CA Access Control Premium Edition

Enterprise Administration Guide

12.6

Third-Party Notices

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

Sample Scripts and Sample SDK Code

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

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

CA Technologies Product References

This document references the following CA Technologies products:

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On (CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management (CA NSM, formerly Unicenter NSM and Unicenter TNG)
- CA Software Delivery (formerly Unicenter Software Delivery)
- CA Service Desk Manager (formerly Unicenter Service Desk)
- CA User Activity Reporting Module (formerly CA Enterprise Log Manager)
- 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

Format	Meaning
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
<u>Underline</u>	Default values
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:

- *ACInstallDir*—The default CA Access Control installation directory.
  - Windows—C:\Program Files\CA\AccessControl\
  - UNIX—/opt/CA/AccessControl/

- *ACSharedDir*—A default directory used by CA Access Control for UNIX.
  - UNIX—/opt/CA/AccessControlShared
- *ACServerInstallDir*—The default CA Access Control Enterprise Management installation directory.
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—The default Distribution Server installation directory.
  - /opt/CA/DistributionServer
- *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 that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- 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.

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.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Planning Your PUPM Implementation (see page 109)
  - Connector Xpress Example: Configure a SUN ONE Endpoint (see page 134)—New topic explains how to configure a SUN ONE endpoint in Connector Xpress
  - Connector Xpress Example: Register the SUN One Endpoint Type in Java Connector Server (see page 136)—New topic explains how to register the SUN ONE endpoint type in the Java Connector Server
- Implementing Privileged Accounts (see page 147)
  - Sybase Server Connection Information—New topic specifies the Sybase Server endpoint type connection information
  - VMware ESX/ESXi Connection Information (see page 170)—New topic specified the VMWare ESX/ESXi endpoint type connection information
  - Create an Endpoint CSV File—Updated topic to include additional rows
  - Create a Privileged Account CSV File—Updated topic to include additional rows

Contents

Chapter 1: Introduction 15

About this Guide 15
Who Should Use this Guide 15
Enterprise Management 15
- Enterprise Management Interface 16
- Central Policy Management 16
- Enterprise View 16
- Privileged User Password Management 17
- UNAB Management 17
- Enterprise Reports 18

Chapter 2: Administering CA Access Control Enterprise Management 19

Administrative Scoping 19
- Admin Roles in CA Access Control Enterprise Management 19
- Create an Admin Role 21
- Privileged Access Roles 22
- Create a Privileged Access Role 23
- Methods to Assign Roles to a User 25
- Create an Admin Task 29

Users, Groups, and Administrative Roles 31
- Active Directory Restrictions 32
- Create a User 32
- Reset a User Password 34
- Enable or Disable a User 34
- Types of Groups 35

Audit Data 40
- Search for Submitted Tasks 41
- View Task Details 44
- View Event Details 44
- Clean Up Submitted Tasks 45
- Route Message Queue Audit Messages to Windows Event Log 47
- Route Message Queue Audit Messages to UNIX Syslog 49

Email Notifications 51
- Email Templates 51
- How Email Notifications Work 54
- Customize Email Templates 55

Chapter 3: Viewing Your Enterprise Implementation 57

World View....57
View Your Enterprise CA Access Control Implementation....58
Open CA Access Control Endpoint Management to Manage an Endpoint....59
Configure a UNIX Endpoint for CA Access Control Endpoint Management SSO....60
Modify a PUPM Endpoint....61

Chapter 4: Managing Policies Centrally 63

Policy Types....63
Methods for Centrally Managing Policies....64
Advanced Policy Management....64
How Advanced Policy-based Management Works....65
    How Deployment Methods Affect Deployment Tasks....66
    Endpoint Data That the DMS Holds....68
    How Endpoints Update the DMS....69
    Advanced Policy Management Classes....69
Hosts and Host Groups....72
    Define an Endpoint as a Host in Your Enterprise....72
    How Automatic Host Group Assignment Works....73
    Define a Logical Host Group....77
    Import a Host Group....78
    Assignment Paths....79
How to Create and Deploy a Policy....80
    Administration Requirements....81
    Policy Dependency....82
    Policy Verification....82
    Create and Store a Policy Version....84
    Create a Policy That Defines a Variable....86
    View the Rules Associated with a Policy....88
    Import a Policy....89
    Assign a Stored Policy Version....90
Policy Maintenance....91
    Unassign an Assigned Policy....91
    Upgrade Assigned Hosts to the Latest Policy Version....92
    Downgrade Assigned Hosts to a Particular Policy Version....92
    Deleted Policies....93
Variables....95
    How You Create Variables....96
    Variable Types....96
    Guidelines for Using Variables....98
    How an Endpoint Resolves Variables....100

Troubleshooting Policy Deployment 101
How to Remove Obsolete Endpoints 102
View Deployment Audit Information 102
How Policy Deviation Calculations Work 103
Deviation Calculation Trigger 104
Policy Deviation Log and Error File 104
Policy Deviation Data File 105

Chapter 5: Planning Your PUPM Implementation 109

Privileged User Password Management 109
What Are Privileged Accounts? 109
Privileged Access Roles and Privileged Accounts 110
Using Privileged Access Roles 110
How Privileged Access Roles Affect Check Out and Check In Tasks 111
How Privileged Access Roles Affect Privileged Account Request Tasks 113
What Happens During the Break Glass Process 116
Password Consumers 117
Types of Password Consumers 118
How a Password Consumer Gets a Password on Demand 119
How PUPM Notifies a Password Consumer of a Password Change 121
Implementation Considerations for Password Consumers 122
PUPM Audit Records 123
Password Consumer Audit Records 123
PUPM Feeder Audit Records 123
Auditing Events on PUPM Endpoints 124
How to Integrate PUPM Endpoints with CA Enterprise Log Manager 125
CA Service Desk Manager Integration 125
How to Integrate Privileged Account Requests with CA Service Desk Manager 126
Configure the Connection to CA Service Desk Manager 126
Implementation Considerations 128
Email Notification of Privileged Account Passwords 129
Restrictions on Domain Users on Windows Agentless Endpoints 129
Minimum Privileges for Managing an Active Directory Endpoint 129
Connector Servers 131
The PUPM SDK 141

Chapter 6: Implementing Privileged Accounts 147

How to Set Up Privileged Accounts 147
Discover Privileged Accounts 150
Create a Privileged or Service Account 152
Create a Password Policy 155

Password Composition Rules 156
PUPM Endpoint and Privileged Account Creation 158
Create an Endpoint 158
Create a Login Application 194
How to Import PUPM Endpoints and Privileged Accounts 196
How the PUPM Feeder Works 197
Configure the Feeder Properties File 198
Create an Endpoint CSV File 201
Create a Privileged Account CSV File 207
Manually Start the Polling Task 211
How to Set Up Password Consumers 211
Discover Service Accounts 215
Create a Password Consumer 217
Password Consumer Example: Windows Run As 220
Password Consumer Example: Windows Scheduled Task 221
PUPM Automatic Login 222
How Automatic Login Works 223
How to Customize the PUPM Automatic Login Application Scripts 224
Customizing the PUPM Remote Desktop Script 229
Advanced Login 232
Terminal Integration 233

Chapter 7: Configuring PUPM Endpoints 237

Prepare a JBoss Application to Use a Database (JDBC) Password Consumer 237
Customize the Datasource Configuration Files for Microsoft SQL Server 239
Customize the Datasource Configuration files for Oracle 239
Password Consumer Example: JDBC Database 240
Additional Information for Oracle Databases 242
Configure an Endpoint to Use a Database (ODBC, OLEDB, OCI) Password Consumer 243
Configure an Endpoint to Use a Database (.NET) Password Consumer 244
Configure an Endpoint to Use a CLI Password Consumer 246
How CLI Password Consumers Work 247
Example: A Script That Gets a Password 247
How to Configure an Endpoint to Use a Password Consumer SDK Application 248
Run a Java PUPM SDK Application 249
How to Configure an Endpoint to Use a Web Services PUPM SDK Application 251
Configure Terminal Integration 252

Chapter 8: Managing Privileged Accounts 255

Force Check In of a Privileged Account Password 255
Automatically Reset a Privileged Account Password 256

Manually Reset a Privileged Account Password 256
Delete a Privileged Account Exception 257
Manual Password Extraction 258
Audit Privileged Accounts 259
Search Attributes for Auditing Privileged Accounts 259
Task Status Description 261
View Audit Events on a PUPM Endpoint 262
Synchronize Password Consumers 263
Restore an Endpoint Administrator Password 265
Show Previous Privileged Account Passwords 266

Chapter 9: Using UNAB 267

UNAB Components 267
How You Set Up UNAB 268
How UNAB Authenticates Users 268
Information Stored on the UNAB Endpoint 269
How You Control Host Access and Configure UNAB 269
Manage UNAB Login Authorization 270
Configure a UNAB Host or Host Group 271
Verify That CA Access Control Enterprise Management Committed the Policies to the Host 273
How to Migrate Users and Groups to Active Directory 274
Resolve Migration Conflicts 275
Display User Information 279
Stop UNAB 280
View UNAB Status 280
UNAB Debug Files 281

Chapter 10: Creating Reports 283

Security Standards 283
Report Types 284
Reporting Service 284
Reporting Service Components 285
How the Reporting Service Works 286
Send an Endpoint Snapshot to the Distribution Server 288
How to View Reports in CA Access Control Enterprise Management 289
Capture Snapshot Data 290
Run a Report in CA Access Control Enterprise Management 290
View a Report 291
Manage Snapshots 292
BusinessObjects InfoView Report Portal 293
Standard Reports 296

What Reports Look Like 297
Account Management Reports 298
Entitlement Reports 302
Miscellaneous Reports 303
Policy Management Reports 305
Password Policies Reports....................309
Privileged Account Management Reports 310
UNIX Authentication Broker Reports 314
CA Enterprise Log Manager Reports 318
Custom Reports....................318
CA Access Control Universe for BusinessObjects....................318
View the CA Access Control Universe 319
Customize the Standard Reports 320
Publish a Custom Report....................320

Chapter 11: Deploying Sample and Best Practice Policies 321

Sample Policies....................321
Where Are Sample Policies Stored? 322
Sample Policy Scripts....................323
Compliance and Best Practice Policies 327
Where Are Compliance and Best Practice Policies Stored? 328
Compliance and Best Practice Policies Scripts 329
Policy Deployment 330
How to Prepare an Endpoint for Policy Deployment 331
How to Deploy Policies in a Staged Manner 332

Chapter 1: Introduction

This section contains the following topics:

About this Guide (see page 15)
Who Should Use this Guide (see page 15)
Enterprise Management (see page 15)

About this Guide

This guide provides information about enterprise administration and reporting in CA Access Control Premium Edition and the CA Access Control Enterprise Management web-based interface. Enterprise administration and reporting for CA Access Control includes advanced policy 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 was written for security and system administrators using CA Access Control who want to take advantage of its enterprise administration and reporting capabilities:

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

Enterprise Management

The CA Access Control Enterprise Management is a Web based user interface that enables you to perform access related management tasks across your enterprise. Using the CA Access Control Enterprise Management you can perform a number of management tasks such as deploying access policies through the enterprise from a central location, managing individual hosts, managing privileged accounts, generating 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.

Central Policy Management

Use the central policy management capabilities of the CA Access Control Enterprise Management to create and assign an uninformed policy to hosts or host groups in the enterprise. The CA Access Control Enterprise Management interface enables assigning an enterprise wide policy using a wizard and displays the status of the deployment process on every host.

Further, you can use the CA Access Control Enterprise Management central policy management capabilities to troubleshoot the policy deployment process, unassign, upgrade or downgrade existing policies.

Enterprise View

You can use CA Access Control Enterprise Management to view information about and manage CA Access Control, PUPM and UNAB hosts from a central location. The CA Access Control Enterprise Management World View displays detailed information about each host type, when it was last updated, which type of devices are configured on each host and enables you to modify the host's settings and manage it remotely.

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.

UNAB Management

UNIX Authentication Broker (UNAB) lets you log in to UNIX computers using an Active Directory data store. This means you can use a single repository for all your users enabling them to log in with the same user name and password to all platforms.

Integrating UNIX accounts with Active Directory enforces strict authentication and password policies, transferring the rudimentary UNIX user and group properties to Active Directory. This lets you manage UNIX users and groups from a single point as you manage Windows users and groups.

Use the CA Access Control Enterprise Management central policy management capabilities to control access to UNIX hosts by creating and assigning a login policy containing a set of login rules.

Enterprise Reports

The CA Access Control Enterprise Management reporting options 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.

[assign the value for eACVPM in your book] 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 (see page 19)
Users, Groups, and Administrative Roles (see page 31)
Audit Data (see page 40)
Email Notifications (see page 51)

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**—Responsible for the definition of hosts and logical host groups.

  This admin role lets users create hosts and host groups, assign hosts to host groups, and modify them. It does not let users define policies or deploy policies but does let users view them and provides access to World View.

- **CA Access Control Policy Deployer**—Responsible for the deployment of policies across the environment.

  This admin role lets users assign policies to hosts and host groups, upgrade and downgrade policies, reset host configuration, and have access to the deployment audit. It lets users view policies and hosts but not define them and provides access to World View.

- **CA Access Control Policy Manager**—Responsible for creating policies.

  This admin role lets users create, modify, view, and delete policies. The admin role does not let users deploy the policies to hosts or host groups but they can view them and have access to the World View.

- **CA Access Control User Manager**—Responsible for user management in CA Access Control Enterprise Management: creating and managing users and groups, and assigning 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**—Responsible for managing CA Access Control Enterprise Management.

  A user with this admin role 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 this user's actions.

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

- **UNAB Administrator**—Responsible for managing UNAB. A user with this role can configure UNAB hosts and host groups, manage login authorization policies, and resolve migration conflicts.

  Note: A user that is assigned the System Manager role is also assigned the UNAB Administrator role.

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

- **CA Enterprise Log Manager Admin**—Responsible for managing 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**—Responsible for delegating work items. A user with this role can delegate work items to users.

- **Self Manager**—Responsible for managing their own user account. A user with this role can perform administrative actions on their account: 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 25).

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.

You should note the following when you assign privileged access roles to users:

- 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 25).

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 27), 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 27).

   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 28), 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 27).

   The admin policy for the role is created.

3. Click the Owners tab, click Add, specify an owner rule (see page 28), 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 30)
Add Tabs (see page 30)
Configure Fields, Events, and Role Use (see page 31)

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 32)
Types of Groups (see page 35)

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 41)
View Task Details (see page 44)
View Event Details (see page 44)
Clean Up Submitted Tasks (see page 45)
Route Message Queue Audit Messages to Windows Event Log (see page 47)
Route Message Queue Audit Messages to UNIX Syslog (see page 49)

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 41), 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 43) 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 43)

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: Viewing Your Enterprise Implementation

This section contains the following topics:

World View (see page 57)
View Your Enterprise CA Access Control Implementation (see page 58)
Open CA Access Control Endpoint Management to Manage an Endpoint (see page 59)
Configure a UNIX Endpoint for CA Access Control Endpoint Management SSO (see page 60)
Modify a PUPM Endpoint (see page 61)

World View

World View in CA Access Control Enterprise Management lets you view the enterprise implementation of CA Access Control that you are managing on the connected DMS.

Using World View you can:

- Identify which endpoints report to the connected DMS.
- Identify the endpoint type, which can be one or more of CA Access Control, PMDB, PUPM, and UNAB.
- See when each endpoint last sent a heartbeat to the DMS.
- View more details about the endpoint, such as which policies are deployed, what is the operating system, and what managed devices are on the endpoint.
- Open CA Access Control Endpoint Management to manage a CA Access Control endpoint.
- Modify a UNAB host or a PUPM managed device.

View Your Enterprise CA Access Control Implementation

Using CA Access Control Enterprise Management you can display your enterprise implementation of CA Access Control. This enterprise "World View" is a snapshot of all your endpoints, the logical host groups they are grouped into, the deployed policies on these endpoints, and the manage devices they have.

To view your enterprise CA Access Control implementation

1. In CA Access Control Enterprise Management click the World View tab, then click the World View link in the task menu on the left.

   The World View page appears with the Search section visible.

2. (Optional) Define the search criteria.

   You can use two types of searches:

   - **Simple**—Use the simple search to define a host name mask and specify the type of endpoint you want to filter the results by.
   - **Advanced**—Click the Advanced link to also filter the results by specified host groups, assigned policies, managed devices name mask, and managed devices type.

   Note: By default, World View displays results for all of the endpoints that are defined to the DMS CA Access Control Enterprise Management is connected to.

3. Click Go.

   The results, matching the criteria you defined, are displayed by one of the following categories:

   - **Results by Host Name**—These are the hosts (endpoints) that you define on the DMS. This is the default display category for the results.
   - **Results by Host Group**—These are the logical host groups you define.
   - **Results by Policies**—These are the policies that are deployed on the endpoints.
   - **Results by Managed Devices**—These are the managed devices on the endpoints.

Open CA Access Control Endpoint Management to Manage an Endpoint

CA Access Control Enterprise Management supports Single-Sign On (SSO) to let you easily log in to CA Access Control Endpoint Management to manage any of the endpoints that CA Access Control Enterprise Management manages.

If you want to set up automatic log in to manage a Windows endpoint, verify that you use identical user name and password in CA Access Control Enterprise Management and the CA Access Control endpoint and have terminal access rights to manage the endpoint using CA Access Control Endpoint Management.

Note: To set up automatic log in to manage a UNIX endpoint, you need to configure the endpoint for CA Access Control Endpoint Management SSO.

To open CA Access Control Endpoint Management to manage an endpoint

1. Use World View to view one or more endpoints you want to manage.
2. Click Manage in the Actions column.

   CA Access Control Endpoint Management opens and the endpoint host name and your credentials are automatically entered. If the CA Access Control Enterprise Management user you are logged in as does not exist in CA Access Control Endpoint Management, you need to enter the credentials manually.

More information:

View Your Enterprise CA Access Control Implementation (see page 58)
Configure a UNIX Endpoint for CA Access Control Endpoint Management SSO (see page 60)

Configure a UNIX Endpoint for CA Access Control Endpoint Management SSO

CA Access Control Enterprise Management lets you easily log in to CA Access Control Endpoint Management to manage any of the endpoints that CA Access Control Enterprise Management manages. In an automatic login, you log in to CA Access Control Enterprise Management with your Active Directory credentials. CA Access Control Enterprise Management retains the credentials and provides them to the endpoint when you open CA Access Control Endpoint Management to manage the endpoint. Automatic login to CA Access Control using CA Access Control Endpoint Management relies on the user account you use to authenticate to CA Access Control Enterprise Management.

Note: To configure automatic login to UNAB endpoints, verify that both CA Access Control Enterprise Management and UNAB use the same Active Directory.

Important! Configure the user you want to use as a UNIX user in Active Directory.

To configure a UNIX endpoint for CA Access Control Endpoint Management SSO

1. On the CA Access Control endpoint, open the seos.ini file, locate the [OS_User] section and set the value of the token osuser_enabled to **1**.

   Enterprise users and groups are enabled.

2. Locate the [seos] section and set the value of the token auth_login to **pam**.

   The login authority method used is PAM.

3. Create a TERMINAL record for the CA Access Control Endpoint Management computer.

   The CA Access Control Endpoint Management computer is assigned TERMINAL access.

4. Configure the user account you use to log in to CA Access Control Enterprise Management as an XUSER and assign it the admin attribute. Use the following format: *<DOMAIN-NAME>user_account*.

5. Define an ACL for the superadmin user in TERMINAL class with read and write access rights. For example:

   ```
   Defaccess         : R, W

   ACLs              :

       Accessor                Access

       DOMAIN\user(XUSER  ) R, W
   ```

   The user can use the CA Access Control Enterprise Management Server to manage the endpoint.

Modify a PUPM Endpoint

Using the CA Access Control Enterprise Management World View you can modify the settings of a PUPM endpoint managed device. Managed devices are applications that you administer using privileged accounts. The PUPM endpoint stores the privileged accounts in a password database, using a role-based management system to grant access to the accounts. The managed devices may be installed on the PUPM endpoint itself or on the enterprise.

To modify a PUPM endpoint

1. Select World View, World View task.

   The World View search screen appears.

2. Type in the query and click Go.

   The query displays the search results.

3. Click the down arrow (Show) icon in the row of the PUPM endpoint that you want to modify.

   The extended information displays the managed devices on the endpoint.

4. Click Modify to modify the endpoint settings.

   The Modify Endpoint window appears, displaying the endpoint settings.

5. Modify the endpoint settings and click Submit.

   A message appears information you that the task completed.

More information:

Create an Endpoint (see page 158)

Chapter 4: Managing Policies Centrally

This section contains the following topics:

Policy Types (see page 63)
Methods for Centrally Managing Policies (see page 64)
Advanced Policy Management (see page 64)
How Advanced Policy-based Management Works (see page 65)
Hosts and Host Groups (see page 72)
How to Create and Deploy a Policy (see page 80)
Policy Maintenance (see page 91)
Variables (see page 95)
Troubleshooting Policy Deployment (see page 101)
How to Remove Obsolete Endpoints (see page 102)
View Deployment Audit Information (see page 102)
How Policy Deviation Calculations Work (see page 103)

Policy Types

In CA Access Control Enterprise Management, you use three types of policies to manage CA Access Control endpoints and UNAB hosts: CA Access Control policies, UNAB configuration policies, and UNAB login policies.

You use CA Access Control policies to create a unified policy for controlling access to resources and setting accessor rights to CA Access Control endpoints throughout the enterprise.

You use UNAB login policies to manage access to the UNIX hosts in your enterprise. Login policies control users' login to UNIX hosts that have UNAB running on them. CA Access Control Enterprise Management automatically creates, assigns, and deploys the login policies based on the authorization lists that you populate.

You use UNAB configuration policies to set the values of tokens in the configuration files on remote UNAB hosts to facilitate deploying and configuring UNAB hosts in the organization.

More information:

Manage UNAB Login Authorization (see page 270)
Configure a UNAB Host or Host Group (see page 271)

Methods for Centrally Managing Policies

CA Access Control lets you manage several databases from a single computer in the following ways:

- **Automatic rule-based policy updates—**Regular rules you define in a central database (PMDB) are automatically propagated to databases in a configured hierarchy.

  Note: Dual control is only available with this method and on UNIX only. Information about dual control for automatic rule-based policy updates is found in the *Endpoint Administration Guide for UNIX*. Information about automatic rule-based policy updates can also be found in the *Endpoint Administration Guide for Windows*.

- **Advanced policy management—**Policies (groups of rules) you deploy are propagated to all databases based on host or host group assignment. You can also undeploy (remove) policies and view deployment status and deployment deviation. You need to install and configure additional components to use this functionality.

  Note: Information about advanced policy management is found in the *Enterprise Administration Guide*.

Advanced Policy Management

Policies (selang commands) you create can be stored and then deployed to your enterprise in the manner you define. Using this policy-based method, you can store policies and then assign them to hosts or group hosts. Once assigned, policies are queued for deployment. Alternatively, you can deploy and undeploy policy versions directly onto hosts or group hosts.

A central database—the Deployment Map Server (DMS)—collects all the information about your enterprise policies, versions, assignments, and deployment. Therefore, you can easily report on deployment status, deployment deviation, and deployment hierarchy.

Note: Dual control is *not* available with this method and is only available on UNIX. For more information, see the *Endpoint Administration Guide for UNIX*.

How Advanced Policy-based Management Works

Advanced policy-based management lets you store, deploy, and undeploy policy versions, and later check the deployment status, deployment deviation, and deployment distribution.

Advanced policy-based management works in the following way:

1. You create a policy.

   Each policy contains a pair of selang command scripts. The first script is a *deployment script* and contains a set of selang commands that construct the policy. The second script is an *undeployment script* and contains commands that are required for undeploying (removing) the policy from the endpoint database.

2. You store policy details in the DMS using either CA Access Control Enterprise Management or the policydeploy utility, and CA Access Control then stores the policy using automatic version-control.

   Policy details include the policy description, deployment and undeployment scripts, and policy dependency.

3. Depending on whether the policy already exists on the DMS, CA Access Control does *one* of the following:

   - If the policy name does not exist on the DMS, CA Access Control creates the first version of the policy *(policy_name*#01) and the logical policy object (GPOLICY class), and then adds the policy version as a member of the logical policy.
   - If the policy name already exists on the DMS, CA Access Control creates a new policy version, incrementing the highest found policy version by one and adds the policy version as a member of the logical policy (GPOLICY object).

4. When you decide it is time, you use CA Access Control Enterprise Management or the policydeploy utility to deploy a stored policy to target databases. CA Access Control creates deployment tasks (DEPLOYMENT objects) automatically on the DMS.

   Note: CA Access Control deploys the latest finalized policy version of the stored policy. New policy versions that you create are not sent automatically to assigned hosts. You need to manually upgrade assigned hosts to the latest policy version.

   Note: CA Access Control Enterprise Management automatically deploys the UNAB login and procedures policies after you create them. You can only assign UNAB login and configuration policies to UNAB hosts.

5. CA Access Control creates a deployment package (GDEPLOYMENT object) automatically on the DMS.

   The deployment package groups all the deployment tasks created in the previous step.

6. The DMS sends the deployment tasks to the Distribution Host (DH).

7. The endpoint, which periodically checks for new policy deployment tasks (using policyfetcher), fetches the pending deployment tasks from the DH and executes each rule-the selang commands specified in the deployment script-on the target databases.

8. The endpoint updates the DH with the deployment task status (failed, success), the resultant selang result messages for failed commands, and the policy status on the HNODE.

   Note: If a policy is deployed with errors, you can use Deployment Audit in CA Access Control Enterprise Management to detail the selang output for the failed commands. Otherwise, you need to view the log file on the computer where the policy was deployed with errors.

9. The DH updates the deployment task status and policy status on the DMS, where this information is stored.

Note: UNAB login policies and UNAB config policies do not work in the same way as advanced policy-based management.

More information:

Policy Dependency (see page 82)
Policy Verification (see page 82)
Assignment Paths (see page 79)
How You Control Host Access and Configure UNAB (see page 269)

How Deployment Methods Affect Deployment Tasks

When you deploy a stored policy to target databases, CA Access Control creates deployment tasks automatically on the DMS. A deployment task (a DEPLOYMENT object) is a work order, generated by the DMS for execution on the endpoint. Each deployment task is intended for one endpoint and contains information about the policy version that needs to be deployed on the endpoint.

Note: CA Access Control uses a different deployment method to deploy UNAB login and config policies.

The method you use to deploy the stored policy affects the deployment tasks that CA Access Control creates. The following shows the results of choosing different methods:

- Assign a policy (GPOLICY object) to one or more hosts

  CA Access Control creates, for each host, a deployment task for the latest finalized version of the policy.

- Assign a policy (GPOLICY object) to one or more host groups

  CA Access Control creates, for each host that is a member of one of the host groups, a deployment task for the latest finalized version of the policy.

- Add a host to a host group that has stored policies (GPOLICY objects) assigned to it

  CA Access Control creates for the new host a deployment task for the latest finalized version of the policy.

- Redeploy a policy to a host

  CA Access Control creates, for the host, a deployment task for the latest finalized version of the policy.

- Restore the policies on an HNODE (redeploy the policies that should be deployed on the host)

  CA Access Control creates, for each policy that should be deployed on the host, a deployment task for the policy version that is effective on the host.

- Upgrade a deployed policy on one or more hosts

  CA Access Control creates, for each host, a deployment task for the latest finalized policy version if the version stored on the host is newer than the one that is deployed on the host.

Example: Assign a Policy to a Host

If you assign policy IIS to hosts host1.comp.com and host2.comp.com, CA Access Control creates two deployment tasks: a task to deploy the latest IIS policy version on host1.comp.com and a task to deploy the latest IIS policy version on host2.comp.com.

Example: Assign a Policy to a Host Group

The host group Servers has two members: hostA.comp.com and hostB.comp.com. If you assign policy IIS to the host group Servers, CA Access Control creates two deployment tasks: a task to deploy the latest IIS policy version on hostA.comp.com and a task to deploy the latest IIS policy version on hostB.comp.com.

Example: Add a Host to a Host Group That Has Assigned Policies

The host group Servers has two assigned policies (IIS and ORACLE). If you add host test.comp.com to the host group, CA Access Control creates two deployment tasks: a task to deploy the latest IIS policy version on test.comp.com and a task to deploy the latest ORACLE policy version on test.comp.com.

Example: Restore a Host

A host has two policies assigned: policy1 and policy2. If you restore the host, CA Access Control creates two deployment tasks: a task to deploy the latest finalized policy1 version and a task to deploy the latest finalized policy2 version on the host.

Example: Upgrade a Deployed Policy

Policy IIS is deployed on two hosts, host1.comp.com and host2.comp.com, but the latest version of policy IIS is not deployed to host1.comp.com. If you upgrade policy IIS on both hosts, CA Access Control creates only one deployment task to deploy the latest IIS policy version on host1.comp.com.

More information:

How You Control Host Access and Configure UNAB (see page 269)

Endpoint Data That the DMS Holds

When you configure your environment for advanced policy management, endpoints in your enterprise notify the DMS, through the configured DHs, of status changes in three areas:

- Policy deployment and undeployment

  When a policy is being deployed or undeployed, the endpoint sends a notification. The following details are then updated according to the result of the operation:

  - Policy details
  - Deployment status (succeeded, failed, and so on)
  - The selang command output for policy commands that failed to execute
  - HNODE policy status (deployed, deployment failed, and so on)

- Host heartbeat

  At regular configurable intervals, each endpoint sends a heartbeat to account for the host being online.

- Deviation status

  After each heartbeat, the endpoint calculates policy deviation, and sends the result (deviation found or not found).

  Note: If the policyfetcher finds deployment and deviation status conflicts between the endpoint and the DH, resolve the conflicts based on the information that you received from the endpoint .

How Endpoints Update the DMS

Each endpoint sends a heartbeat (host status), policy status, and deviation status notifications to the DMS, through the DHs you configured. Those DMS notifications are handled in the following way:

1. The DH stores notification messages in an update file.

   These are heartbeats and policy deployment and undeployment notifications from the endpoint.

2. The DH contacts the DMS, which is its subscriber:

   - If a DMS is unavailable, the DH tries to communicate with the DMS periodically, until all messages are successfully sent.
   - If the DMS is available, the DH sends the stored notifications.

3. The DMS stores the information it receives from each DH for later use.

   Each time you create a report, CA Access Control retrieves the information from the DMS.

Note: UNAB endpoints use a different process to update the DMS.

More information:

How You Control Host Access and Configure UNAB (see page 269)

Advanced Policy Management Classes

CA Access Control uses specific classes that let the DMS:

- Keep an up-to-date map of the status of policies deployed on each computer
- Send deployment information to a DH so that the endpoint can fetch the relevant policy deployment information it should contain

Note: For more information about the properties these classes contain, see the *selang Reference Guide*.

DEPLOYMENT Class

Each object in the DEPLOYMENT class represents a policy *deployment task*. CA Access Control creates the deployment task automatically on the DMS when you assign or unassign a policy to a host, or when you directly deploy or undeploy a policy. It is also created when you add (assign) or remove (unassign) a host to or from a host group that has assigned policies, downgrade or upgrade a policy on a host, and reset or restore a host.

Endpoints use this object as a work order: they deploy or undeploy policy versions based on the information in a pending DEPLOYMENT object. Each work order is intended for one endpoint and contains information about the policy version that needs to be deployed on the endpoint. In addition, the DEPLOYMENT object has a status property which indicates whether deployment was successful or not and a result property (result_message) which contains the selang command output from the policy deployment task.

