CA Identity Manager endpoints in PUPM, you must create an Identity Manager Provisioning type Connector Server.

Note: For more information about how to create a Connector Server, see the Online Help.

Note:When you configure an CA Identity Manager provisioning connector server, specify the full distinguished name of the etaadmin.

For example:

```
eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global
Users,eTNamespaceName=CommonObjects,dc=ProvisioningDomainName,dc=eta
```

CA Identity Manager can enforce a password policy that is different from the one that is configured on the target system. If you enforce a password policy on the target system, PUPM changes the user password. However, the user cannot use the password on the endpoint. Verify that the password policy on the target system complies with the PUPM password policy. For more information about the CA Identity Manager password policy enforce option, see the *CA Identity Manager Administration Guide*.

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

Endpoint

Defines the name of the endpoint exactly as you defined it in CA Identity Manager Provisioning Server.

CA Access Control Enterprise Management displays the CA Identity Manager endpoint types only after you configure the connection in the Provisioning Server.

Host

Defines the host name of the endpoint. This is the logical name you want to assign to this endpoint. CA Access Control Enterprise Management uses this name represent the endpoint in World View.

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.

More information:

Configure CA Identity Manager Provisioning Manager for PUPM (see page 109)

Configure CA Identity Manager Provisioning Manager for PUPM

Before you can use PUPM to manage CA Identity Manager r12.5 and r12.5 SP1 endpoints that you define in your Provisioning Server, you must configure CA Identity Manager Provisioning Manager for PUPM.

To configure CA Identity Manager Provisioning Manager for PUPM

1. Log in to CA Identity Manager Provisioning Manager.
2. Click the System tab.
3. Select the domain that you want to configure, and click Domain Configuration in the left pane.

   The domain configuration tree appears.
4. Expand the Passwords tree and select Enforce Synchronized Account Passwords.

   The Domain Configuration tab for the Enforce Synchronized Account Passwords parameter appears.
5. Click Edit, change the value to No, and click OK.
6. Click Apply.

   The value of the Enforce Synchronized Account Passwords parameter is changed.
7. Restart the CA Identity Manager - Provisioning Server and the CA Identity Manager - Connector Server (Java) services.

   CA Identity Manager Provisioning Manager is configured for PUPM.

Modify the CA Identity Manager Provisioning Connector Search Limitation

When you run the Privileged Accounts Discovery wizard, the CA Identity Manager Provisioning Connector returns up to 1000 results for each endpoint that you configured in the CA Identity Manager Connection Manager. You can modify the default search limit to display more results in each query.

To modify the CA Identity Manager provisioning connector search limitation

1. On the Enterprise Management Server, stop the Java Connector Server. Do the following:

   a. Navigate to the following directory, where *ACServerInstallDir* indicates the directory where the Enterprise Management Server is installed:

      ACServerInstallDir/Connector_Server/bin

   b. Run the following command:

      ```
      ./im_jcs stop
      ```

   The Java Connector Server stops.

2. Open the im_connector_conf.xml file for editing. The file is located in the following directory:

   ACServerInstallDir/Connector_Server/conf/override/imdyn

3. Locate the token "I_SEARCH_SIZE_LIMIT" and specify the search limit as the value. For example:

   ```
   <param name="I_SEARCH_SIZE_LIMIT" value="1500" />
   ```

4. Save and close the file.

5. Start the Java connector Server.

Important! Specifying a search limit value that is higher than the default can cause system performance to degrade.

Disconnected Endpoint Connection Information

The disconnected endpoint type lets you store passwords for privileged accounts that reside on disconnected endpoints.

PUPM does not log in to or manage accounts on disconnected endpoints. Instead, PUPM acts only as a password vault for privileged accounts on the endpoint. Every time you change the password for a privileged account on a disconnected endpoint in CA Access Control Enterprise Management, you must also manually change the account password on the managed endpoint.

You can create only disconnected accounts on disconnected endpoints. A disconnected account is an account that PUPM does not manage; for example, PUPM does not change the password of a disconnected account. In addition, you cannot use the Discover Privileged Accounts Wizard or the Discover Service Accounts Wizard to discover accounts on disconnected endpoints.

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

Host Name

Defines the host name of the endpoint.

Create a Login Application

A login application uses a script to execute an application on the endpoint that automatically logs you in to a privileged account after you check out the privileged account password. Login applications let you configure PUPM automatic login.

You can create the following types of login applications. Each type of login application is a Visual Basic script:

- ORACLE_10G_WEB.vbs—Lets you automatically log in to the Enterprise Manager web interface of an Oracle 10g database.
- ORACLE_10XE_WEB.vbs—Lets you automatically log in to the Database Home Page web interface of an Oracle XE database.
- ORACLE_11G_WEB.vbs—Lets you automatically log in to the Enterprise Manager web interface of an Oracle 11g database.
- PUTTY.vbs—Lets you automatically log in to an SSH Device endpoint.

  Note: You must install PuTTY Release 0.60 and up on your computer to use a PuTTY login application.
- RDP.vbs—Lets you automatically log in to a Windows endpoint.

When you use automatic login to check out a privileged account password on a Windows Agentless endpoint, CA Access Control Enterprise Management propend the host domain to the name of the privileged account. Before you create a login application for a Windows Agentless endpoint, verify the following:

- If the endpoint is part of a workgroup, verify that the computer name is specified in the Host Domain field.
- If the endpoint is part of a domain, verify that the domain name is specified in the Host Domain field.

  Note: You can use the Modify Endpoint task to modify the Host Domain field.

Note the following:

- You must have the System Manager role to create a login application.
- You can use login applications only in Microsoft Internet Explorer browsers.

Follow these steps:

1. In CA Access Control Enterprise Management, click Privileged Accounts, Login Application, Create Login Application task.

   The Create Login Application: Login Application Search screen appears.

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

   a. Select Create a copy of an object of type Login Application.

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

      A list of login application that match the filter criteria appears.

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

3. Click OK.

   The Create Login Application task page appears. If you created the login application from an existing object, the dialog fields are pre-populated with the values from the existing object.

4. Complete the following fields:

   Name

   Defines the name by which you want to refer to this login application.

   Description

   (Optional) Defines the information you want to record for this login application (free text).

Script

Defines the Visual Basic script to use to launch the login application.

Note: We recommend that you do not customize these supplied scripts.

Enable

Specifies that this login application is enabled.

Click Submit.

CA Access Control Enterprise Management creates the login application.

Note: Before a user can use a login application, you must modify your endpoints in CA Access Control Enterprise Management to use the login application. You need to perform additional configuration steps on the endpoints to use terminal integration, and to use login applications on Windows Server 2008 endpoints.

More information:

Modify Windows Server 2008 Endpoints to Use a Login Application (see page 98)

How to Import PUPM Endpoints and Privileged Accounts

You use the PUPM feeder to automate PUPM endpoint and privileged account management. The PUPM feeder lets you import many PUPM endpoints and privileged accounts into CA Access Control Enterprise Management in a single step. You can also use the PUPM feeder to create or modify PUPM endpoints and privileged accounts.

Note: You cannot use the PUPM feeder to delete PUPM endpoints and privileged accounts.

Important! To avoid errors during the process, import the endpoint CSV file into PUPM before you import the privileged accounts CSV file.

To import PUPM endpoints and privileged accounts into CA Access Control Enterprise Management, do the following:

1. Configure the feeder properties file.

   The feeder properties file specifies the polling interval and the name and location of the polling folder, processed file folder, and error file folder.

2. (Optional) Write CA Access Control rules that limit access to the polling folder, processed file folder, and error file folder.

   Limiting access to these folders helps prevent unauthorized users accessing clear-text passwords in the endpoint and privileged account CSV files.

3. Do one or both of the following:
   - Create an endpoint CSV file.
   - Create a privileged account CSV file.

   Each line in the CSV file represents a task to create or modify a PUPM endpoint or privileged account. You must create separate endpoint and privileged account CSV files.

   Note: You can configure an automated process in another application to create the CSV file.
4. (Optional) Start the polling task.

   When the polling task starts, the PUPM feeder uploads the CSV files in the polling folder to CA Access Control Enterprise Management, which then processes the CSV files.

   Note: If you do not manually start the polling task, the PUPM feeder checks for files in the polling folder at the time specified in the feeder properties file.
5. When CA Access Control Enterprise Management completes processing the CSV file, review the CSV file in the error files folder for failed tasks.

   This file lists tasks that failed and tasks that CA Access Control Enterprise Management could not process.
6. Correct the errors in the file and save the file to the polling folder.
7. Start the polling task.
8. Repeat Steps 5-7 until all PUPM endpoints and privileged accounts are imported.

How the PUPM Feeder Works

The PUPM feeder lets you create or modify many PUPM endpoints or privileged accounts in a single step. Understanding how the PUPM feeder works helps you configure PUPM in the most suitable way for your enterprise, and helps you troubleshoot any problems that may occur.

The following process explains how the PUPM feeder works:

1. You, or an automated process, create and save one or more CSV files in the polling folder.

   Each line in the CSV file represents a task to create or modify a PUPM endpoint or privileged account. You create separate CSV files for endpoints and for privileged accounts.

2. When the polling task starts, the PUPM feeder uploads the CSV files in the polling folder to CA Access Control Enterprise Management. You can configure the polling task to run at a specified time, or you can start the polling task manually.

   Note: If the PUPM feeder cannot rename a file, the file cannot be processed. The unprocessed CSV file remains in the polling folder.

3. CA Access Control Enterprise Management renames the CSV file *original_timestamp*.csv, and moves the file to the processed files folder.

   Note: *original* is the name of the original CSV file, and *timestamp* is a timestamp that indicates when the file was processed. For example, if you name the original CSV file endpoints.csv, CA Access Control Enterprise Management names the file in the processed file folder endpoints_091209130256.csv.

4. CA Access Control Enterprise Management processes each line in the CSV file in turn. For each line in the CSV file, the following happens:

   - If CA Access Control Enterprise Management can complete the task, it:
     - Completes the task, for example, creates an endpoint.
     - Creates an audit record for the task.
   - If CA Access Control Enterprise Management cannot complete the task, it:
     - Copies the line in the CSV file to a CSV file in the error files folder.
     - Adds a column named FAILURE_REASON to the CSV file in the error files folder.
     - Adds the reason why the task failed to the FAILURE_REASON column.
     - Creates an audit record for the task.

   The CSV file in the error files folder provides an easy way for you to review failed tasks. The name of this file is also *original_timestamp*.csv.

   Note: The CSV file in the processed files folder lists all processed tasks but it does not specify the status of the task. That is, if the task is completed or failed.

5. CA Access Control Enterprise Management repeats Step 4 for each line in the CSV file.

Configure the Feeder Properties File

The feeder properties file specifies the polling interval and the name and location of the polling folder, processed file folder, and error file folder. JBoss reads the feeder properties file each time it starts.

To configure the feeder properties file

1. Stop JBoss Application Server if it is running.
2. Open the feeder properties file in a text-based editor. The file is located at the following location, where *JBoss_home* is the location in which you installed JBoss:

   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/default/feeder.properties

3. Enable *one* of the following parameters:

   FOLDER_POLLING_INTERVAL_IN_MINUTES

   Defines the interval, in minutes, at which the PUPM feeder polls the polling folder. This parameter is enabled by default.

   Limits: 1-60

   Default: 60

   FOLDER_POLLING_CRON_EXPR

   Defines the times at which the PUPM feeder polls the polling folder. Specify this parameter as a cron expression.

   Important! If you use this parameter, remove the comment mark (#) from the FOLDER_POLLING_CRON_EXPR line and disable the FOLDER_POLLING_INTERVAL_IN_MINUTES parameter by adding a comment mark at the start of the line.

   Example: FOLDER_POLLING_CRON_EXPR=0 0 23 ? * MON-FRI

   This example specifies that the PUPM feeder polls the polling folder at 11 pm Monday through Friday.

   The polling interval is configured.

4. (Optional) Edit the following parameters:

   FOLDER_FOR_POLLING

   Defines the polling folder—the folder that the PUPM feeder polls for CSV files.

   Default: *JBoss_home*/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

   Note: This folder must be located on the Enterprise Management Server computer. You must specify the absolute file path to this folder.

FOLDER_FOR_PROCESSED_FILES

Defines the processed files folder—the folder that the PUPM feeder moves CSV files to after it processes them.

Default:
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/processed

Note: This folder must be located on the Enterprise Management Server computer. You must specify the absolute file path to this folder.

FOLDER_FOR_ERROR_FILES

Defines the error files folder—the folder to which the PUPM feeder moves CSV files that it cannot process.

Default:
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/failedToSubmit

Note: This folder must be located on the Enterprise Management Server computer. You must specify the absolute file path to this folder.

The names of the polling folders are configured.

5. Save and close the file.

   The feeder properties file is configured.