Note: A deployment task can be empty (has no action status) if the policy already exists on the HNODE as a result of another assignment path.

More information:

Assign a Stored Policy Version (see page 90)
Unassign an Assigned Policy (see page 91)
Upgrade Assigned Hosts to the Latest Policy Version (see page 92)
Downgrade Assigned Hosts to a Particular Policy Version (see page 92)

GDEPLOYMENT Class

Each object in the GDEPLOYMENT class represents a *deployment package*. A deployment package is created automatically on the DMS and groups together all the deployment tasks that are created as a result of the same transaction (policy assignment, upgrade, and so on) and for a particular host. This means that each transaction you make creates the required number of deployment tasks (DEPLOYMENT objects) and groups these by host (GDEPLOYMENT objects).

A deployment package lets you track and troubleshoot policy deployment and records the trigger-the reason why the deployment was initiated.

HNODE Class

Each object in the HNODE class represents an endpoint in your enterprise. It holds information about the particular node it represents, the host groups it belongs to, and when it was last detected online. In addition, each HNODE object holds information about the policy versions that are effective on node it represents (through direct or indirect assignment), and the status of each policy (deployed, deployed with errors, and so on).

The name of the HNODE object is the actual host name. For example, myhost.mydomain.com

GHNODE Class

Each object in the GHNODE class represents a group of CA Access Control nodes (HNODE object). It lets you group endpoints into logical groups for the purpose of deploying policies. Each GHNODE object holds information about the policies that are assigned to the nodes it represents.

POLICY Class

Each object in the POLICY class represents a version of a policy (GPOLICY object) that may be deployed on any host (HNODE object) or logical group of hosts (GHNODE object). It contains information about where the associated policy scripts are stored (in which RULESET object) and which nodes or group of nodes it is deployed on.

The name of the object is the name of the policy, suffixed by a version number *(policy_name#xx*).

GPOLICY Class

Each object in the GPOLICY class represents a logical policy. It contains information about the policy versions (POLICY objects) that belong to this policy and the hosts and host groups it is assigned to.

The name of the object is the name of the logical policy.

RULESET Class

Each object in the RULESET class holds both the deployment and undeployment (removal) scripts that are associated with a policy version.

The name of the object is based on the respective POLICY object name.

Hosts and Host Groups

To use advanced policy management, you need to define your enterprise implementation of CA Access Control. To do this, you create HNODE objects to represent endpoints (or hosts) and GHNODE objects to represent logical host groups. Hosts can be members of a number of logical host groups depending on their properties and policy demands. For example, if you have hosts running a Red Hat operating system and Oracle, these can be members of a Red Hat logical host group to get the baseline Red Hat access control policy, and also members of the Oracle logical host group to get the Oracle access control policy.

Define an Endpoint as a Host in Your Enterprise

To deploy policies to your endpoints and to view their deployment status, you need to define your endpoints on the Deployment Map Server (DMS) you manage your enterprise through. When you install CA Access Control on the endpoint with advanced policy management enabled, an HNODE record that represents the endpoint is automatically created on the DMS. You should manually define your endpoints on the DMS only if you want to model the environment before installing CA Access Control on endpoints.

Important! You must use the fully qualified host name as HNODE name, otherwise the endpoint does not collect its deployments.

To define an endpoint as a host in your enterprise

1. In CA Access Control Enterprise Management click Policy Management, then Host subtab, and expand the Host tree in the task menu on the left.

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

2. Click Create Host.

   The Create Host: Host Search screen appears.

3. Verify that Create a new object of type Host is selected and click OK.

   The Create Host task page appears.

4. Complete the following fields in the dialog:

   Name

   Defines the name of the endpoint (HNODE object). This name has to be unique on the DMS (enforced).

   Description

   (Optional) Defines a business description (free text) of the host. Use this field to record any information that helps you identify the endpoint.

   IP address

   (Optional) Defines the IP address of the host.

5. Click Submit.

   The task is submitted and if successful, a message indicating that a new host (HNODE) was created appears shortly afterwards.

How Automatic Host Group Assignment Works

If you install CA Access Control with advanced policy management enabled on your endpoints, CA Access Control Enterprise Management automatically assigns hosts to host groups. CA Access Control Enterprise Management assigns hosts to host groups based on criteria such as host type, operating system, the installed version of CA Access Control, or any other common attributes that you define. You can then assign policies to the host groups.

Note: When you install CA Access Control on a Linux endpoint, that endpoint is automatically assigned to the "All Linux Hosts" host group. If you install UNAB on that endpoint, it is also automatically assigned to the "All UNAB Hosts" host group.

CA Access Control Enterprise Management automatically assigns hosts to host groups in the following way:

1. An endpoint, with advanced policy management configured, sends a heartbeat to the Enterprise Management Server.

   The heartbeat contains information about the endpoint attributes.

2. The Enterprise Management Server evaluates the endpoint attributes against the host group assignment criteria, and assigns the host to the appropriate host groups.

You can use World View to view the hosts assigned to each host group.

Default Out-of-the-Box Host Groups

The following table lists the default out-of-the-box host groups in CA Access Control Enterprise Management:

Host Group Name	Description
AIX 5.2	The default host group for all AIX 5.2 hosts
AIX 5.3	The default host group for all AIX 5.3 hosts
AIX 6.1	The default host group for all AIX 6.1 hosts
All Linux Hosts	The default host group for all Linux hosts
All UNAB Hosts	The default host group for all UNIX hosts
All Windows Hosts	The default host group for all Windows hosts
ESX Server 3.x	The default host group for all ESX Server 3.x hosts
ESX Server 4.x	The default host group for all ESX Server 4.x hosts
HP-UX 11.23	The default host group for all HP-UX 11.23 hosts
HP-UX 11.31	The default host group for all HP-UX 11.31 hosts
RedHat 3	The default host group for all RedHat 3 hosts
RedHat 4	The default host group for all RedHat 4 hosts
RedHat 5	The default host group for all RedHat 5 hosts
SLES 9	The default host group for all SLES 9 hosts
SLES 10	The default host group for all SLES 10 hosts
SELS 11	The default host group for all SLES 11 hosts
Solaris 8	The default host group for all Solaris 8 hosts
Solaris 9	The default host group for all Solaris 9 hosts
Solaris 10	The default host group for all Solaris 10 hosts
Windows Server 2003	The default host group for all Windows Server 2003 hosts
Windows Server 2003 R2	The default host group for all Windows Server 2003 R2 hosts
Windows Server 2008	The default host group for all Windows Server 2008 hosts

Host Group Name	Description
Windows Server 2008 R2	The default host group for all Windows Server 2008 R2 hosts

Modify the Automatic Host Group Assignment Criteria

CA Access Control Enterprise Management automatically assigns hosts to host groups using predefined criteria, for example, operating system type. By default, CA Access Control Enterprise Management automatically adds each host to the host groups that correspond to the host operating system. For example, CA Access Control Enterprise Management automatically assigns a Windows Server 2003 R2 host to the All Windows hosts and Windows Server 2003 R2 host groups. You can specify additional criteria that CA Access Control Enterprise Management uses to automatically assign hosts to host groups.

To modify the automatic host group assignment criteria

1. Open a selang window on the Enterprise Management Server and connect to the DMS.
2. Edit the host group and specify the assignment criteria, using the following selang commands:

```
editres GHNODE host_group_name criteria+(attribute=value)

editres GHNODE host_group_name criteria+(attribute!=value)

editres GHNODE host_group_name criteria+(attribute=value)&&(attribute=value)

editres GHNODE host_group_name criteria+(attribute1=value1)

editres GHNODE host_group_name criteria+(attribute2=value2)

editres GHNODE host_group_name criteria-(attribute=value)
```

host_group_name

Specifies the name of the host group that you assign this criteria to.

attribute=value

Specifies the host group assignment attribute and values. This parameter can have the following values:

HNODE_IP=*IP_address*

Specifies that CA Access Control Enterprise Management adds the defined IP address to the host group assignment criteria.

Example: HNODE_IP=172.24.123.456

NODE_TYPE={AC Windows | AC UNIX | AC UNAB}

Specifies that CA Access Control Enterprise Management adds the specified endpoint type to the host group assignment criteria.

HNODE_VERSION={ACW | ACU | ACUNAB}:*version*

Specifies that CA Access Control Enterprise Management adds the defined endpoint version to the host group assignment criteria.

Example: HNODE_VERSION=ACW:12.53

This example specifies that CA Access Control Enterprise Management adds CA Access Control Windows endpoints of version 12.53.1178 to the host group assignment criteria.

ATTRIBUTES=("*attribute*")

Specifies that CA Access Control Enterprise Management adds the defined attribute information to the host group assignment criteria.

Example: ATTRIBUTES=(Microsoft_Windows_Server_2003_R2)

Note: You can specify asterisks in the value field.

You have modified the assignment criteria of the host group that you specified.

Example: Assign hosts to group by version

In this example, you modify the assignment criteria of a host group named All Windows 12.53 Hosts to automatically assign only those Windows hosts that you installed CA Access Control version 12.53 on:

```
editres GHNODE ("All Windows 12.53 hosts") criteria+(HNODE_VERSION=ACW:12.53)
```

Example: Assign hosts to group by type and version

In this example, you modify the assignment criteria of a host group named All UNIX hosts to automatically assign hosts by their type (ACUNIX) and CA Access Control version:

```
editres GHNODE ("All UNIX hosts") criteria+(NODE_TYPE=AC
UNIX&&HNODE_VERSION=ACU:12.53)
```

Example: Assign hosts to group by type or version

In this example, you modify the assignment criteria of a host group named All UNAB Hosts to automatically assign hosts by type (UNAB) or UNAB version:

```
editres GHNODE ("All UNAB Hosts") criteria+(NODE_TYPE=ACUNAB)
editres GHNODE ("All UNAB Hosts") criteria+(HNODE_VERSION=ACUNAB:12.53)
```

Example: Exclude hosts by type

In this example, you modify the assignment criteria of a host group named Non UNIX Hosts to automatically exclude all hosts of type AC UNIX:

```
editres GHNODE ("Non UNIX Hosts") criteria+(NODE_TYPE!=AC UNIX)
```

Example: Remove assigned criteria

In this example, you remove the assigned NODE_TYPE criteria that you previously assigned to the host group named All Windows Hosts:

```
editres GHNODE ("All Windows Hosts") criteria-(NODE_TYPE=AC Windows)
```

Note: To display the valid attributes of a host, you can view the DMS audit file and locate the host heartbeats. Use the seaudit -a -fn pmd.audit command to display the DMS audit file.

Define a Logical Host Group

To manage policies on a group of related endpoints, you can define the endpoints as a logical host group and perform advanced policy management actions on the whole group. Before you can create meaningful host groups, you must have your endpoints defined on the DMS.

Note: This procedure describes how you use CA Access Control Enterprise Management to define a logical host group on the DMS.

To define a logical host group

1. In CA Access Control Enterprise Management click Policy Management, then Host subtab, and expand the Host Group tree in the task menu on the left.

   The Create Host Group appears in the list of available tasks.

2. Click Create Host Group.

   The Create Host Group: Host Group Search screen appears.

3. Verify that Create a new object of type Host Group is selected and click OK.

   The Create Host Group task page appears.

4. Complete the following fields in the dialog:

   Name

   Defines the name of the logical host group (GHNODE object).

   Description

   (Optional) Defines a business description (free text) of the host group. Use this field to record any information that helps you identify the host group.

5. Click the Host Selection, then click Add.

   The Add Member dialog appears.

6. Select the endpoints you want to add to the host group, then click Select

   The Add Member dialog closes and the endpoints you selected are added to the Members List for the logical group host you are defining.

7. Click Submit.

   The task is submitted and if successful, a message indicating that a new group host (GHNODE) was created appears shortly afterwards.

Import a Host Group

Importing a host group helps you migrate your existing PMDB structure to advanced policy management. When you import a host group, you create or join hosts to a host group. The hosts correspond to the subscribers of a PMDB.

Note: Advanced policy management does not support hierarchical host groups. When you import a host group from a PMDB, you flatten all subscribers into the same host group. CA Access Control Enterprise Management does not create hosts that correspond to subscriber PMDBs.

For each PMDB subscriber that you join to the host group, CA Access Control Enterprise Management checks if a host (HNODE object) that corresponds to the subscriber already exists on the DMS. If a corresponding host exists on the DMS, CA Access Control adds that host to the host group. If a corresponding host does not exist on the DMS, CA Access Control creates a new host and adds the new host to the host group.

If you do not have permission to access an endpoint, the endpoint does not appear in the wizard and you cannot add the corresponding host to the host group.

To import a host group

1. In CA Access Control Enterprise Management, do as follows:

   a. Click Policy Management.

   b. Click Host subtab.

   c. Expand the Host Group tree in the task menu on the left.

      The Host Group Import task appears in the list of available tasks.

2. Click Host Group Import.

   The PMDB Host Login page appears.

3. Type the user name, password, and name of the PMDB, and click Log In.

   Note: Specify the PMDB name in the format *PMDBname@host*, for example, master_pmdb@example

   The Host Group Import wizard appears at the General task stage.

4. Complete the wizard, then click Finish after you read the summary.

   CA Access Control adds the hosts to the host group. If a host does not exist in the DMS, CA Access Control creates a HNODE object for the host before it adds it to the host group (GHNODE).

   Note: When you add a host to an existing host group, CA Access Control automatically deploys to the host any policies that are assigned to the host group.

Assignment Paths

An *assignment path* describes a policy assignment to a specific host or host group. A policy can be assigned to a host by the following paths:

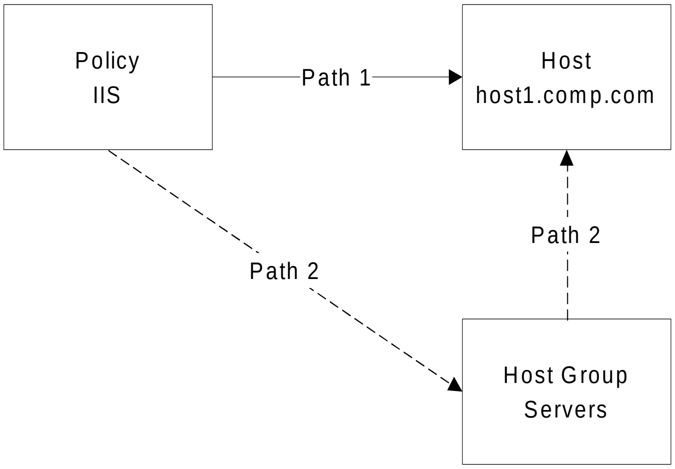
- A policy is directly assigned to a host.
- A policy is assigned to a host group of which a host is a member.
- A host is joined to a host group that has one or more policies assigned to it.

Assignment paths are important because when multiple assignment paths exist it impacts advanced policy management, as follows:

- If you remove an assignment path, CA Access Control does not undeploy the policy because the other assignment paths between the host and the policy still exist.
- If you add an assignment path, a deployment package and deployment tasks are created for tracking and administrative purposes. However, the deployment task has the status of *No Action*, and so does not initiate policy deployment on the endpoint.

Example: Multiple Assignment Paths for Policy IIS

The following illustration shows an example of multiple assignment paths for policy IIS. Host host1.comp.com is a member of the host group Servers. Path 1 shows the assignment path when you directly assign policy IIS to the host host1.comp.com. Path 2 shows the assignment path when you assign policy IIS to the host group Servers:



Example: Remove an Assignment Path

In the previous illustration, policy IIS is assigned to the host group Servers and to the host host1.comp.com. If you remove host1.comp.com from the Servers host group, you remove Path 2. However, CA Access Control does not undeploy policy IIS from host1.comp.com, because the policy is still directly assigned to the host (Path 1).

How to Create and Deploy a Policy

Using advanced policy-based management you can store a draft version of a policy, have it reviewed and modified as required, then deploy the approved version.

To deploy approved policy versions using CA Access Control Enterprise Management, do the following:

1. Store a policy version on the DMS.

   Once you have a stored policy version, the policy can be reviewed and deployed.

2. Review the policy.

   Once the policy version is stored, you should have the rules associated with the policy reviewed.

3. Finalize the policy.

   Once you finalize a policy, you can assign it to the hosts or host groups where you want it to be deployed.

4. Assign the policy to endpoints through one of the available assignment paths:

   - Assign the stored policy to a host or host group.
   - Assign a host to a logical group of hosts that already has the policy assigned.

   Once a policy is assigned, CA Access Control works to deploy the latest finalized version of the policy automatically.

Note: You follow a different process to create and deploy UNAB login and config policies.

More information:

Manage UNAB Login Authorization (see page 270)
Configure a UNAB Host or Host Group (see page 271)
Assignment Paths (see page 79)

Administration Requirements

To store policies on the DMS or assign these policies you, and the computer you are working from, need to have appropriate permissions.

To store policies on the DMS:

- The *computer* from which you are managing the DMS from, or the one you are running the policydeploy utility from, needs to have terminal rights (TERMINAL class) for the DMS.
- *You* need to have sub-administration rights for the POLICY, GPOLICY, and RULESET classes on the DMS.

To assign policies to hosts or host groups:

- The *computer* from which you are managing the DMS from needs to have terminal rights (TERMINAL class) for the DMS.
- *You* need to have sub-administration rights for the DEPLOYMENT, GDEPLOYMENT, POLICY, GPOLICY, HNODE, and GHNODE (if you assign the policy to a host group) classes on the DMS.

Note: For more information about terminal rights and sub-administration rights, see the *Endpoint Administration Guide for UNIX* and the *Endpoint Administration Guide for Windows*.

Policy Dependency

Advanced policy management lets you enforce the order in which policies are deployed and undeployed.

Using policy dependency you can define that a policy that is dependent on one or more other policies, cannot be deployed until all of the prerequisite policies are also deployed. Similarly, you cannot undeploy a prerequisite policy if one or more dependent policies are still deployed.

You define policy dependency when you create or modify a policy.

Policy Verification

When policy verification is enabled, CA Access Control checks that a policy does not contain errors before it deploys the policy. If CA Access Control finds errors in the policy deployment script, the policy script does not execute on the endpoint. This ensures that policies do not deploy with errors and lets you trace script errors on the endpoint. Policy verification is disabled by default.

If policy verification is not enabled and you deploy a policy with errors, some policy commands may still execute despite the errors in other commands.

Policy verification checks CA Access Control database commands only, that is, selang commands in the AC environment. Policy verification does not check commands in the native, configuration, or policy model environments. If a policy contains commands for both the AC environment and another environment, policy verification checks commands in the AC environment only.

Policy verification cannot check undeploy scripts.

How Policy Verification Works

Policy verification verifies that a policy can deploy without errors before it actually deploys on the endpoint.

Note: Policy verification is not enabled by default.

The following process describes how policy verification works:

1. You assign a policy to a host or host group.
2. On each endpoint, CA Access Control Enterprise Management verifies the policy.
3. *One* of the following happens:
   - If the policy does not contain errors, CA Access Control Enterprise Management deploys the policy to the endpoint.

     The endpoint updates the DMS that the policy status is *Deployed*.
   - If the policy script contains an error, CA Access Control Enterprise Management does *not* deploy the policy to the endpoint.

     The endpoint updates the DMS that the policy status is *Not executed*. The DMS also updates the status of each deployment task that corresponds to the policy with the script error to *Fail*.

     Note: You can use the Deployment Audit feature in CA Access Control Enterprise Management to view the scripts with errors.

Enable Policy Verification

Policy verification ensures that a policy can deploy without errors before it actually deploys on the endpoint.

To enable policy verification, set the value of the policy_verification configuration setting in the policyfetcher section to 1.

Policy verification is enabled.

Create and Store a Policy Version

Every policy you create and store on the DMS automatically gets a version number. The first time you store a policy it receives a version number "01". For example, the first time you store policy *myPolicy*, CA Access Control Enterprise Management creates a GPOLICY object named *myPolicy* and a POLICY object named *myPolicy#01*. Every time you store a policy that already exists on the DMS, the latest stored version of the policy is incremented by one to create the new policy version. For example, when you store a version of *myPolicy* for the twenty-eighth time, CA Access Control Enterprise Management creates a POLICY object named *myPolicy#28*.

Note: This procedure describes how you use CA Access Control Enterprise Management to create and store a policy version. This procedure does not apply to UNAB login and configuration policies.

To create and store a policy version

1. (Optional) Create a new script file with selang deployment commands.

   These are the commands necessary to construct the policy you want to deploy on endpoints in your enterprise.

   Important! Policy deployment does not support commands that set user passwords. Do not include such commands in your deployment script file. Native selang commands are supported but will not show in deviation reports.

2. (Optional) Create a new script file with selang undeployment commands.

   These are the commands necessary for undeploying (removing) the policy from endpoints in your enterprise.

3. In CA Access Control Enterprise Management click Policy Management, Policy task, and expand the Policy tree in the task menu on the left.

   The Policy tasks appear.

4. Click Create Policy.

   The Create Policy: Policy Search screen appears.

   Note: If you want to create a new version for an existing policy, click Modify Policy instead and search for the policy you want to modify.

5. Click OK.

   The Create Policy task page appears.

6. Complete the following fields in the dialog:

   Name

   Defines the name of the policy (GPOLICY object). This name has to be unique on the DMS (enforced) and in your enterprise (not enforced but you will not be able to deploy a policy to a host if a policy of the same name already exists).

   Description

   (Optional) Defines a business description (free text) of the policy. Use this field to record what this policy is for and any other information that helps you identify the policy.

7. Click the Policy Script tab and provide a deployment and an undeployment script, using *one* of the following methods:

   - Type the deployment and undeployment scripts into the appropriate fields.

     Use this option if you did not create a script file with the deployment commands.

   - Load the commands from an existing selang script file:

     a. Click Browse and locate the file that contains the selang script you want to use.

     b. Click Load to populate the script field with the contents of the file you selected.

8. (Optional) Provide a description for this policy version.

   Use this to provide specific information about the deployment scripts you use for this policy version.

9. (Optional) Select Finalize on Submit.

   This option specifies that the new policy version you create can be deployed. If you are not finished creating the deployment script, clear this option.

   Note: If you do not select this option, you can modify the deployment scripts without creating a new version of the policy. However, a non-finalized policy version cannot be deployed.

10. Click the Policy Dependency tab, then click Add.

    The Add Member dialog appears.

11. Select the policies you want to add as prerequisites to the policy, then click Select.

    The Add Member dialog closes and the policies you selected are added to the Members List for the policy you are creating.

12. Click Submit.

    The task is submitted and, if successful, a message indicating that a new policy version was created appears shortly afterwards. You follow a different process to create and deploy UNAB login and configuration policies.

Note: You can also use the policydeploy utility to perform this task. For more information about the policydeploy utility, see the *Reference Guide*.

More information:

Manage UNAB Login Authorization (see page 270)
Configure a UNAB Host or Host Group (see page 271)

Create a Policy That Defines a Variable

Creating and deploying a policy that defines a variable lets you define the same variable on many endpoints.

To create a policy that defines a variable

1. Create a script file with selang deployment commands that define the variables. Use the following selang command to define each variable:

   ```
   editres ACVAR ("variable_name") value("variable_value")
   ```

2. (Optional) Add selang commands that use the variable to the script file.

   Note: You must define each variable in the policy before you refer to it in a subsequent rule in the policy. Use the following format to refer to the variable: "<!*variable*>"

3. Store the policy on the DMS.

Example: Create a Policy That Defines a Variable

In this example, the following policy defines a variable named jboss_home that has a value of /opt/jboss, and creates a rule that authorizes user Mark to access any resource in the /opt directory that accesses through JBoss.

```
editres ACVAR ("jboss_home") value("/opt/jboss")
authorize FILE /opt/* uid(Mark) access(all) via(pgm("<!jboss_home>/jboss"))
```

When the endpoint compiles the policy, it creates the following rule:

```
authorize FILE /opt/* uid(Mark) access(all) via(pgm(/opt/jboss/jboss))
```

Example: Create a Policy That Defines Multiple Variable Values

The following policy defines a variable named jboss_home that has a value of C:\JBoss, adds the C:\Program Files\JBoss value to the jboss_home variable, and creates an access rule:

```
editres ACVAR ("jboss_home") value("C:\JBoss")
editres ACVAR ("jboss_home") value+("C:\Program Files\JBoss")
editres FILE ("<!jboss_home>\bin") defacc(none) audit(a)
```

When the endpoint compiles the policy, it creates the following rules:

```
editres FILE ("C:\JBoss\bin") defacc(none) audit(a)
editres FILE ("C:\Program Files\JBoss\bin") defacc(none) audit(a)
```

Example: Use Variables to Deploy the Same Policy to Windows and UNIX Endpoints

The following example explains how you can use variables to deploy the same JBoss policy to Windows and UNIX endpoints, despite the different JBoss installation location on each operating system. This example defines two jboss_home variables that define the JBoss installation location for each operating system:

1. Define two jboss_home variables that define the JBoss installation location for each operating system.

   - Create a policy that defines the JBoss installation location for Windows and deploy the policy to Windows endpoints:

     ```
     editres ACVAR ("jboss_home") value("C:\JBoss")
     ```

   - Create a policy that defines the JBoss installation location for UNIX and deploy the policy to UNIX endpoints:

     ```
     editres ACVAR ("jboss_home") value("/opt/jboss")
     ```

2. Create a policy that uses the jboss_home variable to protect the JBoss installation location, and deploy the policy to Windows and UNIX endpoints:

   ```
   editres FILE "<!jboss_home>" defacc(none) audit(all)
   ```

   - When a Windows endpoint compiles the policy it creates the following rule:

     ```
     editres FILE "C:\JBoss" defacc(none) audit(all)
     ```

   - When a UNIX endpoint compiles the policy it creates the following rule:

     ```
     editres FILE "/opt/jboss" defacc(none) audit(all)
     ```

View the Rules Associated with a Policy

Once a policy is stored on the DMS, you can view the rules in the deploy and undeploy scripts for each policy version.

To view the rules associated with a policy

1. In CA Access Control Enterprise Management click Policy Management, then Policy subtab, and expand the Policy tree in the task menu on the left.

   The Policy tasks appear.

2. Click View Policy.

   The View Policy: Policy Search screen appears.

3. Define a scope for the search, then click Search.

   A list of policies, which match the scope of the search you defined, appears.

4. Select the policy you want to view, then click Select.

   The View Policy: *policyName* page appears. On the various tabs you can view the properties of the policy including, its name and description, deployment and undeployment scripts for the latest version, a list of all policy versions that exist for this policy, any policy dependencies, and generic information about the policy creation and update events.

5. Click the Version History tab.

   A list of policy versions appears, each with a link to a deployment and undeployment script.

6. Do either of the following:

   - Click the Deploy Script link.

     A pop-up window with the deployment script appears.

   - Click the UnDeploy Script link.

     A pop-up window with the undeployment script appears.

Note: You can also use the policydeploy utility to perform this task. For more information about the policydeploy utility, see the *Reference Guide*.

Import a Policy

When you import a policy, CA Access Control Enterprise Management exports the selang rules from a local CA Access Control database or PMDB, and creates and stores a policy that contains the rules on the DMS. This lets you convert the rules that protect an endpoint into a policy that can protect many endpoints, and helps you migrate a PMDB to advanced policy management.

Note: The endpoint or PMDB from which you export the rules must be on a host that has CA Access Control r12.0, or later, installed. To import a policy from earlier CA Access Control versions, upgrade the endpoint first.

To import a policy

1. In CA Access Control Enterprise Management, do as follows:

    a. Click Policy Management.

    b. Click Policy subtab.

    c. Expand the Policy tree in the task menu on the left.

       The Policy Import task appears in the list of available tasks.

2. Click Policy Import.

   The Host Login page appears.

3. Type the user name, password, and name of the PMDB or host that you want to export the rules from, and click Log In.

   Note: Specify the PMDB name in the format *PMDBname@host*, for example, master_pmdb@example

   The Policy Import Process wizard appears at the General task stage.

4. Complete the following fields, and click Next:

   Name

   Defines the name of the policy. The name must be unique on the DMS (enforced) and in your enterprise (not enforced but you will not be able to deploy a policy to a host if a policy of the same name already exists).

   Description

   (Optional) Defines a business description (free text) of the policy. Use this field to record what this policy is for and any other information that helps you identify the policy.

Policy Classes

Specifies the classes whose rules you want to export for inclusion in the policy. If you do not specify any classes in the Selected List column, all classes are exported and included in the policy.

Export dependent classes

Specifies to export all the classes that are dependent on the classes that you specify in the Selected List column. If you do not select this option, CA Access Control exports only the classes that you specify in the Selected List column.

The Policy Script stage appears.

5. Review the exported rules and modify them as necessary, and click Next.

   The Summary stage appears.

6. Click Finish.

   The policy is created.

Assign a Stored Policy Version

You can assign the latest finalized version of a policy to specific hosts or to host groups. Assigned policies are automatically deployed and you can monitor their status from the DMS.

Note: This procedure does not apply to login and configuration policies.

To assign a stored policy version

1. In CA Access Control Enterprise Management click Policy Management, then Policy subtab, expand the Assignment tree in the task menu on the left, and click Assign Policy.

   The Assign Policy wizard appears at the Policy Selection task stage.

2. Complete the wizard, then click Finish after you read the summary.

   CA Access Control submits the policy assignment task. Once a policy is assigned to hosts (directly or through a logical host group membership), CA Access Control creates DEPLOYMENT tasks for each host to retrieve.

Note: You can also use the policydeploy utility to perform this task. For more information about the policydeploy utility, see the *Reference Guide*.

Policy Maintenance

You can perform the following actions on a deployed policy:

- Unassign the policy from an assigned host
- Upgrade a host to the latest policy version
- Downgrade a host to an earlier policy version
- Verify that the policy is deployed without errors
- Delete a policy or a policy version

You perform these actions in CA Access Control Enterprise Management or using the policydeploy utility.

Unassign an Assigned Policy

You can unassign an assigned policy from specific hosts or to host groups. Unassigned policies are automatically undeployed.

To unassign an assigned policy

1. In CA Access Control Enterprise Management click Policy Management, then Policy subtab, expand the Assignment tree in the task menu on the left, and click UnAssign Policy.

   The UnAssign Policy wizard appears at the Policy Selection task stage.

2. Complete the wizard, then click Finish after you read the summary.

   CA Access Control submits the policy assignment task. Once a policy is unassigned from hosts (directly or through a logical host group membership), CA Access Control creates DEPLOYMENT tasks for each host to retrieve.

Note: You can also use the policydeploy utility to perform this task. For more information about the policydeploy utility, see the *Reference Guide*.

Upgrade Assigned Hosts to the Latest Policy Version

New policy versions are not sent automatically to assigned hosts or to hosts where the policy is deployed. You need to manually upgrade hosts where the policy is deployed to the latest policy version.

To upgrade assigned hosts to the latest policy version

1. In CA Access Control Enterprise Management click Policy Management, then Policy subtab, expand the Assignment tree in the task menu on the left, and click Upgrade Policy.

   The Upgrade Policy wizard appears at the Policy Selection task stage.

2. Complete the wizard, then click Finish after you read the summary.

   CA Access Control submits the policy upgrade task. For the policy to be upgraded on a host, CA Access Control creates a DEPLOYMENT task for the host to retrieve.

   Note: When you select host groups to upgrade, CA Access Control Enterprise Management lets you choose from only those host groups that contain hosts that have an older version of the policy deployed.

Note: You can also use the policydeploy utility to perform this task. For more information about the policydeploy utility, see the *Reference Guide*.