6. Restart JBoss Application Server.

Example: Feeder Properties File

The following example configures the PUPM feeder to poll the polling folder every 30 minutes, and defines the location of the polling folder, processed files folder, and the error files folder:

```
# feeder folder polling job configuration
# folder specified as FOLDER_FOR_POLLING will be checked every
FOLDER_POLLING_INTERVAL_IN_MINUTES minutes e.g. 60 equals every 1
hour (max value is every hour)
FOLDER_POLLING_INTERVAL_IN_MINUTES=30
# if cron expression is supplied remark the
FOLDER_POLLING_INTERVAL_IN_MINUTES key
# FOLDER_POLLING_CRON_EXPR=
FOLDER_FOR_POLLING=C:\feeder\waitingToBeProcessed
FOLDER_FOR_PROCESSED_FILES=C:\feeder\processed
FOLDER_FOR_ERROR_FILES=C:\feeder\failedToSubmit
```

Create an Endpoint CSV File

Each row or line in the endpoint CSV file, after the header row or line, represents a task to create or modify an endpoint in CA Access Control Enterprise Management.

Important! When you create the CSV file, verify that no other application uses the file and that the file can be renamed. The PUPM feeder processes only CSV files that can be renamed.

Follow these steps:

1. Create a CSV file and give it an appropriate name.

   Note: We recommend that you create a copy of a sample endpoint CSV file. The sample files are located in the following directory, where *ACServer* is the directory in which you installed the Enterprise Management Server:

   ACServer/IAM Suite/Access Control/tools/samples/feeder

2. Create a header row or line that specifies the names of the endpoint attributes.

   The names of the endpoint attributes are as follows. Some endpoint attributes are valid only for certain endpoint types:

   OBJECT_TYPE

   Specifies the type of the object to import.

   Value: ENDPOINT

   ACTION_TYPE

   Specifies the type of action to perform

   Value: CREATE, MODIFY, DELETE

   %FRIENDLY_NAME%

   Defines the name that you refer to this endpoint by in CA Access Control Enterprise Management.

   DESCRIPTION

   Defines any information that you want to record for this endpoint.

   ENDPOINT_TYPE

   Specifies the type of the endpoint.

   Note: You can view the available endpoint types in CA Access Control Enterprise Management. Before you create endpoints of type CA Identity Manager Provisioning, create an Identity Manager Provisioning type Connector Server in CA Access Control Enterprise Management.

   HOST

   Defines the host name of the endpoint.

LOGIN_USER

Defines the name of an administrative user of the endpoint. This attribute is *not* valid for any of the CA Identity Manager Provisioning endpoint types, but is valid for all other endpoint types.

For all valid endpoint types except SSH Device:

- If you do not specify a privileged administrative account (IS_ADVANCE attribute), PUPM uses LOGIN_USER to connect to the endpoint and to perform administrative tasks on the endpoint, for example, to discover accounts and change passwords.
- If you specify a privileged administrative account, PUPM ignores any values for LOGIN_USER.

For SSH Device endpoints:

- If you do not specify an operation administrator (OPERATION_ADMIN_USER_NAME) or a privileged administrative account, PUPM uses LOGIN_USER to connect to the endpoint and to perform administrative tasks on the endpoint.
- If you specify an operation administrator, PUPM uses LOGIN_USER to connect to the endpoint and the operation administrator to perform administrative tasks on the endpoint.
- If you specify a privileged administrative account, PUPM ignores any values for LOGIN_USER.

PASSWORD

Defines the password of LOGIN_USER. This attribute is *not* valid for the CA Identity Manager Provisioning endpoint type, but is valid for all other endpoint types.

URL

Defines the URL that CA Access Control Enterprise Management uses to connect to the endpoint. This attribute is valid for the MS SQL Server and Oracle Server endpoint types.

Format: (MS SQL Server) jdbc:sqlserver://*servername*:*port*

Format: (Oracle Server) jdbc:oracle:*drivertype*:@*hostname*:*port*:*service*

DOMAIN

Specifies the name of the domain of which this endpoint is a member. This attribute is valid for the Access Control for PUPM and Windows Agentless endpoint types.

IS_ACTIVE_DIRECTORY

Specifies whether the user account is an Active Directory account. This attribute is valid for the Windows Agentless endpoint type only.

Limits: TRUE, FALSE

USER_DOMAIN

Specifies the name of the domain of which the LOGIN_USER is a member. This attribute is valid for the Windows Agentless endpoint type.

CONFIGURATION_FILE

Specifies the name of the SSH Device XML configuration file that you are defining. This attribute is valid for the SSH Device endpoint type.

Note: If you do not specify a value for this attribute, CA Access Control Enterprise Management uses the default configuration file (ssh_connector_conf.xml).

OPERATION_ADMIN_USER_NAME

(Optional) Defines the name of the 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. This attribute is valid for the SSH Device endpoint type, as follows:

- If you specify a privileged administrative account (IS_ADVANCE attribute) and an operation administrator, PUPM uses the privileged administrative account to connect to the endpoint and the operation administrator to perform administrative tasks on the endpoint.
- If you specify LOGIN_USER and an operation administrator account, PUPM uses LOGIN_USER to connect to the endpoint and the operation administrator to perform administrative tasks on the endpoint.

If you specify an operation administrator for an SSH endpoint that uses a Check Point firewall, you must 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_ADMIN_USER_PASSWORD

(Optional) Defines the password for the operation administrator user of the endpoint. This attribute is valid for the SSH Device endpoint type.

ENDPOINT

Defines the name of the endpoint, exactly as it is defined in CA Identity Manager Provisioning Server. This attribute is valid for the CA Identity Manager Provisioning endpoint type.

IS_ADVANCE

(Optional) Specifies whether you want to use a privileged administrative account to connect to the endpoint and to perform administrative tasks on the endpoint, for example, to discover accounts and change passwords. This attribute is valid for all endpoint types.

For all valid endpoint types except SSH Device, if you specify a privileged administrative account (IS_ADVANCE is TRUE), PUPM uses the privileged administrative account to connect to the endpoint and to perform administrative tasks on the endpoint.

For SSH Device endpoints:

- If you specify a privileged administrative account and an operation administrator (OPERATION_ADMIN_USER_NAME), PUPM uses the privileged administrative account to connect to the endpoint and the operation administrator to perform administrative tasks on the endpoint.
- If you specify only a privileged administrator account, PUPM uses the privileged administrative account to connect to the endpoint and to perform administrative tasks on the endpoint.

Limits: TRUE, FALSE

Note: If you set the value of this attribute to TRUE, do not specify a value for LOGIN_USER. However, you must specify PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE, PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME, PROPERTY_ADMIN_ACCOUNT_CONTAINER, and PROPERTY_ADMIN_ACCOUNT_NAME.

PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE

(Optional) Defines the type of endpoint on which the privileged administrative account is defined.

Note: To use a privileged administrative account, you must specify that IS_ADVANCE is TRUE.

PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME

(Optional) Defines the name of the endpoint on which the privileged administrative account is defined. The endpoint must exist in CA Access Control Enterprise Management.

Note: To use a privileged administrative account, you must specify that IS_ADVANCE is TRUE.

PROPERTY_ADMIN_ACCOUNT_CONTAINER

(Optional) Defines the container in which the privileged administrative account is defined. A container is a class whose instances are collections of other objects.

Values: (Windows Agentless and Oracle Server): Accounts

(SSH Device): SSH Accounts

(MS SQL Server): MS SQL Logins

Note: To use a privileged administrative account, you must specify that IS_ADVANCE is TRUE.

PROPERTY_ADMIN_ACCOUNT_NAME

(Optional) Defines the name of the privileged administrative account that PUPM uses to perform administrative tasks on the endpoint, for example, to discover accounts and change passwords. The privileged account must exist in CA Access Control Enterprise Management.

Note: To use a privileged administrative account, you must specify that IS_ADVANCE is TRUE.

LOGIN_APPLICATION

Specify the name of the login application to associate with the endpoint

OWNER_INFO

Specifies the name of the endpoint owner.

DEPARTMENT_INFO

Specifies the name of the department.

CUSTOM1....5_INFO

Specifies up to five customer-specific attributes.

3. Add endpoint task lines to the CSV file.

   Each line represents a task to create or modify an endpoint, and must have the same attributes as the header. The attributes must be in the same order as the header. If a line does not have a value for an attribute, leave the field empty.

4. Save the file to the polling folder.

   The endpoint CSV file is ready to be processed by the PUPM feeder.

   Note: The default polling folder is located as follows, where *JBoss_home* is the directory in which you installed JBoss:

   `JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed`

Example: An Endpoint CSV File

The following is a sample endpoint CSV file. You can find more sample endpoint CSV files in the *ACServer*/IAM Suite/Access Control/tools/samples/feeder directory.

```
OBJECT_TYPE,%FRIENDLY_NAME%,DESCRIPTION,ENDPOINT_TYPE,HOST,LOGIN_USER,
PASSWORD,URL,CONFIGURATION_FILE,DOMAIN,IS_ACTIVE_DIRECTORY,USER_DOMAIN,ENDPOINT

ENDPOINT,Oracle1,oracle 10g,Oracle Server,TEST10,
ORAADMIN1,ORAADMIN1,jdbc:oracle:thin:@TEST10:1521:RNDSRV,,,,,

ENDPOINT,local MSSQL1,local SQL server,MS SQL Server,
localhost,testAdmin,Password1@,jdbc:sqlserver://localhost:1433,,,,,

ENDPOINT,SSH_Device2,unix machine,SSH Device,TEST84,root,Password1@,,,,,,

ENDPOINT,IM_Access Control,Access Control via provisioning,Access
Control,TEST1,,,,,,,,TEST1
```

More information:

Types of SSH Device XML Configuration File (see page 103)

Create a Privileged Account CSV File

Each row or line in the privileged account CSV file, after the header row or line, represents a task to create or modify a privileged account in CA Access Control Enterprise Management.

Important! When you create the CSV file, verify that no other application uses the file and that the file can be renamed. The PUPM feeder processes only CSV files that can be renamed.

Follow these steps:

1. Create a CSV file and give it an appropriate name.

   Note: We recommend that you create a copy of the sample privileged account CSV file. The sample file is located as follows, where *ACServer* is the directory in which you installed the Enterprise Management Server:

   ACServer/IAMSuite/AccessControl/tools/samples/feeder

2. Create a header row or line that specifies the names of the privileged account attributes.

   The names of the privileged account attributes are as follows:

   OBJECT_TYPE

   Specifies the type of the object to import.

   Values: ACCOUNT_PASSWORD

   ACTION_TYPE

   Specifies the type of action to perform

   Value: CREATE, MODIFY, DELETE

   ACCOUNT_NAME

   Defines the name by which you want to refer to the privileged account on CA Access Control Enterprise Management.

   Note: Mainframe systems, for example, RACF, ACF, and Top Secret, and SSH Device endpoint types use case-sensitive user names. Enter the account name in the correct case for these endpoint types. Enter the account name in capital letters for privileged accounts on mainframe systems and on Oracle Server endpoints.

   ENDPOINT_NAME

   Specifies the name of the endpoint on which the privileged account resides. You must define the endpoint in CA Access Control Enterprise Management before you can create any privileged accounts for the endpoint.

   NAMESPACE

   Specifies the endpoint type of the endpoint.

   Note: You can view the available endpoint types in CA Access Control Enterprise Management. Before you create endpoints of type CA Identity Manager Provisioning, you must create an Identity Manager Provisioning type Connector Server in CA Access Control Enterprise Management.

   CONTAINER

   Specifies the name of the container for the privileged account. A container is a class whose instances are collections of other objects. Containers are used to store objects in an organized way following specific access rules.

   Values: (Windows Agentless and Oracle Server endpoints): Accounts

   (SSH Device endpoints): SSH Accounts

   (MS SQL Server endpoints): MS SQL Logins.

DISCONNECTED_SYSTEM

Specifies if the privileged account originates from a disconnected system.

If you specify TRUE, 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 in PUPM, also manually change the account password on the managed endpoint.

Values: TRUE, FALSE

EXCLUSIVE_ACCOUNT

Specifies if only a single user can check out the account at any one time.

If you specify TRUE, PUPM lets only a single user check out the account at any one time.

Values: TRUE, FALSE

NEW_PASSWORD

Defines the password for the privileged account. If you do not specify a value for this attribute, CA Access Control Enterprise Management generates a password that complies with the specified password policy.

Note: The password must comply with the password policy.

PASSWORD_POLICY

Specifies the password policy for the privileged account.

Note: If you specify a password policy that does not exist, the task fails and CA Access Control Enterprise Management does not create the privileged account.

OWNER_INFO

Specifies the name of the account owner.

DEPARTMENT_INFO

Specifies the name of the department.

CUSTOM1....5_INFO

Specifies up to five customer-specific attributes.

3. Add task lines to the CSV file.

   Each line represents a task to create or modify a privileged account, and must have the same number of attribute values as the header. If a line does not have a value for an attribute, leave the field empty.

4. Save the file to the polling folder.

   The privileged account CSV file is ready to be imported by the PUPM feeder.