Downgrade Assigned Hosts to a Particular Policy Version

If you inadvertently assigned the wrong policy version to one or more hosts, or if you want to go back to an older version of a policy on specific hosts, you can downgrade a policy.

To downgrade assigned hosts to a particular policy version

1. In CA Access Control Enterprise Management click Policy Management, then Policy subtab, expand the Assignment tree in the task menu on the left, and click Downgrade Policy.

   The Downgrade Policy wizard appears at the Policy Selection task stage.

2. Complete the wizard, then click Finish after you read the summary.

   CA Access Control submits the policy downgrade task. For the policy to be downgraded on a host, CA Access Control creates a DEPLOYMENT task for the host to retrieve.

Note: You can also use the policydeploy utility to perform this task. For more information about the policydeploy utility, see the *Reference Guide*.

Deleted Policies

You can delete a logical policy (GPOLICY object) or a policy version (POLICY object) from the DMS. When you delete a policy version, CA Access Control Enterprise Management also deletes the deployment and undeployment scripts (RULESET object) associated with the policy version. When you delete a logical policy, you delete every policy version associated with the logical policy, and their associated scripts.

You cannot restore a deleted logical policy or policy version.

Policies That You Cannot Delete

You cannot delete a policy if:

- One or more of the policy's policy versions cannot be deleted.
- The policy is a prerequisite for another policy.

  You must remove any dependencies on a policy before you delete the policy.
- The policy is assigned or deployed on a host.

  You must unassign or undeploy the policy from the host before you delete the policy.

Policy Versions That You Cannot Delete

You cannot delete a policy version if any of the following are true:

- The policy version is effective (assigned or deployed) on a host.

  You must unassign or undeploy the policy version from the host before you delete the policy version.
- The policy version has a status on the DMS.

  You must unassign or undeploy the policy version from the host before you delete the policy version. If you cannot unassign or undeploy the policy version, you must manually remove it from the host.
- The policy has a status of Undeployed with failures.

  You must remove this status before you delete the policy version.

Examples: Policy Versions That You Cannot Delete

The following are examples of policy versions that you cannot delete, because they have a status on the DMS but are not effective on the host:

- Deployed with Failures
- Not Executed

In both these cases, you must manually remove the policy version from the host before you delete the policy version.

Note: For more information about policy status on hosts (HNODEs), see the *Reference Guide*. For more information about removing the status of policy versions, see the *Troubleshooting Guide*.

Delete a Policy

You can delete a policy from CA Access Control Enterprise Management when the policy is no longer assigned to a host or host group.

Important! When you delete a policy (GPOLICY object), CA Access Control Enterprise Management deletes all its policy versions (POLICY objects) and the RULESET object associated with each policy version.

To delete a policy

1. In CA Access Control Enterprise Management click Policy Management, then the Policy subtab, and expand the Policy tree in the task menu on the left.

   The Policy tasks appear.
2. Click Delete Policy.

   The Delete Policy: Policy Search screen appears.
3. Define a scope for the search, and click Search.

   A list of policies, which match the scope of the search you defined, appears.
4. Select the policy you want to delete, and click Select.

   A message appears asking if you want to delete the policy.
5. Click Yes.

   The policy is deleted.

Note: You can also use the policydeploy utility to perform this task. For more information about the policydeploy utility, see the *Reference Guide*.

More information:

Policies That You Cannot Delete (see page 93)

Delete a Policy Version

You can delete saved policy versions (POLICY object) that you no longer need. When you delete a policy version (POLICY object), CA Access Control Enterprise Management deletes all deployment and undeployment scripts associated with the policy version.

To delete a policy version, run the following command:

```
policydeploy -delete name#xx [-dms list]
```

-delete *name#xx*

Deletes the specified policy version.

-dms *list*

(Optional) Specifies a comma-separated list of DMS nodes from which to delete the policy version. If you do not specify DMS nodes, the policydeploy utility uses the list of DMS nodes specified in the local CA Access Control database.

Example: Delete an IIS 5 Protection Policy Version

The following example shows you how to delete the unassigned policy version IIS5#05 from the DMS. In this example, policy version IIS5#05 is not assigned to any hosts or host groups and is stored on the crDMS@cr_host.company.com DMS node.

To delete the IIS 5 protection policy version, open a command prompt window and run the policydeploy utility:

```
policydeploy -delete IIS5#05
```

Policy version IIS5#05 is deleted from the crDMS@cr_host.company.com DMS node.

Variables

Variables let you deploy the same policy to endpoints that have different configurations and different operating systems. For example, you can use variables to deploy the same policy to Windows and Solaris endpoints despite the different CA Access Control installation location on each operating system.

How You Create Variables

Variables are objects in the ACVAR class and can have more than one value. Each variable on an endpoint must have a unique name, and each variable in a policy must have a unique name. You use either of the following methods to create a variable:

- Use CA Access Control Endpoint Management to define a variable on an endpoint.
- Create a policy that defines a variable, and deploy the policy to many endpoints

Important! You can only create rules that use variables in policies. If you directly update the CA Access Control database with a rule that contains a variable, the database cannot compile the rule and CA Access Control cannot enforce the rule. You must define a variable before you refer to it in a policy script.

Variable Types

CA Access Control supports user-defined and built-in variables:

- User-defined variables are variables that you define in the CA Access Control database.
- Built-in variables are variables that CA Access Control creates during installation. You cannot modify built-in variables.

User-Defined Variables

CA Access Control supports the following user-defined variables:

Static variables

Define a fixed location on a CA Access Control endpoint.

You can define static variables that have the same name and different values, but each variable must exist on a separate endpoint and in a separate policy.

Note: If you do not specify a variable type when you create a variable, CA Access Control creates a static variable.

Registry value variables

(Windows) Define a location on a CA Access Control endpoint based on a registry value.

Note: You can only define registry variables that point to REG_SZ or REG_EXPAND_SZ registry types.

Example: The following rule defines a registry variable named jboss_home:

```
editres ACVAR ("jboss_home") value("HKLM\Software\Jboss\home") type(regval)
```

When you deploy this rule in a policy, the Windows endpoint uses the value of the HKLM\Software\Jboss\home registry key to resolve the variable value.

Operating system variables

Define a location on a CA Access Control endpoint based on an operating system environment value.

Example: The following rule defines an operating system variable named jboss_home:

```
editres ACVAR (“jboss_home”) value(“JBOSS_HOME”) type(osvar)
```

When you deploy this rule in a policy, the endpoint uses the value of the JBOSS_HOME operating system environment variable to resolve the variable value.

Built-In Variables

CA Access Control creates built-in variables in the CA Access Control database during the installation process. You cannot modify or delete built-in variables, but you can use built-in variables in policies. Built-in variables are dynamic and dependent on system settings on the CA Access Control endpoint. The value of a built-in variable changes when the corresponding system settings do.

Note: When you export a CA Access Control database, built-in variables are not included in the output. CA Access Control does not create built-in variables when you create a DMS or a PMDB.

CA Access Control supports the following built-in variables:

<!HOSTNAME>

Identifies the fully qualified host name of the local computer.

<!HOSTIP>

Identifies the host IP address or addresses.

<!AC_ROOT_PATH>

Identifies the CA Access Control installation path.

<!AC_REGISTRY_KEY>

(Windows) Identifies the CA Access Control root registry key.

<!USER_OS_ADMIN>

Identifies the administrator of the operating system on the local computer.

<!DOMAINNAME>

Identifies the domain name of the local computer.

<!DNSDOMAINNAME>

Identifies the DNS domain name of the local computer.

Example: Use a Built-in Variable in a Policy

This example creates a network resource rule:

```
authorize TCP 8333 uid(*) host(<!HOSTNAME>) access(WRITE)
```

When you deploy the policy to the endpoint host1.example.com and the endpoint compiles the policy, it creates the following rule:

```
authorize TCP 8333 uid(*) host(host1.example.com) access(WRITE)
```

Guidelines for Using Variables

You should observe the following guidelines when you use variables:

- You cannot delete a variable that is used by another variable or by a policy.
- Variables can have multiple values. You can add and remove variable values.
- Variables can be nested. For example, the following rule defines a variable named ac_data that contains the built-in <!AC_ROOT_PATH> variable:

  ```
  editres ACVAR ac_data value("<!AC_ROOT_PATH>\data")
  ```

  When a Windows endpoint with a default CA Access Control installation compiles this rule, it creates the following rule:

  ```
  editres ACVAR ac_data value("C:\Program Files\CA\AccessControl\data")
  ```

- Each variable can only have one type, for example, you cannot define a variable that is both a static variable and a registry value variable.
- You cannot deploy a policy that contains an undefined variable. If you deploy a policy with an undefined variable, CA Access Control changes the deployment status of the policy to Deploy Pending. To deploy the policy, you must define the undefined variable and redeploy the policy.

  Note: To discover which variable in the policy is undefined, review the DEPLOYMENT object for the policy. CA Access Control checks for undefined variables regardless of whether you have enabled or disabled policy verification.

- CA Access Control cannot resolve rules that combine CA Access Control variables and Windows system variables. For example, CA Access Control cannot resolve the following rule that defines a variable named var1:

  ```
  editres ACVAR var1 value("%SYSTEMROOT%\temp")
  ```

  To create a policy that defines %SYSTEMROOT% as a CA Access Control variable and that protects %SYSTEMROOT%\temp, use the following rules:

  ```
  editres ACVAR var1 value("SYSTEMROOT") type(osvar)
  editres ACVAR var2 value("<!var1>\temp")
  ```

- CA Access Control cannot resolve variables that are dependent on each other. For example, CA Access Control cannot resolve variables var1 and var2 in the following example:

  ```
  editres ACVAR var1 value("<!var2>")
  editres ACVAR var2 value("<!var1>")
  ```

- When you use a slash to define a directory in a variable, CA Access Control resolves the slash in the correct direction for Windows and UNIX endpoints.
- If you use selang rules to define a variable, you must use a policy to deploy the rules to an endpoint. If you use selang rules to directly update the CA Access Control database on the endpoint, CA Access Control cannot compile the rules. For example, if you have defined a variable named jboss_home on an endpoint, and you directly update the database with the following selang rule:

  ```
  editres FILE <!jboss_home> audit(all)
  ```

  CA Access Control cannot compile the rule, but instead creates a FILE object named <!jboss_home> in the database.

Guidelines for Using Operating System Variables on UNIX Endpoints

Valid on UNIX

A CA Access Control operating system variable (ACVAR object of type osvar) uses the value of a UNIX environment variable. Because each UNIX process has its own set of environment variables, we recommend that you do not use operating system variables on UNIX endpoints.

If you do use operating system variables on UNIX endpoints, you must set and export the necessary environment variables before you start CA Access Control. You should observe the following guidelines when you use operating system variables on a UNIX endpoint:

- If you use rc startup scripts to start CA Access Control when the computer boots, verify that the script sets and exports the environment variables before it starts CA Access Control.
- If a user stops and restarts CA Access Control, the user must set and export the environment variables in their session before they restart CA Access Control.

Guidelines for Using Operating System Variables on Windows Endpoints

Valid on Windows

A CA Access Control operating system variable (ACVAR object of type osvar) uses the value of a Windows environment variable.

You should observe the following guidelines when you use operating system variables on a Windows endpoint:

- The environment variable must be a system variable.
- If you change the value of a Windows environment variable, CA Access Control does not recognize the change until after you restart it. In some releases of Windows, you must also restart the computer for any Windows service and CA Access Control to recognize the change.

How an Endpoint Resolves Variables

Variables let you deploy the same policy to endpoints that have different configurations and different operating systems. The following process explains how a CA Access Control endpoint resolves variables in a policy after you have created and deployed the policy:

1. When policyfetcher fetches the policy, CA Access Control checks that the variables in the policy are defined in the policy or in the CA Access Control database. *One* of the following occurs:
   - If the variable is not defined in the policy or in the database, CA Access Control changes the policy status to Deploy Pending.

     Note: To deploy the policy, you must define the undefined variables and redeploy the policy.
   - If the variable is defined in the policy or in the database, CA Access Control compiles the policy and enforces the rules it contains.
2. Every heartbeat, policyfetcher checks if a variable value has changed in the CA Access Control database. *One* of the following occurs:
   - If no variable values have changed, policyfetcher repeats Step 2.
   - If a variable value has changed, CA Access Control changes the policy status to Out of Sync for any policy on the endpoint that uses the changed variable.

     Note: To clear the Out of Sync status for the policy, you must redeploy the policy.

Troubleshooting Policy Deployment

When you assign a policy to a host, the policy is not deployed on the assigned endpoint until policyfetcher retrieves the deployment task and runs the policy script. As a result, deployment errors may occur for different reasons when the policy is transferred or deployed at the endpoint.

To resolve policy deployment errors, advanced policy management provides you with troubleshooting actions. You can perform these actions using either CA Access Control Enterprise Management or the policydeploy utility. In CA Access Control Enterprise Management, the troubleshooting actions are located in the Policy sub-tab of the Policy Management tab.

The troubleshooting actions are as follows:

- **Redeploy**—Creates a new deployment task that contains the policy script and deploys the task to the endpoint.

  Use this option when the policy deploys on the endpoint with errors. That is, selang policy script execution failed. You need to manually fix the reason for the script error on the endpoint before you can redeploy the policy.

  Note: This option is only available in CA Access Control Enterprise Management, and is not supported in the policydeploy utility.

- **Undeploy**—Undeploys the policy from the specified endpoint without unassigning the policy from the corresponding host.

  Use this option to remove any policies from the endpoint that are not assigned to the host on the DMS.

- **Reset**—Resets an endpoint. CA Access Control resets host status, undeploys all effective policies, and deletes all GPOLICY, POLICY, and RULESET objects.

  Use this option to clean an endpoint, and its status on the DMS, from all policy deployments.

  Note: This option does not remove DEPLOYMENT or GDEPLOYMENT objects from the endpoint or from the DMS, because you may need these objects for auditing purposes. You can use the dmsmgr -cleanup function to remove the DEPLOYMENT and GDEPLOYMENT objects after you reset the endpoint. After you reset an endpoint, you can assign policies to the endpoint as normal.

- **Restore**—Undeploys any policies on the specified host, then restores all the policies that should be deployed (assigned or directly deployed) on the host by creating new deployment tasks and sending the tasks to the host for execution.

  Use this option when you re-install CA Access Control or the operating system on the endpoint, or when you restore an endpoint from a backup, to redeploy all the policies that the DMS indicates are effective on that endpoint.

How to Remove Obsolete Endpoints

The DMS stores information about your enterprise. If you remove a computer from the enterprise when you uninstall CA Access Control from that computer, the DMS still contains a reference to that node. As a routine maintenance procedure, you should clean the DMS from these obsolete nodes.

To remove obsolete nodes, do one of the following:

- Run the dmsmgr utility on the DMS computer to perform a routine clean up:

  ```
  dmsmgr -cleanup number_of_days -dms name
  ```

  number_of_days

  Defines the minimum number of days in which the CA Access Control node has been unavailable for.

- Manually delete a specific node by issuing the following selang command on the DMS computer:

  ```
  rr HNODE HNODE_name
  ```

Important! When you delete a node, CA Access Control removes all the HNODE related deployment tasks, removes all the deployment tasks' packages (unless they have other deployment task members), and only then removes the HNODE object.

View Deployment Audit Information

CA Access Control Enterprise Management provides an audit of your policy deployments. This audit gives you a view of your policy deployments—a descriptive list of deployment tasks. The list details what triggered each deployment task, when it was created, and what type of deployment was involved. For each deployment task, you can further explore the following details: which host and policy pair was the deployment task created for, the version of the policy that was deployed, the status of the deployment task (queued, succeeded, or failed), and the selang output (result of deploying the command).

To view deployment audit information

1. In CA Access Control Enterprise Management, do as follows:
   a. Click Policy Management.
   b. Click Policy subtab.
   c. Expand the Deployment tree in the task menu on the left.

      The Deployment Audit task appears in the list of available tasks.
2. Click Deployment Audit.

   The Deployment Audit page appears.

3. Define a scope for the deployment audit, then click Go.

   CA Access Control Enterprise Management retrieves information about deployments that are in the scope you defined and displays the results after a short delay.

4. (Optional) Click on the trigger of a deployment to view more information about the associated deployment tasks.

How Policy Deviation Calculations Work

Advanced policy management lets you see the difference between the access rules that should be deployed on an endpoint (as a result of policy deployment) and the actual rules that have been successfully deployed on the same endpoint. It also resolves property additions and changes made to policy objects. This lets you resolve problems associated with the deployment of your policies.

When the policy deviation calculator runs on an endpoint, it performs the following actions:

1. Retrieves from the local host the list of rules that should be deployed on the endpoint.

   These are the rules that are specified for each of the deployed policies, as specified in the local RULESET object that is associated with the POLICY object for each deployed policy version.

2. Checks that each of these rules is applied to the endpoint.

   Important! The deviation calculation does not check whether native rules are applied. It also ignores rules that remove objects (user or object attributes, user or resource authorization, or actual users or resources) from the database. For example, the calculation cannot verify whether the following rule is applied:
   rr FILE /etc/passwd

3. (Optional) Compares between the local policy objects and the ones on the DMS.

   Normally, the deviation calculator checks for deviations only on the local host. If you specify the *-strict* option, the deviation calculator also compares the policies associated with the local HNODE object to the policies associated with HNODE object on the DMS. It compares the following:

   a. List of policies associated with the HNODE object representing the local host

   b. Policy state of each POLICY object associated with the HNODE object

   c. Policy signature of each POLICY object associated with the HNODE object

4. Outputs the following two files:

   - *ACInstallDir*/data/devcalc/deviation.log

     Log and error messages collected during the last deviation calculation.

   - *ACInstallDir*/data/devcalc/deviation.dat

     List of policies and their deviations. You can get the contents of this file using the selang command *get devcalc* on the endpoint.

   Note: CA Access Control also sends audit events which can be viewed using *seaudit -a*. For more information about the seaudit utility, see the *Reference Guide*.

5. Notifies the DMS of any deviations found.

   Notifications are sent to the DMS through the DHs specified for the local CA Access Control database.

Deviation Calculation Trigger

You should regularly perform a deviation calculation so that the DMS contains recent information about policy deviation status. If you enable advanced policy management on your endpoint, policyfetcher triggers the deviation calculator after each heartbeat.

Note: The deviation calculation that runs by default does not consider items that were added to the endpoint. To view these items, change the devcalc_command configuration setting to to run the deviation calculation in *precise* mode.

We recommend that you modify the policyfetcher settings so that a policy deviation calculation occurs in an interval that supports your requirements.

Policy Deviation Log and Error File

The policy deviation calculation writes a new log during each deviation calculation. This log also contains error messages and is stored in *ACInstallDir*/data/devcalc/deviation.log

Use this log when the deviations you see in your reports (that are retrieved from the DMS) are not gathered from the last time a deviation calculation should have run. It can help you diagnose why the deviation calculation results were not sent to the DMS.

Example: Deviation log and error file

The following is an example deviation log and error file:

```
start time: Mon Jan 23 13:04:48 2006
WARNING,\"failed to retrieve DH host name, deviation will be stored locally\"
found deviation(s) for policy 'iis8#02'
end time: Mon Jan 23 13:05:04 2006
```

Policy Deviation Data File

The policy deviation calculation writes a data file that contains a list of policies and their deviations. This data file is stored in *ACInstallDir*/data/devcalc/deviation.dat

Note: The list of policies included in the data file depends on the policies that a deviation is calculated for (by default, all the policies and all policy versions on the endpoint).

Important! The deviation calculation does not check whether native rules are applied. It also ignores rules that remove objects (user or object attributes, user or resource authorization, or actual users or resources) from the database. For example, the calculation cannot verify whether the following rule is applied:
rr FILE /etc/passwd

The deviation status is sent (whether a deviation exists or not) to the DMS but the actual deviation is stored locally. When a report is created, the actual deviation results can be retrieved from this file and added to the report.

The following lines can appear in the policy deviation data file:

Date

Displays a time stamp for the deviation calculation. A date line is always the first line in the deviation report.

Format: DATE, *DDD MMM DD hh:mm:ss YYYY*

Strict

Specifies that the deviation calculation was run with the -strict option.

Format: STRICT, *DMS@hostname*, *policy_name#xx*, [1|0]

[1|0] signifies whether a deviation was found (1) between the policies associated with the local HNODE object and the ones associated with the HNODE object on *DMS@hostname* (the first available DMS), or not (0).

Policy Start

Starts a policy block, which defines the deviation for this policy version.

Format: POLICYSTART, *policy_name#xx*

Difference

Describes a deviation that was found for a policy. The name of the policy for which the deviation applies to is the nearest *policy line* above this line.

There are eight types of deviations, four showing missing elements and four showing added elements, which are described in the following table:

Deviation Type	Format
Class not found	DIFF, -(*class_name*), (*), (*), (*)
Object not found	DIFF, (*class_name*), -(*object_name*), (*), (*)
Object added	DIFF, (*class_name*), +(*object_name*), (*), (*)
Property not found	DIFF, (*class_name*), (*object_name*), -(*property_name*), (*)
Property added	DIFF, (*class_name*), (*object_name*), +(*property_name*), (*)
Property value missing	DIFF, (*class_name*), (*object_name*), (*property_name*), -*(expected_value*)
Property value added	DIFF, (*class_name*), (*object_name*), (*property_name*), +*(value*)

Note: When the deviation calculator detects a missing class, it also creates a deviation line for all missing objects, properties, and values.

Policy End

Ends a policy block which defines the deviation for this policy.

Format: POLICYEND, *policy_name#xx*, [1|0]

[1|0] signifies whether a deviation was found (1) or not (0).

Warning

Describes a warning.

Format: WARNING, "*warning_text*"

Example: Deviation data file

The following example shows an excerpt from a deviation data file:

```
Date, Sun Mar 19 08:30:00 2006
WARNING, "failed to retrieve DH host name, deviation will be stored locally"
POLICYSTART, iis8#02
DIFF, (USER), (iispers), (*), (*)
POLICYEND, iis8#02, 1
```

Deviations Showing Missing Elements

The deviation calculator differentiates between missing elements and additions of new elements. Missing elements refer to CA Access Control elements that are explicitly defined in a specified policy, but do not exist on the local host. These missing elements can be: classes, objects, properties, and values.

Any combination of missing elements defines a hierarchal requirement. For example, if Policy1 has the following rule:

```
eu mytestuser2 operator
```

The deviation calculator asserts that the following implicit requirements are met:

- Class USER must exist

  The rule defines a user, which belongs to the USER class.

- USER object mytestuser2 must exist

  The mytestuser2 object of the USER class is explicitly referred to by the rule.

- Property OBJ_TYPE must exist

  The rule uses the operator parameter to set the OBJ_TYPE parameter of the USER object.

- The value Operator is assigned to the OBJ_TYPE property

  The rule explicitly sets this value.

Deviations Showing Added Elements

The deviation calculator differentiates between missing elements and additions of new elements. Added elements refer to CA Access Control elements that are defined locally, but do not exist in the specified policies. These added elements can be: classes, objects, properties, and values.

An addition deviation will be included if a local exception has added a new:

- Value to a property of an object mentioned within a policy.
- Property to an object mentioned within a policy.

Note: New objects—those which are not mentioned within any policy—will not be considered as an addition; this also applies to new classes.

Deviations Showing Modified Elements

Deviations showing modified elements occur when no single deviation line in the deviation data file shows a modification. To identify a modification, you need to look for sequential removal and addition lines that apply to the same element. For example, in the following extract from a deviation data file, mytestuser has been modified from having the Operator value to having both the Auditor and Administrator values:

```
DIFF, (USER), (mytestuser2), (OBJ_TYPE), -(Operator)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Auditor)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Administrator)
```

Chapter 5: Planning Your PUPM Implementation

This section contains the following topics:

Privileged User Password Management (see page 109)
What Are Privileged Accounts? (see page 109)
Privileged Access Roles and Privileged Accounts (see page 110)
Password Consumers (see page 117)
PUPM Audit Records (see page 123)
CA Service Desk Manager Integration (see page 125)
Implementation Considerations (see page 128)

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.

More information:

Privileged Access Roles (see page 22)

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 27)

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.

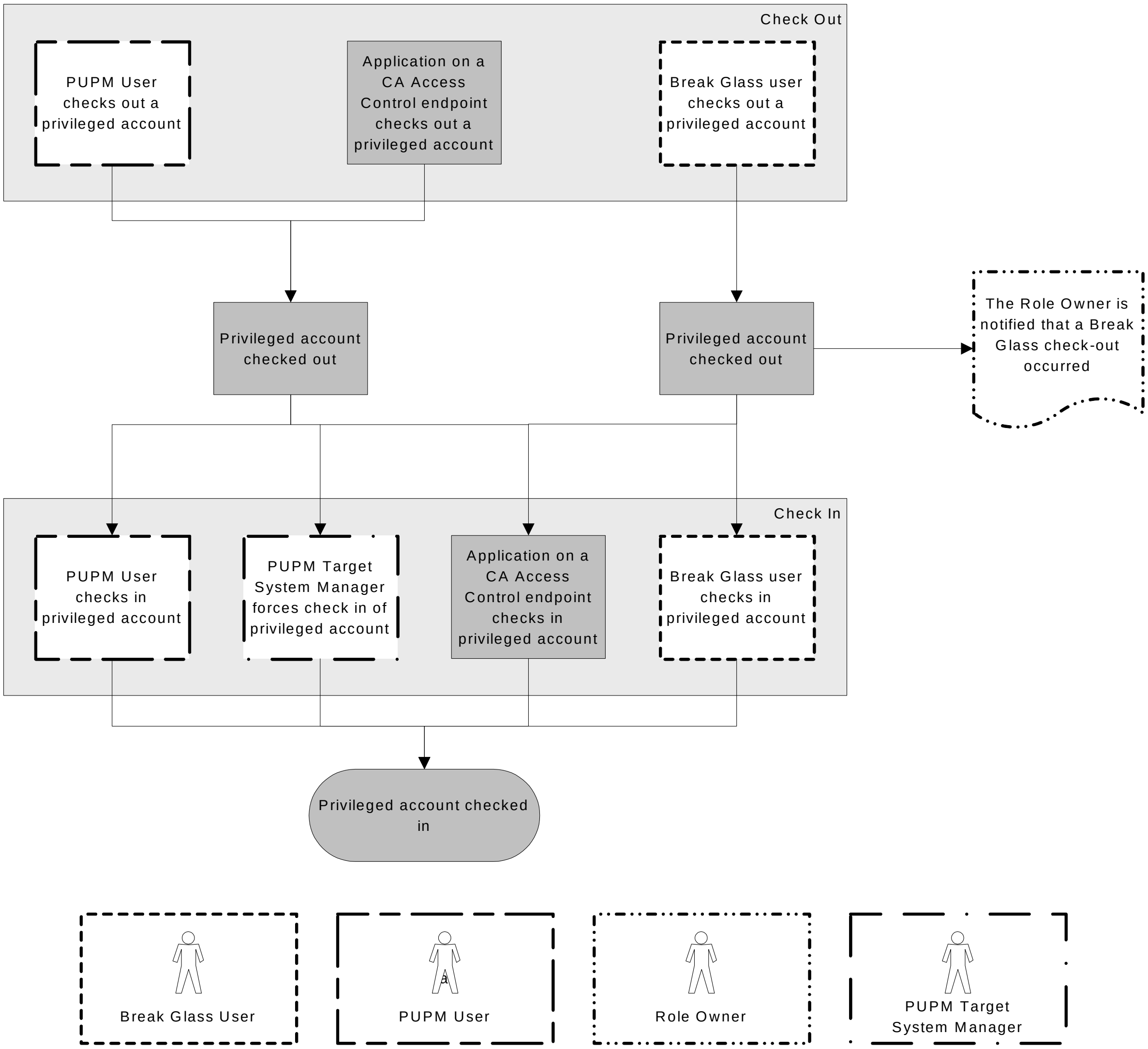
   Note: If a user performs a break glass checkout, CA Access Control notifies the role owner. The role owner can choose to add information to this message for auditing purposes.

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:


Check Out
PUPM User checks out a privileged account
Application on a CA Access Control endpoint checks out a privileged account
Break Glass user checks out a privileged account
Privileged account checked out
Privileged account checked out
The Role Owner is notified that a Break Glass check-out occurred
Check In
PUPM User checks in privileged account
PUPM Target System Manager forces check in of privileged account
Application on a CA Access Control endpoint checks in privileged account
Break Glass user checks in privileged account
Privileged account checked in
Break Glass User
PUPM User
Role Owner
PUPM Target System Manager

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.

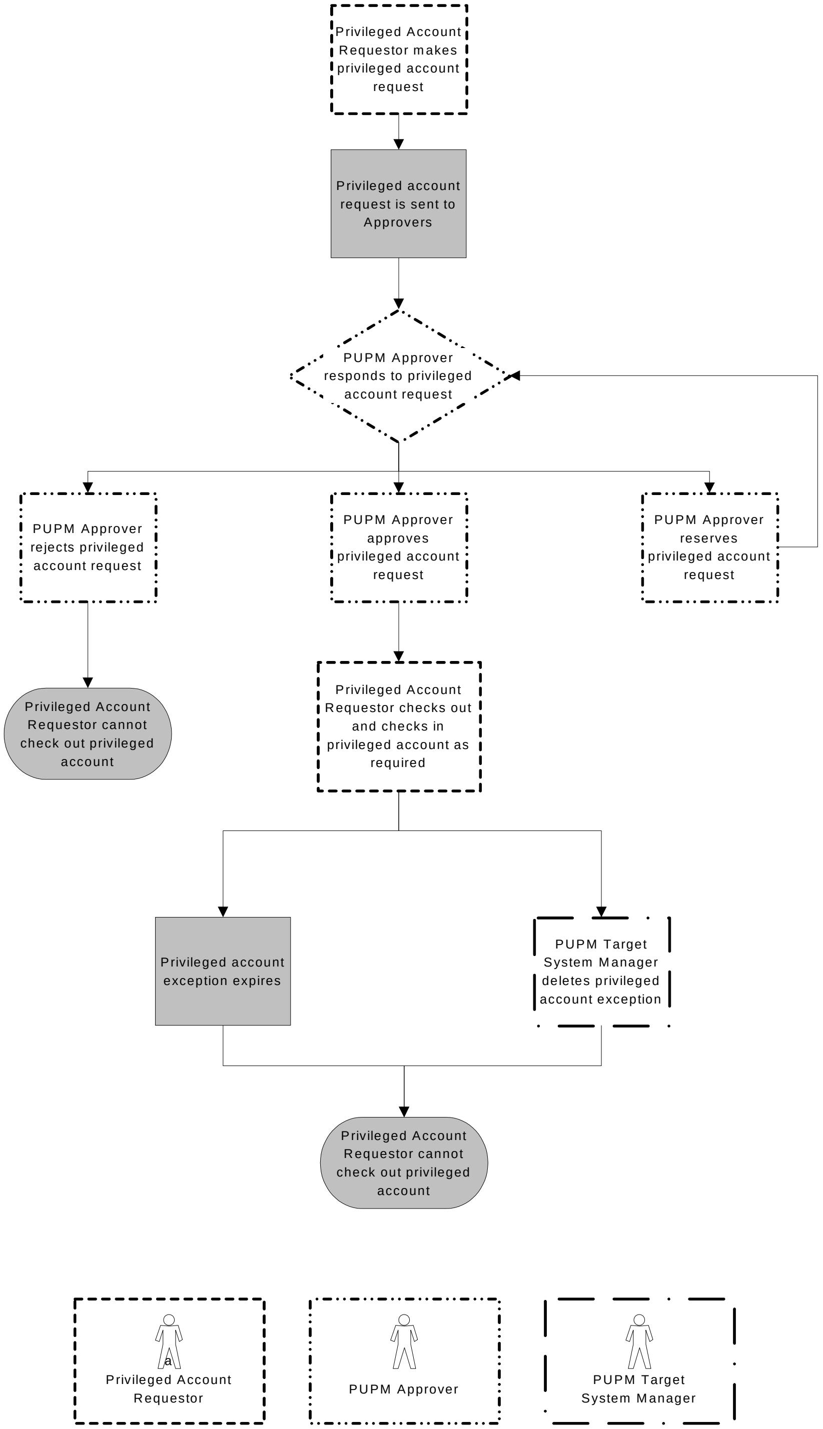
     The user with the Privileged Account Request role is granted a privileged account exception, and can check out and check in the privileged account.

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:


Privileged Account Requestor makes privileged account request
Privileged account request is sent to Approvers
PUPM Approver responds to privileged account request
PUPM Approver rejects privileged account request
PUPM Approver approves privileged account request
PUPM Approver reserves privileged account request
Privileged Account Requestor cannot check out privileged account
Privileged Account Requestor checks out and checks in privileged account as required
Privileged account exception expires
PUPM Target System Manager deletes privileged account exception
Privileged Account Requestor cannot check out privileged account
a
Privileged Account Requestor
PUPM Approver
PUPM Target System Manager

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.

Password Consumers

Password consumers are applications, Windows services, and Windows scheduled tasks that use privileged accounts and service accounts to execute a script, connect to a database, or manage a Windows service, scheduled task, or RunAs command. *Service accounts* are internal accounts used by Windows services. For example, Windows services may use the NT AUTHORITY\LocalService service account to log in to the operating system.

Password consumers let you remove hard-coded passwords from application scripts and enforce a password policy on an endpoint. For example, you can create a password consumer for each scheduled task on a Windows endpoint, and specify that each password consumer uses the same password policy. PUPM will then change the password of each scheduled task at the interval specified in the password policy.

PUPM provides privileged account passwords to password consumers in the following ways:

- On demand—When a password consumer sends a request for a privileged account password, for example, when a privileged account uses ODBC to connect to a database that requires authentication.

  Note: You must install CA Access Control on the PUPM endpoint with the PUPM Integration feature enabled to use password consumers that get passwords on demand.

- On password change—When a password change event occurs for the password consumer in CA Access Control Enterprise Management, for example, when a password policy specifies that the password for a service account must change after a fixed length of time.

  Note: You do not need to install CA Access Control on the PUPM endpoint to use password consumers that get passwords on password change.

Types of Password Consumers

A password consumer is the representation of an application, Windows service, or Windows scheduled task that you run on a PUPM endpoint. Except for software development kit password consumers, all other password consumers get privileged account passwords but do not check out or check in the passwords.

PUPM provides privileged account passwords to the following password consumers on demand:

- **Software Development Kit (SDK/CLI)**—A software development kit password consumer requests a privileged account password when it is executed by a script on the endpoint.

  Use a software development kit password consumer to replace hard-coded passwords in scripts.

  Note: Unlike other password consumers, software development kit password consumers can check out and check in privileged account passwords.

- **Database (ODBC, JDBC, OLEDB, OCI, .NET)**—A database password consumer requests a privileged account password when a program that is running on the endpoint connects to a database.

  Use a database password consumer to replace hard-coded passwords in programs that connect to a database.

- **Windows Run As**—A Windows Run As password consumer requests a password when a user executes the RunAs application to substitute to a privileged account and execute a specific command.

  Use a Windows Run As password consumer to let a user substitute to a privileged account and execute a command without the privileged account password.

Note: You must install CA Access Control on the PUPM endpoint with the PUPM Integration feature enabled to use password consumers that get passwords on demand.

PUPM provides privileged account passwords to the following password consumers on password change:

- **Windows Scheduled Task**—A Windows Scheduled Task password consumer uses a service account to manage a scheduled task. PUPM forces a password change for the task whenever a password change event occurs in CA Access Control Enterprise Management.

  Use a Windows Scheduled Task password consumer to set password policies and automate password changes for scheduled tasks.

- **Windows Service**—A Windows Service password consumer uses a service account to run a Windows service. PUPM forces a password change for the service account whenever a password change event occurs in CA Access Control Enterprise Management.

  Use a Windows Service password consumer to set password policies and automate password changes for Windows services. The service must be run by an account for which you can change the password, for example, your computer's Administrator account or a domain account.

Note: You do not need to install CA Access Control on the PUPM endpoint to use password consumers that get passwords on password change.

More information:

Create a Password Consumer (see page 217)

How a Password Consumer Gets a Password on Demand

A password consumer retrieves a password from PUPM when the associated privileged account authenticates to another application. Password consumers that get passwords on demand forward password requests to the PUPM Agent, which uses the Message Queue to communicate with CA Access Control Enterprise Management.

Software development kit, database, and Windows Run As password consumers get passwords on demand. You use password consumers that get passwords on demand to replace hard-coded passwords in scripts. Whenever an application provides a password for authentication purposes, PUPM replaces the hard-coded password with the privileged account password.

Note: You must install CA Access Control on the PUPM endpoint with the PUPM Integration feature enabled to use password consumers that get passwords on demand.

The following process explains how a password consumer gets a privileged account password on demand:

1. An application uses a hard-coded password to try to connect to a system that requires user authentication.
2. A password consumer intercepts the connection attempt.

   For example, an OCI password consumer intercepts an attempt to connect to an Oracle database.
3. The PUPM Agent checks the cache. *One* of the following happens:
   - If the request is cached, the PUPM Agent forwards the privileged account password to the password consumer. The password consumer replaces the hard-coded password with privileged account password. The application uses the privileged account password to log in to the system. The process ends at this step. CA Access Control Enterprise Management does not write an audit record for the password retrieval.
   - If the request is not cached, the PUPM Agent forwards the password request to CA Access Control Enterprise Management.
4. CA Access Control Enterprise Management receives the message and checks that the password consumer is authorized to obtain the privileged account password.
5. *One* of the following happens:
   - If the password consumer is authorized to obtain the password, CA Access Control Enterprise Management sends the privileged account password to the PUPM Agent. The PUPM Agent replaces the hard-coded password with privileged account password. The application uses the privileged account password to log in to the system. CA Access Control Enterprise Management writes an audit record for the event.
   - If the password consumer is not authorized to obtain the password, CA Access Control Enterprise Management sends an error message to the PUPM Agent. The PUPM Agent does not forward a password to the application, so the application uses the hard-coded password to log in to the system.

How PUPM Notifies a Password Consumer of a Password Change

PUPM forces a password change for a password consumer when a password change event occurs in CA Access Control Enterprise Management, for example, when a password policy specifies that a password must change after a fixed length of time. CA Access Control Enterprise Management uses the JCS to communicate with password consumers that get passwords on password change.

Only Windows Scheduled Task and Windows Service password consumers get passwords on password change.

Note: You do not need to install CA Access Control on the PUPM endpoint to use password consumers that get passwords on password change.

The following process explains how PUPM notifies password consumers of a password change:

1. A password change event generates a new password.
2. CA Access Control Enterprise Management searches the central database for password consumers that use the password.
3. The JCS logs in to each affected endpoint using the administrator credentials that you supplied when you created the endpoint.
4. The JCS tries to change the password of the password consumer on the endpoint. *One* of the following happens:
   - The JCS changes the password of the password consumer on the endpoint and optionally restarts the service.

     Note: You specify if the JCS restarts the service when you create the password consumer.
   - The JCS cannot change the password of the password consumer on the endpoint. CA Access Control Enterprise Management writes a notification message in the task that initiated the change password event.
5. CA Access Control Enterprise Management writes an audit record for the password change.

   Note: You use View Submitted Tasks to view PUPM audit records. If the JCS cannot change the password of a password consumer, you can use Synchronize Password Consumers to retry the password change.

More information:

Synchronize Password Consumers (see page 263)

Implementation Considerations for Password Consumers

Before you implement password consumers, consider the following:

- To use software development kit, database, and Windows Run As password consumers, you must install CA Access Control on the PUPM endpoint with the PUPM Integration feature enabled.
- To use JDBC database password consumers, the application that connects to the database must use JRE 1.5 or later.
- To use OCI database password consumers, the application that connects to the database must use OCI8 or later.
- To use ODBC or OLEDB database password consumers with a non-default driver, you must contact CA Technologies Support.

  Note: The default drivers are defined in the ApplyOnProcess registry entry in the registry sub-key for the ODBC or OLEDB plug-in. For assistance, contact CA Support at http://ca.com/support.
- To use the Java PUPM SDK password consumer, the Java application that you write must use JRE 1.5 or later.
- To use the .NET PUPM SDK password consumer, you must install the .NET Framework 2.0 or later on the endpoint.
- When you discover service accounts to create a Windows Service or Windows Scheduled Task password consumer, CA Access Control discovers only services that are run by accounts for which you can change the password.
- To discover service accounts that are domain accounts, you must create a PUPM endpoint that represents the domain controller (DC) on which the accounts reside. The endpoint must have the following attributes:
  - Endpoint type—Windows Agentless
  - Is Active Directory—True
  - Host Domain—The domain name of which the DC is a member
  - User Domain—The domain name of which users defined on the DC are members

    Note: Specify the user domain only if the administrative account is from a different domain than the domain in which the accounts reside.

More information:

Discover Service Accounts (see page 215)

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 40)
Audit Privileged Accounts (see page 259)

Password Consumer Audit Records

CA Access Control Enterprise Management writes an audit record each time a password consumer makes a password request and the PUPM Agent gets the password from the Enterprise Management Server. CA Access Control Enterprise Management also writes an audit record a password consumer makes a password request and the request fails, for example, if a password consumer requests a password that it is not authorized to access.

CA Access Control Enterprise Management does not write an audit record when a password consumer makes a password request and the PUPM Agent on the endpoint gets the password from the cache.

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 262)

How to Integrate PUPM Endpoints with CA Enterprise Log Manager

Integrating your PUPM endpoints with CA Enterprise Log Manager 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.

To integrate your PUPM endpoints with CA Enterprise Log Manager, do as follows:

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

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

Note: For more information about how to configure the connection to CA Enterprise Log Manager, see the *Implementation Guide*. For more information about how to configure CA Enterprise Log Manager, see the CA Enterprise Log Manager documentation.

More information:

Create an Endpoint (see page 158)
View Audit Events on a PUPM Endpoint (see page 262)

CA Service Desk Manager Integration

PUPM is able to communicate with CA Service Desk Manager to accept and validate tickets as part of the privileged account request and approval processes. When integrated with CA Service Desk Manager, PUPM validates each request for a privileged account password against an active ticket. Integrating PUPM with CA Service Desk Manager lets you create a validation process for privileged accounts requests that includes multiple approval processes.

How to Integrate Privileged Account Requests with CA Service Desk Manager

Understanding how to integrate PUPM with CA Service Desk Manager helps you to set up the connection to CA Service Desk Manager and implement the validation process.

To integrate PUPM with CA Service Desk Manager, do the following:

1. Deploy and configure CA Service Desk Manager.
2. Configure the connection to CA Service Desk Manager from CA Access Control Enterprise Management.
3. Use CA Service Desk Manager to open a service desk ticket requesting access to a privileged account.
4. Approve the service desk request using CA Service Desk Manager.
5. Create a privileged account request in CA Access Control Enterprise Management and provide the CA Service Desk Manager ticket number.
6. Approve or deny the privileged account request.

Configure the Connection to CA Service Desk Manager

You define the connection to CA Service Desk Manager from CA Access Control Enterprise Management to integrate PUPM with CA Service Desk Manager.

To configure the connection to CA Service Desk Manager

1. In CA Access Control Enterprise Management, select System, Connection Management, CA Service Desk Manager, Managed CA Service Desk Manager Connection.

   The Managed CA Service Desk Manager Connection window opens.

2. Complete the form using the following:

   Connection Name

   Defines the connection name.

   Default: Primary CA Service Desk Manager Connection

   Connection Type

   Specifies the connection type.

   Default: CA Service Desk Manager

   Connection Description

   Specifies a description for the connection.

Host Name

Defines the CA Service Desk Manager Web Service URL.

Default: http://*host_name*:8080/axis/services/USD_R11_WebService?wsdl

User ID

Defines the user ID used to connect to CA Service Desk Manager.

Note: The user must have privileges to query service desk tickets through the Web Service API.

Password

Defines the password for the user ID.

Mandatory

Specifies whether a user must enter a ticket number when requesting access to a privileged account.

Note: If not selected, supplying a ticket number when requesting access to a privileged account is not enforced.

Enabled

Specifies whether the connection is enabled.

Note: If not selected, the ticket number field is not displayed in the request privileged account task.

Advanced

Specifies whether you want to define advanced settings. If you select this option, the following fields appear:

Ticket Type

Defines the type of CA Service Desk Manager ticket that is used to request a privileged account password.

Limits: cr, iss, chg

Default: cr

Note: This field is case-sensitive.

Ticket Query

Defines a custom query used to validate the ticket. Specify any valid CA Service Desk Manager query.

Example: active=1 AND status='OP

Note: If this field is left empty, CA Access Control Enterprise Management enumerates all service desk tickets to validate the requestor ticket.

3. Click Submit.

   CA Access Control Enterprise Management tests the connection settings and creates the connector server.

Note: For more information about CA Service Desk Manager, see the CA Service Desk Manager documentation.

More information:

How to Integrate Privileged Account Requests with CA Service Desk Manager (see page 126)

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.

Minimum Privileges for Managing an Active Directory Endpoint

Valid on Windows

If you want to use PUPM Windows Agentless endpoint type to manage Active Directory endpoints and do not want to specify a domain administrator account, you can specify a delegated user account with the minimum privileges required to manage regular user accounts.

Example: Delegating an Active Directory user the privileges to manage other Active Directory users on Windows Server 2008

The following example shows you how to delegate the privileges for a regular user to manage other regular Active Directory users on Windows Server 2008.

1. Select Start, Administrative Tools, Component Services

   The component services console opens.

2. Expand the Component Services list, select Computers then right-click My Computer and select Properties.

   The My Computer properties window opens.

3. Navigate to the COM Security tab and do the following:
    a. Click the Edit Default button in the Access Permissions section
    b. Click Add to locate the user account to assign access permissions
    c. Select Edit Defaults in the Launch and Activation Permissions section.
    d. Click Add to locate the user account to assign access permissions.
    e. Select the Local and Remote Access and Local and Remote Activation options under the Allow column.
    f. Click OK and exit the properties window.
4. Select Start, Administrative Tools, Active Directory Users and Computers. Do the following:
    a. From the Users list, right-click the user account.
    b. Move to the Member Of tab and select Add to a group.
    c. Add the user as a member of the following groups, then click OK:
        - Domain Users
        - Distributed COM Users

    You have configured the security attributes for the delegated user. You now configure the security attributes for the container that you want this user to manage.
5. From the Active Directory Users and Groups console, right-click the Users folder and select Properties.
6. Move to the Security tab, Select Add User and click Advanced.

    The advanced security settings window opens. Do the following:
    a. In the Permissions tab select the user and click Edit.

        The permissions entry window opens.
    b. From the Apply onto list, select Descendant User Objects and apply the following permissions:
        - List contents
        - Read all properties
        - Write all properties
        - Read permissions
        - Modify permissions
        - Change password
        - Rest password
    c. Click OK and exit the properties window.

You have configured the security attributes for the user in the Users container.

7. From a Command Prompt window, run the command wmimgmt to open the WMI Control Console. Do the following:

   a. Right-click WMI Control and select Properties.

      The WMI Control properties window opens.

   b. Move to the Security tab and expand the root directory.

   c. Select directory and click on the Security button.

   d. Click Add to add the user account that you are editing, then add the following permissions for Read Security for Root namespaces and subnamespaces:

      - Partial Write
      - Provider Write
      - Enable Account
      - Remote Enable

   e. Close the WMI Control Console.

8. From a Command Prompt window, run the regedit utility and locate the following registry entry:

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

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

9. Right-click each registry key and select Permissions

   The permissions window opens.

10. Add the user to the list and assign Full Control to the key and all child objects

11. Click OK to close the regedit utility.

    You have delegated a regular Active Directory user the permissions to manage other regular Active Directory users.

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 SUN ONE Endpoint

In this example, the system administrator Steve creates a SUN ONE endpoint type in Connector Xpress to connect to a SUN ONE directory.

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

1. Goes to 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 JNDI and clicks OK.

   The Edit Source window opens.

5. Enters the following details:

   - Name—SUN ONE
   - Server Name—server1
   - Port—389
   - Bind DN— uid=user1,ou=cont1,ou=ldapConnector,dc=company,dc=com

     Important! Specify an existing directory user account and not a Directory Manager account, that is not located directly under the base DN.

   - Base DN—ou=ldapConnector,dc=company,dc=com

6. Clicks Test to verify the connection settings.

   The Enter password for data source window opens.

7. Enters the administrator account password and clicks OK.

   A confirmation message appears, if no errors were discovered. The new data source is created. Steve now creates a new project.

8. Selects Project, new, data source, Edit and enters the administrator account password.

   The Endpoint Type Details screen opens.

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

   The Map Class and Attributes window opens.

10. In the Select Object Classes, adds the structural class inerOrgPerson and maps the following attributes:

- cn—AccountID
- sn—last name
- uid—AccountID
- userPassword—the user account password

11. Saves the project to save the endpoint type definitions.

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

Connector Xpress Example: Register the SUN One Endpoint Type in 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.

More information:

Connector Xpress Example: Load the Endpoint Type to the Enterprise Management Server (see page 140)

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.

More information:

How to Configure an Endpoint to Use a Password Consumer SDK Application (see page 248)

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.

More information:

How to Configure an Endpoint to Use a Password Consumer SDK Application (see page 248)

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.

More information:

How to Configure an Endpoint to Use a Password Consumer SDK Application (see page 248)

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.

More information:

How to Configure an Endpoint to Use a Web Services PUPM SDK Application (see page 251)

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.

More information:

How to Configure an Endpoint to Use a Web Services PUPM SDK Application (see page 251)

Chapter 6: Implementing Privileged Accounts

This section contains the following topics:

How to Set Up Privileged Accounts (see page 147)
Create a Password Policy (see page 155)
PUPM Endpoint and Privileged Account Creation (see page 158)
How to Import PUPM Endpoints and Privileged Accounts (see page 196)
How to Set Up Password Consumers (see page 211)
PUPM Automatic Login (see page 222)

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.

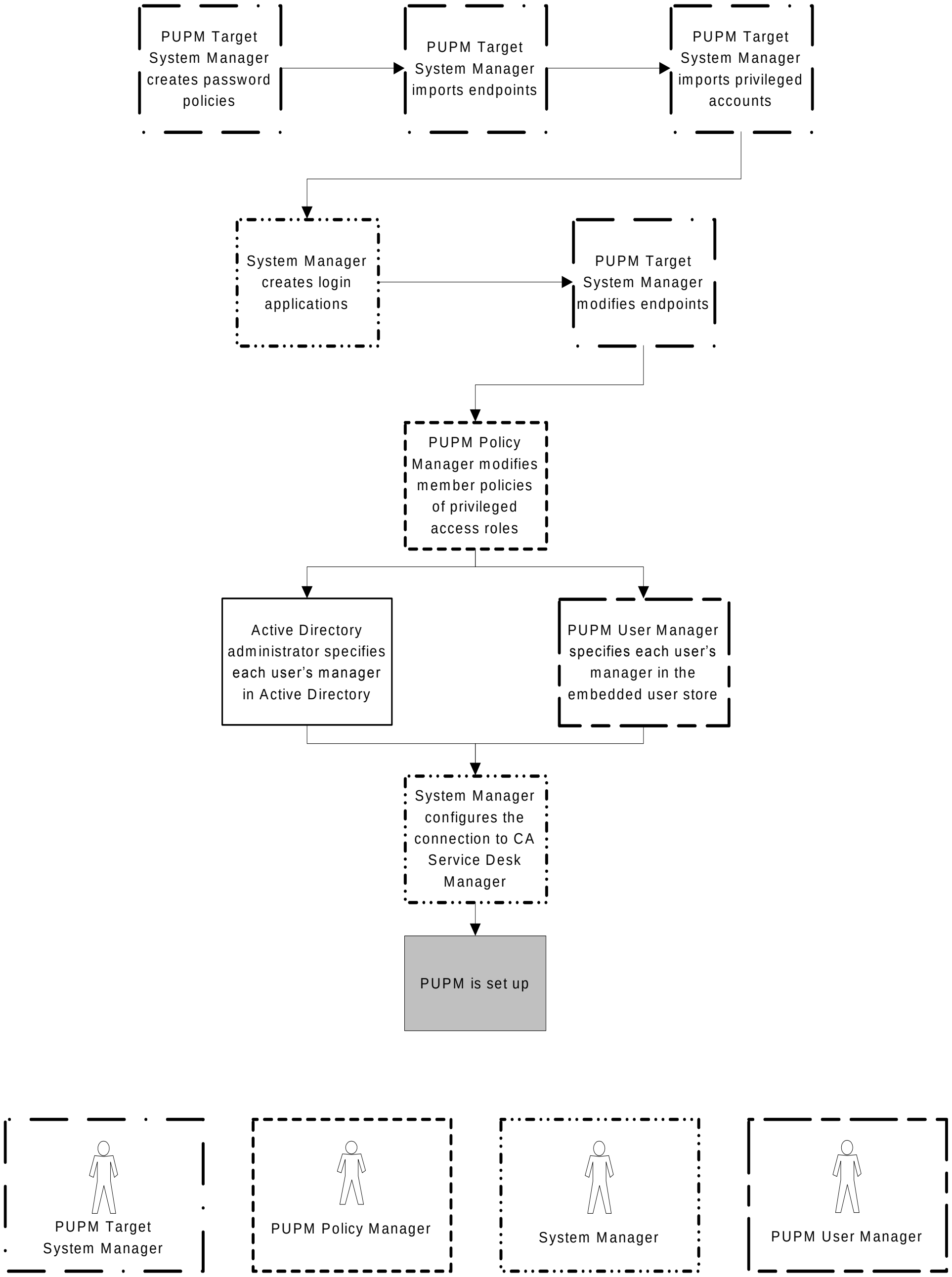
6. (Embedded user store) The PUPM User Manager specifies the manager of each user.

   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 CA Service Desk Manager.

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

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


PUPM Target System Manager creates password policies
PUPM Target System Manager imports endpoints
PUPM Target System Manager imports privileged accounts
System Manager creates login applications
PUPM Target System Manager modifies endpoints
PUPM Policy Manager modifies member policies of privileged access roles
Active Directory administrator specifies each user's manager in Active Directory
PUPM User Manager specifies each user's manager in the embedded user store
System Manager configures the connection to CA Service Desk Manager
PUPM is set up
PUPM Target System Manager
PUPM Policy Manager
System Manager
PUPM User Manager

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 that it discovers in a table, so that you can easily tell which accounts you already manage with PUPM.

The first time that 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.

To discover privileged accounts

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 that 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.

   Exclusive Session specifies that only a single user can use the account, if no open sessions are currently running on the endpoint.

   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.

   Service Account

   Specifies whether the discovered account is a service account.

   Note: You can also use the Discover Service Accounts Wizard to discover service accounts.

   Click Finish.

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

More information:

Discover Service Accounts (see page 215)

Create a Privileged or Service Account

You create privileged and service accounts to manage account passwords on managed and disconnected systems. You use privileged and service accounts for different purposes:

- To let users check-out and check-in privileged account passwords, create a privileged account.
- To set up CLI, database, or Windows RunAs password consumers, create a privileged account.
- To set up Windows Services and Windows Scheduled Tasks password consumers, create a service account.

  Note: You cannot check-out and check-in service account passwords.

To create multiple accounts, use the discover privileged accounts wizard and the discover service accounts wizard to search for privileged and service accounts on the endpoints. 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 pre-populated 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, you also need to manually change the account password on the managed endpoint.

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 or service 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 the password you want 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.

Exclusive Session specifies that only a single user can use the account, if no open sessions are currently running on the endpoint.

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.

5. (Optional) Move to the Password Consumers tab.

   If configured, CA Access Control Enterprise Management displays the password consumers that use the privileged account.

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 creates the new privileged or service 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 156)

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
- **llllaaaa**—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 that 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 pre-populated 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 that 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, an additional dialog opens that lets you supply the credentials PUPM requires to manage privileged accounts on that type of endpoint. The endpoint type that you select affects the connection information you have to supply.

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.

   Disable Advance Login

   Specifies to disable the Advanced Login option for this endpoint.

6. (Optional) Click the CA Enterprise Log Manager tab and complete the fields in the tab.

   This tab lets you view CA Enterprise Log Manager reports of privileged account audit events on PUPM endpoints in CA Access Control Enterprise Management. If you have not configured a connection to CA Enterprise Log Manager, this tab does not appear.

   Host Name

   Defines the host name as specified in CA Enterprise Log Manager.

   If you do not type a value in this field, CA Access Control Enterprise Management uses the host name that you specify in the Name field of the General tab.

Event Log Name

Defines the event log name as specified in CA Enterprise Log Manager. For example, the event log name for a Windows Agentless endpoint may be NT-Security.

If you do not type a value in this field, audit events for all endpoint types are displayed when you view a report of privileged account audit events in CA Access Control Enterprise Management.

Note: For more information about event log names, see the CA Enterprise Log Manager documentation.

7. (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.

8. 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 161)
VMware ESX/ESXi Connection Information (see page 170)
Windows Agentless Connection Information (see page 171)
SSH Device Connection Information (see page 180)
SAP R3 Connection Information (see page 189)
CA Identity Manager Provisioning Connection Information (see page 191)
Disconnected Endpoint Connection Information (see page 194)
Create a Login Application (see page 194)

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 the following points:

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.

ACF2 Connection Information

The ACF2 endpoint type lets you manage privileged ACF2 accounts.

When you create endpoints of this type, provide the following information so that the Enterprise Management Server 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 the following points:

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.

Example: *cn=user1,acf2admingrp=lids,host=ACF2,o=company,c=com*

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.

Note: Specify a user account with administrative privileges on both itself and other users accounts.

IBM OS/400 Connection Information

The IBM OS/400 endpoint type lets you manage privileged IBM OS/400 managed accounts.

The administrative user that you specify for an IBM OS/400 endpoint must have privileges to:

- View other user accounts
- View its own user account
- View other user account passwords

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

Name

Specifies the name of the endpoint

Important! Endpoint name must match the host name.

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 the following points:

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.

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.

Important! Host name must match the endpoint 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.

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 the following points:

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.

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.

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 the following points:

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.

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.

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 the following points:

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.

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.

RACF Connection Information

The RACF endpoint type lets you manage privileged RACF accounts.

When you create the RACF endpoint, provide the following information to connect Enterprise Management Server 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 the following points:

- 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.

Important! If you specify the Use IBM LDAP option, enter the IBM LDAP user login.

Example: (CA LDAP) cn=user1,host=RACF,o=company,c=com

Example: (IBM LDAP) racfid=user1,profiletype=user,host=RACF,o=company,c=com

Important! Verify that the administrative user account has the NOEXPIRES operand with PASSWORD or PHRASE options assigned.

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.

Example: (CA LDAP) ldap://host_name.company.com:1589

Example: (IBM LDAP) ldap://host_name.company.com:389

Use IBM LDAP

Specify if IBM LDAP manages RACF.

Note: If you specify the Use IBM LDAP option, then enter the IBM LDAP user login, password, and URL respectively.

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.

Note: Specify a user account with administrative privileges on both itself and other users accounts.

Configure SSL Communication to the RACF Connector

We recommend that you secure the connection between RACF and CA Access Control over SSL. Using SSL you can encrypt data and can reduce security risks. You can configure the Enterprise Management Server to communicate with the RACF endpoint over SSL by installing the RACF certificate in the Enterprise Management Server.

Note: This procedure assumes that you have set up SSL on the RACF endpoint and acquired your RACF certificate.

Important! In environments that are configured for high availability, perform this procedure on all the Distribution and Connector Servers (Primary, Secondary, and Distribution servers).

Follow these steps:

1. Click Windows Start Menu, Settings, Control Panel, Services.

   The Windows Services dialog appears.

2. Stop CA Identity Manager - Connector Server (Java) service.
3. Copy the RACF certificate to the following location:

   CA_home\AccessControlServer\Connector Server\conf

   CA_home

   Specifies the directory where you have installed CA products.

4. Open a command prompt window.
5. Navigate to *CA_home*\AccessControlServer\Connector Server\conf
6. Run the following command:

   ```
   keytool -importcert -trustcacerts -file your_RACF_certificate -keystore
   ssl.keystore
   ```

   Note: When prompted for a password enter the communication password.

   The RACF certificate is registered with JCS.

7. Open the Windows Services dialog.
8. Start CA Identity Manager - Connector Server (Java) service.

You have successfully secured the connection between RACF and CA Access Control.

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 [assign the value for eACVPM in your book] 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.

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 the following points:

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 129)

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 173)

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 172)

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.

More information:

Create a Login Application (see page 194)

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

Modify the Admin Approval Mode

Valid on Windows Server 2008 and Windows 7

PUPM endpoint administration tasks run in the background and require access privileges of a native administrator account. If the PUPM endpoint administrators do not have access to this native administrator account, you must allow all endpoint administrators to run in Admin Approval Mode.

Important: If the policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

Follow these steps:

1. Select Control Panel, Administrative Tools, Local Security Policy

   The Local Security window opens.

2. Browse to Local Policies, Security Options

   The Policy Pane opens.

3. Right-click User Account Control: Run all administrators in Admin Approval Mode and select Properties

   The Properties dialog appears

4. Change the operation mode to Disable and click OK

   The Properties dialog closes.

5. Reboot your computer to apply the change.

   Your background endpoint administration tasks now run successfully.

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 the following points:

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.

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.

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 158). 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 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.

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

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

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.

Network Device Connection Information

The network device endpoint type lets you manage privileged account passwords on network devices.

Note: Currently, you can configure the endpoint type to work with a Cisco 2600 network device only.

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

User Authentication

Specifies the user authentication mode on login:

- Anonymous—No username or password that is required to log in
- Password Only—A password is required to login.
- Username and Password—Username and password are required to log in

Enable Mode Authentication

Specifies the authentication mode to set the device to enable mode:

- Anonymous—No username or password required to login
- Password Only—A password is required to login.
- Username and password—Username and password are required to login.

Note: In Anonymous authentication modes, the following fields are disabled: Username, Password, and Enable Mode Username.

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 the following points:

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.

Enable Login

Defines the name of an administrative user with privileges to set the device to enable mode. Enable mode lets you modify the network device settings.

Host

Defines the host name of the endpoint.

Port

Specifies the server listening port number.

Default: 23

Use Telnet

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

Note: Use Telnet protocol only to connect to the Cisco 2600 network device.

Configuration File

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

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

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.

More information:

Types of SSH Device XML Configuration File (see page 183)
Example: How an SSH Device XML File Defines PUPM Commands (see page 184)

SAP R3 Connection Information

The PUPM SAP R3 endpoint type lets you manage privileged SAP R3 accounts. Before you create SAP R3 endpoints in PUPM, you must configure the SAP R3 connector.

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 the following points:

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.

System ID

Defines the SAP R3 system ID.

System Number

Defines the SAP R3 system number.

Client Number

Defines the SAP R3 system client number.

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.

Note: For more information about the System ID, System Number, and Client Number, see the SAP R3 documentation.