   Note: The default polling folder is located as follows, where *JBoss_home* is the directory in which you installed JBoss:

   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

Example: A Privileged Account CSV File

The following is a sample privileged account CSV file. You can find more sample privileged account CSV files in the *ACServer*/IAMSuite/AccessControl/tools/samples/Feeder directory.

```
OBJECT_TYPE,ACCOUNT_NAME,ENDPOINT_NAME,NAMESPACE,CONTAINER,
DISCONNECTED_SYSTEM,EXCLUSIVE_ACCOUNT,NEW_PASSWORD,PASSWORD_POLICY

ACCOUNT_PASSWORD,demo1,local windows 2003,Windows Agentless,
Accounts,FALSE,FALSE,Password1@,default password policy

ACCOUNT_PASSWORD,demo2,local windows 2003,Windows Agentless,
Accounts,FALSE,FALSE,,default password policy

ACCOUNT_PASSWORD,disconnected1,local windows 2003,Windows Agentless,
Accounts,TRUE,FALSE,Password1@,default password policy
```

Manually Start the Polling Task

When the polling task starts, the PUPM feeder uploads the CSV files in the polling folder. CA Access Control Enterprise Management then processes each line in the CSV files.

Note: If you do not manually start the polling task, the PUPM feeder checks the polling folder at the time specified in the feeder properties file. You must have the System Manager or PUPM Target System Manager role to start the polling task.

To manually start the polling task

1. In CA Access Control Enterprise Management, do as follows:
   a. Click Privileged Accounts.
   b. Click the Accounts subtab.

      The Feeder Folder Polling task appears in the list of available tasks.
2. Click Feeder Folder Polling.

   The Feeder Folder Polling screen appears.
3. Click Submit.

   The PUPM feeder polls the CSV files in the polling folder.

PUPM Automatic Login

PUPM automatic login lets you check out a privileged account password and log in to the PUPM endpoint in a single step. PUPM automatic login does not display the password after you check it out, but uses the password to log you in to the privileged account on the endpoint automatically. You can view the password in CA Access Control Enterprise Management after you check it out.

Important! You can use PUPM automatic login on Microsoft Internet Explorer browsers only.

To manage automatic login, you create login applications in CA Access Control Enterprise Management. A login application uses a script to open a window on the user's computer and log the user in to the privileged account that they checked out. For example, if you use a PuTTY login application to check out the root account on an SSH Device endpoint, CA Access Control Enterprise Management opens a PuTTY window on your computer and logs you in to the root account on the endpoint.

How Automatic Login Works

PUPM automatic login lets you check out a privileged account password and log in to the PUPM endpoint in a single step.

The following process explains how PUPM automatically logs you in to an endpoint. You must create a login application in CA Access Control Enterprise Management and assign the application to a PUPM endpoint before you begin this process:

1. You check out a privileged account password and select the login application that CA Access Control Enterprise Management uses to log in to the endpoint.

2. If ActiveX is not installed on your computer, the following occurs:
    a. CA Access Control Enterprise Management sends an ActiveX package to your computer.
    b. You install ActiveX.

       If you do not install ActiveX, you cannot automatically log in to the endpoint.
3. Once ActiveX is installed, ActiveX downloads the script file defined in the login application from the Enterprise Management Server to your computer.

   The script file contains the privileged account password. The script file runs, connects to the endpoint, and automatically enters the credentials of the privileged account.

   Note: ActiveX does not save the script file on your computer.
4. A terminal, Windows Remote Desktop, or Internet browser window opens.

   You are logged in to the privileged account on the endpoint.
5. When you finish the session, *one* of the following occurs:
   - If you check in the privileged account password before you close the remote window, PUPM sends a notification that it will close the window after a grace period. After the grace period elapses, PUPM closes the window and ends the session.

     Note: The grace period is defined in the script file. You can customize the script file to increase or decrease the grace period.
   - If you close the remote window and do not check in the privileged account password, PUPM sends a notification that asks if you want to check in the password.

How to Customize the PUPM Automatic Login Application Scripts

You can enhance the PUPM automatic login capability by customizing the PUPM automatic login application scripts. You use the PUPM automatic login SDK to create a custom script to enable users to automatically log in to an endpoint.

The following process explains how you customize the automatic login application scripts:

1. Create a Visual Basic script

   You can use a standard COM object or the ACLauncher ActiveX method to create the script.
2. Configure a login application in CA Access Control Enterprise Management and associate the script you created with the application
3. Associate the login script to an endpoint

More information:

The PUPM Automatic Login Application Visual Basic Script (see page 129)

The PUPM Automatic Login Application Visual Basic Script

The PUPM automatic login application uses Visual Basic scripts to enable automatic users login. You can customize the Visual Basic scripts to create new login applications or modify existing login applications.

The PUPM automatic login application script contains variables that the ActiveX replaces with values when downloaded to the client machine from the Enterprise Management Server. The Enterprise Management Server processes the scripts and replaces the keywords with values. The ActiveX then executes the script on the client machine.

The PUPM automatic login application scripts are located in the following directory:

JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts

Elements

The PUPM login application script contains the following keys:

#host#

Specifies the name of the endpoint that the user automatically logs in to

#username#

Specifies the checked out privileged account

#password#

Specifies the privileged account password to check out

#userdomain#

(Active Directory) Specifies the privileged account domain name

#isActiveServletUrl#

Specifies the URL that the ACLauncher ActiveX uses to check for an account password check in event.

#CheckinUrl#

Specifies the URL that the ACLauncher ActiveX uses to check in the account password in case the user logged out of the endpoint.

#SessionidUrl#

Specifies the URL that the ACLauncher ActiveX uses to send recorded session ID if the sessions is recorded in ObserverIT Enterprise

The following snippet of a PUPM automatic login application script displays how the variables appears:

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#\#userName#", "#password#")
' Set window close event
pupmObj.SetWindowCloseEvent(hwnd)
' Set server checkin event
pupmObj.SetServerCheckinEvent("#isActiveServletUrl#")
' Wait until one of the events signaled
rc = pupmObj.WaitForEvents()
If rc = 1 Then 'user has closed the window - notify the server side
        pupmObj.SendCheckinEvent("#CheckinUrl#")
ElseIf rc = 2 Then 'timeout elapsed - close the window
    call pupmObj.CloseWindow(hwnd, 0)
ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
    call pupmObj.CloseWindow(hwnd, 120)
End If
```

Structure

The PUPM automatic login application script structure is as follows:

- Initialization of the COM object

  ```
  Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
  ```

- Execution of the automatic login application

  ```
  hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#\#userName#", "#password#")
  ```

- Post execution tasks—password check in, interactive login or timeout

  ```
  ' Wait until one of the events signaled
  rc = pupmObj.WaitForEvents()
  If rc = 1 Then 'user has closed the window - notify the server side
      pupmObj.SendCheckinEvent("#CheckinUrl#")
  ElseIf rc = 2 Then 'timeout elapsed - close the window
      call pupmObj.CloseWindow(hwnd, 0)
  ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
      call pupmObj.CloseWindow(hwnd, 120)
  End If
  ```

To record the login application session, add recording instructions to the script, as follows:

- In the initialization section. add the following:

```
Set observeIT = CreateObject("ObserverIT.AgentAPI.Proxy")
```

- In the application execution section, add the following:

```
'Get application processid
processID = pupmObj.GetWindowProcessID(hwnd)
'Start recording
sessionid = observeIT.StartByProcessID(processID, true)
'Send the sessions if to the ENTM server
pupmObj.AssignSessionID "#SessionidUrl#" ,sessionId
```

- In the post execution section, add the following:

```
'Stop recording

observeIT.StopBySessionId sessionId, true
```

Methods

The ACLauncher ActiveX uses the following methods:

```
LauncheRDP (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT *phWindow);
```

Launch the remote desktop session with the input credentials and return the remote desktop window handle

Example: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LauncheRDP("hostname.com", "hostname\administrator", "password")

```
LaunchePUTTY (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT *phWindow);
```

Launch the PuTTY session with the input credentials and return the PuTTY window handle

Example: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test. LaunchePUTTY ("hostname.ca.com", "root", "password")

```
LauncheProcessAsUser (BSTR bsApplication, BSTR bsCommandline, BSTR bsUsername, BSTR bsPassword, VARIANT *phWindow);
```

Launch process with the input credentials and return the process window handle

Example: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LauncheProcessAsUser("cmd.exe", "/k echo This console is run under %USERNAME% account...", "administrator" , "password")

`GetWindowProcessID(VARIANT *phWindow, LONG *pProcessID);`

Return the process ID of a specified window handle

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") id = test.GetWindowProcessID(hwnd) test.Echo "Process ID = " & id

`GetWindowTitle(VARIANT *phWindow, BSTR *pbsTitle);`

Return the Title of a specified window handle

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") title = test.GetWindowTitle(hwnd)

`CloseWindow(VARIANT *phWindow, LONG Seconds);`

Display a dialog box with a message specifying that the window will close in X seconds and close the window of a specified window handle

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.Sleep(5000) test.CloseWindow(hwnd, 60)

`SetTimeoutEvent(LONG seconds);`

Specify the timeout for "WaitForEvents" method. Once reached, the WaitForEvents method returns from its blocking call with a return value that indicates the timeout reached

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetTimeoutEvent(10)

`SetWindowCloseEvent(VARIANT *phWindow);`

Specify the window closing event for the "WaitForEvents" method. After the window is closed, the "WaitForEvents" method returns from its blocking call and displays the return value that indicates that the window was closed

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetWindowCloseEvent(hwnd)

`SetServerCheckinEvent(BSTR bsURL);`

Sets the PUPM check in event as a block execution condition. The ActiveX queries PUPM every 5 seconds

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb") (replace with variable)

```
WaitForEvents(VARIANT *pRetVal);
```

Blocks the script execution until one of the register conditions is correct.

Options:1—the user closed the window, 2—timeout elapsed, 3—password checked in at the server side

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb")

test.SetWindowCloseEvent(hwnd) test.SetTimeoutEvent(360) rc = test.WaitForEvents() If rc = 3 Then call test.CloseWindow(hwnd, 10) End If

```
SwitchToThisWindow(VARIANT *phWindow);
```

Positions the window at the top of the Z order

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SwitchToThisWindow(hwnd)

```
SendCheckinEvent(BSTR bsURL);
```

Send check in event when user closes the window

Example: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password")

```
Sleep(LONG milliseconds);
```

Pauses the script execution

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Sleep(2000)

```
Echo(VARIANT* pArgs);
```

Print messages to screen

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Echo("Password Checkin")

Advanced Login

Advanced login is a type of automatic login that lets you check out a privileged account defined on one endpoint and use that account to log in to another endpoint. Advanced login lets you use automatic login to check out privileged accounts that are defined in Active Directory.

For example, you define a UNAB endpoint named example1 in Active Directory, and migrate the example1 users and groups (including root) to Active Directory. You define root as a privileged account in CA Access Control Enterprise Management. If you use automatic login when you check out root, you log in to the endpoint on which the root account is defined, which is the Active Directory Domain Controller. If you use advanced login when you check out root, you can choose to log in to the example1 endpoint.

CA Access Control Enterprise Management displays the advanced login option for each endpoint to which you have assigned a login application. Once you assign a login application to an endpoint, you do not need to perform additional steps to configure advanced login.

Chapter 5: Managing Privileged Accounts

This section contains the following topics:

Force Check In of a Privileged Account Password

You can force check in of a privileged account password that is currently checked out by one or more users.

To force check in a privileged account password

1. Click Privileged Accounts, Accounts, Force Check-In.

   The Force Check-In: Select Privileged Account page appears.

2. 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. The Checked Out By Users column lets you know whether the privileged account is checked out and by whom.

3. Select the privileged account passwords to check in and click Select.

   A confirmation message appears.

4. Click Yes to confirm the changes.

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

Automatically Reset a Privileged Account Password

Use the automatic password reset tasks to reset the password of selected privileged accounts. When initiated, CA Access Control Enterprise Management generates a new password for the selected accounts, based on the password policy assigned to the accounts.

Important! When you reset the password on an account, the previous password becomes obsolete. Any users that are using the previous password must check in the account and check out the account to continue to log in to the managed devices.

Note: This option is not valid for disconnected accounts.

To automatically reset a privileged account password

1. Click Privileged Accounts, Accounts, Automatic Account Reset.

   The Automatic Account Reset: Select Privileged Account page appears.

2. 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.

3. Select the privileged account password to reset and click Select.

   A confirmation message appears.

4. Click Yes to confirm the changes.

   CA Access Control Enterprise Management submits the task to reset the account password.

Manually Reset a Privileged Account Password

Use the manual password reset task to reset an account password and manually generate a new password for the privileged account. The new password must comply with the password policy that is assigned to the selected privileged account.

Important! When you reset the password on an account, the previous password becomes obsolete. Any users that are using the previous password must check in the account and check out the account to continue to log in to the managed devices.

We strongly recommend that you use the manual password reset only when managing privileged accounts originating from disconnected endpoints. Change the password CA Access Control Enterprise Management stores each time you change the password on the disconnected endpoint.

To manually reset a privileged account password

1. Click Privileged Accounts, Accounts, Manual Password Reset.

   The Manual Password Reset: Select Privileged Account page appears.

2. 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.

3. Select the privileged account to change the password of and click Select.

   The Manual Password Reset page appears.

4. Type the new password and confirm it, then click Submit.

   CA Access Control Enterprise Management submits the task to change the account password.

Delete a Privileged Account Exception

A *privileged account exception* lets a user check out a privileged account that they are otherwise not authorized to check out. Once a PUPM Approver approves a privileged account access request, the requester can check out the privileged account during the period in which the request is valid. You can delete the privileged account exception to prevent the user from being able to check out the account the exception applies to. To delete privileged account exceptions your account must have the default Privileged Account Request or PUPM Target System Manager roles assigned, or an equivalent role that contains this task.

To delete a privileged account request

1. In CA Access Control Enterprise Management, click Privileged Accounts, Exceptions, Delete Privileged Account Exception.

   The Delete Privileged Account Exception: Select Privileged Account Exception page appears.

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

   A list of privileged account exceptions that match the filter criteria appears.

3. Select the privileged account exceptions you want to delete and click Select.

   A confirmation message appears asking you if you want to delete the selected privileged account exceptions.

4. Click Yes.

   The privileged account request is deleted.

Manual Password Extraction

If the application server is not running and PUPM is unavailable, you cannot use PUPM to check out privileged accounts. Instead, you can use pwextractor, the PUPM password extraction utility, to export privileged account passwords from the database. You can then use the passwords to log in to privileged accounts as usual or, for back up of privileged account passwords.

If you extract privileged account passwords from the database because PUPM is unavailable, you do not need to complete any post-recovery steps when PUPM is restored.

You install pwextractor when you install the Enterprise Management Server. By default, CA Access Control rules do not protect pwextractor, but you can write rules to protect it.

To use pwextractor, you must:

- Have access to the database tables
- Know the user name and password for the account that PUPM uses to access the database

  Note: You provide these credentials when you install the Enterprise Management Server.

You can use pwextractor whether CA Access Control Enterprise Management is running or stopped, and whether the application server is running or stopped. You can also run pwextractor remotely.

Note: For more information about pwextractor, see the *Reference Guide*.

Example: Extract Privileged Account Passwords from an Oracle Database

The following example extracts the privileged account passwords from an Oracle database and writes the output to the file C:\tmp\pwd.txt. The schema name is orcl and the database is located on host myhost.example.com. The Enterprise Management Server is installed on a Windows computer:

```
pwextractor.bat -h myhost.example.com -d orcl -t oracle -l joesmith -p P@ssw0rd -f
C:\tmp\pwd.txt
-k
C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\config\com\netegrity\c
onfig\keys\FipsKey.dat
```

Audit Privileged Accounts

You can search for and view high-level details about privileged account operations that CA Access Control Enterprise Management performs. Detail screens provide additional information about each task and event. Depending on the status of the task, you can cancel or resubmit a task.

To audit privileged accounts

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

   The Audit Privileged Accounts task appears in the list of available tasks.

2. Select Audit Privileged Accounts.

   The Audit Privileged Accounts task opens.

3. Specify the search criteria (see page 139), enter the number of rows to display, and click Search.

   The tasks that satisfy your search criteria are displayed.

Search Attributes for Auditing Privileged Accounts

To review tasks that have been submitted for processing, you can use the search feature in Audit Privileged Accounts. You can search for tasks based on the following criteria:

Initiated by

Identifies the name of the user who has initiated a task as the search criteria. Searches are based on the user name. To ensure that you entered a valid user name, use the Validate button.

Approved by

Identifies the name of the task approver as the search criteria. Searches are based on the user name. To ensure that you entered a valid user name, use the Validate button.

Note: If you select Approval Tasks Performed By criteria to filter the tasks, the Show approval tasks criteria is also enabled by default.

Task Name

Identifies the task name as the search criteria. You can refine the search by specifying conditions such as equals, contains, starts with, or ends with the value of the Where task name field. For example, you can specify the search criteria "task name equals Create Endpoint" by selecting the equals condition, and entering Create Endpoint in the text field.

Account Name

Identifies the account name as the search criteria. You can refine the search by specifying conditions such as equals, contains, starts with, or ends with the value of the Where account name field. For example, you can specify the search criteria "account name equals Administrator" by selecting the equals condition, and entering Administrator in the text field.

Endpoint Type

Identifies the endpoint type as the search criteria. You can refine the search by specifying conditions such as equals, contains, starts with, or ends with the value of the Where endpoint type field. For example, you can specify the search criteria "endpoint type equals Windows Agentless" by selecting the equals condition, and entering Windows Agentless in the text field.

Endpoint Name

Identifies the endpoint name as the search criteria. You can refine the search by specifying conditions such as equals, contains, starts with, or ends with the value of the Where Endpoint Name field. For example, you can specify the search criteria "endpoint name equals exampleHost" by selecting the equals condition, and entering exampleHost in the text field.

Event Name

Identifies the event name as the search criteria. You can refine the search by specifying conditions such as equals, contains, starts with, or ends with the value of the Where event name field. For example, you can specify the search criteria "event name equals CheckInAccountPasswordEvent" by selecting the equals condition, and entering CheckInAccountPasswordEvent in the text field.

Task Status

Identifies task status as the search criteria. You can select the task status by enabling Where task status equals, and selecting the condition. You can further refine the search based on the following conditions:

- Completed
- In progress
- Failed
- Rejected
- Partially completed
- Cancelled
- Scheduled

Task Priority

Identifies task priority as the search criteria. You can select the task priority by enabling Where task priority equals, and selecting the condition. You can further refine the search based on the following conditions:

Low

Specifies that you can search for tasks that have a low priority.

Medium

Specifies that you can search for tasks that have a medium priority.

High

Specifies that you can search for tasks that have a high priority.

Submitted Between

Identifies the dates between which you want to search submitted tasks. You must provide the From and To dates in the Submitted between fields.

Show unsubmitted tasks

Identifies the tasks in the Audited state. Identifies the tasks that have initiated other tasks or tasks that have not been submitted. All such tasks will be audited and displayed if you select this checkbox.

Show approval tasks

Identifies the tasks that have to be approved as part of a workflow.

More information:

Task Status Description (see page 39)

Task Status Description

A submitted task exists in one of the states described below. Based on the state of the task, you can perform actions such as cancelling or resubmitting a task.

Note: To cancel or resubmit a task, you must configure View Submitted Tasks to display the cancel and resubmit buttons based on the task status.

In progress

Displayed when any of the following occurs:

- Workflow is initiated but not yet completed
- Tasks, which are initiated before the current tasks, are in progress
- Nested tasks are initiated but not yet completed

- The primary event is initiated but not yet completed
- Secondary events are initiated but not yet completed

You can cancel a task in this state.

Note: Cancelling a task will cancel all the incomplete nested tasks and events for the current task.

Cancelled

Displayed when you cancel any of the tasks or events in progress.

Rejected

Displayed when CA Access Control Enterprise Management rejects an event or task that is part of a workflow process. You can resubmit a rejected task.

Note: When you resubmit a task, CA Access Control Enterprise Management will resubmit all the failed or rejected nested tasks and events.

Partially Completed

Displayed when you cancel some of the events or nested tasks. You can resubmit a partially completed event or nested task.

Completed

Displayed when a task is completed. A task is completed when the nested tasks and nested events of the current task are completed.

Failed

Displayed when a task, nested task, or event nested in the current task are invalid. This status is displayed when the task fails. You can resubmit a failed task.

Scheduled

Displayed when the task is scheduled to execute at a later date. You can cancel a task in this state.

View Audit Events on a PUPM Endpoint

If you integrate your PUPM endpoints with CA Enterprise Log Manager, you can record audit events on the endpoints for each privileged account session. The audit events are collected in CA Enterprise Log Manager reports, which you can view from CA Access Control Enterprise Management. The reports let you track the actions that a privileged account performs after a user checks out the account.

You can view CA Enterprise Log Manager reports only for CheckOutAccountPasswordEvent or CheckInAccountPasswordEvent events.

To view audit events on a PUPM endpoint

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

   The Audit Privileged Accounts task appears in the list of available tasks.

2. Select Audit Privileged Accounts.

   The Audit Privileged Accounts task opens.

3. Specify the search criteria (see page 139), enter the number of rows to display, and click Search.

   The tasks that satisfy your search criteria appear.

4. For the selected task, click the icon in the Session Details column in the Audit Privileged Account page.

   Note: The icon appears only for CheckOutAccountPasswordEvent or CheckInAccountPasswordEvent events.

   The CA Enterprise Log Manager report appears. The report contains the audit events for the privileged account session that you selected.

5. Click Preview.

   The report closes and CA Access Control Enterprise Management displays the Audit Privileged Account page with the tasks list.

More information:

Auditing Events on PUPM Endpoints (see page 62)

Restore an Endpoint Administrator Password

Each time that the administrator password is changed, PUPM stores the previous passwords in the database according to the date and time of the password change. If you restored an endpoint from a backup, in case of failure to the endpoint, the current administrator password is different than the administrator password set on the endpoint. To connect and log into the endpoint, you need to restore the administrator password to match the period of the backup you used.

To restore an endpoint administrator password

1. In CA Access Control Enterprise Management, Select Privileged Accounts, Endpoints, Endpoint Password Restore Point task.

   The Endpoint Password Restore Point: Search Endpoint screen opens.

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

   A list of endpoints that match the search criteria appears.

3. Select an endpoint from the list and click Select.

   The endpoint and administrator account details appear.

4. Select an administrator password to restore from the Password Date menu.

   The Password Date menu lists the date and time of each password change. Select a password that is the closest to the date of the backup you used.

5. Click Verify.

   PUPM attempts to verify the password. If successful, a confirmation message appears.

6. (Optional) Select additional privileged account passwords to reset.

7. Click Submit.

   PUPM restores the selected password and sets that password as the current administrator password. If you have selected additional privileged accounts, PUPM also restores these account passwords.

Show Previous Privileged Account Passwords

If as a result of a failure to the endpoint you have restored the endpoint from a backup, the administrator account password on the endpoint is not synchronized with the one that is stored in the PUPM databse. To log in or connect to the endpoint, you must have the administrator password from the period of the backup you used.

On each password change, PUPM stores the previous passwords, which enable you to select one of the previously used password to connect to the endpoint you restored.

To show previous privileged account password

1. In CA Access Control Enterprise Management, select Privileged Accounts, Accounts, Show Previous Account Password.

   The Show Previous Account Passwords: Select Privileged Account search screen opens.

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

   A list of endpoints and privileged accounts that match the criteria appear.

3. Select a privileged account from the list and click Select.

   A screen appears, displaying the account details and password history, sorted by date.

4. Select an entry from the list and click Show Password.

   CA Access Control Enterprise Management displays the privileged account password at the top of the screen. You can now log in to the endpoint using the password.

5. Click Close.

Chapter 6: Using Privileged Accounts

This section contains the following topics:

Check Out a Privileged Account Password

You check out a privileged account password to log into an endpoint that the account belongs to. When you check out a privileged account, you can select to display the password, copy the password to a clipboard, or to log into the endpoint.

If you want to use SSH to connect to an SSH Device endpoint and PUPM uses different accounts to connect to and manage the endpoint, you check out both accounts. Use the credentials for the connection account to connect to the SSH Device endpoint, then use the credentials for the administration account to su to that account.

To check out a privileged account password

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

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

2. (Optional) Select an attribute for the search, type in the filter value, and click Search.

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

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

   - Select Checkout to check out the password
   - Select the Login Application you configured to log into the endpoint
   - Select Show Password to display the password
   - Select Copy to Clipboard to copy the password to a clipboard
   - Select Advanced Login to configure the login application and host name of the endpoint you want to log in to

   CA Access Control Enterprise Management submits the task and proceeds according to the option you selected.

   If you have selected to log in to the endpoint, CA Access Control Enterprise Management displays a confirmation message and a window on the endpoint opens and logs you in.

   Note: If this is the first time that you attempt to log in to the endpoint, a dialog box opens requesting you to confirm the action before you can connect to the endpoint.

   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.

More information:

How PUPM Connects to UNIX Endpoints (see page 102)

Check In a Privileged Account Password

You check in a privileged account password after you have logged out of the managed endpoint. Once you check in the privileged account password, CA Access Control Enterprise Management may change the password if it was configured to do so.

To check in a privileged account password

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

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

2. (Optional) Select an attribute for the search, type in the filter value, and click Search.

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

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

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

More Information:

Check Out a Privileged Account Password (see page 147)
Request Access to a Privileged Account (see page 149)

Request Access to a Privileged Account

If you need a privileged account password, but your user account does not have privileged access to check out the account, you can submit a request to check out that account. CA Access Control Enterprise Management forwards your request to an approver who can approve or deny your request. If approved, you can then check out the privileged account.

To request a password for a privileged account

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

   The Privileged Account Request: Select Privileged Account page appears.

2. 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.

3. Select the privileged account you want to check out and click Select.

4. Complete the request and click Submit. You may also need to provide a Unicenter Service Desk ticket number.

   A window opens informing you that the request was submitted.

   The request is forwarded to the approver and remains pending until approved or rejected. If the request is approved, you can check out the privileged account.

Respond to a Privileged Account Request

If you have the default PUPM Approver role or an equivalent role assigned, you can respond to pending privileged account access requests submitted by users. You can respond with *one* of the following actions:

- **Approve**—Approve the request and let the user check out the privileged account.
- **Reject**—Reject the privileged account request.
- **Reserve Item**—Reserve the request for later consideration. When you reserve a request, CA Access Control Enterprise Management removes this work item from work lists of other approvers. You can return to this item later and approve or reject it.
- **Release Item**—Release the request for others to respond to. You can only release an item that you previously reserved for yourself.

You can also add additional approvers and reassign the work item so that they too receive it in their pending approvals.

Note: Break Glass checkout requests are displayed in the Waiting For My Approval list of requests. However, you do not need to approve or reject these requests. These requests are displayed only as a notification that a user checked out a Break Glass account.