Configure the SAP R3 Connector

Before you can use PUPM to manage privileged accounts on SAP R3 endpoints, you must configure the SAP R3 connector.

To configure the SAP R3 connector, install the SAP JCo library on the Enterprise Management Server or on any server that the Java Connector Server (JCS) is installed on.

You can use your SAP login to download the SAP JCo library from the SAP marketplace. Verify that you select the SAP JCo library that suits the system platforms you use.

Example: Install the SAP JCo library on Windows

The following example shows you how to install the SAP JCo library on a x86 Windows 2003 Server.

1. Extract the sapjco-ntamd64-2.1.9.zip to a temporary directory.
2. Copy the sapjcorfc.dll and librfc32.dll files to the Windows system32 directory.

   Note: If prompted, overwrite any existing files in this directory.
3. Copy the sapjco.jar file to the Java Connector Server extlib directory. This directory is located at:

   ```
   [set Access Path variable]\Connector Server\extlib
   ```
4. Restart the CA Identity Manager - Connector Server service.

   You can now use PUPM to manage privileged accounts on SAP R3 endpoints.

More information:

SAP R3 Connection Information (see page 189)

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 192)

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 *one* of the following:

   a. On Windows, open the Services window, select the CA Identity Manager - Connector Server (Java) service and click stop.

   b. On UNIX, navigate to the following directory, where *ACServerInstallDir* indicates the directory where the Enterprise Management Server is installed:

      ```
      ACServerInstallDir/Connector_Server/bin
      ```

   c. 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 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.

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

To create a login application

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 applicationa 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. 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:

Configure Terminal Integration (see page 252)
Modify Windows Server 2008 Endpoints to Use a Login Application (see page 176)

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, modify, or delete 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, 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, 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.

ADMIN_ACCOUNT_IS_DISCONNECTED

Specifies if the endpoint administrator account is disconnected.

Values: TRUE, FALSE

Default: TRUE

DISABLE_EXCLUSIVE_SESSIONS

Specifies whether to disable the exclusive sessions option on this endpoint.

Values: TRUE, FALSE

Default: FALSE

DENY_BREAKGLASS_EXCLUSIVE

Specifies whether to prevent access to exclusive accounts who are in operation using break glass.

Values: TRUE, FALSE

Default: FALSE

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 for processing 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/waiting
   ToBeProcessed
   ```

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 183)
How to Create a Customized SSH Device Endpoint (see page 182)

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. 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, 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 that you change the password in PUPM, manually change the account password on the managed endpoint.

Values: TRUE, FALSE

EXCLUSIVE_ACCOUNT

Specifies if a single user can check out the account at any time.

If you specify EXCLUSIVE, PUPM lets a single user check-out the account at any time. If you specify EXCLUSIVE_SESSIONS, PUPM denies check-in to an open session exclusive account. If you specify NONE, PUPM allows multiple users to check-out simultaneously.

Values: EXCLUSIVE_SESSIONS, EXCLUSIVE, NONE

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.

CHANGE_PASSWORD_ON_CHECKOUT

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

Values: TRUE, FALSE

Default: FALSE

CHANGE_PASSWORD_ON_CHECKIN

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, program, or when the checkout period expires.

Values: TRUE, FALSE

Default: TRUE

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.

How to Set Up Password Consumers

Password consumers are applications, Windows services, and Windows scheduled tasks that use privileged accounts and service accounts to execute a script, connect to a database, or manage a Windows service, scheduled task, or RunAs command. Password consumers let you remove hard-coded passwords from application scripts and enforce a password policy on service accounts.

There are two groups of password consumers:

- Password consumers that get passwords on demand—Database, Windows Run As, software development kit
- Password consumers that get passwords on password change—Windows Scheduled Task, Windows Service

Software development kit password consumers get, check out, and check in privileged account passwords. All other types of password consumer get privileged account passwords, but do not check out or check in passwords.

The following process explains the tasks that users in your enterprise must complete to set up password consumers. 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.

To set up password consumers, users do the following:

1. A system administrator configures the endpoints, as follows:

   a. Installs CA Access Control on endpoints that use database, Windows Run As, and software development kit password consumers.

      The system administrator enables the PUPM Integration feature during the installation process.

      Note: You do not need to install CA Access Control on the endpoint to use Windows Scheduled Task or Windows Service password consumers.

   b. Performs additional configuration steps on endpoints that use the following password consumers:

      - Database (JDBC)—Prepares the endpoint to use a database (JDBC) password consumer (see page 237).
      - Database (ODBC, OLEDB, OCI)—Configures the endpoint to use a database (ODBC, OLEDB, OCI) password consumer (see page 243).
      - Database (.NET)—Configures the endpoint to use a database (.NET) password consumer (see page 244).
      - Software Development Kit (CLI)—Configures the endpoint to use a CLI password consumer (see page 246).
      - Software Development Kit (SDK)—Configures the endpoint to use the PUPM SDK (see page 248).

   The endpoints are configured to use password consumers.

2. The PUPM Target System Manager role creates password policies in CA Access Control Enterprise Management. Password policies set password rules and password expiration intervals for privileged and service accounts.

3. The PUPM Target System Manager creates endpoints in CA Access Control Enterprise Management. Endpoints are devices that are managed by privileged and service accounts. You can create endpoints in CA Access Control Enterprise Management or use the PUPM feeder to import endpoints.

   Note: If you have already created your endpoints when you set up privileged accounts, do not complete this step.

4. To create database, Windows Run As, or software development kit password consumers, users do the following:

   a. The PUPM Target System Manager discovers or creates privileged accounts in CA Access Control Enterprise Management.

      This user can discover and create privileged accounts in CA Access Control Enterprise Management or use the PUPM feeder to import privileged accounts.

b. The System Manager creates database, Windows Run As, and software development kit password consumers in CA Access Control Enterprise Management.

   The System Manager associates database, Windows Run As, and software development kit password consumers with privileged accounts as part of the password consumer creation task.

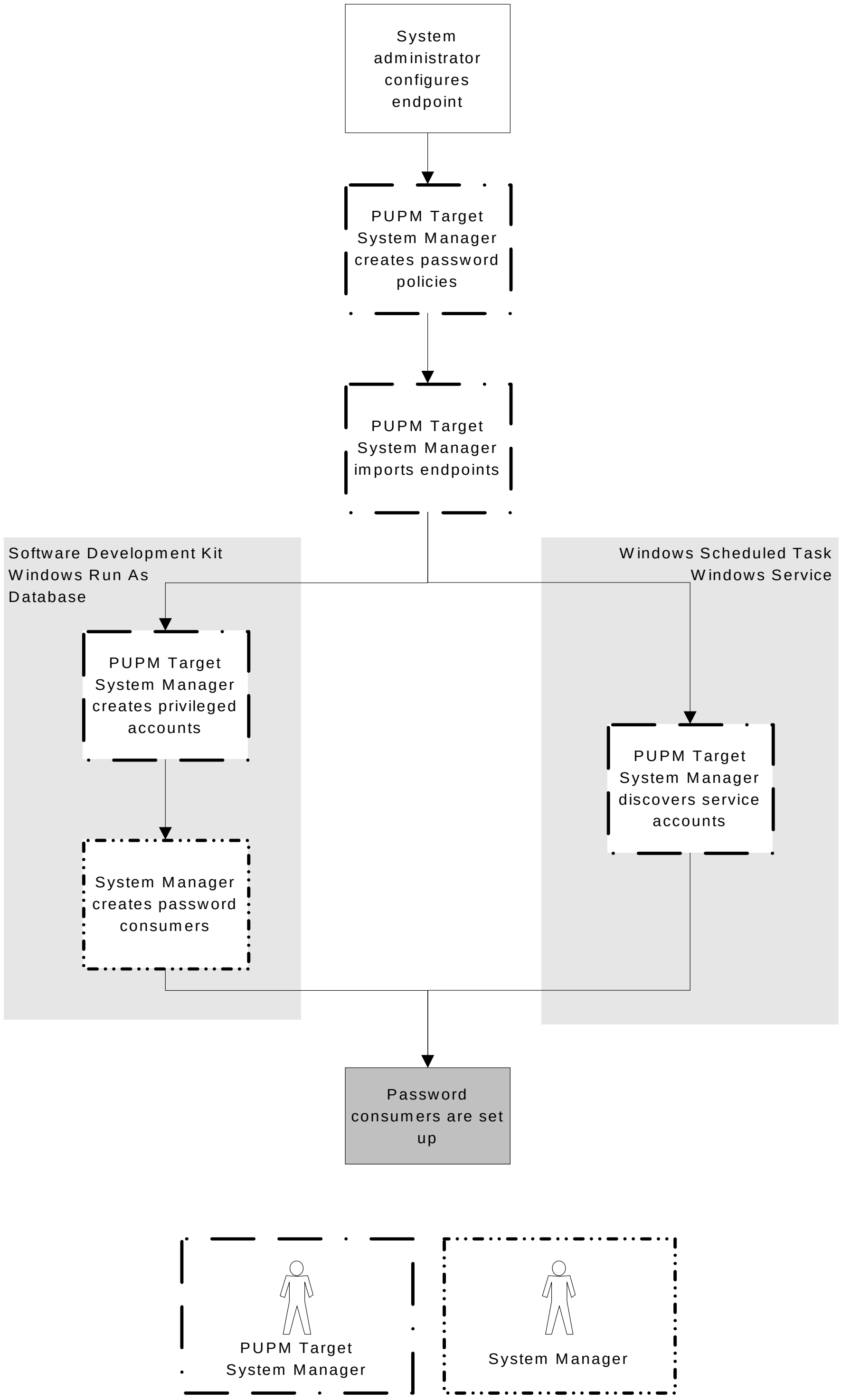
5. To create Windows Scheduled Task or Windows Service password consumers, the PUPM Target System Manager discovers service accounts.

   CA Access Control Enterprise Management creates password consumers for each service and scheduled task that it discovers.

   Note: CA Access Control Enterprise Management discovers only services that are run by accounts for which you can change the password. For example, CA Access Control Enterprise Management discovers services that are run by your computer's Administrator account or domain accounts, but does not discover services that are run by the NT AUTHORITY\Local Service account.

   Password consumers are now set up for your enterprise.

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


System administrator configures endpoint
PUPM Target System Manager creates password policies
PUPM Target System Manager imports endpoints
Software Development Kit
Windows Run As
Database
Windows Scheduled Task
Windows Service
PUPM Target System Manager creates privileged accounts
System Manager creates password consumers
PUPM Target System Manager discovers service accounts
Password consumers are set up
PUPM Target System Manager
System Manager

Discover Service Accounts

Service Accounts are internal accounts used by Windows services. These services provide core operating system and other functionality to the computer. You can protect these services from potential attacks by managing the service account passwords from CA Access Control Enterprise Management.

You can discover service accounts that manage services and scheduled tasks on Windows Agentless endpoints. Discovering service accounts lets you create multiple service accounts in CA Access Control Enterprise Management at the same time and assign password consumers to the service accounts. If you do not want to create password consumers for the service account, use the Create a Privileged or Service Account task to create the service account.

Note: To discover privileged accounts, use the Discover Privileged Accounts Wizard.

The Discover Service Accounts Wizard does not discover all the services on the endpoint. It discovers only services run by accounts for which you can change the password. For example, CA Access Control Enterprise Management discovers services that are run by your computer's Administrator account or domain accounts, but does not discover services that are run by the NT AUTHORITY\Local Service account.

To discover service accounts

1. (Optional) To discover service accounts that are domain accounts, verify that the domain controller (DC) on which the accounts exist is defined in CA Access Control Enterprise Management with the following attributes:

   - Endpoint type—Windows Agentless
   - Is Active Directory—True
   - Host Domain—The domain name of which the DC is a member
   - User Domain—The domain name of which users defined on the DC are members

     Note: Specify the user domain only if the administrative account is from a different domain than the domain in which the accounts reside.

   The Discover Service Accounts Wizard can now discover service accounts that are domain accounts.

2. In CA Access Control Enterprise Management, select Privileged Accounts, Accounts, Discover Service Accounts Wizard.

   The Discover Service Accounts Wizard window opens.

   Note: The value of the Endpoint Type field is Windows Agentless because PUPM manages service accounts only on Windows Agentless endpoints.

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

   A list of service accounts that match the filter criteria appears, and a list of Windows services and scheduled tasks that use the service accounts. If the wizard discovers an account from an unknown domain, a warning message appears.

   Note: The process may take some time to complete. The services and scheduled tasks are listed in the Password Consumer column. The icons in this column let you see at a glance which password consumers are services and which are scheduled tasks.

4. Select the services and scheduled tasks that you want to use password consumers to manage, then click Next.

   The General Account Properties window appears.

5. Select the password policy to assign to the services and scheduled tasks, then click Next.

   The Summary window appears.

6. Review the summary then click Finish.

   CA Access Control Enterprise Management submits the task and adds the service accounts if there are no errors. After CA Access Control Enterprise Management adds the service account, it automatically creates a password consumer for each service and scheduled task that you selected. You can use the appropriate password consumer task to view and modify the password consumers.

Create a Password Consumer

Password consumers are applications, Windows services, and Windows scheduled tasks that use privileged accounts and service accounts to execute a script, connect to a database, or manage a Windows service, scheduled task, or RunAs command.

There are two groups of password consumers:

- Password consumers that get passwords on demand—Software development kit, database, Windows Run As

  Note: You must install CA Access Control on the PUPM endpoint with the PUPM Integration feature enabled to use password consumers that get passwords on demand.

- Password consumers that get passwords on password change—Windows Scheduled Task, Windows Service

You provide different information to create password consumers from each group. By default, you must have the System Manager role to create a password consumer.

Note: Complete this task if you create a password consumer of types software development kit, database, and Windows Run As. We recommend that you use the Discover Service Accounts Wizard to create Windows Scheduled Task or Windows Service password consumers.

To create a password consumer

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

   The Create Password Consumer: Password Consumer Search screen page appears.

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

   a. Select Create a copy of an object of type Password Consumer.

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

      A list of password consumers that match the filter criteria appears.

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

3. Click OK.

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

4. Complete the following fields in the General tab:

   Name

   Defines the name you want to refer to this password consumer by.

   Description

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

   Consumer Type

   Specifies the type of the password consumer.

   Application Path

   (Software development kit, database, Windows Run As, Windows Scheduled Task) Defines the full pathname of the password consumer on the endpoint.

   - For software development kit password consumers, specify the pathname of the application that performs the password request.
   - For database password consumers, specify the pathname of the application that connects to the database.
   - For Windows Run As password consumers, specify the pathname of the application that the user executes.
   - For Windows Scheduled Task password consumers, specify the pathname of the scheduled task.

   Note: You can use wildcards (*) and CA Access Control variables in the pathname, for example, <!AC_ROOT_PATH>\bin\acpwd.exe.

   Service Name

   (Windows Service) Defines the pathname of the Windows service. Specify the pathname exactly as it appears in the Windows service properties page.

   Enabled

   Specifies that the password consumer is enabled, that is, that PUPM accepts requests from this consumer or enforces password change on this consumer.

   Status

   (Windows Scheduled Task or Windows Service) Indicates whether the last password change succeeded or failed.

   Last Synchronized Date

   (Windows Scheduled Task or Windows Service) Displays the last successful password synchronization.

   Restart

   (Windows Service) Specifies whether to restart the Windows service after a password change.

5. Click the Privileged Accounts tab and specify the privileged accounts that are associated with the password consumer.

   If you create a software development kit, database, or Windows Run As password consumer, the password consumer can get the passwords for the privileged accounts that you specify.

   If you create a Windows Scheduled Task or Windows Service password consumer, PUPM forces a password change for the password consumer when the passwords for these privileged accounts are changed.

6. Specify the entities that can use the password consumer. Do *one* of the following:

   - To create a software development kit, database, or Windows Run As password consumer, do the following:

     a. Click the Hosts tab and specify the hosts or host groups from which the password consumer can get the privileged account password, or select All Hosts to grant all hosts or host groups access to the privileged account password.

        Note: You can type the name of the host or host group in the Name field, or click "..." to search for a CA Access Control host or host group (HNODE or GHNODE object).

     b. Click the Users tab and specify the users or groups who can request the privileged account password, or select All Users to let every user request the privileged account password.

        Specify the name of the user or group as it appears on the endpoint, for example, DOMAIN\user1. Do not specify a CA Access Control Enterprise Management user or group.

   - To create a Windows Scheduled Task or Windows Service password consumer, click the Endpoints tab and specify the endpoints on which you want to create the password consumer.

7. Click Submit.

   CA Access Control Enterprise Management creates the password consumer.

More information:

Types of Password Consumers (see page 118)

Password Consumer Example: Windows Run As

The Windows RunAs application lets a user borrow permissions from a privileged account to perform a specific task. You can create a Windows Run As password consumer so that when a user executes RunAs, the PUPM Agent provides the privileged account password directly to the RunAs application. The Windows Run As password consumer removes the need for users to know privileged account passwords to perform administrative tasks.

You can create Windows Run As password consumers only on Windows Agentless endpoints.

In the following example, a backup task is scheduled to run weekly. The task is located at C:\backup\backup.exe and is run by Administrator. If the scheduled backup fails, the system administrator Steve wants to let user John manually start the backup. Steve can use a Windows Run As password consumer to let John start the backup task without the Administrator password.

The following process describes the steps that Steve and John perform to create and use a Windows Run As password consumer on an endpoint named win123_PUPM:

1. Steve installs CA Access Control on win123_PUPM with the PUPM Integration feature enabled.
2. Steve does the following in CA Access Control Enterprise Management:
    a. Creates a Windows Agentless endpoint named win123_PUPM.
    b. Discovers the Administrator privileged account on the win123_PUPM endpoint.
    c. Creates a Windows Run As password consumer using the following parameters:
        - Name—win123_PUPM Backup RunAs
        - Consumer Type—Windows Run As
        - Application Path—C:\backup\backup.exe
        - Account—Administrator
        - Host—win123_PUPM
        - User—Domain1\John

          Note: Steve enters John's user name as it appears on the endpoint.

   The Windows Run As password consumer is created.

3. The scheduled backup task fails and John logs on to win123_PUPM to manually start the backup. He executes the RunAs command to start the backup task, using the following parameters:

   - Account—Administrator
   - Password—no password

     Note: The PUPM Agent ignores any value that John provides for the password.

   The PUPM Agent checks the cache for previous requests by John to start the backup task. Because John has made this request for the first time, the request is not cached. The PUPM Agent retrieves the privileged account password from CA Access Control Enterprise Management and provides it to the RunAs application. The backup task starts.

Password Consumer Example: Windows Scheduled Task

Windows Scheduled Task and Windows Service password consumers help you automate password changes for service accounts. Service accounts are internal accounts used by Windows services. For example, if you configure a scheduled task to regularly check for software updates, the scheduled task uses a service account to log in to the endpoint and perform the task.

You can create Windows Scheduled Task and Windows Service password consumers only on Windows Agentless endpoints. You do not need to install CA Access Control on the endpoint to use Windows Service and Windows Scheduled Task password consumers.

You can create Windows Service password consumers only for services that are run by accounts for which you can change the password. For example, you can create a password consumer for a service that is run by your computer's Administrator account; you cannot create a password consumer for a service that is run by the NT AUTHORITY\Local Service account.

In the following example, the system administrator Steve wants to create a password consumer for a scheduled task that checks for software updates on a Windows endpoint named win456. The scheduled task uses the win456\ServiceAdmin account to log in to the endpoint.

Steve does the following in CA Access Control Enterprise Management:

1. Steve creates a password policy named 30days. The password policy specifies that CA Access Control Enterprise Management changes the password for service accounts every 30 days and that the password can be changed only on Sundays between 1 a.m. and 3 a.m.
2. Steve creates a Windows Agentless endpoint named win456.

3. Steve uses the service account discovery wizard to discover the win456\ServiceAdmin account on the win456 endpoint, and applies the 30days password policy to the service account.

4. CA Access Control Enterprise Management creates a Windows Scheduled Task password consumer using the following parameters:

   - Name—UpdateTask (C:\WINDOWS\Tasks\UpdateTask.bat) at win456
   - Consumer Type—Windows Scheduled Task
   - Application Path—C:\WINDOWS\Tasks\UpdateTask.bat
   - Privileged Account—win456\ServiceAdmin
   - Endpoints—win456

   Steve has created the password consumer. Each time that CA Access Control Enterprise Management changes the password for the win456\ServiceAdmin account, the JCS logs in to the win456 endpoint and changes the password of the software update scheduled task. If the password change does not succeed, Steve can use the Synchronize Password Consumers task to retry the password change.

More information:

Synchronize Password Consumers (see page 263)

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.

More information:

Create a Login Application (see page 194)

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 224)

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")

`LaunchеProcessAsUser (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")

Customizing the PUPM Remote Desktop Script

The PUPM remote desktop script configures the Remote Desktop settings. PUPM launches the remote desktop script to automatically login a user into a Windows Agenless endpoint. You can customize the PUPM remote desktop script to control the application parameters.

The PUPM remote desktop uses the following commands:

SetRDPOption(BSTR *bsName*, BSTR *bsType*, BSTR *bsValue*

bsName

Specifies the name of the parameter to modify

bsType

Specifies the parameter type

bsValue

Defines the parameter value

Example: Configure the Remote Desktop application settings

The following example shows the commands you use to set the remote desktop window to full screen and re-direct the local drive to the remote endpoint drive:

```
Dim hwnd
Set test = CreateObject("ACLauncher.ACWebLauncher")
test.SetRDPOption "screen mode id","i","2"
test.SetRDPOption "redirectdrives","i","1"
hwnd = test.LauncheRDP("computer1", "computer1\administrator", "xxxxxx")
```

The following table contains the possible parameters and values that you can use to modify the Remote Desktop script:

	Type	Value	Options
alternate shell	String	c:\winnt\system32\notepad.exe	Defines the shell to use within the Terminal Services session. Use this parameter to set an alternate shell such as progman.exe. You can also use it to set the application that the user uses to login to the Terminal Server.
audiomode	Integer	2	0 - Bring audio to this computer 1 - Leave audio on remote computer 2 - Do not play audio
autoreconnection enabled	Integer	1	Automatically connect when file is opened.
connect to console	Integer	1	0 - connect to a virtual session 1 - connect to the console session
desktopheight	Integer	768	Defines the height of remote desktop in pixels
desktopwidth	Integer		Defines the width of remote desktop in pixels
disable full window drag	Integer	1	Disables window display while dragging
disable menu anims	Integer	1	Disables menu animations
disable themes	Integer	1	Disables themes in session
disable wallpaper	Integer	1	Disable wallpaper display
displayconnection bar	Integer	1	Displays the connection bar in a full screen session

	Type	Value	Options
keyboardhook	Integer	2	Applies standard Windows key combinations 0 - On the local computer 1 - On the remote computer 2 - In fullscreen mode only
maximizeshell	Integer	0	Specifies to maximize any alternate shell used in the session
redirectcomports	Integer	1	Specifies to redirect client COM ports in session
redirectdrives	Integer	1	Specifies to redirect client drives in session
redirectprinters	Integer	1	Specifies to redirect client printers in session
redirectsmartcards	Integer	1	Specifies to redirect client smart cards in session
screen mode id	Integer	1	Defines the screen mode 1 - windowed 2 - fullscreen
server port	Integer	3389	Define the port number in the "full address" parameter
session bpp	Integer	16	Specifies the bit depth per session 8, 16, 24. 8 bit is valid for Windows 2000 Terminal Servers
shell working directory	String	c:\program files\microsoft office	Defines a working directory for an alternate shell if specified
smart sizing	Integer		Specifies to scale the client window display of desktop when resizing 0 or not present - do not scale 1 - Scale (Takes extra resources to scale)

	Type	Value	Options
winposstr	String	0,1,0,249,808, 876	Specifies the "window mode" sizes - maximized versus sized.

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.

Terminal Integration

Terminal integration lets you integrate your CA Access Control endpoints with PUPM to track the activities of users who use privileged accounts. Terminal integration works only when a user checks out a privileged account password and uses automatic login to log in to the CA Access Control endpoint.

Terminal integration lets you increase security and accountability, as follows:

- To increase security, you can specify that a user must use PUPM automatic login to log in to the endpoint.
- To increase accountability, you can specify that CA Access Control uses the original user name, not the privileged account user name, when it writes audit records and makes authorization decisions.

If you specify that CA Access Control uses the original user name when it writes audit records and makes authorization decision, CA Access Control accumulates the audit mode for the login session. The accumulated audit mode uses the audit mode for the original user and the audit mode for the privileged account. If the original user is not defined in the CA Access Control database, CA Access Control accumulates the audit mode for the default user and the audit mode for the privileged account.

For example, you configure terminal integration for an endpoint. On the endpoint, the audit mode for user1 (the original user) is Failure and the audit mode for a privileged account named privileged_user is Success. When user1 uses automatic login to log in to the endpoint as privileged_user, CA Access Control sets the audit mode for the login session to Failure, Success.

You can use terminal integration only on Windows Agentless and SSH Device endpoints on which CA Access Control is installed. In addition, the user must use automatic login to check out the privileged account password.

Terminal integration is enabled by default when you install CA Access Control with the PUPM integration feature enabled. After you install CA Access Control, you use CA Access Control Endpoint Management to configure terminal integration on the endpoint.

Example: A Login Event Audit Record

The following example shows a login event audit record for an account for which you configured terminal integration. You specified that a user must use PUPM automatic login to log in to the endpoint.

```
Event type: Login attempt
Status: Denied
User name: example1\administrator
Terminal: example1.domain.com
Program: Terminal services
Date: 27 May 2010
Time: 17:35
Details: Automatic login is required for this account
User Logon Session ID: 7dd2b3dc-8a1a-4ffa-8e7d-f9bc20d2b341
Audit flags: OS user
```

Example: A Resource Access Audit Record

The following example shows a resource access audit record for an account for which you configured terminal integration. You specified that CA Access Control uses the original user name, not the privileged account user name, when it writes audit records and makes authorization decisions. The original user name (user1) is listed in the user name field and the privileged account (administrator) is listed in the effective user name field.

```
Event type: Resource access
Status: Denied
Class: FILE
Resource: C:\tmp\core.txt
Access: Exec
User name: domain\user1
Terminal: example1.domain.com
Program: C:\WINDOWS\system32\cmd.exe
Date: 02 Feb 2010
Time: 14:20
Details: No Step that allowed access
User Logon Session ID: 7dd2b3dc-8a1a-4ffa-8e7d-f9bc20d2b341
Audit flags: OS user
Effective user name: example1\administrator.
```

More information:

Configure Terminal Integration (see page 252)
Implementation Considerations for Terminal Integration (see page 236)

How Terminal Integration Works

Terminal integration lets you integrate your CA Access Control endpoints with PUPM to increase security and accountability.

The following process explains how terminal integration works:

1. A user uses automatic login to check out a privileged account password in CA Access Control Enterprise Management.
2. CA Access Control Enterprise Management retrieves the endpoint details from the DMS and sends a pre-login message to the Message Queue. The message contains the name of the privileged account, the name of the user that checked out the account, and the name of the endpoint.
3. The PUPM Agent on the CA Access Control endpoint retrieves the pre-login message from the Message Queue.
4. When a user uses the privileged account to log in to the endpoint, the CA Access Control authorization engine checks the local database record for the privileged account and takes the following actions:
   a. The engine checks if the account requires an account checkout prior to login, that is, if a user must use automatic login to log in to the endpoint. *One* of the following occurs:
      - If an account checkout is required and the PUPM Agent has not received a pre-login message for the privileged account, the engine rejects the login attempt.
      - If an account checkout is required and the PUPM Agent has received a pre-login message for the privileged account, the engine permits the login if no additional restrictions exist, for example, if no TERMINAL restrictions exist that prevent the login.
      - If an account checkout is not required, the engine permits the login if no additional restrictions exist.

   b. The engine checks if the user's original identity must be used to make authorization decisions. *One* of the following occurs:
      - If the user's original identity must be used, the engine uses the original user name to evaluate resource access requests and to write audit records.
      - If the user's original identity is not used, the engine uses the privileged account name to evaluate resource access requests and to write audit records.

More information:

Configure Terminal Integration (see page 252)
Implementation Considerations for Terminal Integration (see page 236)

Implementation Considerations for Terminal Integration

Before you implement terminal integration, consider the following:

- You can configure terminal integration on Windows Agentless and SSH endpoint types on which CA Access Control is installed. You cannot configure terminal integration on other endpoint types.
- (UNIX) CA Access Control must use PAM login interception for the login program that is used to connect to the endpoint. For example, if users use SSH to connect to the endpoint, CA Access Control must use PAM login interception to intercept SSH logins.

  To specify that CA Access Control uses PAM login interception for a login program, set the loginflags(pamlogin) flag in the LOGINAPPL record for the login program. For example:

  ```
  editres loginappl SSH loginflags(pamlogin)
  ```
- You can enable terminal integration only for privileged account logins. Login integration does not work for service account logins.
- Terminal integration works only if you use automatic login to check out the privileged account.
- (UNIX) You can use terminal integration for only SSH logins. This restriction exists because terminal integration works only when a user uses PUPM automatic login to check out a privileged account password and log in to the CA Access Control endpoint, and PUPM provides only a login script for SSH logins.

  If you write customized scripts to create login applications for other login types and you want to enable terminal integration for the other login types, set the loginflags(pamlogin) property for the LOGINAPPL record for the appropriate login program.

More information:

Configure Terminal Integration (see page 252)

Chapter 7: Configuring PUPM Endpoints

This section contains the following topics:

Prepare a JBoss Application to Use a Database (JDBC) Password Consumer (see page 237)
Additional Information for Oracle Databases (see page 242)
Configure an Endpoint to Use a Database (ODBC, OLEDB, OCI) Password Consumer (see page 243)
Configure an Endpoint to Use a Database (.NET) Password Consumer (see page 244)
Configure an Endpoint to Use a CLI Password Consumer (see page 246)
How to Configure an Endpoint to Use a Password Consumer SDK Application (see page 248)
How to Configure an Endpoint to Use a Web Services PUPM SDK Application (see page 251)
Configure Terminal Integration (see page 252)

Prepare a JBoss Application to Use a Database (JDBC) Password Consumer

You can use JDBC database password consumer to replace hard-coded passwords in applications that use JDBC to connect to a database. Whenever an application provides a password for authentication purposes, the PUPM Agent gets the privileged account password from CA Access Control Enterprise Management and replaces the hard-coded password with the privileged account password.

Before you configure the databases that the password consumer uses, you should prepare the endpoint to use a JDBC password consumer.

To prepare a JBoss application to use a database (JDBC) password consumer

1. Verify that CA Access Control is installed on the endpoint with the PUPM Integration feature enabled, and that the application that connects to the database uses JRE 1.5 or later.

   Note: Install CA Access Control on the endpoint on which the application that connects to the database is installed. You do not need to install CA Access Control on the database host.

2. Stop the application that connects to the database, if it is running.

3. Navigate to the following directory, where *ACInstallDir* is the directory in which you installed CA Access Control:

   ```
   ACInstallDir/SDK/JDBC
   ```

4. Locate the following files:

    - CAJDBCService.sar
    - CAJDBCDriver.jar
    - CAPUPMClientCommons.jar
    - jsafeFIPS.jar

5. Copy the CAJDBCService.sar to the following directory, where *JBOSS_HOME* is the directory where you installed JBoss*:*

    ```
    JBOSS_HOME/server/default/deploy
    ```

6. Copy the files CAJDBCDriver.jar, CAPUPMClientCommons.jar, and jsafeFIPS.jar to the following directory:

    ```
    JBOSS_HOME/server/lib
    ```

7. On the Enterprise Management Server, locate the data source XML files you defined for the password consumer.

8. Open the files for editing. Do *one* of the following:

    - Customize the datasource configuration files for Microsoft SQL Server (see page 239)
    - Customize the datasource configuration files for Oracle (see page 239)

    You customize the datasource configuration files to specify the database connection settings and datasource class.

9. Start CA Access Control.

    You have configured the endpoint to use the password consumer. You must now create a password consumer for the application in CA Access Control Enterprise Management. You start the application after you create the password consumer.

More information:

Password Consumer Example: JDBC Database (see page 240)
Create a Password Consumer (see page 217)

Customize the Datasource Configuration Files for Microsoft SQL Server

You can configure a JDBC database password consumer to replace hard-coded passwords in applications that use JDBC to connect to a Microsoft SQL Server database. Complete the following steps after you have prepared the endpoint to use a JDBC password consumer.

To customize the datasource configuration files for Microsoft SQL Server

1. Locate the <driver-class> tag and replace the default value with the JDBC driver class properties. For example:

   ```
   <driver-class>com.ca.ppm.clients.jdbc.CAJDBCDriver</driver-class>
   ```

2. Locate the <connection-url> tag and replace the default value with the database connection settings. For example:

   ```
   <connection-url>>@@@com.microsoft.sqlserver.jdbc.SQLServerDriver@@@jdbc:sqlse
   rver://SQLServer1:1433;selectMethod=cursor;DatabaseName=tempdb</connection-ur
   l>
   ```

3. Start CA Access Control.

   You have customized the datasource configuration files to Microsoft SQL Server. You must now create a password consumer for the application in CA Access Control Enterprise Management. You start the application after you create the password consumer.

Customize the Datasource Configuration files for Oracle

You can configure a JDBC database password consumer to replace hard-coded passwords in applications that use JDBC to connect to an Oracle database. Complete the following steps after you have prepared the endpoint to use a JDBC password consumer.

To customize the datasource configuration files for Oracle

1. Locate the <xa-datasource-class> tag and replace the default value with the CAJDBCDataSource class properties. For example:

   ```
   <xa-datasource-class>com.ca.ppm.clients.jdbc.CAJDBCDataSource</xa-datasource-
   class>
   ```

   Important! The property names must remain in the same case as the default value.

2. Locate all the <xa-datasource-property name=> tags. For example:

   ```
   <xa-datasource-property
   name="URL">jdbc:oracle:oci8:@tc</xa-datasource-property>
   <xa-datasource-property name="User">scott</xa-datasource-property>
   <xa-datasource-property name="Password">tiger</xa-datasource-property>
   ```

3. Formulate the properties into a single string. For example:

   ```
   <xa-datasource-property
   name="CAJDBCProperties">CAJDBCPropertyRealDatasourceClass="oracle.jdbc.xa.cli
   ent.OracleXADataSource";URL="jdbc:oracle:oci8:@tc";User="scott";Password="tig
   er";</xa-datasource-property>
   ```

4. Start CA Access Control.

   You have customized the datasource configuration files for Oracle. You must now create a password consumer for the application in CA Access Control Enterprise Management. You start the application after you create the password consumer.

Password Consumer Example: JDBC Database

In this example, the system administrator Steve uses a JBoss application server to run an application that contains a password in clear text. The application uses the clear-text password to authenticate a connection to a Microsoft SQL Server database. Steve wants to modify the JBoss application server so that the application gets the privileged account password from PUPM each time the application connects to the database.

Steve has installed JBoss application server version 4.2.3.GA and Java Development Kit (JDK) 1.6.0_19 on the Windows endpoint. The endpoint is named JBossEndpoint. The user named JBossEndpoint\Administrator uses the run.bat file to start the JBoss application server, which runs the application that connects to the Microsoft SQL Server database. The application uses the sa account to connect to the database.

1. Steve does the following on JBossEndpoint:

   a. Stops JBoss.

   b. Installs CA Access Control with the PUPM Integration feature enabled.

   c. Navigates to the following directory:

      ```
      C:\Program Files\CA\AccessControl\\SDK\JDBC
      ```

   d. Locates the following files:

      - CAJDBCService.sar
      - CAJDBCDriver.jar
      - CAPUPMClientCommons.jar
      - jsafeFIPS.jar

   e. Copies the file CAJDBCService.sar to the following directory:

      ```
      C:\jboss-4.2.3.GA\server\default\deploy
      ```

   f. Copies the files CAJDBCDriver.jar, CAPUPMClientCommons.jar, and jsafeFIPS.jar to the following directory:

      ```
      C:\jboss-4.2.3.GA\server\default\lib
      ```

g. Navigates to the following directory:

```
C:\jboss-4.2.3.GA\server\default\deploy
```

h. Opens the following files for editing:

- imworkflowdb-ds.xml
- objectstore-ds.xml
- reportsnapshot-ds.xml
- userstore-ds.xml

i. Locates the <driver-class> tag and replaces the default value with the JDBC driver class properties. For example:

```
<driver-class>com.ca.ppm.clients.jdbc.CAJDBCDriver</driver-class>
```

j. Locates the <connection-url> tag and replaces the default value with the database connection settings. For example:

```
<connection-url>>@@@com.microsoft.sqlserver.jdbc.SQLServerDriver@@@jdbc:sqlserver://SQLServer1:1433;selectMethod=cursor;DatabaseName=tempdb</connection-url>
```

k. Saves and closes the files.

l. Starts CA Access Control.

2. Steve does the following in CA Access Control Enterprise Management:

   a. Creates an endpoint of type Windows Agentless named JBossEndpoint_PUPM.

   b. Discovers the sa privileged account on the JBossEndpoint_PUPM endpoint.

   c. Creates a database password consumer using the following parameters:

      - Name—JBossEndpoint MS SQL connection
      - Consumer Type—Database (ODBC/JDBC/OLEDB/OCI)
      - Application Path—C:\jboss-4.2.3.GA\bin\run.bat
      - Account—sa
      - Host—JBossEndpoint
      - User—JBossEndpoint\Administrator

3. The JBossEndpoint\Administrator user starts the JBoss application server on the endpoint by running the run.bat file.

   The JBoss application server starts and the application attempts to connect to the SQL Server. The PUPM Agent intercepts the connection attempt and provides the privileged account password to the application.

4. Steve checks the JBoss log file in the following directory for errors:

```
C:\jboss-4.2.3.GA\server\default\log
```

Additional Information for Oracle Databases

The tnsnames.ora file is an Oracle configuration file that defines database addresses that clients use to connect to an Oracle database. The tnsnames.ora file may contain multiple host names, ports, service names, instance names, or SIDs.

The PUPM Agent resolves the $ORACLE_HOME and $TNS_ADMIN environment variables to resolve the full path of the tnsnames.ora file. The environment variables are defined in the following registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\Plug
Ins\plugin\EnvironmentVariables
```

plugin

Specifies the name of the plug-in that intercepts the connection attempt.

Values: OCIPlg, ODBCPlg, OLEDBPlg

The PUPM Agent parses the tnsnames.ora file each time it intercepts a connection attempt to an Oracle database. If the file contains multiple values for any of these attributes, the PUPM Agent creates a separate network set for each possible attribute combination. The PUPM Agent sends all the network sets to CA Access Control Enterprise Management, which gets the password for the privileged account that most closely matches the network set.

Example: Network Sets In a tnsnames.ora File

The following is an example of the tnsnames.ora file:

```
SAMPLE_INSTANCE=
 (DESCRIPTION=
   (SOURCE_ROUTE=yes)
   (ADDRESS=(PROTOCOL=tcp)(HOST=host1)(PORT=1630))    # hop 1
   (ADDRESS_LIST=
     (FAILOVER=on)
     (LOAD_BALANCE=off)                               # hop 2
     (ADDRESS=(PROTOCOL=tcp)(HOST=host2a)(PORT=1630))
     (ADDRESS=(PROTOCOL=tcp)(HOST=host2b)(PORT=1630)))
   (ADDRESS=(PROTOCOL=tcp)(HOST=host3)(PORT=1521))    # hop 3
   (CONNECT_DATA=(SERVICE_NAME=Sales.example.com)))
```

When the PUPM Agent parses this tnsnames.ora file, it sends the following network sets to CA Access Control Enterprise Management:

- HOST=host1, PORT=1630
- HOST=host2a, PORT=1630
- HOST=host2b, PORT=1630
- HOST=host3, PORT=1521, SERVICE_NAME= Sales.example.com

Configure an Endpoint to Use a Database (ODBC, OLEDB, OCI) Password Consumer

Valid for Windows Agentless endpoints

You can use ODBC, OLEDB or OCI database password consumers to replace hard-coded passwords in applications that use ODBC, OLEDB or OCI to connect to a database. When an application tries to connect to the database, the PUPM Agent intercepts the connection attempt and replaces the hard-coded password with the privileged account password that it retrieves from CA Access Control Enterprise Management.

The application must reside on a Windows Agentless endpoint on which CA Access Control is installed. If you want to create an OCI database password consumer, verify that the application uses OCI8 or later.

PUPM uses a different plug-in to intercept each type of connection attempt. For example, the OCI plug-in intercepts connection attempts that use OCI. The following registry key controls the behavior of CA Access Control plug-ins:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\Plug
Ins
```

The settings for each plug-in are located in the following subkeys:

- OCI—Instrumentation\PlugIns\OCIPlg
- ODBC—Instrumentation\PlugIns\ODBCPlg
- OLEDB—Instrumentation\PlugIns\OLEDBPlg

To configure an endpoint to use a database (ODBC, OLEDB, OCI) password consumer

1. Verify that CA Access Control is installed on the endpoint with the PUPM Integration feature enabled.

   Note: Install CA Access Control on the endpoint on which the application that connects to the database is installed. You do not need to install CA Access Control on the database host.

2. Stop CA Access Control on the endpoint.

3. In the appropriate registry subkey for the connection type, do the following:

   - Verify that the value of the OperationMode registry entry is 1.

     This registry entry enables the plug-in.

- Verify that the name of the process that runs the application is a value of the ApplyOnProcess registry entry.

  This registry entry specifies the processes to which the plug-in applies. For example, if you are creating a password consumer for an IIS application, verify that w3wp.exe is a value of the registry entry.

  Note: We recommend that you do not change the value of this registry entry yourself. For assistance, contact CA Support at http://ca.com/support.

4. Start CA Access Control.

   You have configured the endpoint to use a database password consumer. You must now create a database password consumer for the application in CA Access Control Enterprise Management.

   Note: If you create a password consumer for an IIS application, you must specify that the NT_AUTHORITY\NETWORK SERVICE and *hostname*\IUSR_*hostname* users can use the password consumer to get the privileged account password, where *hostname* is the name of the endpoint.

Configure an Endpoint to Use a Database (.NET) Password Consumer

Valid on Windows Agentless Endpoints

You can use a .NET database password consumer to replace hard-coded passwords in applications that use .NET to connect to a database. When an application tries to connect to the database, the PUPM Agent intercepts the connection attempt and replaces the hard-coded password with the privileged account password that it retrieves from CA Access Control Enterprise Management.

Note: The application must reside on a Windows Agentless endpoint on which CA Access Control is installed.

PUPM uses a profiler to load a plugin to intercept each connection attempt. The .NET plug-in intercepts connection attempts that use .NET. The following registry key control the behavior of CA Access Control .NET:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\.NET
\
```

The settings for the profiler and plug-in are located in the following subkeys:

- Profiler—Instrumentation\.NET\Profiler\
- Plugin—Instrumentation\.NET\Profiler\Plugin

To configure an endpoint to use a .NET database password consumer

1. Verify that CA Access Control is installed on the endpoint with the PUPM Integration feature enabled.

   Note: Install CA Access Control on the endpoint on which the application that connects to the database is installed. You do not need to install CA Access Control on the database host.

2. Stop CA Access Control on the endpoint.

3. In the appropriate registry subkey for the connection type, do the following:

   - Verify that the value of the OperationMode registry entry is 1.

     This registry entry enables the plug-in.

     Important! Verify that the OperationMode registry entry is set to 1 for the profiler and plugin.

   - Verify that the name of the process that runs the application is a value of the ApplyOnProcess registry entry.

     This registry entry specifies the processes to which the plug-in applies. For example, if you are creating a password consumer for an IIS application, verify that w3wp.exe is a value of the registry entry.

     Note: We recommend that you do not change the value of this registry entry yourself. For assistance, contact CA Support at http://ca.com/support.

4. Start CA Access Control.

   You have configured the endpoint to use a database password consumer. You must now create a database password consumer for the application in CA Access Control Enterprise Management.

   Note: If you create a password consumer for an IIS application, specify the NT_AUTHORITY\NETWORK SERVICE and *hostname*\IUSR_*hostname* as users that can use the password consumer to get the privileged account password, where *hostname* is the name of the endpoint.

Configure an Endpoint to Use a CLI Password Consumer

A CLI password consumer is a type of software development kit password consumer. You can use CLI password consumers to replace hard-coded passwords in scripts with privileged account passwords. A CLI password consumer is a representation of a script that gets, checks out, or checks in privileged account passwords. The script calls the PUPM Agent, which retrieves the privileged account password from CA Access Control Enterprise Management.

Use CLI password consumers to write .bat or .sh scripts that are limited in their ability to change other files or scripts. For example, you can write a script that uses the acpwd utility to manually update a hard-coded password in a file. You also use CLI password consumers to let users run the acpwd utility from the command line on an endpoint.

Note: You can also use the PUPM SDK to replace hard-coded passwords in scripts with privileged account passwords. For example, use the PUPM SDK to write a customized script that replaces passwords in multiple files.

To configure an endpoint to use a CLI password consumer

1. Verify that CA Access Control is installed on the endpoint with the PUPM Integration feature enabled.
2. Add the following command to your script:

   ```
   acpwd {-checkout | -get} -account name -ep name -eptype type [-container name]
   -nologo
   ```

   Note: For more information about the acpwd utility syntax, see the *Reference Guide.*
3. Modify your script to use the output of the command (the privileged account password).

   You have configured the endpoint to use a CLI password consumer. You must now create a Software Development Kit (SDK/CLI) password consumer for the script in CA Access Control Enterprise Management.

More information:

Create a Password Consumer (see page 217)

How CLI Password Consumers Work

You can use CLI password consumers to replace hard-coded passwords in scripts with privileged account passwords. A CLI password consumer is a representation of a script that uses the acpwd utility to get, check out, or check in privileged account passwords. You also use CLI password consumers to let users run the acpwd utility from the command line on an endpoint. Understanding how CLI password consumers work helps you use the acpwd utility.

Note: To use the acpwd utility in a script or from the command line, you must first define the script or utility as a Software Development Kit (SDK/CLI) password consumer in CA Access Control Enterprise Management. The password consumer defines a list of users that are permitted to obtain the privileged account password.

The following process describes how CLI password consumers work:

1. The acpwd utility on the endpoint is called in one of the following ways:
   - A user runs the utility from a command prompt window.
   - A script or application server runs and calls the utility.
2. The acpwd utility requests a privileged account password. The PUPM Agent forwards the request to CA Access Control Enterprise Management for authorization.
3. CA Access Control Enterprise Management sends the privileged account password to the endpoint. The PUPM Agent displays the password or forwards the password to the originating program, and logs a confirmation message.
4. You, a script or application server, or CA Access Control Enterprise Management checks in the account password back in and the PUPM Agent logs a confirmation message.
5. The PUPM Agent logs a confirmation message that the check-in was successful.

   Note: A confirmation message with the number zero (0) indicates that the PUPM Agent successfully retrieved, checked out, or checked in the password. For more information about the acpwd utility syntax, see the *Reference Guide.*

Example: A Script That Gets a Password

The following is an example script extract that gets a privileged account password on Windows. This example assumes that the PUPM Agent is installed on the CA Access Control endpoint.

The script in this example attempts to add and delete an entry in the Windows registry using a privileged account password it obtains from CA Access Control Enterprise Management.

```
set AdminUser=PowerUser
FOR /F "tokens=*" %%i IN ('"C:\Program Files\AccessControl\bin\acpwd.exe" -get
-account PowerUser
 -ep comp1_123 -eptype "Windows Agentless" -container "Windows Accounts" -nologo')
DO SET AdminPassword=%%i
set runasadmin="C:\utils\psexec.exe" -u %AdminUser% -p
%runasadmin% %AdminPassword% REG ADD "HKLM\SOFTWARE\PUPM Registry"
%runasadmin% %AdminPassword% REG DELETE "HKLM\SOFTWARE\PUPM Registry" /F
```

In this example, the script runs the PUPM Agent to get a privileged account password. The script contains the account name (*PowerUser),* the endpoint name (*comp1_123*), the endpoint type (*Windows Agentless*), the container name of the user (*Windows Accounts*). The script instructs the PUPM agent to display only the password, and uses the password to run the PsExec program as an administrative user to add and delete a registry entry.

How to Configure an Endpoint to Use a Password Consumer SDK Application

You can use the password consumer SDKs to write applications for CA Access Control endpoints. The applications get, check out, and check in privileged account passwords, and provide password caching and user authentication.

When you run the application, the application calls the PUPM Agent, which gets, checks out, or checks in the privileged account password from CA Access Control Enterprise Management.

There are two types of password consumer SDK:

- Java PUPM SDK—Use this SDK to write Java applications for Windows and UNIX endpoints.

  The Java application that you write must use JRE 1.5 or later.

- .NET PUPM SDK—Use this SDK to write C# applications for Windows endpoints.

  You must install the .NET Framework 2.0 or later on the endpoint to use the .NET PUPM SDK.

To configure an endpoint to use a password consumer SDK application, do the following:

1. Verify that CA Access Control is installed on the endpoint with the PUPM Integration feature enabled.
2. Use the password consumer SDK samples to write your application. You can find the samples at the following locations:
   - Java PUPM SDK—*ACInstallDir*/SDK/JAVA/Samples/PUPMJavaSDK/src/cpm/ca/pupm/javasdk/Tester.java
   - .NET PUPM SDK—*ACInstallDir*/SDK/DOTNET/Examples

   You have configured the endpoint to use a password consumer SDK application. You must now create a Software Development Kit (SDK/CLI) password consumer for the application in CA Access Control Enterprise Management.

More information:

How a Password Consumer SDK Application Gets a Password (see page 142)
The Java PUPM SDK (see page 143)
The .NET PUPM SDK (see page 144)
Create a Password Consumer (see page 217)

Run a Java PUPM SDK Application

After you configure an endpoint to use a password consumer SDK application, you can run the application to get, check out, and check in privileged account passwords.

To run a Java PUPM SDK application

1. Verify that you have created a password consumer for the application in CA Access Control Enterprise Management.
2. Open a Command Prompt window and navigate to the folder in which the application is installed.
3. Run the following command:

```
java -cp PupmJavaSDK.jar;CAPUPMClientCommons.jar;jsafeFIPS.jar;[log4jLib];.
applicationName {explicit | keyvalues} {checkout | checkin} "endpointType"
"endpointName" "accountName" "accountContainer" flags
```

   log4jLib

   (Optional) Defines the name of the log4j library that the application uses to log runtime events and information.

   applicationName

   Defines the name of the Java PUPM SDK application.

explicit

Specifies that the command provides explicit values for each parameter.

keyvalues

Specifies that the command uses key/value pairs.

checkout

Specifies that the application retrieves (gets or checks out) a privileged account password.

Note: The *flags* parameter specifies the get or check out action that application performs.

checkin

Specifies that the application checks in a privileged account password.

endpointType

Defines the type of endpoint on which the privileged account is defined.

Note: You can use the View Endpoint Type task in CA Access Control Enterprise Management to view a list of available endpoint types. Define the endpoint type exactly as it appears in CA Access Control Enterprise Management, for example, "SAP R3 via Provisioning".

endpointName

Defines the name of the endpoint on which the privileged account is defined.

accountName

Defines the name of the privileged account.

accountContainer

Defines the name of the container in which the privileged account is defined.

If the privileged account is not defined in a container, specify "Accounts" for this parameter.

flags

Specifies if the application checks out or gets the privileged account password.

Values: 0—check out or check in the privileged account password (GetOnly flag is false); 1—get the privileged account password (GetOnly flag is true)

The application performs the specified action on the privileged account password and displays the result.

Note: You can use the semsgtool utility to view the textual explanation of numerical PUPM SDK error codes. For more information about the semsgtool utility, see the Reference Guide.

How to Configure an Endpoint to Use a Web Services PUPM SDK Application

You can use the Web Services PUPM SDK to write Java applications that check out and check in privileged account passwords. Because the application communicates directly with the Enterprise Management Server, you do not need to install CA Access Control on the endpoint on which the application runs.

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)

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.

To configure an endpoint to use a Web Services PUPM SDK, do the following:

1. Review the Web Services PUPM SDK readme.

   The readme contains instructions on how to configure the environment, build the Java samples, and run the Java samples. The readme is located at:

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

2. Use the Java samples to write your SDK application.

   You have configured the endpoint to use a Web Services PUPM SDK application. You must now create a user that represents the application in CA Access Control Enterprise Management and assign the user the appropriate privileged access roles.

More information:

How a Web Services SDK Application Gets a Password (see page 146)
The Web Services PUPM SDK (see page 145)

Configure Terminal Integration

Terminal integration lets you integrate your CA Access Control endpoints with PUPM to track the activities of users who check out privileged accounts. Terminal integration also lets you specify that a user must use automatic login to log in to a CA Access Control endpoint with the privileged account.

Before you configure terminal integration, verify the following:

- The privileged account for which you want to configure terminal integration exists in CA Access Control Enterprise Management.
- Terminal integration is enabled on the endpoint, that is, the value of the EnableLogonIntegration configuration setting in the PUPMAgent section is 1.

  Note: Terminal integration is enabled by default when you install CA Access Control with the PUPM integration feature enabled. If you enable terminal integration but do not configure it, CA Access Control does not enforce terminal integration on any accounts.
- (UNIX) CA Access Control uses PAM login interception for the login program that is used to connect to the endpoint.

  For example, if users use SSH to connect to the endpoint, verify that CA Access Control uses PAM login interception to intercept SSH logins.

  Note: For more information about PAM login interception and the LOGINAPPL class, see the *selang Reference Guide*.

The following procedure explains how to configure terminal integration for a single privileged account. You can use a policy to configure terminal integration for privileged accounts with the same name on multiple endpoints.

To configure terminal integration

1. In CA Access Control Endpoint Management, click Users tab, Users subtab, and search for the privileged account for which you want to configure terminal integration.

   Note: For more information about how to manage users in CA Access Control Endpoint Management, see the *Online Help*.
2. Select the privileged account.

   The General tab of the Modify User task page appears.

3. Select one or both of the following options in the Account section:

   Use original identity

   > Specifies that CA Access Control uses the name of the user who checked out the privileged account, not the privileged account user name, when it writes audit records and makes authorization decisions.

   Requires an account checkout prior to login

   > Specifies that a user must use automatic login to log in to the endpoint with this privileged account. Automatic login lets a user check out a password and automatically log in to an endpoint from CA Access Control Enterprise Management.

4. Click Save.

   You have enabled and configured terminal integration for the privileged account.

Example: A Policy That Configures Terminal Integration

The following policy configures terminal integration for an account named administrator. The policy specifies that CA Access Control uses the original user name when it writes audit records and makes authorization decisions, and that users must use automatic login to log in to the endpoint as administrator:

```
editusr administrator pupm_flags(use_original_identity)
editusr administrator pupm_flags(required_checkout)
```

More information:

Terminal Integration (see page 233)
How Terminal Integration Works (see page 235)
Implementation Considerations for Terminal Integration (see page 236)

Chapter 8: Managing Privileged Accounts

This section contains the following topics:

Force Check In of a Privileged Account Password (see page 255)
Automatically Reset a Privileged Account Password (see page 256)
Manually Reset a Privileged Account Password (see page 256)
Delete a Privileged Account Exception (see page 257)
Manual Password Extraction (see page 258)
Audit Privileged Accounts (see page 259)
Synchronize Password Consumers (see page 263)
Restore an Endpoint Administrator Password (see page 265)
Show Previous Privileged Account Passwords (see page 266)

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 259), 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 43)

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 259), 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 124)
How to Integrate PUPM Endpoints with CA Enterprise Log Manager (see page 125)

Synchronize Password Consumers

When the password for a service account changes in CA Access Control Enterprise Management, the JCS attempts to change the password for each password consumer that is associated with the service account. If the JCS does not change the password for a password consumer, you can use Synchronize Password Consumers to retry the password change.

To synchronize password consumers

1. In CA Access Control Enterprise Management, click Privileged Accounts, Password Consumers, Synchronize Password Consumers.

   The Synchronize Password Consumers task page appears.

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

   A list of password consumers that match the filter criteria appears.

   Note: The value of the Endpoint Type field is Windows Agentless because PUPM manages service accounts only on Windows Agentless endpoints.

3. Select the password consumers that you want to synchronize and click Submit.

   The JCS tries to update the password for the selected password consumers.

   Note: The JCS makes five (5) attempts to update the password consumer. If the JCS failed to update the password consumer, it is marked as out of sync and requires you to manually synchronize the password consumer.

More information:

How PUPM Notifies a Password Consumer of a Password Change (see page 121)
Password Consumer Example: Windows Scheduled Task (see page 221)

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 9: Using UNAB

This section contains the following topics:

UNAB Components (see page 267)
How You Set Up UNAB (see page 268)
How UNAB Authenticates Users (see page 268)
Information Stored on the UNAB Endpoint (see page 269)
How You Control Host Access and Configure UNAB (see page 269)
Display User Information (see page 279)
Stop UNAB (see page 280)
View UNAB Status (see page 280)
UNAB Debug Files (see page 281)

UNAB Components

The UNIX Authentication Broker (UNAB) consists of several components that manage and control access to the UNIX host by Active Directory users.

- **UNAB authentication agent**—The UNAB authentication agent (uxauthd) daemon services the connection with Active Directory and is responsible for maintaining a secure connection with Active Directory for user authentication and login authorization purposes, host registration with Active Directory, user and group migrations, administering the local access files and more.
- **uxconsole**—The uxconsole is the UNAB management console that you use to register the UNIX host with Active Directory, migrate users and groups and to register and activate UNAB.
- **uxpreinstall**—The uxpreinstall utility verifies that a UNIX computer complies with UNAB system requirements. Use the uxpreinstall utility to diagnose possible problems and suggest solutions for the problems.
- **CA Access Control Enterprise Management**—CA Access Control Enterprise Management enables you to manage your UNAB hosts from a central location. Using CA Access Control Enterprise Management, you control Active Directory users access to every UNAB host in the enterprise, manage hosts login authorizations, resolve hosts migration conflicts and generate reports.

How You Set Up UNAB

Understanding how the UNIX Authentication Broker (UNAB) controls access to the UNIX host provides you with information that will help you during the implementation and configuration process.

After you install UNAB on the UNIX host, you register UNAB with Active Directory and activate UNAB to enable enterprise users authentication to UNIX endpoint. You then begin the migration process to migrate local users and groups in to Active Directory.

1. Register the UNIX host with Active Directory.

   At this stage UNAB does not intercept any login requests.

2. Define which enterprise users and groups are permitted or denied access to the UNIX host. You do so by creating login authorization policies from CA Access Control Enterprise Management.
3. Activate UNAB to enable enterprise users authentication to the UNIX host.
4. Add additional enterprise users and groups to the UNAB login authorization policies to enable new users to login.

   At this stage login is permitted for users defined in the local user store (for example: etc/passwd) and enterprise users permitted by UNAB login authorization policies.

5. Migrate users and groups into Active Directory.

How UNAB Authenticates Users

After you install and configure UNAB on the UNIX host, users can log in with their Active Directory user account or their local user account, according to the integration mode you selected to use.

When a user attempts to log into a UNIX host where UNAB is running, the following occurs:

1. The user is prompted for an Active Directory or local account user name and password.
2. UNAB authenticates the user credentials with Active Directory, with the login authorization policy or the local host access files and checks for additional information that is taken from the user account.
3. If the user is authenticated, UNAB grants the user access to the UNIX host. If not, UNAB blocks the user access to the host.

Information Stored on the UNAB Endpoint

After UNAB authenticates a user, UNAB stores the following information on the endpoint:

- user name
- hashed password in SHA-1
- user class attributes
- user account control
- time of the last good login
- time of the last bad login
- number of bad logins since last good login

UNAB saves the user details in the logon.db file while the NSS database saves the user and groups attributes in the nss.db file, both located in the following directory:

```
/opt/CA/uxauth/etc
```

How You Control Host Access and Configure UNAB

You can control users and groups access to the UNIX hosts and configure your UNAB hosts all from CA Access Control Enterprise Management. You control user and group access to the UNIX host by granting access to only those users and groups that are permitted to log into that host.

You configure the UNAB hosts in the same manner that you configure control access to the host. You use CA Access Control Enterprise Management to control the functionality of the UNAB hosts in the enterprise once and apply it to all the hosts.

After you assigned user and group login authorizations or defined the configuration token values, CA Access Control Enterprise Management formulates the information into a policy and does the following:

1. CA Access Control Enterprise Management creates a deployment package containing the list of users and groups or the configuration parameters and assigns the package to the host or host group to which the policy applies.
2. CA Access Control Enterprise Management forwards the package to the distribution server for distribution to the host.
3. UNAB retrieves the package from the distribution server, installs the policy and sends a confirmation message back to CA Access Control Enterprise Management.

Note: If you deployed both an enterprise login policy and a UNAB login policy to the host, then the enterprise login policy takes precedence over the UNAB login policy.

Manage UNAB Login Authorization

To control user logins to UNAB hosts or host groups, you create a list of users or groups who are granted access. The list is then formulated into a policy that CA Access Control Enterprise Management assigns and deploys to the selected host or host group. The login policy is named login@*hostName*.

Note: You can use the Deployment Audit task to view the deployment status of the policy.

To manage UNAB login authorization

1. In CA Access Control Enterprise Management, do as follows:

   a. Click Policy Management.

   b. Click the UNIX Authentication Broker subtab.

   c. Expand the Host or Host Group tree in the task menu on the left, as appropriate.

      A list of available tasks appears.

2. Do *one* of the following:

   - Click Manage Host Login Authorization.

     The Manage Host Login Authorization: Host Search screen appears.

   - Click Manage Host Group Login Authorization.

     The Manage Host Group Login Authorization: Host Group Search screen appears.

3. Type the name of the host or host group that you want to modify and click Search.

   A list of hosts or host groups that match the filter criteria appear.

4. Select the host or host group to modify and click Select.

   The Manage Host Login Authorization: *HostName* or Manage Host Group Login Authorization: *HostGroupName* page appears.

5. (Optional) Add a user, as follows:

   a. Select User from the pull down menu.

   b. Type the name of the user in the following format: *domain/user*.

   c. Click Add.

      The users you added appear in the Authorized users and groups list.

6. (Optional) Add a group, as follows:
    a. Select Group from the pull down menu.
    b. Type the name of a group that you want to add.
    c. Click Add.

       The groups you added appear in the Authorized users and groups list.
7. (Optional) Remove users and groups, as follows:
    a. Select the users and groups to remove in the Authorized users and groups list.
    b. Click Remove.

       The users and groups you selected are removed from the Authorized users and groups list.
8. Click Submit.

   CA Access Control Enterprise Management assigns the updated list of users and groups to the specified host or host group.