Note: To respond to a privileged account request, a user must have the PUPM Approver privileged access role and be the requesting user's manager.

To respond to a privileged account request

1. Click Home, My Accounts, Waiting For My Approval.

   A list of pending privileged account requests appears.

2. Click the pending request that you want to consider.

   The Approve Privileged Account Request page appears.

3. (Optional) To add approvers for this request, follow these steps:

   a. Click Add Assignees.

      The Select User search pane opens.

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

      A list of users that match the filter criteria appears.

   c. Select the users you want to add and click Select.

      The user is added to the approvers list.

4. (Optional) Review request details and modify required parameters, as follows:
   a. Click the Privileged Account tab.

      The Privileged Account tab appears, displaying the account and request details.
   b. Use the Valid Until field to override the checkout expiration timeout.
   c. Use the Ticket Number field to review the Unicenter Service Desk ticket.
   d. Type a comment to explain your response to the request.
5. Do *one* of the following:
   - Click Approve.

     The request is approved, removed from the list of pending requests, and the requester can now check out the privileged account.
   - Click Reject.

     The request is rejected and removed from the list of pending requests.
   - Click Reserve Item.

     The request is reserved for you and removed from the list of pending requests of other approvers.
   - Click Release Item.

     The request is released to all other approvers. You can only release items that you reserved.

Break Glass

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 wait for the request to be approved.

To break glass

1. 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: Checkout, Login Application, and Show Password.

Check In a Break Glass Privileged Account Password

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

To check in a break glass privileged account password

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.

Chapter 7: Integrating with CA User Activity Reporting Module

This section contains the following topics:

About CA User Activity Reporting Module

CA User Activity Reporting Module focuses on IT compliance and assurance. It lets you collect, normalize, aggregate, and report on IT activity, and generate alerts requiring action when possible compliance violations occur. You can collect data from disparate security and non-security devices.

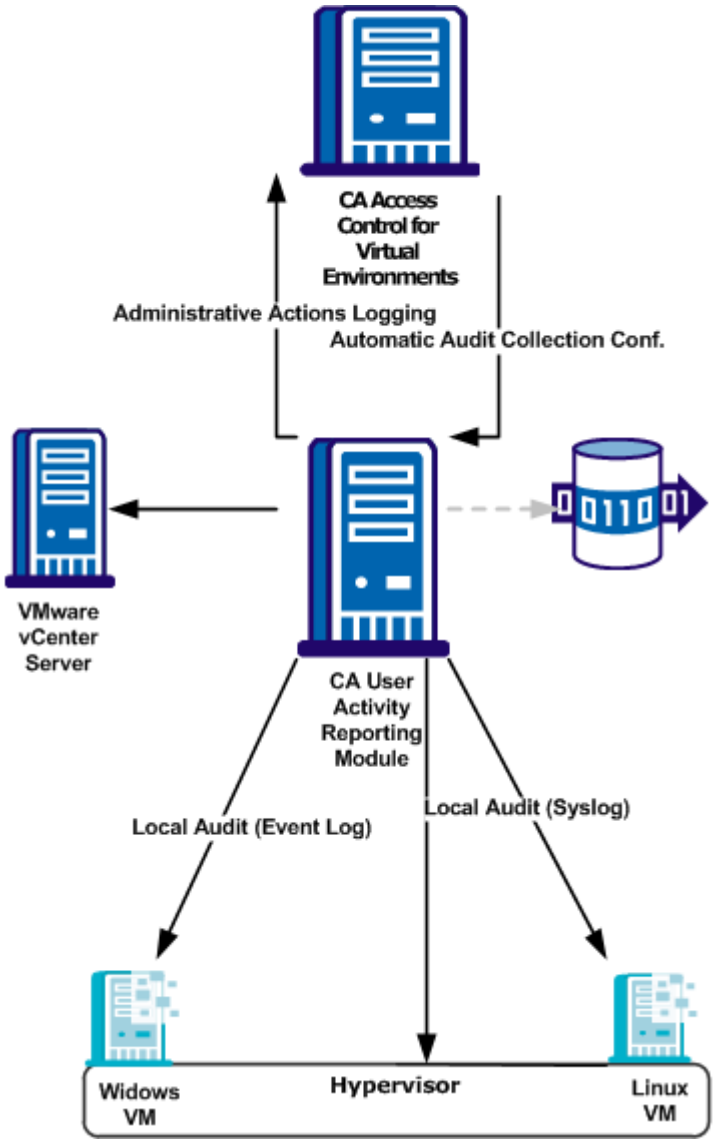
CA User Activity Reporting Module Integration Architecture

Integration with CA User Activity Reporting Module lets you collect audit events from each of your managed devices for reporting by CA User Activity Reporting Module.

You can configure each manage device to collect audit events to the audit file on the local machine. You can then configure a CA User Activity Reporting Module to pull events (messages) from it. CA User Activity Reporting Module processes these events and sends them to the CA User Activity Reporting Module server.

The CA Access Control for Virtual Environments installation supports CA User Activity Reporting Module integration.

The following diagram shows the architecture of CA User Activity Reporting Module integration components:



The preceding diagram illustrates the following:

- Each managed device collects audit data to local files
- CA User Activity Reporting Module pulls the audit records from the managed devices when an audit collection policy is applied
- CA User Activity Reporting Module collects audit records on administrative actions you do in CA Access Control for Virtual Environments
- CA User Activity Reporting Module collects audit records from the VMware vCenter Server and the hypervisor

Note: CA User Activity Reporting Module integration relies on reporting service components. As such, your architecture includes other reporting service components and features that are not used for CA User Activity Reporting Module integration. These components and features are dimmed in the diagram.

CA User Activity Reporting Module Integration Components

CA User Activity Reporting Module integration uses the following CA Access Control for Virtual Environments components. These components are part of the CA Access Control enterprise reporting service:

- The *Report Agent* runs on each managed device and sends information to queues on a configured Message Queue that resides on the CA Access Control Server. For CA User Activity Reporting Module integration, the Report Agent collects audit messages from the audit log files on a scheduled basis, and sends these events to the audit queue on a configured Distribution Server.
- A *Message Queue* is a component of the Distribution Server that is configured for receiving information that Report Agents send. For reporting, the Message Queue forwards the CA Access Control for Virtual Environments database snapshots to the central database.

Note: CA Access Control for Virtual Environments installs the Distribution Server on the CA Access Control Server by default.

CA User Activity Reporting Module integration also uses the following CA User Activity Reporting Module components:

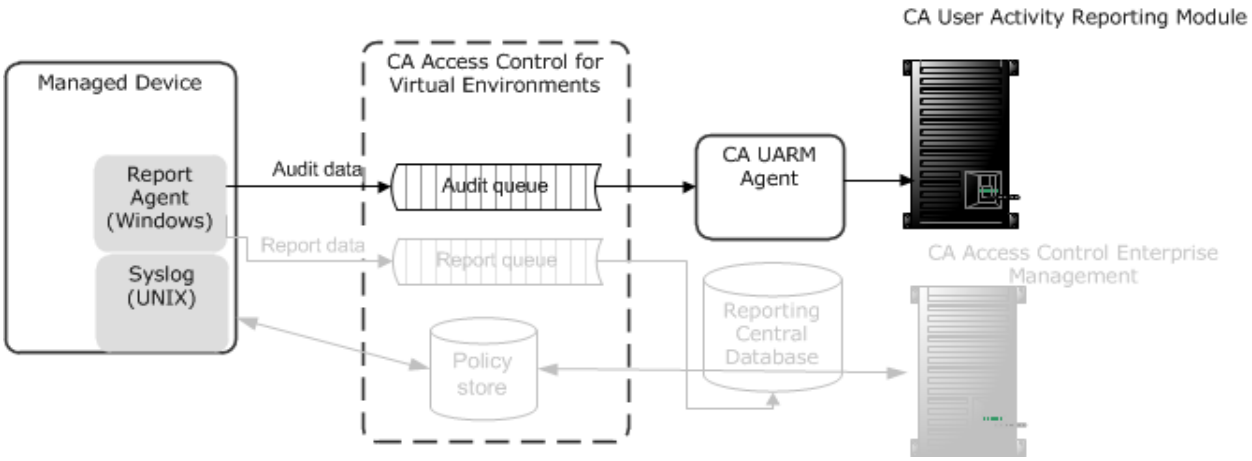
- A *CA Access Control connector* is an out-of-the-box CA User Activity Reporting Module integration for a CA Access Control for Virtual Environments audit event source. The connector enables raw event collection from a Distribution Server and the rule-based transmission of converted events to an event log store, where they are inserted into the hot database.

- A *collection server* is a CA User Activity Reporting Module server that refines incoming event logs, insert them into the hot database, compresses the hot database when it reaches the configured size into a warm database, and auto-archives the warm database to the related management server on the configured schedule.

Note: For more information about CA User Activity Reporting Module components, see the CA User Activity Reporting Module documentation.

How Audit Data Flows from CA Access Control for Virtual Environments to CA User Activity Reporting Module

To understand how CA Access Control for Virtual Environments integrates with CA User Activity Reporting Module, and what to consider when configuring this integration, first consider the flow of audit data between CA Access Control for Virtual Environments and CA User Activity Reporting Module. The following illustration describes how CA Access Control for Virtual Environments routes audit events to a messaging queue on a Distribution Server, where the CA Access Control connector of CA User Activity Reporting Module pulls, maps, transforms, and then sends the events to the CA User Activity Reporting Module server:



1. The Report Agent collects audit events from the local audit files, applies any filtering policies, and places the events on a audit queue located on the Distribution Server.
2. A CA User Activity Reporting Module connector connects with the audit queue and pulls events (messages) from it.

3. CA User Activity Reporting Module maps the events to the Common Event Grammar (CEG) using data mapping and parsing files, and then applies suppression and summarization rules before routing the events to the CA User Activity Reporting Module server.
4. The CA User Activity Reporting Module server receives the events and may apply additional suppression and summarization rules before the events are stored.

Note: For more information about how CA User Activity Reporting Module works, see the CA User Activity Reporting Module documentation.

How to Set Up CA User Activity Reporting Module for CA Access Control for Virtual Environments

To use CA User Activity Reporting Module to create reports that contain audit data from all your virtual machines, first implement enterprise reporting. You must implement enterprise reporting before you integrate with CA User Activity Reporting Module because implementing enterprise reporting enabled the Report Agents on the CA Access Control Server. Once you have enterprise reporting implemented, set up CA User Activity Reporting Module for CA Access Control for Virtual Environments.

To set up CA User Activity Reporting Module for CA Access Control for Virtual Environments, follow these steps:

1. Install the CA User Activity Reporting Module server

   Note: For more information, see the *CA User Activity Reporting Module Implementation Guide*.
2. Configure the CA User Activity Reporting Module API certificate in CA User Activity Reporting Module

   You specify the certificate details when you create the connection to CA User Activity Reporting Module from CA Access Control Enterprise Management
3. Configure the CA User Activity Reporting Module connector (see page 158)
4. Configure the audit collection profiles in CA User Activity Reporting Module

   You can configure custom audit collection profiles or use the default collection profiles
5. Create a connection to CA User Activity Reporting Module from CA Access Control Enterprise Management

   You configure the connection settings to enable CA User Activity Reporting Module to collect audit records from the managed devices
6. Configure an audit collection policy in CA Access Control Enterprise Management

Connector Details

After you install the CA User Activity Reporting Module agent on a computer, that computer appears in the CA User Activity Reporting Module server management interface (for example, to view a computer in the Default Agent Group click Administration, Log Collection, Agent Explorer, Default Agent Group, *computer_name*). You must now create a connector. This topic describes the settings that you *must* configure on the Connector Details page of the Connector Creation wizard.

Integration

Specifies the integration you want to use as a template.

Select the appropriate CA Access Control integration.

Example: AccessControl_R12SP5_TIBCO

You can optionally change the name of the connector and add a description. You can then apply suppression rules to events handled by the connector.

Note: For information about other optional settings that let you customize your event collection, see the *CA User Activity Reporting Module Administration Guide* and the *Online Help.*

Suppression and Summarization Rules

Once you create the connector and specify the connector details, you can optionally apply suppression rules on the Apply Suppression Rules page of the Connector Creation wizard.

The name of the Ideal Model for the suppression and summarization rules for CA Access Control is Host IDS/IPS. When you create rules, select the values for Event Category, Event Class, and Event Action as needed to identify events.

Note: For information about other optional settings that let you customize your event collection, see the *CA User Activity Reporting Module Administration Guide* and the *Online Help.* For more information on field identification or individual values, see the Common Event Grammar Reference in the *CA User Activity Reporting Module Online Help*.

Connector Configuration Requirements

Once you create the connector and specify the connector details, you can configure the connector. This topic describes the settings that you *must* configure on the Connector Configuration page of the Connector Creation wizard to begin event collection.

Note: For information about other optional settings that let you customize your event collection, see the *CA User Activity Reporting Module Administration Guide* and the *Online Help.*

TIBCO Server

Specifies the host name or IP address of the Message Queue (TIBCO server) in the following format:

Protocol`://`*server IP or name*`:`*Port number*

The Message Queue is installed on CA Access Control Enterprise Management.

- Define the following value:

  `ssl://ACentmserver:7243`

The port values and communication method are the default ports that CA Access Control Enterprise Management uses. If you configured different values after installing CA Access Control Enterprise Management, use that port and communication method values.

TIBCO User

Specifies the user name for Message Queue authentication. CA Access Control defines a default user named "reportserver".

TIBCO Password

Specifies the password for Message Queue authentication. Enter the password that you defined in the "Communication Password" dialog when you installed CA Access Control Enterprise Management.

Event Log Name

Specifies the log name for the event source.

Accept the default, "CA Access Control".

PollInterval

Specifies the number of seconds the agent waits before polling for events when the Message Queue has become unavailable or disconnected.

SourceName

Specifies the identifier for the Message Queue queue.

Accept the default, "queue_audit".

TIBCO Queue

Specifies the name of the Message Queue queue from which the log sensor is to read messages (events).

Accept the default, "queue/audit".

Number of Collection threads

Specifies the number of threads the log sensor spawns to read Message Queue messages.

You should consider the number of events in the Message Queue queue and the CPU of the CA User Activity Reporting Module agent system when you adjust this value.

Limits: The minimum value is 1. The maximum number of threads that the log sensor can spawn is 20.

How Configuration Settings Affect the Report Agent

For CA User Activity Reporting Module integration, the Report Agent collects endpoint audit messages from the audit log files on a scheduled basis, and routes these events to the audit queue on a configured Distribution Server. You can affect performance by tuning the Report Agent settings.

Note: The Report Agent is part of the CA Access Control enterprise reporting service and is also responsible for sending database snapshots for endpoint reporting purposes. This process describes only those actions that the Report Agent takes for audit event routing to CA User Activity Reporting Module.

The Report Agent does the following when you enabled audit collection (set the audit_enabled configuration settings to 1):

- Collects new audit records by reading records from the endpoint audit files and committing them to memory.

  The Report Agent reads the number of audit records that you defined in the audit_read_chunk configuration setting and then waits for the duration that you defined in the audit_sleep configuration setting before reading the audit files again. The Report Agent reads previously unread records in the active audit log *and* all the backup audit files. It then commits to memory those records that pass the audit filter as defined in the audit filter file (audit_filter configuration setting).

- Sends a group of audit records it has in memory to the Distribution Server Message Queue that you defined in the audit_queue configuration setting.

  The Report Agent sends audit records when *one* of the following applies:

  - The number of records in memory reaches the number defined by the audit_send_chunk configuration setting.
  - The amount of time that has passed because the last audit records were sent equals the interval defined by the audit_timeout configuration setting.

Example: Default Report Agent Settings for Audit Collection and Routing

This example illustrates how we set the default Report Agent configuration settings, what environment these are set for, and how they affect performance.

We expect an average environment to have 30 events per second (EPS). Therefore, the Report Agent reads 30 events for every second that passes. To reduce the impact on other running applications (CPU use and context switches) we chose to have the Report Agent read 300 events every 10 seconds, as follows:

```
audit_sleep=10
audit_read_chunk=300
```

The message bus CA Access Control uses to transport messages between the Report Agent and the Distribution Server handles large packets that are sent at long intervals better than it handles small packets at short intervals. The following configuration setting specifies that when the number of audit records the Report Agent collects reaches the defined number, the Report Agent sends the records to the Distribution Server. Assuming 30 events per second, if we want the Report Agent to send audit records at approximately one-minute intervals (60 seconds), we et the Report Agent as follows:

```
audit_send_chunk=1800
```

However, at night, or at other times when there are less than 30 events per second, there are less than 1800 events per minute. To verify that the Report Agent still regularly sends audit records to the Distribution Server, we set a maximum interval of 5 minutes between sending audit records, as follows:

```
audit_timeout=300
```

Filter Events from CA User Activity Reporting Module

You can use a filter file to prevent CA Access Control from sending every audit record in the log file to CA User Activity Reporting Module. The filter file specifies the audit records that are not sent to CA User Activity Reporting Module.

Note: This filter file prevents CA Access Control from sending the specified audit events to the Distribution Server, but does not stop CA Access Control from writing the audit events to the local files. To filter out audit events from the local audit file, modifyfilter rules in the file defined be the AuditFiltersFile configuration setting in the logmgr section (by default, audit.cgf).

To filter events from CA User Activity Reporting Module, edit the audit filter file on the endpoint. If you want to apply the same filtering rules to more than one endpoint, we recommend that you create an audit filtering policy and assign the policy to the endpoints where you want it to be effective.

Note: For more information, see the *Reference Guide*.

Example: Audit Filter Policy

This example shows you what an audit filtering policy looks like:

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

This policy writes the following line to the auditrouteflt.cfg file:

```
FILE;*;*;R;P
```

This line filters audit records that record a permitted attempt by any accessor to access any file resource for reading. CA Access Control will not send these audit records to the Distribution Server.

Secure Communications using SSL

When you install CA Access Control Enterprise Management you can select to either secure the communication between the Distribution Server and Report Agent by using SSL or select not to secure the communication. Whichever option you select, specify the same option when you install the Report Agent on the endpoint.

For example, if you use SSL to encrypt the communications between the Report Agent and the Distribution Server (the default), then you must provide authentication information when you install CA Access Control Enterprise Management, such as the password required for the Report Agents to communicate with the Distribution Server.

This is the password you provide when you configure the CA Access Control Report Agent on the endpoint and in the CA User Activity Reporting Module agent Connector Configuration page.

You must provide the same information when you install the Report Agent. Only Report Agents that can provide the correct certificate and password information can write events to the audit queue on the Distribution Server and thus be retrieved by CA User Activity Reporting Module.

Audit Log Files Backup for CA User Activity Reporting Module Integration

To collect audit data, the Report Agent reads the CA Access Control audit log files according to its configuration settings. The Report Agent reads a configured number of audit records from the audit log files at configured intervals. In a default legacy installation, or when you do not enable audit log routing during installation, CA Access Control keeps a single size-triggered audit log backup file. Every time the audit log reaches the configured maximum size, it creates a backup file, overwriting the existing audit log backup file. As a result, it is possible that the backup file will be overwritten before the Report Agent read all of its records.

We strongly recommend that you set CA Access Control to keep time-stamped backups of your audit log file. This way, CA Access Control does not overwrite the backup audit log files until it reaches a configured maximum of audit log files it should keep. This is the default setting when you enable the audit log routing sub-feature during installation on the endpoint.

Example: Audit Log Backup Settings

This example illustrates how the recommended configuration settings affect CA User Activity Reporting Module integration. When you enable the audit log routing sub-feature during installation on an endpoint, CA Access Control sets the following logmgr section configuration settings:

```
BackUp_Date=yes
audit_max_files=50
```

In this case, CA Access Control timestamps each backup copy of the audit log file and keeps a maximum of 50 backup files. This provides plenty of opportunity for the Report Agent to read all of the audit records from the files and for you to copy the backup files for safe keeping if required.

Important! If you set audit_max_files to 0, CA Access Control does not delete backup files and will keep accumulating the files. If you want to manage the backup files through an external procedure, remember that CA Access Control protects these files by default.

Queries and Reports for CA Access Control Events

The queries, reports, and action alerts for CA Access Control are grouped under the Server Resource Protection tags in the CA User Activity Reporting Module interface.

Note: For information, visit the CA User Activity Reporting Module Product page at http://ca.com/support

How to Enable CA User Activity Reporting Module Reports in CA Access Control

Before you can view CA User Activity Reporting Module reports in CA Access Control Enterprise Management, you must enable CA User Activity Reporting Module reporting, export and add the CA User Activity Reporting Module certificate and configure the connection to CA User Activity Reporting Module from CA Access Control Enterprise Management.

1. Enable CA User Activity Reporting Module reporting by configuring advanced settings.
2. Export and add the CA User Activity Reporting Module trusted certificate to the keystore.
3. Configure the connection to CA Enterprise Log Manager.
4. (Optional) Configure an audit collector (see page 169).

   Configure an audit collector if you want to send PUPM audit events to CA User Activity Reporting Module.

Add the CA User Activity Reporting Module Trusted Certificate to the Keystore

CA User Activity Reporting Module reports are authenticated using trusted certificates. The certificate verifies that the information displayed in the reports originated from a trusted CA User Activity Reporting Module source, which verifies the authenticity of the data.

Note: Obtain and install the CA User Activity Reporting Module trusted certificate the before you start this procedure. For more information about installing the CA User Activity Reporting Module trusted certificate, see the CA User Activity Reporting Module documentation.

Follow these steps:

1. On the Enterprise Management Server, open a Command Prompt window and navigate to the following directory:

jbossInstallDir/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore

1. Enter the following command:

   `keytool -import -file <certificate.cert> -keystore`

   -import

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

   -file

   Specifies the full pathname of the trusted certificate file.

   A password prompt appears.

2. Enter the keystore password. The default password is 'secret'.
3. Click Yes to trust the certificate.

   The certificate is added to the keystore.

Configure the Connection to CA User Activity Reporting Module

CA Access Control Enterprise Management communicates with CA User Activity Reporting Module to display reports with CA Access Control related information. To display these reports you need to configure the connection to CA User Activity Reporting Module.

Follow these steps:

1. In CA Access Control Enterprise Management, do as follows:
   a. Click System.
   b. Click Connection Management subtab.
   c. Expand the UARM tree in the task menu on the left.

   The Manage CA User Activity Reporting Module Connection task appears in the list of available tasks.
2. Click Manage CA User Activity Reporting Module Connection .

   The Manage CA User Activity Reporting Module Connection: *PrimaryCALMServer* task page appears.
3. Complete the fields in the dialog. The following fields are not self-explanatory:

   Connection name

   Identifies the name of the CA User Activity Reporting Module connection.

   Description

   (Optional) Defines a description for this connection.

   Host Name

   Defines the name of the CA User Activity Reporting Module host you want CA Access Control Enterprise Management to work against.

   Example: host1.comp.com

   Port #

   Defines the port that the CA User Activity Reporting Module host uses for communication.

   Default: 5250

   Validate Trusted Root Certificate

   Specifies whether the connection to CA User Activity Reporting Module uses a trusted root certificate signed by a certificate authority.

   Note: Verify that you Installed the CA User Activity Reporting Module trusted root certificate to ensure proper functionality.

Certificate name

Defines the name of the certificate.

Password

Defines the certificate password.

4. Click Submit.

   CA Access Control Enterprise Management saves the CA User Activity Reporting Module connection settings.

Example: Obtain the CA User Activity Reporting Module Certificate Information

The following example shows you how to obtain the CA User Activity Reporting Module certificate information that you need to provide when creating and managing the CA User Activity Reporting Module connection settings in CA Access Control Enterprise Management.

1. Enter the CA User Activity Reporting Module URL in a web browser using the following format:

   `https://host:port/spin/calmapi/products.csp`

   Example: https://localhost:5250/spin/calmapi/products.csp

2. Enter a valid user name and password to log in to CA User Activity Reporting Module.

3. Select the Register option to register a certificate with CA User Activity Reporting Module.

   The New Product Registration screen appears.

4. Enter the certificate name and password and select Register.

   A message appears informing you that the certificate registered successfully.

Configure an Audit Collector

CA Access Control Enterprise Management collects audit events, including PUPM audit events, and stores them in the central database. You can configure CA Access Control Enterprise Management to send the audit events to CA User Activity Reporting Module.

To configure an audit collector

1. In CA Access Control Enterprise Management, do as follows:
   a. Click System.
   b. Click Connection Management subtab.
   c. Expand the UARM tree in the task menu on the left.

      The Create Audit Collector task appears in the list of available tasks.
2. Click Create Audit Collector.

   The Create Audit Collector: Audit Collector Search Screen appears.
3. (Optional) Create a copy of an existing audit collector, as follows:
   a. Select Create a copy of an object of type UARM Sender.
   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of UARM Senders that match the filter criteria appear.
   c. Select the object you want to use as a basis for the new audit collector.
4. Click OK.

   The Create Audit Collector task page appears. If you created the audit collector from an existing object, the dialog fields are pre-populated with the values from the existing object.
5. Complete the fields in the dialog. The following fields are not self-explanatory:

   Job Enable

   Specifies whether the audit collector is enabled.

   Name

   Defines the name of audit collector.

   Queue Jndi

   Defines the name of the Message Queue queue that CA Access Control Enterprise Management sends audit event messages to.

   Example: *queue/audit*

   Sleep

   Defines the interval, in minutes, between database queries.

   Default: 1

Time Out

Defines the collector time out period, in minutes, for sending the audit event messages to the messages queue.

Default: 10

Note: Once the timeout period has passed, the collector sends the messages although the number of messages in the queue did not reach the level defined in the Msg Block Size field.

Msg Block Size

Defines the maximum number of messages to accumulate in the database before sending the message to the queue.

Default. 100

6. Click Submit.

   CA Access Control Enterprise Management creates the audit collector.

Chapter 8: Creating Reports

This section contains the following topics:

Security Standards

With the migration from a paper-based operational environment to one that focuses on electronic media, corporations have become significantly exposed to local and remote attacks on those data. To address these concerns, several security initiatives have been implemented in the areas of general global security, financial accuracy and reporting, the safe guarding of private monetary information and individual identities, the protection of health-care related information, and a US government-wide standardization of security best practices.

The following security standards, acts, and requirements provide a useful summary of the root of the best practice reporting that is being performed by CA Access Control reporting service:

Payment Card Industry Data Security Standards (PCI DSS)

PCI DSS is an industry standard that was developed by the major credit card companies to help prevent security issues including fraud and hacking. Companies who accept, capture, store, transmit, or process credit and debit card data must comply with PCI DSS.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a United States federal law that protects health insurance coverage when workers change or lose their jobs. HIPAA also addresses the security and privacy of health data.

Sarbanes-Oxley Act (SOX)

SOX is a United States federal law that stipulates standards for financial reporting. It applies to the boards and management of all U.S. public companies.

Report Types

You can view information about CA Access Control for Virtual Environments data and events in two different report types:

- CA Access Control for Virtual Environments reports—Describe who can do what.

  CA Access Control reports provide information about the data in the CA Access Control for Virtual Environments database on each managed device, that is, the policies that you deploy on the endpoint and policy deviations. You view CA Access Control for Virtual Environments reports in [assign the value for cabi in your book] and in CA Access Control Enterprise Management.

- Audit reports—Describe who did what.

  Audit reports provide information about the data on each managed device, that is, information about which users performed what actions on the endpoint. You view audit reports in CA User Activity Reporting Module in the VMware vSphere Client and in CA Access Control Enterprise Management.

  Note: For more information about viewing audit reports in CA User Activity Reporting Module, see the *CA User Activity Reporting Module Overview Guide*.

Note: Additional components to view CA Access Control for Virtual Environments reports and CA Access Control for Virtual Environments audit reports must be installed. For more information, see the *Product Guide*.

Reporting Service

CA Access Control for Virtual Environments reporting service lets you view the security status of each endpoint (users, groups, and resources) in a central location. The collection of data from each endpoint can be scheduled or on demand. You do not need to connect to each endpoint to find out who is authorized to access which resource. CA Access Control for Virtual Environments reporting service, once set up, works independently to collect data from each endpoint and report it to a central server and continues to report endpoint status without the need for manual intervention.

CA Access Control reporting service is useful for BS 7799/ISO 17799, Sarbanes-Oxley (SOX), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA) environments, and others. It offers a solution wherever you must know the status of users, groups, and resource access across thousands of endpoints.

The reporting service is structured to let you interrogate the data that is collected from each endpoint. You can build custom reports for a variety of purposes, or use the existing reports that CA Access Control for Virtual Environments provides by default. Because the reporting service is server-based, it lets you centralize report storage and management and provides secure access (SSL) to reports. The reporting service can be configured for high availability. You can install the reporting service components on a single server or in a distributed configuration.

Note: The reporting service components are external to the CA Access Control for Virtual Environments enforcement system and add value to an existing implementation without the need to reconfigure it.

Reporting Service Components

The reporting service comprises the following core components:

- A *Report Agent* is a Windows service or a UNIX daemon that sends information to queues on a configured Message Queue that resides on the CA Access Control Server.
- A *Message Queue* is a component of the CA Access Control Server that is configured for receiving endpoint information that Report Agents send. For reporting, the Message Queue forwards endpoint database snapshots from to the central database.
- A *central database* is a Relational Database Management System (RDBMS) that holds information for CA Access Control Enterprise Management functionality, including reporting. You can use various tools to interrogate the data stored in the database about your CA Access Control implementation.
- A *Report Portal* is an application server that serves CA Access Control reports. The server uses BusinessObjects InfoView portal to let you interact with the reporting information that is stored on the central database.
- Enterprise Management Server is used to read reporting data from the Message Queue and store the data in the central database.
- Built-in reports are included to let you easily present data for common reporting scenarios.

How the Reporting Service Works

The reporting service lets you examine the data that is collected from each managed device, the user store, and the PUPM policy store. To set up the reporting service correctly, you need to know how it works to collect, store, and generate reports from the data.

The reporting service does the following:

- Collects data from each managed device.

  Each managed device sends report data to the Message Queue.

- Stores the data in the central database.

  CA Access Control for Virtual Environments retrieves the report data from the Message Queue and stores it in the central database.

- Captures snapshots of the report data and stores it in the central database.

  CA Access Control for Virtual Environments captures PUPM report data as part of the snapshot.

- Generates reports from the stored data.

  Once there is data available in the central database, you use the Report Portal to generate reports and queries the stored data. The Report Portal is a CA Technologies version of the BusinessObjects InfoView portal, configured to connect to the central database, and bundled with the ready-made CA Access Control for Virtual Environments reports.

How Data for Reporting Is Collected

To generate reports, data from each managed device has to be collected. The reporting service uses a Report Agent to collect data from that managed device at scheduled times or on-demand.

The Report Agent performs the following actions on each endpoint:

1. Performs a deviation calculation and sends the results to the CA Access Control Server.
2. Creates a copy of the CA Access Control database on the managed device.

   This is a temporary copy that the Report Agent takes so that it can process data without affecting performance.

3. Dumps the data from each database into an XML structure.

   This is a dump of all of the objects in the database, meaning that all data is captured.

4. Sends an XML version of the database to the CA Access Control Server.

   The Report Agent sends the data to the reporting queue on the CA Access Control Server.

More information:

How Configuration Settings Affect the Report Agent (see page 160)

How Data is Processed and Stored

When data is collected on each managed device, it is sent for processing on the CA Access Control Server. The processed data is then sent for storage on the central database for report generation.

The CA Access Control Server performs the following actions:

1. Receives, from the Report Agent, an XML dump of the entire database.
2. Processes the XML dumps using a Message Driven Bean (MDB) according to the database schema.

   Each incoming XML dump is transformed into Java objects for placement in a central database.

3. Inserts each Java object into the central database.

   The data from each endpoint is now available for retrieval from the central database.

Note: Endpoint data must be retrieved by the Report Portal, that is, captured in a snapshot, before it is available for inclusion in reports.

How CA Access Control Enterprise Management Captures Snapshots

CA Access Control Enterprise Management must capture report data, including endpoint dumps, in a snapshot before the data appears in a report. After CA Access Control Enterprise Management captures a snapshot, you can generate and view CA Access Control reports.

At the time specified in the snapshot definition, CA Access Control Enterprise Management performs the following actions to capture a snapshot:

- Extracts data from the user store into the central database.
- Extracts data from the PUPM policy store into the central database.
- Flags the latest endpoint snapshots that exist in the central database for inclusion in the snapshot.

How to View Reports in CA Access Control Enterprise Management

This process explains how to create and view CA Access Control for Virtual Environments reports, which provide information about the managed devices. You can also view CA Access Control for Virtual Environments reports in [assign the value for cabi in your book].

To view reports in CA Access Control Enterprise Management, do the following:

1. Create a snapshot definition.

   A snapshot definition specifies the report data that CA Access Control for Virtual Environments collects and defines the snapshot schedule.

2. Verify that you have configured the managed devices for reporting.
3. (Optional) Capture snapshot data.

   If you do not want to wait for the scheduled snapshot, you can use the Capture Snapshot Data task to collect a snapshot now.

4. Run a report.

   The report is created.

5. View the report.

Capture Snapshot Data

Typically, report data is captured in snapshots in scheduled intervals. If you want to capture snapshot data on demand, use the Capture Snapshot Data task to export the data immediately to the central database.

Important! Exporting snapshot data can take a long time if you have a large amount of data to export. When the reporting snapshot includes large amounts of data, we recommend that you create a snapshot definition to schedule your snapshots.

Note: By default, you must have the System Manager role to capture snapshot data.

Do the following

1. In CA Access Control Enterprise Management, do as follows:
   a. Click Reports.
   b. Click the Tasks subtab.
   c. Click Capture Snapshot Data.

      The Capture Snapshot Data page appears.