Configure a UNAB Host or Host Group

You can define the configuration settings that govern UNAB hosts and host groups. CA Access Control Enterprise Management helps you set the value of the settings in the UNAB configuration file (uxauth.ini) or the CA Access Control configuration file (accommon.ini). After you finish assigning values to the configuration settings, CA Access Control Enterprise Management creates a configuration policy that contains the updated settings values and assigns it to the host or host group. The policy is named config@*hostName.*

Note: You can use the Deployment Audit task to view the deployment status of the policy.

To configure a UNAB host or host group

1. In CA Access Control Enterprise Management, do as follows:
    a. Click Policy Management.
    b. Click the UNIX Authentication Broker subtab.
    c. Expand the Host or Host Group tree in the task menu on the left, as appropriate.

       A list of available tasks appears.

2. Do *one* of the following:
   - Click Configure a UNAB Host.

     The Configure a UNAB Host: Host Search screen appears.
   - Click Configure a UNAB Host Group.

     The Configure a UNAB Host Group: Host Group Search screen appears.
3. Type the name of the host or host group you want to modify and click Search.

   A list of hosts or host groups that match the filter criteria appear.
4. Select the host or host group to modify and click Select.

   The UNAB Configuration: *HostName* or UNAB Configuration: *HostGroupName* screen appears.
5. Select the section and token to modify and click Add token.

   The selected configuration tokens appear.
6. Modify the value of the configuration tokens.

   Note: For more information about the configuration tokens, see the *Reference Guide*.
7. (Optional) Select another section and token to modify, click Add token, and modify the value of the configuration tokens as required.
8. Click Submit.

   CA Access Control Enterprise Management sets the values of the configuration tokens on the selected UNAB host or host group.

Verify That CA Access Control Enterprise Management Committed the Policies to the Host

After you formulated the authorization and configuration lists, you can verify that CA Access Control Enterprise Management committed the changes to the UNAB host in the deployment audit option.

To verify that CA Access Control Enterprise Management committed the policies to the host

1. In CA Access Control Enterprise Management select the Policy Management tab, Policy task and expand the Deployment option.

   The deployment option menu opens.

2. Select the Deployment Audit option.

   The deployment audit search screen opens.

3. Select the host and the policy to display and click GO.

   The query displays the search results.

   Note: Login policies contains the prefix **login@**

4. Click the results line to display the deployment status.

   CA Access Control Enterprise Management displays the deployment task's status and output.

How to Migrate Users and Groups to Active Directory

Migrating users from a UNIX host to Active Directory simplifies user and group management on UNIX hosts, by consolidating management tasks into a single management application.

To migrate users and groups to Active Directory, do the following:

1. Run the migration process in emulation mode.

   In emulation mode, UNAB does not migrate users or groups to Active Directory. If found, UNAB logs the conflicts in a log file that reports on possible conflicts in users and groups attributes. By default, the UNAB conflicts file, migrate.conflicts, is located in the following directory:

   ```
   /opt/CA/uxauth/log
   ```

2. Download the conflicts file.

   You download the conflicts file from the host in a CVS format from CA Access Control Enterprise Management.

   Note: You must wait for the next scheduled report snapshot to complete before you can download the CSV.

3. Create Active Directory accounts for each local account that you want to migrate to Active Directory.

   UNAB migrates only those users that have an existing Active Directory user account.

   Note: Do not need to specify the UNIX attributes when you create the user accounts. You do not need to create the groups in Active Directory, the migration tool creates the groups during the migration process.

4. Upload a CSV file that resolves the conflicts to the host.

   UNAB restarts the migration process, attempting to migrate the resolved accounts and groups.

5. Review the conflicts file again after the migration ends to verify that the user accounts and groups that were previously reported in the file were successfully migrated.

Resolve Migration Conflicts

UNAB logs conflicts found during the migration process in the conflicts file. This file details the cause of the conflicts that prevented the migration of users and groups from the local host to Active Directory.

You export the conflicts file into a CSV file, download the spreadsheet to your computer, review, and resolve the conflicts. You can later upload the modified spreadsheet back into CA Access Control Enterprise Management, which sends it to the Message Queue. UNAB retrieves the file and restarts the migration process to migrate the users and groups that were not previously migrated.

Note: If you migrate a host group, you cannot download the conflicts file. However, you can upload a corrected conflicts file to resolve conflicts in the migration process.

To resolve migration conflicts

1. In CA Access Control Enterprise Management, do as follows:

   a. Click Policy Management.

   b. Click the UNIX Authentication Broker subtab.

   c. Expand the Host or Host Group tree in the task menu on the left, as appropriate.

      A list of available tasks appears.

2. Do *one* of the following:

   - Click Resolve Host Migration Conflicts.

     The Resolve Host Migration Conflicts: Host Search screen appears.

   - Click Resolve Host Group Migration Conflicts.

     The Resolve Host Group Migration Conflicts: Host Group Search screen appears.

3. Type in the name of the host or host group you want to resolve conflicts for and click Search.

   A list of hosts or host groups that match the filter criteria appear.

4. Select the host or host group for which you want to resolve conflicts and click Select.

   The UNAB Migration: *HostName* or UNAB Migration: *HostGroupName* page appears.

5. (Optional) Download the conflicts file for a host migration and resolve the conflicts, as follows:

   a. Select the Export and Download link in the Download UNAB Migration Conflicts Details section.

      A dialog window opens.

   b. Navigate to the location to save the file and select Save.

      The CSV file downloads to the specified location.

   c. Open the CSV file, resolve the conflicts that are reported in the file, then save and close the file.

6. (Optional) Create and save a CSV file that resolves the conflicts for a host group migration.

7. Upload a CSV file that resolves the conflicts for a host or host group migration, as follows:

   a. Select the Browse button in the Upload UNAB Migration Solution section.

      A dialog window opens.

   b. Browse for the file and click Open.

   c. Click Upload.

      The file is uploaded.

8. Click Submit.

   CA Access Control Enterprise Management sends the file to the Message Queue. UNAB retrieves the file from the queue and restarts the migration process, attempting to migrate the resolved accounts and groups.

9. Review the conflicts file again after the migration ends to verify that the user accounts and groups that were previously reported in the file were successfully migrated.

Note: You cannot migrate a user or group if a user or group with the same name exists in Active Directory. For example, if you try to migrate a group named g1, but a user named g1 exists in Active Directory, UNAB cannot migrate the group.

Example: The UNAB Conflicts File Output

The following example is an extract of the UNAB conflicts file output that was created during the migration process:

```
*** Conflict Details as found by the CA Access Control UNAB Migration tool at 12/29/10
10:49 ***

***  CRITICAL
Conflicts:
                                                                          ***
***     The next found  conflicts prevent the user/group migration and need the
intervention    ***
***     of the system administrator as they cannot be solved by the migration
tool.                          ***

User 'John' conflicts:
    User 'John' from domain 'development.computer.com' is assigned id '47670' and Unix
id is '300821'
    User 'John' from domain 'development.computer.com' is assigned primary group
'47670' and Unix primary group is '1011'
    User 'John' from domain 'development.computer.com' is assigned home directory
'/home/aletestu' and Unix home directory is '/home/john1'
    User 'John' from domain 'development.computer.com' is assigned shell
'/sbin/nologin' and Unix shell is '/bin/bash'

***  AUTOMATIC
Conflicts:
                                                                           ***
***     Migration tool will try to solve the next found conflicts when run in
"administrative mode",
***
***      if not solved this conflicts will prevent the user/group
migration
Group 'alegcheck' conflicts:
    Cannot add members to Active Directory group 'dev_users' because UNIX group
'dev_users' contains member[s] that do not exist in domain
'development.computer.com'.
      UNIX group 'alegcheck' members: aleucheck1;aleucheck2
User 'John1' conflicts:
    User 'John1' from domain 'development.computer.com' has no UNIX attributes.

***  IGNORED
Conflicts:
                                                                              ***
***     The next found Conflicts are shown for informational purpose,  they will be
ignored for
***      while migration the
user/group
                                                 ***
```

```
User 'John' conflicts:
    User 'John' from domain 'development.computer.com' is assigned gecos '' and Unix
gecos is 'gecos of John'
    User 'John' primary group '1011' was not migrated
```

In this example UNAB reported on the following critical conflicts:

- The user 'john' is missing the following attributes:
  - The user id (47670) conflicts with the UNIX user id (300821)
  - The user primary group (47670) conflicts with the Active Directory group (1011)
  - The user home UNIX directory (home/john1) conflicts with the Active Directory home directory settings (/home/john)
  - The user UNIX shell (/bin/bash) conflicts with the Active Directory shell attribute (/sbin/nologin)

UNAB reported on the following conflicts that UNAB will attempt to resolve the next time the migration process runs:

  - The UNIX group (dev_users) does not exist in Active Directory
  - UNIX attributes are not configured for user 'john1'

<una> reported on the following minor conflicts that it will ignore during the migration process:

- The user gecos ("") conflicts with the UNIX assigned gecos (gecos for john)
- The user primary group (1011) was not migrated

Example: The UNAB Conflicts Resolution File

The following example is an extract of the UNAB conflicts resolution CSV file you create to resolve the conflicts that UNAB reported in the conflicts file. You use CA Access Control Enterprise Management to submit the CSV file to the UNAB host:

Solution Entity Type	Solution Entity Name	Solution Operation	Solution AD Mapping Name	Conflicts	UID	Home Directory	GID	Member of	Members	GECOS
USER	superuser		root	Group Migration,NO AD	1	/home/superuser/	1			

In this example, the conflicts resolution CSV file contains the following:

- Solution Entity Type—USER
- Solution Entity Name—superuser
- Solution AD Mapping Name—root
- Conflicts—The user group not found in Active Directory
- UID—1
- Home Directory—/home/superuser/
- GID—1

Note: For more information about migrating users, see the *Implementation Guide*.

Display User Information

UNAB can display information about user accounts, for example, the account type (local or enterprise user account), login status (allowed or denied) and login reason. You can choose to display the list of local and enterprise accounts and show detailed account information.

To display user information

1. Navigate to the bin directory. By default the directory is under the following path:

   ```
   /opt/CA/uxauth/bin
   ```

2. Enter either of the following commands:

   ```
   ./uxconsole –manage –find –user <filter>
   ```

   ```
   ./uxconsole –manage –show -detail –user <filter>
   ```

   UNAB displays the user details according to the options you specified.

   Note: You can use wildcard characters (*).

Note: For more information about the uxconsole utility, see the *Reference Guide*.

Stop UNAB

If you install a new version of UNAB or update the operating system, you need to stop UNAB.

You stop UNAB by stopping the uxauthd.sh script.

To stop UNAB

1. Log in to the UNIX computer as root.
2. Navigate to the UNAB bin directory.
3. Enter the following command:

   ```
   ./uxauthd.sh -stop
   ```

   The UNAB daemon stops.

View UNAB Status

Use this option to view the current status of UNAB.

To view UNAB status

1. Log in to the UNIX computer as a user that has management privileges on that computer.
2. Navigate to the UNAB bin directory.
3. Run the following command.

   ```
   ./uxconsole -status -detail
   ```

   A message informs you about the current status of UNAB.

Note: For more information about the uxconsole utility, see the *Reference Guide*.

UNAB Debug Files

The agent section of the UNAB configuration file (in the uxauth.ini file) defines the debugging information collected by the agent at run time. By default, UNAB collects debug information in the following file, where *UNABInstallDir* is the directory in which you installed UNAB:

```
UNABInstallDir/log/debug/agent_debug
```

The UNAB agent logs debug messages in the debug file when the uxauthd daemon starts, so long as the debug mechanism is enabled in the UNAB configuration file.

When you use the -debug option to start UNAB, a debug message appears in the user console.

Chapter 10: Creating Reports

This section contains the following topics:

Security Standards (see page 283)
Report Types (see page 284)
Reporting Service (see page 284)
How to View Reports in CA Access Control Enterprise Management (see page 289)
Standard Reports (see page 296)
Custom Reports (see page 318)

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 data and events in two different report types:

- CA Access Control reports—Describe who can do what.

  CA Access Control reports provide information about the data in the CA Access Control database on each endpoint, that is, the rules and policies that you deploy on the endpoint and policy deviations. You view CA Access Control reports in CA Business Intelligence and in CA Access Control Enterprise Management.

- Audit reports—Describe who did what.

  Audit reports provide information about the data in the audit log file (seos.audit) on each endpoint, that is, information about which users performed what actions on the endpoint. You view audit reports in CA Enterprise Log Manager and in CA Access Control Enterprise Management.

  Note: For more information about viewing audit reports in CA Enterprise Log Manager, see the *CA Enterprise Log Manager Overview Guide*.

Note: You must install and configure additional components to view CA Access Control reports and CA Access Control audit reports. For more information, see the *Implementation Guide*.

Reporting Service

CA Access Control 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 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 true endpoint 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 provides out of the box. 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 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 runs on each CA Access Control or UNAB endpoint and sends information to queues on a configured Message Queue that resides on the Distribution Server.
- A *Message Queue* is a component of the Distribution 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. For redundancy and failover, you can have multiple Distribution Servers collecting and forwarding the information.
- 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.
- CA Access Control 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.
- A computer on which you run a web browser to view and manage reports.

Note: For more information about CA Access Control reporting service implementation and architecture, see the *Implementation Guide*.

How the Reporting Service Works

The reporting service lets you examine the data that is collected from each CA Access Control and UNAB endpoint, 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 CA Access Control and UNAB endpoints.

  Each endpoint sends report data to the Message Queue on the Distribution Server.

- Stores the data in the central database.

  CA Access Control Enterprise Management 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 Enterprise Management 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 interrogate 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 reports.

Note: For information about the reporting service architecture, see the *Implementation Guide*.

How Data for Reporting Is Collected from Each Endpoint

To generate reports, data from each endpoint has to be collected. The reporting service uses a Report Agent, installed on each CA Access Control and UNAB endpoint, to collect data from that endpoint at scheduled times or on-demand.

Note: The Report Agent is also responsible for collecting and routing audit data for integration with CA Enterprise Log Manager. This process describes only those actions that the Report Agent takes for reporting on the endpoint.

The Report Agent performs the following actions on each endpoint:

1. Performs a deviation calculation and sends the results to the Distribution Server.

   Important! If you have the Report Agent set to run regularly, and you do not need to have the DMS updated, you do not need to schedule a policy deviation calculation separately.

2. Creates a copy of the CA Access Control database (seosdb) and each Policy Model database (PMDB) on the CA Access Control endpoint, or creates a copy of the UNAB database on the UNAB endpoint.

   This is a temporary copy that the Report Agent takes so that it can process data without affecting CA Access Control 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, not just data that is visible through database interface utilities (such as selang).

4. Sends an XML version of the database to the Distribution Server.

   The Report Agent sends the data to the reporting queue on the Distribution Server.

Note: Data for reporting is not collected from PUPM endpoints.

How Data from Each Endpoint is Processed and Stored

When data is collected on each endpoint, it is sent for processing on the Distribution Server. The processed data is then sent for storage on the central database for report generation.

The Distribution Server performs the following actions:

1. Receives, from the Report Agent on each endpoint, an XML dump of the entire database of the endpoint.

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.

Send an Endpoint Snapshot to the Distribution Server

When you configure an endpoint for reporting, you specify the times at which the Report Agent collects scheduled snapshots of the local CA Access Control database and any PMDBs on the endpoint and sends the snapshot to the reports queue on the Distribution Server. If you do not want to wait for the scheduled time, you can send an endpoint snapshot to the Distribution Server immediately.

Note: You can change the Report Agent schedule by changing the schedule configuration setting in the ReportAgent section of the accommon.ini file or the CA Access Control registry key.

To send an endpoint snapshot to the Distribution Server on demand

1. Open a command prompt window on an endpoint.
2. (UNIX) Set the library path environment variable, as follows:
   a. su to root.
   b. Set the library path environment variable to *ACSharedDir*/lib. By default, *ACSharedDir* is the following directory:

      ```
      /opt/CA/AccessControlShared
      ```

   c. Export the library path environment variable.

3. (UNIX) Navigate to the following directory:

   ACSharedDir/bin

4. Run the Report Agent on the endpoint. Do *one* of the following:

   - (Windows) Run the following command:

     ```
     ReportAgent -report snapshot
     ```

   - (UNIX) Run the following command:

     ```
     ./ReportAgent -report snapshot
     ```

   The Report Agent sends a snapshot of the CA Access Control database and any local PMDBs to the report queue on the Distribution Server.

Note: For more information about configuring an endpoint for reporting, see the *Implementation Guide*. For more information about the ReportAgent section, see the *Reference Guide*. For more information about the library path environment variable, see the *Troubleshooting Guide*.

How to View Reports in CA Access Control Enterprise Management

This process explains how to create and view CA Access Control reports, which provide information about PUPM, CA Access Control and UNAB endpoints, and the user store. You can also view CA Access Control reports in CA Business Intelligence.

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 collects and defines the snapshot schedule.

2. Verify that you have configured the CA Access Control and UNAB endpoints 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.

Note: For more information about creating a snapshot definition and configuring endpoints for reporting, see the *Implementation Guide*.

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.

To capture snapshot data

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 *Implementation Guide*.

Run a Report in CA Access Control Enterprise Management

CA Access Control reports provide information about PUPM, CA Access Control and UNAB endpoints, and the data in the user store.

Reports consist of data that CA Access Control Enterprise Management captures in snapshots. After CA Access Control Enterprise Management 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 CA Business Intelligence. If you schedule a report in CA Business Intelligence, 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 CA Business Intelligence.

To run a report in CA Access Control Enterprise Management

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 numeric parameter but enter a non-numeric value for that parameter, the report fails.
   - 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 294)

View a Report

CA Access Control reports provide information about PUPM, CA Access Control and UNAB endpoints, and the data in user store. 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.

To view a report

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).

To open InfoView for working with reports

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.

Note: For more information about using BusinessObjects InfoView, see the *BusinessObjects Enterprise XI Release 2 InfoView User's Guide*.

Run a Report

Once you open reporting interface (BusinessObjects InfoView), you can select a report, and run it.

To run 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 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.

Note: For more information about using BusinessObjects InfoView, see the *BusinessObjects Enterprise XI Release 2 InfoView User's Guide*.

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

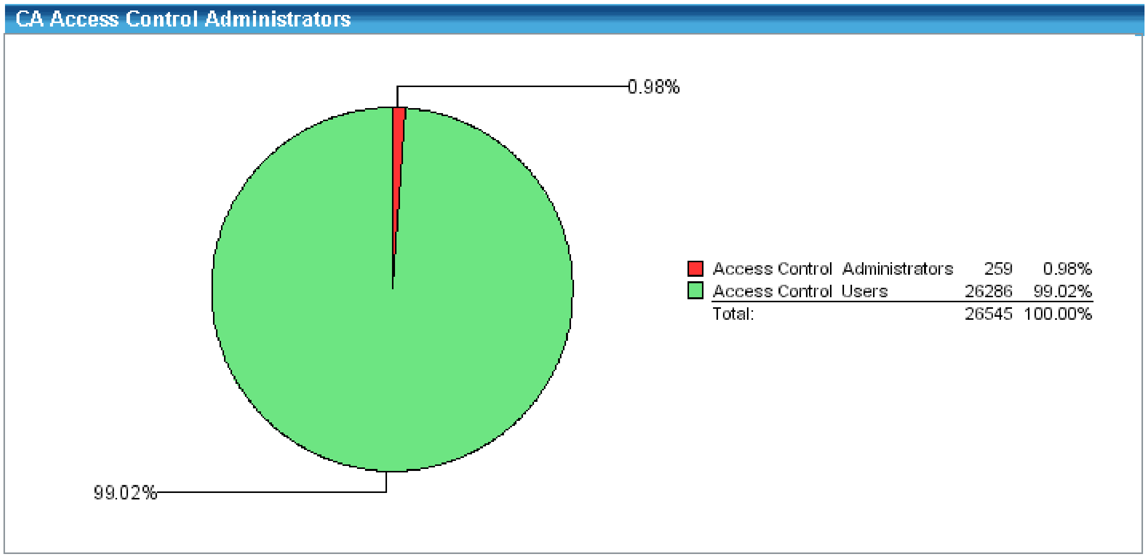
Out of the box, CA Access Control reporting service comes with standard reports that are deployed as part of the report portal installation. The reports are divided into the following categories:

- Account management reports (see page 298)
- Entitlement reports (see page 302)
- Miscellaneous reports (see page 303)
- Policy management reports (see page 305)
- Password policies reports (see page 309)
- Privileged accounts management reports (see page 310)
- UNIX Authentication Broker reports (see page 314)

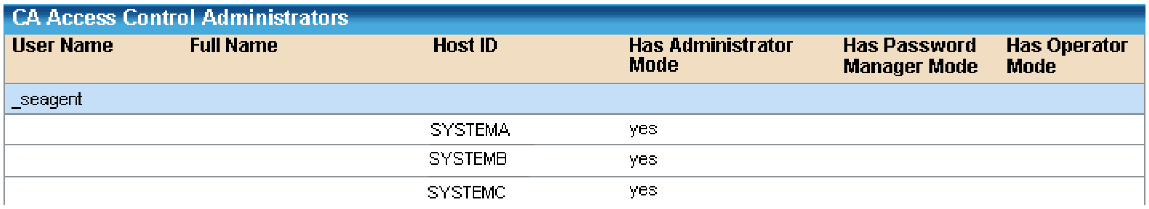
In addition to the standard reports, you can augment the reports and make similar reports with different features, or generate completely new reports.

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		

Account Management Reports

The standard account management reports provide an overview of user accounts.

Note: The report title is the name as it appears in BusinessObjects InfoView.

Following is the list of standard account management reports:

CA Access Control Administrators (see page 298)
CA Access Control Group User Membership (see page 298)
CA Access Control Groups (see page 299)
CA Access Control Inactivity Days (see page 299)
CA Access Control Password Change (see page 299)
CA Access Control Password Expiration (see page 300)
CA Access Control Password Policy Compliance (Accounts) (see page 300)
CA Access Control Password Policy Compliance (Hosts) (see page 300)
CA Access Control Segregation of Duties (see page 301)
CA Access Control User Group Membership (see page 301)
CA Access Control Users Creation Date (see page 301)
CA Access Control Users Suspend Date (see page 301)
CA Access Control Users Update Date (see page 302)

CA Access Control Administrators

The CA Access Control Administrators report displays a list of all the users that have CA Access Control administrative privileges. These include users that have the ADMIN, PWMANAGER, or OPERATOR attribute. The report displays summary data in a pie chart and a detailed listing by user name in a tabular format.

If a large number of users can administer CA Access Control then this may expose the enterprise to a security risk. Of course, if the endpoints being evaluated are in a development or test environment then it may be perfectly normal for the majority of users on the systems to be CA Access Control administrators.

CA Access Control Group User Membership

The CA Access Control Group User Membership report provides a view of user groups and their members. The report displays the details in a tabular format.

To simplify administration, each user in the CA Access Control environment can be included as a member of one or more currently defined CA Access Control groups. Because resource access is typically applied to groups, group membership should be reviewed on a regular basis.

CA Access Control Groups

The CA Access Control Groups report displays the defined hosts on which a group exists, the group's description, and whether it contains any child groups known as nested groups.

Understanding which groups exist on which hosts throughout your enterprise helps you manage your environment. Additionally, knowing which groups contain other groups is useful in determining why a particular user or group can access a specific resource.

CA Access Control Inactivity Days

The CA Access Control Inactivity Days report displays users that have not logged on during the specified period, such as 90 days. It also displays whether those users are suspended, or whether they are still able to access the system. The report includes a summary pie chart that highlights users whose accounts are inactive but suspended, and those that are inactive but not suspended.

A significant audit point in all enterprise environments is knowing what users have current access to the environment and when the last access was performed. In addition to showing when a user last accessed a resource, logging into an endpoint, for example, it is also required to show how long accounts have been inactive. This report is useful in proving the access regularity of service accounts and identifying accounts that are still open but have not been accessed in a specific time frame.

CA Access Control Password Change

The CA Access Control Password Change report displays the list of user accounts who must change their password within a specified time period. The report provides a summary pie chart of the user accounts that do not need to change their password, those who need to update their password, and those whose passwords have expired. The report also provides details such as host ID and days remaining until passwords expiration for user accounts.

An audit requirement that is similar to knowing the state of stale passwords is the requirement to know the list of users who have pending password changes. Using this knowledge, you can determine the pending security exposure from accounts that may go stale soon.

CA Access Control Password Expiration

The CA Access Control Password Expiration report displays the user accounts that have not updated their passwords within a specified number of days. The report provides a summary pie chart that identifies user accounts that have updated their passwords, those whose system access has been suspended due to an expired password, and those whose password has expired, but still have access to the system. The report provides details on user accounts that have not changed their passwords in the last x days including host ID, last password change date, and the reason the user account still has access to the system.

CA Access Control has the ability to enhance endpoint password security by providing additional quality checks, and maintaining a history of prior passwords to prevent frequent reuse. As part of this component, the password last change date is maintained. By using this component of the password quality model, CA Access Control can identify which users in the enterprise have not changed their password in a specified time period. The significance of this report is that you can use it to centrally determine possible weaknesses in the enterprise login environment due to stale passwords.

CA Access Control Password Policy Compliance (Accounts)

The CA Access Control Password Policy Compliance (Accounts) report displays the user accounts whose passwords do not comply with your password policy, such as password length and minimum numeric and alphabetic characters. The report provides a summary pie chart that identifies the number of user accounts that comply with the policy and those that do not. The report also provides details on the user accounts that do not apply with the policy in tabular format.

CA Access Control Password Policy Compliance (Hosts)

The CA Access Control Password Policy Compliance (Hosts) report displays the hosts on which the passwords for user accounts do not comply with your password policy, such as password length and minimum numeric and alphabetic characters. The report provides a summary pie chart that identifies the number of hosts that comply with the policy and those that do not. The report also provides details on the hosts that do not apply with the policy and the user accounts on those hosts in tabular format.

CA Access Control Segregation of Duties

The CA Access Control Segregation of Duties report displays the user accounts that violate a segregation of duties policy such as users cannot be members of both the administrators and auditors user groups. The report provides a summary pie chart the compares the number of users that comply and do not comply with the policy. The report also includes details about the user accounts that do not comply with the policy and the host ID.

All endpoints in all enterprise environments require maintenance by users that must have access to OS and application components. Commonly, the system administrator maintains the computer from the OS viewpoint, and an application administrator maintains the computer from an application viewpoint. For example, a Solaris system administrator may update entries in the UNIX host file while an Oracle DBA may maintain tables in the Oracle database.

The advantage of this model is that the system administrator is limited in the ability to compromise an application, and the application administrator is limited in the ability to compromise the OS. It is generally not a good practice to have a system administrator that is also an application administrator.

This report helps identify potential conflicts where users belong to two groups representing different roles. This group intersection detection and reporting is highly beneficial to satisfying one of the major audit points for ISO7799, SOX, PCI, HIPAA and the DoD.

CA Access Control User Group Membership

The CA Access Control User Group Membership report displays users and groups membership for each host in the environment. The report provides details arranged by host of the users and the groups to which they belong.

CA Access Control Users Creation Date

The CA Access Control Users Creation Date reports displays the user accounts created within a specific time period on a specified host or all hosts in your environment. The report provides details on the date the user account was created arranged by host and then user account.

CA Access Control Users Suspend Date

The CA Access Control Users Suspend Date reports displays the user accounts suspended within a specific time period on a specified host or all hosts in your environment. The report provides details on the date the user account was suspended arranged by host and then user account.

CA Access Control Users Update Date

The CA Access Control Users Update Date reports displays the user accounts updated within a specific time period on a specified host or all hosts in your environments. The report provides details on the date the user account was updated arranged by host and then user account.

Entitlement Reports

The standard entitlement reports provide an overview of user and resource entitlements.

Note: The report title is the name as it appears in BusinessObjects InfoView.

Following is the list of standard entitlement reports:

CA Access Control Baseline Resource Compliance (Hosts) (see page 302)
CA Access Control Group Privileges (see page 302)
CA Access Control Resource Access by Group (see page 303)
CA Access Control Resource Access by User (see page 303)
CA Access Control User Privileges (see page 303)

CA Access Control Baseline Resource Compliance (Hosts)

The CA Access Control Baseline Resource Compliance (Hosts) report displays the user accounts that have non-default access to a specified resource. The report provides a summary pie chart that displays a count of the hosts on which the non-default access is permitted and the total number of user accounts that have non-default access. The report also provides details by host of the access permissions for each of the user accounts with non-default access.

CA Access Control Group Privileges

The CA Access Control Group Privileges report displays a list of all the resources that a user group can access. The report displays a detailed listing by resource name in a tabular format that identifies the following:

- Host ID
- Access privileges
- Whether is access is granted by default or by using a program
- Any restrictions such as the name of an applicable calendar or other time restriction
- Whether the access is granted because the user group owns the resource

Using this report, you can determine which user groups have access to defined resources throughout your enterprise or for a particular host. After review, you may decide to change the access privileges to meet your security policy.

CA Access Control Resource Access by Group

The CA Access Control Resource Access by Group report displays the access privileges granted to user groups for a specified resource. The report provides a detailed list of the all the user groups that have access to the resource including Host ID, access privileges, whether default access is granted, and any other restrictions, such as day and time are specified.

CA Access Control Resource Access by User

The CA Access Control Resource Access by User report displays the access privileges granted to user accounts for a specified resource. The report provides a detailed list of the all the user accounts that have access to the resource including Host ID, access privileges, whether default access is granted, and any other restrictions, such as day and time are specified.

CA Access Control User Privileges

The CA Access Control User Privileges report displays access permissions for a user, arranged by resource. For each resource that the user can access, the report provides the user's access types, default access, any programs the users can use to access the resource, and any time restrictions on the user's access to the resource. The report also specifies if the user is the resource owner.

Miscellaneous Reports

The standard miscellaneous reports provide information about monitored files, monitored programs, and the readiness of UNIX hosts to unload the CA Access Control kernel without rebooting the system.

Note: The report title is the name as it appears in BusinessObjects InfoView.

Following is the list of standard miscellaneous reports:

CA Access Control Monitored Files (see page 304)
CA Access Control Monitored Programs (see page 304)
CA Access Control UNIX Hosts with Unload Considerations (see page 304)
CA Access Control UNIX Unload Readiness (see page 305)

CA Access Control Monitored Files

The CA Access Control Monitored Files report displays the state of critical system files on hosts throughout the enterprise. The report provides a summary pie chart indicating on which hosts the file is not monitored, on which hosts the file is monitored but has been modified, and on which hosts the file is monitored and remains in a trusted state. The report also provides details on the file such as host ID so that you can review the policy for the file on that host or so you can review whether modifications to the file were made by authorized users.

Ensuring that critical system files are monitored is essential to protecting the integrity of your data. Knowing when changes are made to the files provides an audit trail so that you can verify that authorized users made the changes according to your security policy.

CA Access Control Monitored Programs

The CA Access Control Monitored Programs report displays the state of critical programs on hosts throughout the enterprise. The report provides a summary pie chart indicating on which hosts the program is not monitored, on which hosts the program is monitored but has been modified, and on which hosts the program is monitored and remains in a trusted state. The report also provides details on the program such as host ID so that you can review the policy for the program on that host or so you can review whether modifications to the program were made by authorized users.

Ensuring that critical programs are monitored is essential to protecting the integrity of your data. Knowing when changes are made to the programs provides an audit trail so that you can verify that authorized users made the changes according to your security policy.

CA Access Control UNIX Hosts with Unload Considerations

The CA Access Control UNIX Hosts with Unload Considerations report displays UNIX hosts that have intercepted system calls that may prevent you unloading the CA Access Control kernel. On these hosts, you need to reboot the computer before you can unload the kernel and upgrade CA Access Control.

The report lists the process and parent process IDs, the program name, blocking time, and threshold time for each host with unload considerations. The report also specifies if each system call is blocking or non-blocking.

The report groups hosts in the following categories:

- **Not ready (overflow)**—The system calls table exceeds its size, and a reboot is required to unload the kernel.
- **Not ready (blocking system calls)**—Blocking intercepted system calls exist, and a reboot is required to unload the kernel.
- **Probable (non-blocking system calls)**—Non-blocking intercepted system calls exist, and a reboot is probably not required to unload the kernel.

CA Access Control UNIX Unload Readiness

The CA Access Control UNIX Unload Readiness report displays the readiness of UNIX hosts to unload the CA Access Control kernel and upgrade CA Access Control without rebooting the system.

The report provides a summary pie chart that shows the proportion of hosts that are ready for the kernel unload, probably ready for the kernel unload, and not ready for the kernel unload. The report also provides the number of intercepted and non-blocking system calls for each host.

The report groups hosts in the following categories:

- **Not ready (overflow)**—The system calls table exceeds its size, and a reboot is required to unload the kernel.
- **Not ready (blocking system calls)**—Blocking intercepted system calls exist, and a reboot is required to unload the kernel.
- **Probable (non-blocking system calls)**—Non-blocking intercepted system calls exist, and a reboot is probably not required to unload the kernel.
- **Ready**—No intercepted system calls exist, and a reboot is not required to unload the kernel.
- **Not applicable**—The host is not a UNIX host.
- **Unknown status**—No information is available for the host.

Policy Management Reports

The standard policy management reports provide information about your CA Access Control Enterprise Management policies.

Note: The report title is the name as it appears in BusinessObjects InfoView.

Following is the list of standard policy management reports:

CA Access Control Policy Assignment (see page 306)
CA Access Control Policy Deployment Scorecard (see page 306)
CA Access Control Policy Deployment Scorecard by Host (see page 306)
CA Access Control Policy Deployment Scorecard by Host Group (see page 307)
CA Access Control Policy Deployment Status by Host (see page 307)
CA Access Control Policy Deployment Status by Host Group (see page 307)
CA Access Control Policy Inventory (see page 308)
CA Access Control Policy Rules (see page 308)
CA Access Control Policy Versions (see page 308)
CA Access Control Rule Deviations by Host (see page 308)
CA Access Control Rule Deviations by Host Group (see page 309)

CA Access Control Policy Assignment

The CA Access Control Policy Assignment report displays assignment details for policies deployed on the hosts and host groups that are defined on a specified DMS. The report displays the following information:

- Policy name
- Assignment type (host or host group)
- The names of the hosts and host groups on which the policy is deployed

CA Access Control Policy Deployment Scorecard

The CA Access Control Policy Deployment Scorecard report displays deployment information for a specified policy. The report provides a summary pie chart with the following information:

- The number of hosts on which the policy is correctly deployed.
- The number of hosts on which the policy is deployed with errors or deviations.
- The number of hosts that are At Risk (the policy is assigned to the host, but the policy is not deployed on the host).

The report also provides details of any problems with the policy deployment, arranged by host.

CA Access Control Policy Deployment Scorecard by Host

The CA Access Control Policy Deployment Scorecard by Host report displays deployment information for policies, arranged by host. The report provides a summary pie chart with the following information:

- The number of hosts on which the policy is correctly deployed.
- The number of hosts on which the policy is deployed with errors or deviations.
- The number of hosts that are At Risk (the policy is assigned to the host or a host group of which the host is a member, but the policy is not deployed on the host).

The report also provides details of any problems with the policy deployment, arranged by host.

CA Access Control Policy Deployment Scorecard by Host Group

The CA Access Control Policy Deployment Scorecard by Host Group report displays deployment information for policies, arranged by host group. The report provides a summary pie chart with the following information:

- The number of hosts in the host group on which the policy is correctly deployed.
- The number of hosts in the host group on which the policy is deployed with errors or deviations.
- The number of hosts in the host group that are At Risk (the policy is assigned to the host group, but the policy is not deployed on the hosts).

The report also provides details of any problems with the policy deployment, arranged by host group.

CA Access Control Policy Deployment Status by Host

The CA Access Control Policy Deployment Status by Host report displays status information for policies, arranged by host. The report provides version information for each policy, including:

- Deviation status
- Deployment time
- The name of the user who deployed the policy

CA Access Control Policy Deployment Status by Host Group

The CA Access Control Policy Deployment Status by Host Group report displays status information for policies, arranged by host group. The report provides version information for each policy, including:

- Deviation status
- Deployment time
- The name of the user who deployed the policy

The report also lists the hosts within the host group on which the policy is deployed.

CA Access Control Policy Inventory

The CA Access Control Policy Inventory report displays a snapshot of the policies stored on a DMS, including:

- The time each policy was last updated
- The name of the user who last updated the policy
- The number of deployed versions of the policy
- The last finalized version of the policy
- The name of any policies that the policy is dependent on

Note: If a policy is dependent on another policy, it cannot be deployed until the policy that it depends on is deployed.

CA Access Control Policy Rules

The CA Access Control Policy Rules report displays the deploy and undeploy scripts for each rule in a policy, arranged by policy name. The report provides the date the rules were last updated, and the name of the user who last updated the rules. The report also specifies if the policy is finalized and ready for deployment, and the policy version number.

CA Access Control Policy Versions

The CA Access Control Policy Versions report displays version information for each policy, arranged by policy name. For each policy, the report provides:

- The current version number
- The date the version was deployed
- The name of the user who deployed the current version

The report also specifies if the current version is finalized.

CA Access Control Rule Deviations by Host

The CA Access Control Rule Deviations by Host report displays policy status and rule deviations, arranged by host. The report provides a list of policies on each host, and the status, version, and deviation status of each policy. If a rule deviation exists for the policy, the report provides details of the deviation, that is, details of the resources and properties to which the deviation applies.

CA Access Control Rule Deviations by Host Group

The CA Access Control Rule Deviations by Host Group report displays policy status and rule deviations, arranged by host group. The report provides a list of policies on each host group, and the status, version, and deviation status of each policy. If a rule deviation exists for the policy, the report provides details of the deviation for each host member of the host group, that is, details of the resources and properties to which the deviation applies.

Password Policies Reports

The password policies reports provide information about the password policies defined in CA Access Control.

Following is the list of standard password policy reports:

CA Access Control Privileged Accounts by Password Policy (see page 309)
CA Access Control PUPM Password Policy (see page 310)

CA Access Control Privileged Accounts by Password Policy

This report display the list of all the privileged accounts in the system and their corresponding password policy. Using this report, you can determine which privileged accounts are associated with which password policy. After reviewing the report, you can determine if password policies are assigned correctly and take corrective action as required.

The report displays the following information:

- Snapshot time
- Password policy name
- Endpoint type and name
- Account name
- Last check out date
- Last password change

CA Access Control PUPM Password Policy

This report displays the current password policies according to their complexity. Using this report you can determine if the existing password policy minimum and maximum length and other policy parameters meet you security standards.

This report displays the following information:

- Snapshot date
- Password policy name and description
- Maximum length
- Minimum length
- Password policy parameters

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 (see page 310)
CA Access Control PUPM Roles and Privileged Accounts by User (see page 311)
CA Access Control Privileged Accounts Requests by Endpoint (see page 311)
CA Access Control Privileged Accounts Requests by Approver (see page 312)
CA Access Control Privileged Accounts Requests by Requester (see page 313)
CA Access Control PUPM Users by Privileged Accounts (see page 313)
CA Access Control PUPM Users by Role (see page 314)

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

UNIX Authentication Broker Reports

The UNAB reports provide a detailed view of UNAB management tasks.

Following is the list of standard UNIX Authentication Broker reports:

CA Access Control UNAB Enterprise User Access by Host (see page 314)
CA Access Control UNAB Access to Hosts by Enterprise User (see page 315)
CA Access Control UNAB Enterprise Users (see page 315)
CA Access Control UNAB Enterprise Users Activity (see page 315)
CA Access Control UNAB Enterprise Groups (see page 315)
CA Access Control UNAB Hosts by Host Group (see page 315)
CA Access Control UNAB Local Groups Migration Status (see page 316)
CA Access Control UNAB Local Groups Summary (see page 316)
CA Access Control UNAB Local Users Summary (see page 317)
CA Access Control UNAB Local Group Migration Status by Group (see page 317)
CA Access Control UNAB Local Group Migration by Host (see page 317)
CA Access Control UNAB Local User Migration Status (see page 317)
CA Access Control UNAB Local User Migration Status by Host (see page 317)
CA Access Control UNAB Local User Migration Status by User (see page 317)
CA Access Control UNAB Nonstandard Local Groups by Group (see page 318)
CA Access Control UNAB Nonstandard Local Users by User (see page 318)

CA Access Control UNAB Enterprise User Access by Host

This report displays a list of enterprise users that accessed UNAB hosts by host. The report provides you with information about the enterprise users that accessed each host, their last login attempts, and who was granted access to the host (user or group). After you review this report, you can change the access rights enterprise users have to hosts.

CA Access Control UNAB Access to Hosts by Enterprise User

This report displays a list of enterprise users that accessed UNAB hosts by user. The report provides you with information about the enterprise users that accessed each host, their last login attempts, and who was granted access to the host (user or group). After you review this report, you can change the access rights enterprise users have to hosts.

CA Access Control UNAB Enterprise Users

This report displays a list of enterprise users that are permitted to access the host. The report displays the current enterprise user accounts, user ID, home directory, and shell type. After you review this report, you can change user properties and add or remove enterprise users.

CA Access Control UNAB Enterprise Users Activity

This report displays the activity list for migrated and partially migrated enterprise user accounts. Using this report you can review the activity of enterprise users on the UNIX hosts. The report provides you with information about the most recent successful and failed login attempts, the last successful password change done by the users, and more.

CA Access Control UNAB Enterprise Groups

This report displays the attributes of the enterprise groups. The report provides you with the details (such as group IDs) of enterprise groups.

CA Access Control UNAB Hosts by Host Group

This report displays the UNAB hosts by host groups. Using this report gives you an overview of the current grouping of the UNAB hosts.

This report contains the following properties:

- Host group
- Host name
- Total number

CA Access Control UNAB Local Groups Migration Status

This report displays the status of the migration process of each endpoint of each group. Using this report lets you review the current status of the migration process on every host.

This report displays the following information:

- Host name
- Migration status
- Group name
- Group ID
- Name conflicting
- GID conflicting
- Members conflicting
- No Active Directory group conflict
- Number of entries

CA Access Control UNAB Local Groups Summary

This report displays a summary of the local groups properties. Using this report you gain an overview of how many instances of the same group appears on each UNAB host.

This report displays the following information:

- Number of hosts
- Group name
- Group ID
- Number of instances

CA Access Control UNAB Local Users Summary

This report displays a summary of local user parameters. The information in this report displays the number of instances that a single user account appears on the UNIX hosts.

This report displays the following information:

- Number of hosts
- User name
- User ID
- Group ID
- Home directory
- Login shell
- Number of entries

CA Access Control UNAB Local Group Migration Status by Group

This report displays the migration status of local groups by group. Using this report lets you review the current status of the migration process of each group.

CA Access Control UNAB Local Group Migration by Host

This report displays the migration status of the local groups by host. Using this report gives you a detailed view of the migration status of the groups on each host.

CA Access Control UNAB Local User Migration Status

This report displays the migration status of local users. Using this report you can view the migration status of each user and compare between the local user attributes and the enterprise user attributes.

CA Access Control UNAB Local User Migration Status by Host

This report display the migration status of local users by host. Using this report lets you view the migration status of the user on each host.

CA Access Control UNAB Local User Migration Status by User

This report displays the migration status of local users by user. Using this report enables you to view the migration status of each local user.

CA Access Control UNAB Nonstandard Local Groups by Group

This report displays information about nonstandard local groups by group. Using this report enables you to view details on local groups whose local attributes differ from their enterprise attributes.

CA Access Control UNAB Nonstandard Local Users by User

This report displays information about nonstandard local users by user. Using this report lets you view information about users whose local attributes differ from their enterprise attributes.

CA Enterprise Log Manager Reports

The CA Enterprise Log Manager reports display detailed information about CA Access Control and UNAB accounts activity, resource management and more.

For more information about CA Enterprise Log Manager reports, refer to the CA Enterprise Log Manager 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.

Chapter 11: Deploying Sample and Best Practice Policies

This section contains the following topics:

Sample Policies (see page 321)
Where Are Sample Policies Stored? (see page 322)
Sample Policy Scripts (see page 323)
Compliance and Best Practice Policies (see page 327)
Where Are Compliance and Best Practice Policies Stored? (see page 328)
Compliance and Best Practice Policies Scripts (see page 329)
Policy Deployment (see page 330)

Sample Policies

The sample policies that come with CA Access Control provide you with segregation of duties and best practices that we recommend for the protection of operating system and application resources. Each policy is a selang script that includes comments that explain the policy's purpose and the rules it contains.

The sample policies provide a baseline for securing your systems with CA Access Control. Using the sample policies as a basis for your own policies simplifies the process of creating policies for your organization.You should customize the sample policies for your security policies and environment (operating system policies depend on the actual OS packages you have installed).

After you customize the sample policies, you use CA Access Control Enterprise Management to deploy the policies to the endpoints.

Sample policies are available for the following common applications and operating systems:

- Applications:
  - Apache
  - JBoss application server
  - CA Access Control Web Service
  - Microsoft SQL Server 2005
  - Oracle Database 10g

- Operating systems:
  - AIX
  - HP-UX
  - Red Hat Enterprise Linux
  - SuSe Linux Enterprise Server
  - Sun Solaris
  - Windows 2003
- Virtualization systems:
  - VMware ESX Server
  - Hyper-V
  - Solaris 10 Zones

Where Are Sample Policies Stored?

CA Access Control installs sample policies into the following directory:

```
ACInstallDir/samples/Policies/
```

ACInstallDir

Defines the directory where CA Access Control is installed.

There are three (3) subdirectories in this location:

- **Applications**—contains application specific policies.
- **OS**—contains operating system policies.
- **Virtualization**—contains virtualization system policies.

CA Access Control provides the policies as text files that contain the selang script that executes the policy. Each policy also has a matching policy that you can use to undeploy the protection policy. You deploy and undeploy the policies from CA Access Control Enterprise Management.

Sample policies have the following naming convention: *OS_ACTION*

OS

Defines the operating system the policy is designed for.

ACTION

Specifies the policy action the script takes.

Values: deploy and undeploy

For example, the following file contains the sample deployment policy for Red Hat Enterprise Linux 4.0: _LINUX40_deploy.txt

Note: Application policies do not have an undeployment script.

Sample Policy Scripts

Each policy is a selang script that includes comments that explain the policy's purpose and the rules it contains. Sample policy scripts are written to demonstrate best practices:

- Comments

  Sample policies are annotated to help you understand what each section of the sample policy is set to achieve.

- Containers

  Sample policies group related resources into a single container resource. Using this method, a common policy is applied to all the related resources once. Policy rules (ACLs) do not need to be applied to individual resources. For example, a policy can use a container to group all of the system's configuration files.

  Policy containers use the following naming convention: POL_*container_name*. You can think of these containers as sub-policies. For example, OS sample policies use the POL_SYS_CONF container to protect OS configuration files.

- Roles

  To simplify user management, sample policies apply ACLs to roles. Each role uses a CA Access Control group of users that you can add real users to.

  Policy roles use the following convention: ROL_*role_name*. For example, sample policies use the ROL_SYSTEM group for built-in system users like adm and lp. Many policies assign these users with wide-ranging permissions (for proper system operation) but also expire them so that users cannot use them to log in.

- Variables

  So that you have to apply minimum changes when you deploy them, sample policies make use of CA Access Control variables. Sample policies use built-in variables to protect local system resources, for example, a terminal rule for the local host. Sample policies also use user-defined variables to simplify policy changes. For example, a user-defined variable can contain the home directory of the administrative user. If the administrative user uses a different home directory, you only need to change it once for all affected rules to automatically change.

Example: Policy Script Comments

The following snippet from the Solaris SPARC 9 sample policy illustrates how sample policies are annotated. Using selang syntax rules, the lines that begin with a hash symbol (#) are comments.

```
#
# * Home Directories Protection Policy *
# **************************************
#
# This policy uses the FILE class to protect the home
# directories of sensitive users so that only the owner
# of each directory can access it.
#
# Prerequisites:
#     None
#
# Roles:
#     None
#
# Containers:
#     POL_HOME_DIR      - home directories of sensitive users
#
# define container POL_HOME_DIR
# Protect home directories
editres   CONTAINER POL_HOME_DIR audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
comment("AC Sample - Protect home directories")
authorize CONTAINER POL_HOME_DIR uid(* _undefined)   access(NONE)
```

```
editres ACVAR ("HOME_OS_ADMIN") value("/root") type(static)
editusr (<!USER_OS_ADMIN>)
# define specific FILE resources and connect them with POL_HOME_DIR
editres FILE ("<!HOME_OS_ADMIN>/*") audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
defaccess(NONE) <!POLICY_WARNING_MODE>  comment("AC Sample")
authorize FILE ("<!HOME_OS_ADMIN>/*") uid(<!USER_OS_ADMIN>) access(ALL)
chres CONTAINER POL_HOME_DIR mem+("<!HOME_OS_ADMIN>/*") of_class(FILE)
```

Example: Containers in Sample Policies

The following selang output shows the properties of the POL_SYS_FILES. An AIX sample policy contains this sub-policy that protects system files.

```
AC> sr container POL_SYS_FILES
Data for CONTAINER 'POL_SYS_FILES'
------------------------------------------------------------------------
ACLs              :
    Accessor                Access
    ROL_SYSADMIN  (GROUP  ) All
    ROL_SYSTEM    (GROUP  ) All
    *             (USER   ) R, Chdir
    _undefined    (USER   ) R, Chdir
Members           :
    /boot/*       (FILE  )
    /dev/kmem     (FILE  )
    /dev/mem      (FILE  )
    /dev/port     (FILE  )
Audit mode        : Failure
Owner             : +nobody       (USER  )
Create time       : 10-Dec-2008 10:32
Update time       : 10-Dec-2008 10:35
Updated by        : root          (USER  )
Comment           : AC Sample - Protect OS system files
```

Example: Variables in Sample Policies

The following snippet from the Red Hat Enterprise Linux 5 sample policy illustrates how sample policies use variables. In this snippet, the sample policy defines possible names for the local host and the home directory of the administrative user root.

```
#
# * AC Variables Definitions *
# ****************************
#
# The rules in this section define variables that policies use.
# Variables:
#     LOCALHOST            : list of possible names for local host
#     POLICY_AUDIT_MODE    : set policies audit mode
#     POLICY_DEFACCESS     : set defaccess of policies` resources
#
editres ACVAR ("LOCALHOST") value("localhost") type(static)
editres ACVAR ("LOCALHOST") value+("127.0.0.1")
editres ACVAR ("LOCALHOST") value+("0.0.0.0")
editres ACVAR ("POLICY_AUDIT_MODE")   value("FAILURE") type(static)
editres ACVAR ("POLICY_DEFACCESS")    value("ALL")     type(static)
```

More information:

User-Defined Variables (see page 96)
Built-In Variables (see page 97)
Guidelines for Using Variables (see page 98)
How an Endpoint Resolves Variables (see page 100)

Compliance and Best Practice Policies

The compliance and best practice policies let you rapidly deploy compliance and best practice policies on the endpoints. Each policy is a selang script that includes comments that explain the purpose of the policy, the rules it contains, and the variables that it uses.

The policies adhere to the Payment Card Industry Data Security Requirements and Security Assessment Procedures (PCI DSS) standard and to the VMWare VSphere Hardening Requirements.

The compliance and best practice policies are available for the following operating systems and virtualization platforms:

- Operating Systems
    - Red Hat Advanced Server Linux
    - SuSE Linux
    - SLES
    - AIX
    - HP-UX
    - Solaris
    - Windows 2003 R2
    - Windows 2008 R2
- Virtualization Platforms
    - VMWare Server ESX
    - Solaris zones on Solaris 10
    - Hyper-V

Where Are Compliance and Best Practice Policies Stored?

The Enterprise Management Server stores the compliance and best practice policies on the DMS during installation. This is done automatically when you deploy a fresh installation of the Enterprise Management Server.

You manage the compliance and best practice policies from CA Access Control Enterprise Management in the Policy Management section.

On each new CA Access Control installation, the compliance and best practice policies are stored in the following location:

```
ACInstallDir/samples/Policies/OutOfTheBox
```

ACInstallDir

Defines the directory where CA Access Control is installed.

CA Access Control provides the policies as text files that contain the selang script that executes the policy. Each policy also has a matching policy that you can use to undeploy the protection policy. You deploy and undeploy the policies from CA Access Control Enterprise Management.

Sample policies have the following naming convention: *REGULATION_ACTION*

REGULATION

Defines the name of the regulation the policy is designed for.

ACTION

Specifies the policy action the script takes.

Values: deploy and undeploy

For example, the following file contains the sample deployment policy for the PCI DSS section 7.1.1: pci_dss_7.1.1_deploy.txt

Note: Compliance and best practice policies are OS independent and are applicable to Windows and UNIX systems.

Compliance and Best Practice Policies Scripts

Each policy is a selang script that includes comments that explain the policy's purpose and the rules it contains:

- Comments

  Sample policies are annotated to help you understand what each section of the sample policy is set to achieve.

- Variables

  Compliance and best practices policies are operating system independent. However, resources groups vary from system to system. To overcome this problem, resource lists use variables and the ACLs use the variables in the policies. When an endpoint connects to the Enterprise Management Server, it is automatically added to the matching host group according to the operating system and a policy is deployed to the endpoint.

- Roles

  To simplify user management, sample policies apply ACLs to roles. Each role uses a CA Access Control group of users that you can add real users to.

  Policy roles use the following convention: ROL_*role_name*. For example, sample policies use the ROL_SYSTEM group for built-in system users like adm and lp. Many policies assign these users with wide-ranging permissions (for proper system operation) but also expire them so that users cannot use them to log in.

Example: compliance and best practices policies comments

The following snippet from the PCI_DSS_7.1.1 compliance policy illustrates how compliance and best practices policies are annotated. Using selang syntax rules, the lines that begin with a hash symbol (#) are comments.

```
#
# * 2. Protect <!USER_OS_ADMIN> Logon and Access Control Administration *
# ***********************************************************************
#
# This section uses the TERMINAL class to restrict administrator users from
# logging in directly (read access). Access Control administration is blocked as
# well (write access).
#
# To separate security administration from system administration, the policy
# sets READ access only to these special terminals.
#
editres   TERMINAL ("<!HOSTNAME>") audit(ALL) warning
authorize TERMINAL ("<!HOSTNAME>") uid("<!USER_OS_ADMIN>") deniedaccess(READ)
# The following line is commented because the warning mode in UNIX is not
# applicable for write access to class TERMINAL.
#authorize TERMINAL ("<!HOSTNAME>") uid("<!USER_OS_ADMIN>") deniedaccess(WRITE)
```

Example: compliance and best practices policies roles

The following snippet from the PCI_DSS_7.1.1 compliance policy illustrates how the policy applies ACLs to roles.

```
#
# * 1. Role Definitions *
# ***********************
#
# The rules in this section define the roles that the policy uses.
#
#  * Define built-in OS users with the logical property. This prevents users
#    from logging in to the system.
#  * Create the user +nobody in CA Access Control only. CA Access Control
#    sets this user as the owner of many resources (to disable ownership
#    bypass). You cannot create this user in the native OS.
#  * Create at least one user in ROL_AC_ADMIN. Without this user you cannot
#    login into CA Access Control.
#    Note: By default, the rules add the superuser account to ROL_AC_ADMIN.
#          We recommend that you remove this user and add security
#          administrators to this group.
# Roles:
#     ROL_SYSTEM        : built-in OS users
#     ROL_SYSADMIN      : system administrators
#     ROL_RESTRICTED    : restricted users with permissions for specific tasks
#     ROL_AC_ADMIN      : CA Access Control administrators
#     ROL_AC_AUDITOR    : CA Access Control auditors
#     ROL_AC_OPERATOR   : CA Access Control operators
#     ROL_AC_SERVICE    : CA Access Control service managers
#     ROL_AC_PWMANAGER  : CA Access Control password managers
#

editgrp (ROL_SYSTEM ROL_SYSADMIN ROL_RESTRICTED ROL_AC_ADMIN ROL_AC_AUDITOR
ROL_AC_OPERATOR ROL_AC_SERVICE ROL_AC_PWMANAGER)
chgrp (ROL_SYSADMIN ROL_AC_ADMIN) audit(LOGINSUCCESS LOGINFAILURE FAILURE)
editusr (+nobody) comment("AC OOTB - Resource owner used for disabling ownership
bypass")
chusr (+nobody) owner(+nobody)
join ("<!USER_OS_ADMIN>") group(ROL_SYSTEM)
join ("<!USER_OS_ADMIN>") group(ROL_AC_ADMIN)
```

Policy Deployment

When you deploy any CA Access Control policy, you should follow some common steps to ensure that the policy deploys and performs as expected and without errors. The following section describes the actions you should take before and after you deploy sample policies.

How to Prepare an Endpoint for Policy Deployment

Before you implement any policy, you should prepare the endpoint for the policy. This lets you later isolate issues that are specifically related to this policy.

To prepare an endpoint for policy deployment:

- Use a fresh installation of the operating system or application

  Use the latest available manufacture-supplied version and patch of the OS for OS policies. This lets you protect the system before a modification potentially compromises the system. After you apply the policy, you can apply patches and configure the system as required knowing that the policy protects the system from malicious or accidental changes. The same logic applies to applications.

- Implement separation of duties

  Review the policy rules and add additional roles if required. Create your own policy that defines roles, users, and their relationship (role membership). You can then deploy this policy before or after the sample policy.

  Make sure you do not give any single user too many privileges. For example, by default the superuser is added to ROL_AC_ADMIN, which provides CA Access Control administration privileges. However, the best practice is to remove this user and add security administrators to this group instead.

- Create a new CA Access Control database or back up your existing database

  Create a new database before you implement the policy. This ensures that policy rules are not going to conflict or otherwise change existing rules in the database. If you cannot create a new database, you should back up the database so that you can restore it to the state before you applied the policy.

- Assign users with appropriate admin roles: sys admin, security admin, applications admin.

- Use a new audit log file

  Back up the existing audit log file and then remove it. This ensures that CA Access Control will create a new audit log file when it logs new events. Having an audit log file that only contains events that relate to the policy you deploy can help you identify and isolate issues relating to the policy more quickly.

- Set CA Access Control user-defined variables

  Verify that the preset CA Access Control variable values ("AC Variables Definitions" section), match your environment and add or modify values as required.

How to Deploy Policies in a Staged Manner

When you deploy your policy, there are several actions you can take to ensure that the policy deploys and performs as expected and without errors. After you have prepared your endpoint for policy deployment, we recommend that you proceed with a staged policy deployment.

We recommend that you deploy the policies first in a test environment and after you have adjusted the policies as required, deploy the policies in the production environment.

To deploy policies in a staged manner:

1. Deploy the policy in Warning mode

   The policy is now active but does not enforce its rules. You can then examine the audit log to preview the results of your intended policy before you put that policy into effect.

   Note: By default, the sample policies' scripts set Warning mode for all policy rules.

2. Review the CA Access Control audit log for warning messages

   After you deploy the policy, any policy breaches show up in the audit log as warnings (assuming your policy rules use Warning mode).

3. Use the system in real scenarios and analyze the audit log again

   To test your policy effectively you can perform regular operating procedures on the computer (log in, start and stop services and applications, and so on). You can then analyze the audit log again to see if any new warnings appear.

4. Adjust the policy as required

   Using the information you gathered from the audit log, you can adjust the policy to account for expected use in your environment.

5. Remove Warning mode to enable the policy

   Once you are confident your policy is ready to enforce rules in your production environment, you can remove Warning mode to enable it.

   The policy is now enforced.

Note: If you want to make changes to a policy, you should first disable policy enforcement (use Warning mode), make the changes to the policy and then reactivate it when you are confident the changes are working as desired.

More information:

Policy Deployment (see page 333)
How to Customize the Policies for Your Environment (see page 333)
Enable Sample Policy Enforcement (see page 334)

Policy Deployment

Because sample and best practice policies contain CA Access Control variables, you must deploy them using the advanced policy management method.

Note: You cannot directly run the sample policy files in selang on the endpoint.

Use CA Access Control Enterprise Management to store the sample policy on the DMS and then assign it to multiple endpoints as required.

More information:

Advanced Policy Management (see page 64)
How to Create and Deploy a Policy (see page 80)

How to Customize the Policies for Your Environment

The sample and best practice policies are provided as a basis for your own security policy. To deploy a policy, you should customize it for your environment.

To customize a policy for your environment:

- Review the CA Access Control and system log files.

  Look for and identify warnings or errors that occurred during the deployment process and modify the policy to account for these.

- Join users to policy roles.

  The policies use roles for authorization. You need to assign users in your organization to these roles.

  Important! When you undeploy a policy, do not delete the users or groups you created. This may affect the normal behavior of the ACL lists and accessor associations in other policies that use those same users and groups.

- (Windows only) Run the coexistence utility eACoexist.exe.

  This utility identifies conflicts between CA Access Control and other installed programs and resolves them by creating a bypass for that program.

Enable Sample Policy Enforcement

By default, the sample policy scripts set Warning mode for all policy rules. When you deploy the policy it is active but does not enforce its rules. After you familiarize yourself with the policy and customize it as required, you should be ready to enable the policy so that policy rules are enforced.

Note: This procedure explains how to enable policy enforcement for a single policy. For more information about how to enable policy enforcement for multiple policies after you perform system maintenance, see the *Endpoint Administration Guide* for your operating system.

To enable sample policy enforcement

1. Edit the policy script to change each instance of **warning** to **warning-**.

   When you run a rule that sets warning- for a resource or accessor, CA Access Control removes Warning mode from the resource or accessor.

2. Deploy the edited policy.

   Policy enforcement is enabled.

Example: Enable Windows Sample Policy Enforcement

The following snippet is from the sample JBoss policy for Windows. The policy is enabled because "warning" is changed to "warning-".

```
# Protect JBoss files
# -------------------

# Protect JBoss files in the application directory.
# These rules apply protection to files that are not protected by other rules.
editfile    ("<!JBOSS_HOME>\*") owner(nobody) defaccess(NONE) warning- comment ("AC
Sample - JBoss base dir")
authorize FILE ("<!JBOSS_HOME>\*") id(ROL_JBOSS_ADMIN) access(ALL)
via(pgm("<!JBOSS_HOME>\bin\*"))
authorize FILE ("<!JBOSS_HOME>\*") id(jboss_pgm)      access(READ,CHDIR)
via(pgm("<!JBOSS_HOME>\bin\*", "<!JBOSS_JAVA_PGM>"))
```

Disable Sample Policy Enforcement

By default, the sample policy scripts set Warning mode for all policy rules. When you enable policy enforcement, you remove Warning mode. To disable policy enforcement, you reintroduce Warning mode.

Note: This procedure explains how to disable policy enforcement for a single policy. For more information about how to disable policy enforcement for multiple policies when you perform system maintenance, see the *Endpoint Administration Guide* for your operating system.

To disable sample policy enforcement

1. Edit the policy script to change each instance of **warning-** to **warning**.

   When you run a rule that sets warning for a resource or accessor, CA Access Control sets Warning mode for the resource or accessor.

2. Deploy the edited policy.

   Policy enforcement is disabled.