2. Select the name of the snapshot definition to capture, and click Submit.

   CA Access Control Enterprise Management exports snapshot data to the central database.

Note: You can use the View Submitted Tasks task to check the progress of the task. For more information about creating a snapshot definition, see the *Online Help*.

Run a Report in CA Access Control Enterprise Management

Reports consist of data that CA Access Control for Virtual Environments captures in snapshots. After CA Access Control for Virtual Environments captures a snapshot, the data in the snapshot is available for reports. You must run a report before you can view it. By default, you must have the System Manager or Reporting role to run a report; you must have the specific Reporting role for the report that you want to run.

Note: You cannot schedule recurring reports in CA Access Control Enterprise Management. However, you can schedule recurring reports in [assign the value for cabi in your book]. If you schedule a report in [assign the value for cabi in your book], you cannot view it in CA Access Control Enterprise Management; however, if you run a report in CA Access Control Enterprise Management, you can view it in [assign the value for cabi in your book].

Do the following

1. In CA Access Control Enterprise Management, do as follows:
   a. Click Reports.
   b. Click the language subtab.

      The language subtab is the name of the language in which you installed CA Access Control Enterprise Management. For example, if you installed CA Access Control Enterprise Management in English, the English subtab is displayed.

   c. Expand the tree for the report type that you want to run in the task menu on the left.

      A list of reports appears.
2. Select the report that you want to run.

   A parameters screen appears.
3. Provide any parameter information required.

   Consider the following when you enter parameter information:

   - If you specify a parameter and the central database does not have any values for that parameter, the report is empty.

     For example, if you define a report on one or more users and the central database does not have any user data, the report is empty because there is no user data to report.

   Note: Press Ctrl+click to select multiple parameters.
4. Click Submit.

   The report is submitted to the Report Server.

More information:

Schedule a Report (see page 181)

View a Report

CA Access Control for Virtual Environments reports provide information about the managed devices. You must run a CA Access Control report before you can view it.

Note: Enable third-party session cookies in your browser to view reports in CA Access Control Enterprise Management. By default, you must have the System Manager or Reporting role to view reports.

Do the following

1. In CA Access Control Enterprise Management, do as follows:
   a. Click Reports.
   b. Click Tasks subtab.
   c. Click View My Reports.

      The View My Reports: Configure Manage Reports Screen appears.
2. Search for the report that you want to view.

   A list of reports matching the search criteria is displayed.
3. Select the report that you want to view.

   The report is displayed.
4. (Optional) Click Export this report (top left corner) to export the report to the following formats:
   - Crystal Reports
   - Excel
   - PDF
   - Word
   - RTF

   The report is exported.

Manage Snapshots

CA Access Control Enterprise Management lets you view, modify, and delete your snapshot definitions. When you view or modify a snapshot definition, the Profile, Recurrence, and Maintenance tabs are shown. The Maintenance tab will only appear after a snapshot has been captured once.

Important! Do not enable more than one snapshot definition. CA Access Control Enterprise Management cannot successfully run all reports if more than one snapshot definition is enabled.

To view, modify, or delete a snapshot definition, go to Reports, Tasks, Manage Snapshot Definition and click the task that you want to execute.

Note: If a snapshot definition is being used to export data to the central database, you cannot delete the snapshot definition. When you delete a snapshot definition that is being used, the export of the data to the central database stops, but the snapshot definition is still available.

BusinessObjects InfoView Report Portal

A *Report Portal* is an application server that serves CA Access Control reports. The server uses BusinessObjects InfoView portal to let you interact with the reporting information that is stored on the central database.

Open InfoView for Working with Reports

You access CA Access Control reports using BusinessObjects InfoView. The following procedure describes how you access the reporting interface (BusinessObjects InfoView).

Follow these steps:

1. Launch InfoView in *one* of the following ways:
   - On the computer where BusinessObjects InfoView is installed, select Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, BusinessObjects Enterprise Java InfoView.
   - From a browser on any computer, navigate to the following URL:

     `http://ACRPTGUI_host:ACRPTGUI_port/businessobjects/enterprise115`

     ACRPTGUI_host—The name or IP address of the computer where the InfoView is installed (Report Portal).

     ACRPTGUI_port—The port number used to access InfoView, by default, 9085.

   The InfoView Log On page appears.
2. Enter the credentials you set up when you installed InfoView, and click Log On.

   The InfoView Home page appears.

Run a Report

Once you open reporting interface (BusinessObjects InfoView), you can select a report, and run it.

Follow these steps:

1. Open InfoView.

   The InfoView Home page appears.
2. Expand Home, Public Folders, CA Reports, and click CA Access Control in the left-hand frame.

   The CA Access Control page appears.

3. Click the linked title of the report you want to view.

   The report's page appears, letting you enter additional values to define the scope of the report you want to view.

4. Fill the form fields to define the scope of the report you want to get, and then click OK.

   The report's output page appears.

   You can perform additional queries to affect report generation. For example, you can choose to include All or select hosts to generate a report from all known hosts or a single host. Additionally you can specify a date range to view all historical data or only data for a specific date range.

   Note: You can use the % (percent) symbol to specify a wildcard value. The use of % is a standard SQL selection notation and does *not* represent a single character as it normally does in wildcard specifications.

Schedule a Report

There are many ways to run a report. You can run a report by clicking the report title and specifying values, or you can choose from a variety of options to schedule the report.

To schedule a report

1. Open InfoView.

   The InfoView Home page appears.

2. Expand Home, Public Folders, CA Reports, and click CA Access Control in the left-hand frame.

   The CA Access Control page appears.

3. Click Schedule under the title of the report you want to schedule.

   The Schedule page for the selected report appears.

4. Modify the Run object drop-down list selection to specify when you want the scheduled report to run.

5. Expand the Parameters section to specify values for the execution of the report:

   a. Click Empty to define a value for each parameter.

      The Enter prompt values section fields appear.

   b. Define the value as required, and click OK.

      The value you defined is saved for use in running the report.

6. Click Schedule to run the report according to the scheduling options you chose.

   The History page appears, confirming the instance of the report schedule you set.

Note: For more information about using BusinessObjects InfoView, see the *BusinessObjects Enterprise XI Release 2 InfoView User's Guide*.

View a Generated Report

After a report is generated, you can view it by doing either of the following from the CA Access Control report list:

- Click View Latest Instance for the report you want to view.
- Click History, and then click the date and time to choose a report instance to view.

Note: For more information about using BusinessObjects InfoView, see the *BusinessObjects Enterprise XI Release 2 InfoView User's Guide*.

View Report Status

You can find out whether a scheduled report has successfully run by checking its status.

To view report status

1. Open InfoView.

   The InfoView Home page appears.

2. Expand Home, Public Folders, CA Reports, and click CA Access Control in the left-hand frame.

   The CA Access Control page appears.

3. Click the History link for the report that you want to view.

   The report's History page appears letting you view the list of dates and times the reports were run.

   Each entry in the list displays the following:

   - Instance Time—Date and time the report was run
   - Title—Report title
   - Run By—Name of the user who ran the report
   - Parameters—Parameters selected for that report run
   - Format—Output format of the report
   - Status—The current status of the report, such as Success
   - Reschedule—A link that lets you run the report again

Note: For more information about using BusinessObjects InfoView, see the *BusinessObjects Enterprise XI Release 2 InfoView User's Guide*.

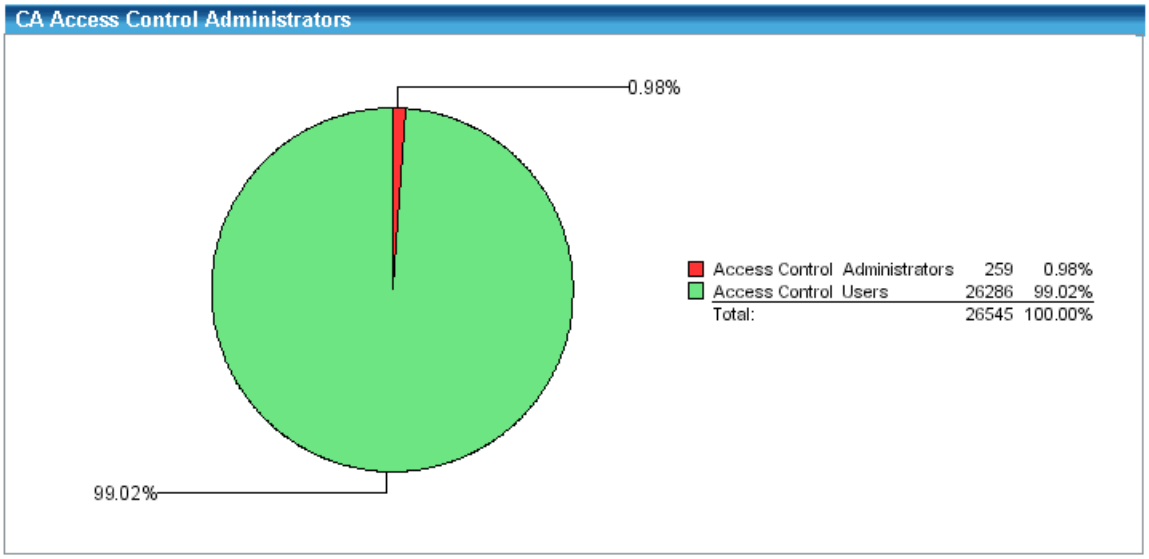
Standard Reports

By default, CA Access Control for Virtual Environments reporting service comes with standard reports that are deployed as part of the report portal installation.

In addition to the standard reports, you can augment the reports and make similar reports with different features, or generate completely new reports.

What Reports Look Like

The reports output uses tables, and graphics when appropriate. For example, some reports include a pie chart to convey meaning at a glance while still providing supporting details. As shown in the figure below, the CA Access Control Administrators report provides a pie chart of how many endpoint users are CA Access Control administrators. A high ratio of administrators to normal users may pose as security risk, so the graphic quickly shows if there is a security exposure. In this example, a large red wedge in the chart is significant because it shows that almost 1% of the current enterprise user base can perform CA Access Control administration.



In addition to the graphic, each report has an associated listing of the actual endpoint values. Following is a sample of this table of the CA Access Control Administrators report:

CA Access Control Administrators

User Name	Full Name	Host ID	Has Administrator Mode	Has Password Manager Mode	Has Operator Mode
_seagent					
		SYSTEMA	yes		
		SYSTEMB	yes		
		SYSTEMC	yes		

Privileged Account Management Reports

The Privileged Account Management reports provide a detailed view of privileged accounts management.

Following is the list of standard privileged account management reports:

CA Access Control Privileged Accounts by Endpoint

This report lists the privileged accounts by endpoint type and endpoint name. Using this report lets you see the privileged accounts according to their endpoint type and name. After you review the report, you can determine the of number privileged accounts are associated with each endpoint.

This report displays the following information:

- Snapshot time
- Endpoint type and name
- Account name
- Last check out user
- Last check out
- Last password change

CA Access Control PUPM Roles and Privileged Accounts by User

This report displays a list of privileged access roles and privileged accounts according to user account. Using this report, you can review the privileged accounts according to their associated roles and user accounts.

This report displays the following information:

- Snapshot time
- User ID
- Endpoint time and name
- Roles name and description
- Account name
- Exception
- Last password change

CA Access Control Privileged Accounts Requests by Endpoint

This report displays a list the privileged account requests by endpoint type and endpoint name. Using this report you can review the requests that were made for checking out privileged accounts and their corresponding endpoint type and name.

This report displays the following information:

- Snapshot time
- Endpoint type and name
- Host name
- Account
- Requestor
- Request justification
- Request time
- Approval time
- Valid from
- Valid until
- Approver
- Approver comments

Note: The report displays active privileged account requests only.

CA Access Control Privileged Accounts Requests by Approver

This report displays a list of the privileged accounts requests based on to the approver. Using this report you can review the privileged account requests that a specific user approved the requests. After reviewing the report, you can change the approver role,assign additional users or remove users from the role.

This report displays the following information:

- Snapshot time
- Approver user ID
- Endpoint type and name
- Host name
- Account
- Requestor name and ID
- Request justification
- Request time
- Approval time
- Valid from
- Valid until
- Approver comments

Note: The report displays active privileged account requests only.

CA Access Control Privileged Accounts Requests by Requester

This report displays privileged accounts requests based on the user who requested the privileged account's password. Using this report you can review the requests the were made by users for checking out a privileged account. After reviewing this report you can determine how many check out requests were made and by which user.

This report has the following information:

- Snapshot name
- Approver user ID
- Endpoint type and name
- Host name
- Account
- Request justification
- Request time
- Approval time
- Valid from
- Valid until
- Approver
- Approver comments

Note: The report displays active privileged account requests only.

CA Access Control PUPM Users by Privileged Accounts

This report displays a list of users that have access to privileged accounts according to the endpoint type and name. Using this report you can determine how user access privileged accounts, the endpoint type and name that each privileged account originated from.

This report displays the following information:

- Snapshot type
- Endpoint type and name
- Privileged account name
- User name
- User ID
- Request

CA Access Control PUPM Users by Role

This report displays the list of users and their associated privileged accounts role. Using this report you can determine how users are associated to privileged accounts roles and decide whether the current status meets your security standards.

This report displays the following information:

- Snapshot time
- Role name
- Number of members
- User name
- User ID
- e-mail address

CA User Activity Reporting Module Reports

The CA User Activity Reporting Module reports display detailed information about CA Access Control for Virtual Environments activity, resource management and more.

For more information about CA User Activity Reporting Module reports, see the CA User Activity Reporting Module documentation.

Custom Reports

All of the CA Access Control reports were created using Crystal Reports Designer XI. These are then presented through BusinessObjects InfoView in a web-based format. To customize the provided reports, you must have Crystal Reports Designer XI.

Note: The instructions in this guide provide some hints to help you start with report customization. For more information about Crystal Reports Designer XI, see the *BusinessObjects Enterprise XI Release 2 Designer's Guide*.

CA Access Control Universe for BusinessObjects

The CA Access Control Universe for BusinessObjects represents a simplified view of the CA Access Control reporting service central database. Universe is a semantic layer, which maps to data in the database. This layer isolates the end user from the complex structure of database. Universe is a collection of classes and objects.

Universes are created using BusinessObjects Enterprise Designer. The CA Access Control Universe is provided by CA Technologies to simplify the creation of reports from the CA Access Control reporting service central database. You should not modify the CA Technologies-developed CA Access Control Universe. If necessary, create a copy as a base for your own universe.

View the CA Access Control Universe

You can view CA Access Control Universe using BusinessObjects Designer.

To view the CA Access Control Universe

1. Select Start, Programs, BusinessObjects XI Release 2, BusinessObjects Enterprise, Designer.

   The User Identification dialog appears, letting you log in to BusinessObjects Designer.

2. Enter your credentials and click OK.

   The welcome screen of the Quick Design wizard appears.

3. Clear the Run this Wizard at Startup check box, and click Cancel

   An empty Designer session opens. The user name and repository name appear in the title bar.

4. Click File, Open, browse to the directory that contains the CA Access Control Universe, select the *CA Access Control.unv* file, and click Open.

   The CA Access Control Universe opens in the current Designer window.

   Note: The CA Access Control Universe is stored under *CA Universe**CA Access Control* in the directory designated as the default universe file store.

Customize the Standard Reports

You can customize any of the standard reports. For example, you can change titles, colors, logos and fonts to meet your needs. You must open a report in Crystal Reports Designer XI to make changes. Every report is has a corresponding .rpt file. You open this file to customize the report.

To customize a standard report

1. Open the .rpt file you want to customize in Designer.

   The Design view of the report appears.

2. Do *any* of the following:

   - To change the report's title, click File, Summary Info and enter a title in the Title field.
   - To customize text, highlight the desired text in the Design view and double-click it to edit.
   - To change the way the text looks, right-click on the text in an open report, select Format text, and change the properties as desired.

3. Save the custom .rpt file.

   The new custom report is saved and ready to be published.

Publish a Custom Report

You must publish custom reports using BusinessObjects InfoView.

To publish a custom report

1. Open BusinessObjects InfoView and log in as Administrator.

   The InfoView Home page appears.

2. Click New, Folder and create a new folder under Public Folders.

   The Create A New Folder task page appears.

3. Enter a name and a description for the custom reports folder, and click OK.

   A new folder is created.

4. Click New, Document from local computer, Crystal Report in the new folder you created.

   The Add a document from your local computer task page appears.

5. Enter the report title and the path name to your customized rpt file, and click OK.

   The custom report is published and can be viewed from BusinessObjects InfoView now. It can be also scheduled like any other report.